A Thesis submitted for the degree of Doctor of Philosophy

Characterizing entanglement and quantum correlations constrained by symmetry

Jordi Tura i Brugués
advisor: Prof. Dr. Maciej Lewenstein
co-advisor: Dr. Remigiusz Augusiak

submitted: Apr 2015, defended: Jul 2015

ICFO–Institut de Ciències Fotòniques,
08860 Castelldefels, Spain

UPC – Universitat Politècnica de Catalunya

Cover picture: Artistic impression of [Tur+14a].

Abstract

English

Entanglement and nonlocal correlations constitute two fundamental resources for quantum information processing, as they allow for novel tasks that are otherwise impossible in a classical scenario. However, their elusive characterization is still a central problem in Quantum Information Theory. The main reason why such a fundamental issue remains a formidable challenge lies in the exponential growth in complexity of the Hilbert space, as well as the space of nonlocal correlations. Physical systems of interest, on the other hand, display symmetries that can be exploited to reduce this complexity, opening the possibility that, for such systems, some of these questions become tractable.

This PhD Thesis is dedicated to the study and characterization of entanglement and nonlocal correlations constrained under symmetries. It contains original results in these four threads of research: PPT entanglement in the symmetric states, nonlocality detection in many-body systems, the non-equivalence between entanglement and nonlocality and elemental monogamies of correlations.

First, we study PPT entanglement in fully symmetric n-qubit states. We solve the open question on the existence of four-qubit PPT entangled states of these kind, providing constructive examples and methods. Furthermore, we develop criteria for separability, edgeness and the Schmidt number of PPT entangled symmetric states. Geometrically, we focus on the characterization of extremal states of this family and we provide an algorithm to find states with such properties.

Second, we study nonlocality in many-body systems. We consider permutationally and translationally invariant Bell inequalities consisting of two-body correlators. These constitute the first tools to detect nonlocality in many-body systems in an experimentally-friendly way with our current technology. Furthermore, we show how these Bell inequalities detect nonlo-

cality in physically relevant systems such as ground states of Hamiltonians that naturally arise *e.g.*, in nuclear physics. We provide analytical classes of Bell inequalities and we analytically characterize which states and measurements are best suited for them. We show that the method we introduce can be fully generalized to correlators of any order in any Bell scenario. Finally, we provide some feedback from a more experimental point of view.

Third, we demonstrate that entanglement and nonlocality are inequivalent concepts in general; a question that remained open in the multipartite case. We show that the strongest form of entanglement, genuinely multipartite entanglement, does not imply the strongest form of nonlocality, genuinely multipartite nonlocality, in any case. We give a constructive method that, starting from a multipartite genuinely multipartite state admitting a K-local model, extends it to a genuinely multipartite entangled state of any number of parties while preserving the degree of locality.

Finally, we show that nonlocal correlations are monogamous in a much stronger sense than the typical one, in which the figure of merit compares a Bell inequality violation between two sets of parties. We show that the amount of Bell violation that a set of parties observes limits the knowledge that any external observer may gain on any of the outcomes of any of the parties performing the Bell experiment. We show that this holds even if such observer is not limited by quantum physics, but it only obeys the no-signalling principle. Apart from its fundamental interest, we show how these stronger monogamy relations boost the performance of some device-independent (DI) protocols such as DI quantum key distribution or DI randomness amplification.

Castellano

El entrelazamiento y las correlaciones no-locales constituyen dos recursos fundamentales para el procesamiento cuántico de la información, ya que abren la posibilidad de realizar tareas que serían imposibles en el sentido clásico. Sin embargo, su elusiva caracterización aún representa uno de los problemas más importantes en la teoría cuántica de la información. La razón principal por la que una cuestión tan básica sigue siendo un reto formidable subyace en el incremento exponencial de la complejidad del espacio de Hilbert, así como del espacio de las correlaciones no-locales. Por

otro lado, los sistemas físicos de interés muestran simetrías que pueden ser aprovechadas para reducir dicha complejidad, abriendo la posibilidad que, para tales sistemas, algunas de esas cuestiones devengan tratables.

La presente tesis doctoral está enfocada al estudio de la caracterización del entrelazamiento cuántico y las correlaciones no-locales bajo simetrías. Contiene resultados originales en las siguientes líneas de investigación: entrelazamiento del tipo PPT en estados simétricos, detección de no-localidad en sistemas de muchos cuerpos, la no equivalencia entre el entrelazamiento cuántico y la no-localidad y las correlaciones monogámicas elementales.

En primer lugar, estudiamos el entrelazamiento del tipo PPT en estados totalmente simétricos de n bits cuánticos. Resolvemos el problema abierto referente a la existencia de estados PPT entrelazados de cuatro bits cuánticos de este tipo, proporcionando ejemplos y métodos constructivos. Además, desarrollamos criterios de separabilidad, estados frontera y número de Schmidt para estados PPT entrelazados y simétricos. Desde el punto de vista geométrico, nos centramos en la caracterización de estados extremos dentro de esta familia y proporcionamos un algoritmo para encontrar estados cuánticos con tales propiedades.

En segundo lugar, estudiamos la no-localidad en sistemas de muchos cuerpos. Consideramos desigualdades de Bell, invariantes bajo permutaciones o traslaciones, que involucran correladores entre dos cuerpos como mucho. Dichas desigualdades constituyen los primeros tests de detección de no-localidad en sistemas de muchos cuerpos que son accesibles desde el punto de vista experimental, con el presente nivel de tecnología. Además, demostramos cómo esas desigualdades de Bell pueden detectar no-localidad en estados físicamente relevantes, como los estados de mínima energía de hamiltonianos que aparecen de forma natural, por ejemplo, en física nuclear. Proporcionamos clases analíticas de desigualdades de Bell y caracterizamos, también analíticamente, qué estados y medidas son los más adecuados para ellas. Vemos que el método que introducimos es totalmente generalizable a correladores de cualquier orden en cualquier escenario de Bell. Finalmente, comentamos aspectos de interés desde un punto de vista experimental.

En tercer lugar, demostramos que el entrelazamiento y las correlaciones no-locales son conceptos no equivalentes en general, resolviendo un problema que persistía abierto en el caso multipartito. Probamos que la forma más fuerte de entrelazamiento −entrelazamiento multipartito genuino−

no implica la forma más fuerte de no-localidad —no-localidad multipartita genuina— en ningún caso. Para ello, damos un método constructivo que, dado un estado cuántico multipartito genuinamente entrelazado que admite un modelo K-local, lo extiende a un estado consistente en un número de subsistemas arbitrario, genuinamente entrelazado, preservando el mismo grado de localidad.

Finalmente, demostramos que las correlaciones no-locales son monógamas en un sentido mucho más estricto que el que se considera típicamente, donde se compara la violación de una desigualdad de Bell entre dos conjuntos de observadores. Vemos que la cantidad de violación que un conjunto de observadores mide impone restricciones fundamentales en la información que puede obtener cualquier observador externo sobre los resultados de las medidas hechas por los observadores realizando el experimento de Bell. Este resultado se mantiene aun si tal observador externo no está limitado por las leyes que rigen la mecánica cuántica, sino que solamente tiene la imposibilidad de transmitir información de manera instantánea. A parte de su interés básico, demostramos que tales relaciones monógamas pueden ser aplicadas para incrementar la eficiencia de protocolos de procesado cuántico de la información independientes del dispositivo (ID), tales como la distribución cuántica de llaves ID o la amplificación de aleatoriedad ID.

Català

L'entrellaçament i les correlacions no-locals constitueixen dos recursos fonamentals per al processament quàntic de la informació, ja que obren la possibilitat de realitzar tasques que serien impossibles en el sentit clàssic. Tot i així, la seva elusiva caracterització és encara un dels problemes més rellevants en la teoria quàntica de la informació. La raó principal per la qual una qüestió tan bàsica segueix essent un repte formidable rau en l'increment exponencial en complexitat de l'espai de Hilbert, així com el de l'espai de les correlacions no-locals. Nogensmenys, molts sistemes físics d'interès gaudeixen de simetries que poden servir per reduir tal complexitat, obrint la possibilitat que, per a tals sistemes, algunes d'aquestes preguntes esdevinguin tractables.

La present tesi doctoral està dedicada a l'estudi i la caracterització de l'entrellaçament quàntic i les correlacions no-locals restringides per sime-

tries. Conté resultats originals en les línies de recerca que s'esmenten a continuació: entrellaçament del tipus PPT en estats simètrics, detecció de no-localitat en sistemes de molts cossos, la no equivalència entre l'entrellaçament quàntic i la no-localitat i les monogàmies elementals de les correlacions.

En primer lloc, s'estudia l'entrellaçament en estats PPT totalment simètrics de n bits quàntics. Es resol el problema obert referent a l'existència d'estats simètrics PPT entrellaçats de quatre bits quàntics proporcionant-ne exemples i mètodes constructius. A més a més, es desenvolupen criteris de separabilitat, estats frontera i nombre de Schmidt per a estats simètrics PPT entrellaçats. Des del punt de vista geomètric, es posa èmfasi en la caracterització d'estats extrems dins d'aquesta família i es desenvolupa un algoritme per trobar estats amb tals propietats.

En segon lloc, s'estudia la no-localitat en sistemes de molts cossos. Es consideren desigualtats de Bell, invariants permutacionalment o cíclica, formades per correladors de, com a molt, dos cossos. Tals desigualtats representen les primeres eines per a la detecció de no-localitat en sistemes de molts cossos que són accessibles des d'un punt de vista experimental, tenint en compte el nivell tecnològic d'avui en dia. Àdhuc es demostra la capacitat d'aquestes desigualtats per detectar no-localitat en estats quàntics rellevants des del punt de vista físic, com ara els estats de mínima energia corresponents a hamiltonians que apareixen de manera natural, per exemple, en física nuclear. Es proposen classes analítiques de desigualtats de Bell i es caracteritza, també de forma analítica, quins estats i observables són els més adequats per a aquestes. El mètode que es proposa és generalitzable a correladors de qualsevol ordre i a escenaris de Bell qualssevol. Finalment, es comenten aspectes d'interès des d'un punt de vista experimental.

En tercer lloc, es demostra que l'entrellaçament i les correlacions no-locals són conceptes no equivalents en general, resolent un problema que romania obert en el cas multipartit. Es demostra que la forma més forta d'entrellaçament —l'entrellaçament multipartit genuí— no implica la forma més forta de no-localitat —la no-localitat multipartita genuïna— en cap cas. Es dóna un mètode constructiu que, partint d'un estat multipartit genuïnament entrellaçat que admet un model K-local, l'estén a un estat genuïnament entrellaçat consistent en un nombre de subsistemes arbitrari, preservant-ne el grau de localitat.

Finalment, es demostra que les correlacions no-locals són monògames

en un sentit molt més estricte que el que es considera convencionalment, on es compara la violació d'una desigualtat de Bell entre dos conjunts d'observadors. Es demostra que la quantitat de violació mesurada per un conjunt d'observadors imposa restriccions fonamentals en la quantitat d'informació que un observador extern pot extreure dels resultats de les mesures que han fet els observadors que estan realitzant l'experiment de Bell. Tal resultat es manté àdhuc si l'observador extern no es troba limitat per les lleis que regeixen la mecànica quàntica, sinó que tan sols té la impossibilitat de transmetre informació de manera instantània. A part del seu interès bàsic, es demostra que els resultats que es deriven poden ser aplicats per incrementar l'eficiència de protocols de processament quàntic de la informació independents del dispositiu (ID), tals com la distribució quàntica de claus ID o l' amplificació d'aleatorietat ID.

Acknowledgements

This PhD Thesis is the result of a wonderful period of my life, in which I have had the privilege to learn amazing stuff and meet great people.

I am specially indebted to Maciek Lewenstein. He has taught me lots of cool things -even jazz- throughout these years, always with a great sense of humour. I am very grateful for his support and encouragement in pursuing my PhD with him, which he already offered when I was just a summer fellow at ICFO. I have enjoyed many enriching discussions with him and I have been given many opportunities, never getting a no as a response. I very much appreciate his belief in me.

And I have been very lucky to have had Remik as a co-supervisor. With him I have enjoyed endless discussions about research, countless insights, tips and techniques. Through his careful reading I have learnt many of the things you are not taught in class, but do matter when doing research. He was always ready with some good advice whenever I needed it, with new ideas to be discussed on the blackboard... and his hopeless attempts to teach me Polish language and/or history showed me that one does not simply give up on a problem, no matter how complicated it looks like :)

There is another person I must thank, for none of this would have ever happened without him. On the 25th-Feb-2010 Toni Acín gave a talk that marked my life: I decided to embark on the field of quantum information[1]. During my PhD he has had the generousity to invite me to their group meetings -and dinners- and we have co-authored many papers these years, as well as shared many fruitful discussions.

I would also like to thank Ignacio Cirac for his support and kind hospitality at the Max Planck Institut für Quantenoptik, where I had a wonderful research stay in which I learnt so much while having a great time.

[1] This was an inspiring seminar organized by Toni and Sebastià Xambó, my Coding Theory teacher at the moment, whom I straightorwardly asked to supervise my Master's Thesis, in quantum information, Toni ended up co-supervising it.

At ICFO I have always found a great atmosphere for work and I would like to thank all the colleagues and friends I have met on the way. There are many names in this list. In a somehow chronological order: the summer fellows I met in 2010; all the people in the QOT group, in particular, my office mates Ulrich and Julia; all the people in the QIT group, specially Alexia, Belén, Gonzalo and Martí; the people I met at the MPQ, specially Gemma; and many other good friends or colleagues that have been or are still at ICFO.

I would also like to thank my friends and flatmates Narcís, Sergi, Lander, María and Teixi for the uncountable adventures in that piece of Elo hell called Vallcarca 52, where we live.

I, per acabar, el més important de tot: donar les gràcies a la meva família per fer-me costat per arribar fins aquí, pel seu suport constant i incondicional durant tots aquests anys; la gratitud que sento envers ells no es pot expressar en paraules. A l'Oriol, la Fina i l'Isidre; i als meus avis, en Pep i la Caterina; i especialment als meus pares, Jordi i Maria, a qui aquesta tesi està dedicada.

List of Publications

Peer-reviewed Publications forming part of the Thesis

[Aug+12] R. Augusiak, J. Tura, J. Samsonowicz, and M. Lewenstein Entangled symmetric states of N qubits with all positive partial transpositions in: *Phys. Rev. A*, **86**: (4 2012), 042316 DOI: 10.1103/PhysRevA.86.042316

[Aug+14b] R. Augusiak, M. Demianowicz, M. Pawłowski, J. Tura, and A. Acín Elemental and tight monogamy relations in nonsignaling theories in: *Phys. Rev. A*, **90**: (5 2014), 052323 DOI: 10.1103/PhysRevA.90.052323

[Tur+12] J. Tura, R. Augusiak, P. Hyllus, M. Kuś, J. Samsonowicz, and M. Lewenstein Four-qubit entangled symmetric states with positive partial transpositions in: *Phys. Rev. A*, **85**: (6 2012), 060302 DOI: 10.1103/PhysRevA.85.060302 Published as a Rapid Communication

[Tur+14a] J. Tura, R. Augusiak, A. B. Sainz, T. Vértesi, M. Lewenstein, and A. Acín Detecting nonlocality in many-body quantum states in: *Science*, **344**:6189 (2014), 1256–1258 DOI: 10.1126/science.1247715

[Tur+14b] J Tura, A B Sainz, T Vértesi, A Acín, M Lewenstein, and R Augusiak Translationally invariant multipartite Bell inequalities involving only two-body correlators in: *Journal of Physics A: Mathematical and Theoretical*, **47**:42 (2014), 424024 DOI: 10.1088/1751-8113/47/42/424024 Part of the special issue *50 years of Bell's Theorem*

Preprints forming part of the Thesis

[Aug+14c] R. Augusiak, M. Demianowicz, J. Tura, and A. Acín *Entanglement and nonlocality are inequivalent for any number of particles* 2014 arXiv:1407.3114. Under review in Physical Review Letters

[Tur+15a] J. Tura, A. B. Sainz, T. Graß, R. Augusiak, A Acín, and M. Lewenstein *Entanglement and Nonlocality in Many-Body Systems: a primer* 2015 arXiv:1501.02733. To be published in the Proceedings of the International School of Physics *Enrico Fermi* 2014, Course 191 - Quantum Matter at Ultralow Temperatures

[Tur+15b] J. Tura, R. Augusiak, A. B. Sainz, B. Lücke, C. Klempt, M. Lewenstein, and A. Acín *Nonlocality in many-body quantum systems detected with two-body correlators* 2015 arXiv : 1505.06740. To be submitted to Communications in Mathematical Physics

Peer-reviewed publications relevant to the Thesis, but not forming part of it

[ATL11] R Augusiak, J Tura, and M Lewenstein A note on the optimality of decomposable entanglement witnesses and completely entangled subspaces in: *Journal of Physics A: Mathematical and Theoretical*, **44**:21 (2011), 212001 DOI: 10.1088/1751-8113/44/21/212001 Featured with insights. Editor's choice: Highlights of 2011.

[Aug+14a] R Augusiak, J Bae, J Tura, and M Lewenstein Checking the optimality of entanglement witnesses: an application to structural physical approximations in: *Journal of Physics A: Mathematical and Theoretical*, **47**:6 (2014), 065301 DOI: 10.1088/1751-8113/47/6/065301 Editor's choice: Highlights of 2014.

Preprints relevant to the Thesis, but not forming part of it

[PL+15] M. Perarnau-Llobet, K. V. Hovhannisyan, M. Huber, P. Skrzypczyk, J. Tura, and A. Acín *The most energetic passive states* 2015 arXiv:1502.07311. Under review in Physical Review Letters

Contents

1. Introduction

The rules governing the behavior of very small-scale physics have no classical analogy. Below the nanoscale, molecules, atoms and subatomic particles happen to be very accurately described by Quantum Theory (QT). However, the anti-intuitive nature of QT made it hard to be accepted by the scientific community, since its very genesis[1], for accepting QT implies the acceptance that Nature behaves as something that we can not make any parallelism with.

Moreover, QT introduced several shifts of paradigm with the existing physics. Classical physics is deterministic: if one is given complete information about the state of a system at a given time, its past, present and future are unambiguously determined. However, QT is intrinsically random: even if one is given maximal information about the state of a quantum system, it is not possible to guarantee which is going to be the result of a measurement performed on that system, and we can only quantify its probability. In addition, quantum observables do not have a definite value prior to the measurement process and measuring processes disturb the state of the system. One cannot simultaneously know the value of a set of observables and the order in which they are measured becomes essential, making QT non-commutative.

A plethora of extraordinary phenomena emerges due to QT, the quintessential being entanglement. If one is given a composite system, QT states that the description of its components is, in general, not enough to describe the whole system; such quantum state is said to be entangled. In some cases, measurements on entangled quantum states lead to nonlocal correlations, meaning that the statistics produced by the measurements can not

[1] Even Max Planck, the father of QT, formulated the quantum hypothesis of energy quantization in what he called an *act of desperation* in order to explain the black-body radiation. More than a century has passed since that 14th of December 1900, and the revolution that Planck initiated has had an unthinkably huge impact in technology, society and our lives.

be mimicked by observers having access to correlated classical variables.

Entanglement and nonlocality tell us that some measurements performed in spacelike separated regions may have perfectly correlated outcomes, as if each of them would be knowing what is happening in the other region. Although this cannot be used to transmit information instantaneously, such phenomenon was seen by skepticism, and QT was regarded as an incomplete theory[2]. However, equipped with a new theory that explained a multitude of previously incomprehended phenomena, physicists of the twentieth century decided that entanglement and nonlocality could wait[3].

However, things changed at the beginning of the 1990s, when it was realized that the peculiarities of entanglement could be employed as a resource for many Quantum Information Processing (QIP) tasks [NC00; Hor+09], comprising Quantum Key Distribution (QKD) [BB84; Eke91], quantum teleportation [Ben+93] or an efficient algorithm to solve the discrete logarithm problem, which implies efficient factorization [Sho94]. A new field, *Quantum Information Theory*, emerged from this synergy between quantum physics and information theory.

The first QIP technology that was mature enough to be commercialized was QKD, as it poses the least number of challenges. Although it is mathematically proven that QKD protocols are ultrasecure[4], there is nothing *unconditionally* secure in real life, and a commercial QKD device was recently *hacked* [Lyd+10], exploiting the mismatches between the theory and the implementation. Thus, another shift of paradigm deemed necessary, which we now know as the Device-Independent (DI) approach.

The goal of Device-Independent Quantum Information Processing (DIQIP) is to perform QIP tasks with the minimal number of assumptions; in particular, without any assumption about the internal working of the devices.

[2] It was thought that, clearly, there must have been some degree of freedom or hidden variable that was not taken into account by QT, with which these correlations could be explained. This was formalized in the Einstein-Podolsky-Rosen (EPR) paradox in 1935 [EPR35].

[3] In 1964, John Bell started the second quantum revolution by sending [Bel64] to the obscure and now defunct journal *Physics*. There he proposed to think of entanglement as a resource that would be useful in some tasks; like two parties, Alice and Bob, trying to win in a cooperative game. He observed that the probability that was given by QT was notably higher than the probability under the EPR assumptions. Hence, one needed only to ask Nature by performing an experiment [AGR82].

[4] Even someone who is eavesdropping the channel can be detected.

Devices are treated as some black boxes that recieve some classical information that tells them which measurement to perform and output some classical information as a result. This is a qualitative change in various aspects: first, the advantadge to be able to distrust your own device does not come for free, as the requirements to be met to achieve security in DIQIP protocols are much more stringent, albeit possible; second, the resource used in DI protocols is not (only) entanglement, but nonlocal correlations, which are of different nature. Nonlocal correlations are useful for other QIP tasks [Bru+14], such as Certified Quantum Random Number Generation (CQRNG) [Pir+10], Device-Independent Quantum Key Distribution (DIQKD) [Pir+13], Dimensionality Witnessing (DW) [Gal+10] or Randomness Amplification (RA) [CR12].

Our understanding of entanglement and nonlocality is still severily limited. There is no general efficient method answer the simplest of the questions we can pose: whether a given quantum state is entangled or not, nor whether a set of correlations is local or nonlocal. Fortunately, many of the cases of physical relevance enjoy some symmetries that are inherent to these kind of systems (*e.g.*, permutational invariance, translational invariance). This Thesis is aimed towards this direction: characterizing entanglement and nonlocal correlations constrained by symmetries.

1.1. Motivation

With this Thesis we want to contribute to the characterization of entanglement and nonlocal correlations in systems in which symmetry constraints can be assumed. The main questions which are addressed are the following:

1.1.1. Entanglement in the symmetric states

One of the most powerful criteria that are sufficient (although not necessary in general) to certify that a quantum state is entangled is the so-called Positive under Partial Transposition (PPT) criterion [Per96]. This criterion is, by definition, bipartite. It consists in applying a map to one part of the system, while leaving the other part untouched. Such map has the property that, if the whole system is separable (not entangled), it will preserve the positiveness of the density matrix. Hence, if the resulting state is unphysical,

the original state had to be entangled; if it is phyisical, the PPT criterion does not decide. The PPT criterion is known to be necessary and sufficient in the case of quantum states consisting of two qubits or a qubit and a qutrit [Stø63; Wor76; HHH96].

In the multipartite scenario, one can easily generalize the PPT criterion: If a multipartite quantum state fails the PPT criterion with respect to a single bipartition, the state is entangled across this bipartition. However, the number of bipartitions scales exponentially with the number of subsystems, thus checking if a state is PPT with respect to every bipartition is an inefficient task.

Symmetries significantly reduce this complexity. If one considers physical systems in which particles are indistinguishable, such as bosonic particles, the state of the system remains invariant under any permutation of its particles. This implies that one can find more efficient representations of the state and that the PPT criterion can be tailored to symmetric states [Eck+02]: the only relevant variable is the number of elements in each bipartition, and not which particular elements form the bipartition. Hence, the relevant number of bipartitions now scales linearly with the number of subsystems.

Despite this drastic simplification, a lot of questions remain open for symmetric states. It is known that there do not exist PPT entangled symmetric states (PPTESS) of 2 or 3 qubits, and there exist some of 5 and 6 qubits, although they are not PPT with respect to every bipartition [TG09]. It was an open question whether the PPT criterion was necessary and sufficient for 4 symmetric qubits. Do fully PPTESS of 4 qubits or more exist? What are their algebraic and geometrical properties? To what extent can they be characterized?

Entangled bipartite quantum states that are PPT are entangled in a weak way [HHH98; Hor+09], meaning that, no matter how many copies of them one has, a maximally entangled state can never be distilled. Can one find fully PPT states that, nevertheless, possess the strongest form of multipartite entanglement, Genuinely Multipartite Entangled (GME)?

1.1.2. Detecting nonlocality in many-body systems

Due to the intensive studies of entanglement properties of quantum many-body systems, our understanding of them has rapidly grown in the last

decade. For instance, in lattice spin models described by local Hamiltonians, entanglement is a signature of a Quantum Phase Transition (QPT) [Ost+02]. Moreover, entanglement has also inspired an efficient description of the lowest energy states of local Hamiltonians in terms of Matrix Product States (MPS) or, more generally, tensor networks.

Much less, however, is known about the role of quantum nonlocality in many-body systems. First of all, the mathematical complexity of finding the so-called Bell inequalities that characterize the frontier between locality and nonlocality scales very badly with the number of particles, measurements and/or outcomes that one considers in an experiment. Secondly, in order to check nonlocality, typically one needs to measure correlators between many particles, and these are difficult to access experimentally, as a high degree of control of is required: one needs to address each particle individually and perform the corresponding local measurement on it. In the lab, however, what we have within our reach is severely limited, as typically one has access to few-body correlations, often one- and two-body.

Is it possible, then, to detect nonlocality in many-body systems from the least amount of information; namely, two-body correlations? This presents several challenges: the first one is to tailor Bell inequalities to involve only those lowest-order correlators; another challenge is whether such inequalities would be strong enough to detect nonlocality, as higher-order correlations contain much more information than its marginals. Apart from these questions, which are of fundamental interest, another challenge is whether there exist quantum states that are physically relevant; in particular, ground states of physical Hamiltonians, such that their nonlocality can be revealed with these tools?

Symmetry also plays a significant role in lowering the complexity of this problem to an accessible level. Of particular interest are Permutationally Invariant (PI) and Translationally Invariant (TI) Bell inequalities, as these symmetries are present in physical systems. However, application of symmetries further constrains the set of Bell inequalities that can be obtained, making the question whether there exist physically relevant quantum states whose nonlocality can be detected with two-body PI or TI Bell inequalities even more demanding.

1.1.3. The relation between entanglement and nonlocality

Entanglement and nonlocality are fundamental resources for Quantum Information Processing tasks. In order to obtain quantum nonlocal correlations, one needs to have an entangled state. It was shown that, for pure states; *i.e.*, those for which our information is maximal, every entangled state is also nonlocal [Gis91; PR92]. This apparent equivalence between entanglement and nonlocality no longer holds for mixed states, as there exist mixed entangled states that can never display nonlocal correlations [Wer89; Bar02].

So far our knowledge about entangled states that do not display nonlocality is very scarce, and most of the known examples are generalizations of Werner's model [Wer89] concerning a bipartite scenario. This lack of knowledge is caused, to some extent, by the difficulty in proving that a state is local: whereas nonlocality of a state is certified by giving measurements that produce statistics that violate some Bell inequality, certifying locality of a state requires the construction of a Local Hidden Variable Model (LHVM) that works for any set of measurements that is performed on it.

In the multipartite scenario, except for a single tripartite example [TA06], almost nothing is known. What is the relation between entanglement and nonlocality when many parties are involved? Note that the relevant question now concerns the strongest form of entanglement: Genuinely Multipartite Entangled (GME). Otherwise, one can trivially pick a bipartite local state which is product with as many parties as needed, and it will be entangled and local. Another technical challenge comes with the operational definition of Genuinely Multipartite Nonlocal (GMN), which, unlike the generalization of bipartite entanglement to GME, it is not a straightforward generalization of bipartite nonlocality. As GME is the strongest form of multipartite entanglement, does it become too demanding at some point so that GME states always display some form of nonlocality, or does this inequivalence hold in general?

1.1.4. Atomic monogamies of correlations

Another feature that entanglement and nonlocal correlations share is that they are monogamous. Entanglement is monogamous in the sense that, given a multipartite 3-qubit state shared between parties A, B and C, the

more entangled A and B are, the less entangled A and C can be [CKW00].

In the case of nonlocal correlations (either quantum or no-signalling), something similar happens. If we take as a measure of nonlocality the amount of a Bell inequality violation, then there is a trade-off between the observed violation between A and B, and between A and C. However, how essential is this relation? Bell inequalities are, after all, (linear) combinations of correlators. Is there any fundamental limitation when we compare the amount of violation of a Bell inequality with a *single* (hence, the terminology *atomic*) correlator?

Many proofs of security in QIP protocols rely on this monogamy property: If A and B share a high degree of entanglement, then the state of any spy E is -by monogamy of entanglement- product with respect to AB. In DIQIP protocols, an analogy can be made with correlations. However, if there exist stronger monogamy relations, the power of any spy E can be more accurately estimated. To which extent do these atomic monogamies of correlations allow for an improvement of performance in DIQIP tasks?

1.2. Main results

In this Thesis, we address the open questions posed above.

1.2.1. Characterization of PPT Entangled Symmetric States

Entanglement properties of symmetric PPT states lack a systematic study [Eck+02]. We start to fill this gap [Tur+12] by proving the existence of four-qubit entangled PPT states. We follow two different approaches to arrive at this result: numerically, we adapt a search algorithm for extremal bipartite PPT states [LMO07] to the multipartite scenario and we apply it to search for PPT entangled symmetric states (PPTESS); we also propose a half-analytical, half-numerical method that constructs classes of PPTESS, starting from bipartite $2 \otimes 4$ PPT entangled states, such as those introduced by Horodecki [Hor97].

We further characterize PPTESS of many qubits [Aug+12]. We provide several separability criteria in terms of the ranks of the state and its respective positive partial transpositions. We also study edge states in these systems. In particular, for 4 and 5 qubits, we show that the study of generic

PPT states can be reduced to few (2 and 3, respectively) configurations of ranks. We also expand the numerical search up to 23 qubits and study the typicality of configurations of ranks of PPTESS: For an even number of qubits we observe few configurations, whereas for odd number of qubits we find only one configuration.

1.2.2. Detecting nonlocality with two-body correlators

We construct Bell inequalities that involve standard theory- and experiment-friendly many-body observables, since they involve correlations which are one- and two-body. We present a detailed and rigorous derivation of such inequalities, focusing on those which are invariant under the action of a symmetry group [Tur+15b]. In particular, we study Permutationally Invariant [Tur+14a] and Translationally Invariant [Tur+14b] inequalities of such kind. We study the structure the local polytope of correlations and derive analytical classes of inequalities. For those classes, we study the states that give the maximal quantum violation; *i.e.*, those states whose nonlocality is best revealed with these kind of Bell inequalities. We study the asymptotic behavior or such states as the number of parties goes to infinity, as well as the robustness against different sources of noise.

We show how these inequalities reveal the nonlocality of physical systems, such as ground states of the isotropic Lipkin-Meshkov-Glick (LMG) Hamiltonian [LMG65]. These states are the so-called Dicke states [Dic54], and we provide a class of PI Bell inequalities that detects every entangled Dicke state.

We also discuss the possible generalization of the methods introduced to obtain PI Bell inequalities with two-body correlators to K-body correlators, with any number of parties, measurements and outcomes.

For TI Bell inequalities, we find all 3- and 4-partite inequalities with at most 2-body correlators and classify them. We analyse their maximal quantum and no-signalling violations and we show that a TI Bell inequality can always be violated with a TI quantum states and the same set of measurements at each site, at the possible cost of having to increase the local dimensions of the state.

Finally, we address the role of imperfections and errors that are typically introduced in an experiment, motivated by discussions with the Hannover group [LK14] and we discuss several experimental setups in which nonlo-

cality in many-body systems can be tested using the inequalities that we have proposed [Tur+15a].

1.2.3. Entanglement and nonlocality are inequivalent for any number of particles

Understanding the relation between nonlocality and entanglement is one of the central problems in Quantum Information Theory (QIT). Except for a single example of a three-qubit state that admits a Local Hidden Variable Model, almost nothing is known in the multipartite scenario. We address this problem in the multipartite case and show that, for any number of particles, GME is not equivalent to GMN. In particular, we give a construction that, starting from a GME state that admits a K-local model, extends that state to more parties in such a way that this extended state is GME but not GMN. In particular, we discuss how this extension can be applied to isotropic and Werner states and we further show how this extension is compatible with the operational definitions of GMN [Aug+14c].

1.2.4. Elemental and tight monogamy relations in no-signalling theories

The way that nonlocal correlations can be distributed among parties is constrained by the physical theory that one considers (such as Quantum Theory (QT) or the No-Signalling (NS) principle). Such constraints are often expressed as monogamy relations (trade-offs) that bound the amount of a Bell inequality violation between different sets of parties. Here we provide stronger monogamy relations for NS theories: the existence of nonlocal correlations among a set of parties limits *any* form of correlations (local or not) that are shared with an external party [Aug+14b].

We provide tight bounds between the amount of violation of a family of Bell inequalities involving an arbitrary number of parties and the information that an external observer can get about the outcomes of any measurement performed by any of the parties participating in the Bell experiment. Such inequalities are a generalization of the Clauser-Horne-Shimony-Holt (CHSH) inequality to an arbitrary Bell scenario with any number of parties, measurements and outcomes [Aol+12; BKP06].

This result implies an improvement in performance with respect to existing Device-Independent protocols. In particular, we show how they

boost the key rate with respect to previous Device-Independent Quantum Key Distribution (DIQKD) protocols and how they enable Randomness Amplification (RA) under less demanding constraints.

1.3. Outline of the Thesis

This Thesis is organized as follows:

- Chapter 2 reviews the basic concepts that are needed to introduce and derive this Thesis' results. We have included this chapter for completeness, although readers with expertise in quantum information may skip it.
- Chapter 3 is dedicated to the study of PPT entanglement in the symmetric states. This chapter is based on the following original results: [Tur+12; Aug+12].
- Chapter 4 is devoted to the study of nonlocality in multipartite quantum states. This chapter is based on the following original results: [Tur+14a; Tur+14b; Tur+15a; Tur+15b]. The results in Section 4.5 are new and unpublished.
- Chapter 5 studies the relation between entanglement and nonlocality in the multipartite scenario and is based on the following original work: [Aug+14c].
- Chapter 6 studies monogamy relations in NS theories and is based on the following original work: [Aug+14b].
- Chapter 7 summarizes the obtained results and discusses future research directions.
- Appendix A is added in the interest of self-containedness and it comprises several results on representation theory which provide a mathematical background to efficiently work with PI quantum states.
- Appendix B contains technical proofs from Chapter 4.
- Appendix C contains various tables that have been included for the sake of completeness.

2. Background

In this chapter we present the basics that will be used in the rest of the Thesis, as well as the results that represent the state of the art. Expert readers may skip this chapter.

2.1. Entanglement

If one had to describe quantum physics in just one word, this would probably be *entanglement*. Quantum physics predicts that, for a multipartite system, there exist states which cannot be written as a product of the states of its subsystems; such states are called entangled. This fact is just a direct consequence of the tensor product structure of the Hilbert space that describes a composite quantum system and the linearity of quantum mechanics, also known as the superposition principle; however, it entails deep consequences.

Historically, Einstein, Podolsky and Rosen argued in 1935 that quantum mechanics was an incomplete description of Nature[1], and entanglement was at the heart of their argument [EPR35]. However, Schrödinger, who first coined the term entanglement, noted that it was the most characteristic feature of quantum mechanics [Sch35]:

Entanglement is not one but rather the characteristic trait of quantum mechanics, the one that enforces its entire departure from classical lines of thought.

In 1964 the physicist John Bell came up with a way to test the EPR paradox, and he proved that the statistics obtained through some quantum experiments cannot be reproduced by any local theory [Bel64]. This means that Nature can produce correlations between spacelike separated events

[1] The authors argued that any complete theory should have an element that describes every 'element of reality' (*i.e.*, a physical quantity whose values can be predicted with certainty without disturbing the system).

that can be explained neither by an influence continuously propagating (at arbitrary finite speed) from one event to the other nor by a common local cause.

Surprisingly, very few works appeared from 1935 to the early 1990s, when Artur Ekert proposed to use the correlations arising from entangled states for cryptography [Eke91].

Nowadays, entanglement is considered a resource for many quantum information tasks, comprising quantum cryptography [Eke91], quantum teleportation [Ben+93], quantum dense coding [BW92], quantum repeaters based on entanglement purification [Dür+99], lowering bounds on communication complexity [CB97; Gro97], and it is a prerequisite for another important resource in quantum information theory: nonlocal correlations [Bar+05].

2.1.1. Characterization of entanglement

Quantum states are represented by positive semi-definite linear operators of unit trace acting on a Hilbert space $\mathcal{H}$. Recall that a Hilbert space is an inner product space[2] which is also complete (every Cauchy sequence in $\mathcal{H}$ converges in $\mathcal{H}$ with the norm induced by the inner product in $\mathcal{H}$). For the purposes of this Thesis, $\mathcal{H}$ will be a finite-dimensional complex Hilbert space; *i.e.*, $\mathcal{H} = \mathbb{C}^d$. The set of bounded linear operators acting on $\mathcal{H}$ will be denoted $\mathcal{B}(\mathcal{H})$. By picking a basis of $\mathcal{H}$, typically named computational, consisting of the vectors $\{|i\rangle,\ 0 \leq i < d\}$, the elements of $\mathcal{B}(\mathcal{H})$ are represented by $d \times d$ matrices with complex entries, and we denote such set by M_d. The identity matrix from M_d is denoted $\mathbb{1}_d$. The set of elements of $\mathcal{B}(\mathcal{H})$ that correspond to quantum states is denoted by $\mathcal{D}(\mathcal{H})$ and it contains the elements of $\mathcal{B}(\mathcal{H})$ with unit trace and non-negative eigenvalues. The elements of $\mathcal{D}(\mathcal{H})$ are called density matrices or density operators. Formally, one has $\mathcal{D}(\mathcal{H}) = \{\rho \in \mathcal{B}(\mathcal{H}) \mid \rho \succeq 0,\ \mathrm{Tr}\rho = 1\}$.

Any density operator $\rho \in \mathcal{D}(\mathcal{H})$ can be written as a convex combination of rank-one projectors:

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|, \tag{2.1}$$

[2] Unless stated otherwise, throughout this Thesis we consider that $\mathcal{H}$ is a vector space defined over the field of complex numbers, denoted $\mathbb{C}$.

where p_i is a probability distribution (*i.e.*, for all i, $p_i \geq 0$ and $\sum_i p_i = 1$) and $|\psi_i\rangle$ are unit vectors from $\mathcal{H}$, called *kets*. The co-vectors $\langle\psi_i|$, called *bras*, are the Hermitian transposition of the vectors $|\psi_i\rangle$ with respect to the computational basis; two vectors $|\psi_i\rangle$ are considered equivalent if they differ only by a global phase. Note that the decomposition (2.1) is not unique in general. The set $\{p_i, |\psi_i\rangle\}_i$ is called *ensemble* and different ensembles may lead to the same quantum state ρ. The probability distribution p_i indicates the ignorance or the lack of information that one has on the state of the system. In the case that $p_i = 1$ for some i, the information about the quantum state is maximal and then $\rho = |\psi_i\rangle\langle\psi_i|$ is said to be in a pure state; otherwise we say that the state is mixed. Thus, Equation (2.1) indicates that any mixed quantum state ρ can be obtained as a convex combination of pure states (rank-one projectors). Thus, $\mathcal{D}(\mathcal{H})$ forms a convex set, and it is completely determined by its extremal points (*i.e.*, those that cannot be written as a convex combination of other elements in $\mathcal{D}(\mathcal{H})$). The extremal points of $\mathcal{D}(\mathcal{H})$ are denoted $\mathrm{Ext}(\mathcal{D}(\mathcal{H}))$.

The Hilbert space $\mathcal{H}$ corresponding to a composite quantum system consisting of parts $A_1, \ldots, A_n$ is endowed with a tensor product structure $\mathcal{H} = \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n$, where $\mathcal{H}_i$ is the Hilbert space corresponding to the $i-$th subsystem. This tensor product structure and the linearity of $\mathcal{H}$ are the two key ingredients that lead to the notion of entanglement.

Entanglement definition

Many concepts in quantum information are defined through a negative qualifier; *i.e.*, one defines what a certain concept is *not*. This is as well the case of entanglement, which is defined as not being separable. The reason for that is the operational interpretation that a separable state has: any separable state can be created by Local Operations and Classical Communication (LOCC) from scratch starting from a pure product state $|\psi\rangle = |\psi_1\rangle \cdots |\psi_n\rangle$ [Wer89]; in other words, a separable state can be produced by parties in separated laboratories that are allowed to exchange classical information via *e.g.* a classical telephone line.

Let us illustrate the simplest case; of a bipartite Hilbert space between parties A and B: $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$.

Definition 2.1. *A state $\rho \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$ is called separable if it admits the*

following convex decomposition [Wer89]:

$$\rho = \sum_i p_i \rho_A^{(i)} \otimes \rho_B^{(i)}, \quad \sum_i p_i = 1, \quad p_i \geq 0, \tag{2.2}$$

where $\rho_A^{(i)} \in \mathcal{D}(\mathcal{H}_A)$ *and* $\rho_B^{(i)} \in \mathcal{D}(\mathcal{H}_B)$.

In the multipartite case, one has a Hilbert space $\mathcal{H} = \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n$, where there are different notions of separability. The reason for that is that there are many ways to partition a set of n parties, whereas in Defintion 2.1 there is only one. Let us denote by $\mathbf{A} = \{A_1, \ldots, A_n\}$ the set of n parties and let us consider $\rho_{\mathbf{A}} \in \mathcal{D}(\mathcal{H}_{\mathbf{A}})$, where $\mathcal{H}_{\mathbf{A}} = \bigotimes_{i=1}^n \mathcal{H}_{A_i}$ and $\mathcal{H}_{A_i}$ is the Hilbert space corresponding to party A_i. We say that a set of subsets $S = \{S_1, \ldots, S_K\}$, where $S_i \subseteq \mathbf{A}$, is a K-partition of $\mathbf{A}$ if $\bigcup_{i=1}^K S_i = \mathbf{A}$ and for all i and j, $S_i \cap S_j \neq \emptyset$. Thus, a K-partition of $\mathbf{A}$ is a way to split the set of n parties into K non-empty, pairwise disjoint, subsets. Let $\mathcal{S}_K$ be the set of all K-partitions.

Definition 2.2. *A state* $\rho_{\mathbf{A}} \in \mathcal{D}(\mathcal{H}_{\mathbf{A}})$ *is* K*-separable if it admits the following convex decomposition*

$$\rho_{\mathbf{A}} = \sum_{S \in \mathcal{S}_K} p_S \sum_i q_{S,i} \bigotimes_{k=1}^K |\psi_{S_k,i}\rangle\langle\psi_{S_k,i}|, \tag{2.3}$$

where p_S *and* $q_{S,i}$ *are probability distributions and* $|\psi_{S_k,i}\rangle \in \mathcal{H}_{A_i}$.

Remark 2.3. Observe that Definition 2.2 is the same as Definition 2.1 for $K = 2$ and $n = 2$. If $K = 2$ and n is arbitrary, the state is called bi-separable, as it can be prepared by allowing the n parties to gather in bipartitions; in this case we abuse notation and we simply denote S as $S|\overline{S}$ with $\overline{S} = \mathbf{A} \backslash S$. A state $\rho_{\mathbf{A}}$ is fully separable if it is $n-$separable, and it is Genuinely Multipartite Entangled (GME) if it does not admit any form of $K-$separability; in particular, if it is not bi-separable.

Remark 2.4. Definition 2.2 is clearly inspired in the operational way to construct a quantum state: the higher the K, the less effort the parties need to make to produce the state. However, there are other ways to generalize Definition 2.1, also with a clear operational interpretation. This is the case of $K-$producibility [GTB05]. A state is $K-$producible if it can be

prepared by allowing parties to gather in groups consisting of at most K parties. This leads to another characterization of the set of quantum states. However, the two definitions coincide for the case of GME states that we will mostly consider in Chapters 3 and 5: GME states are those which are not biseparable or, equivalently, those which are not $(n-1)$-producible.

2.1.2. The separability problem

Despite having an operationally clear interpretation, deciding in practice if a state $\rho_{\mathbf{A}}$ is $K-$separable or not is far from trivial, even in the bipartite case where $\mathbf{A} = \{A, B\}$. It was shown by Gurvits in 2003 that this problem is NP-hard[3] [Gur03].

For a few particular cases this question does have a simple complete answer. In general, however, one can obtain only partial results: sufficient, but not necessary, conditions that certify that a state is entangled.

The bipartite case

Let us begin with considering the simplest case of two parties. Any bipartite pure state $|\psi_{AB}\rangle \in \mathcal{H}_{AB}$ admits the following decomposition, called Schmidt decomposition [NC00]:

$$|\psi\rangle = \sum_{i=1}^{r(|\psi\rangle)} \alpha_i |e_i\rangle \otimes |f_i\rangle, \tag{2.4}$$

where $\{|e_i\rangle\}_{i=1}^{d_1}$ and $\{|f_i\rangle\}_{i=1}^{d_2}$ form orthonormal basis of their respective Hilbert spaces and $\sum_i |\alpha_i|^2 = 1$. The minimal number of terms $r(|\psi\rangle)$ for which the decomposition in Equation (2.4) is possible is called the Schmidt rank. A bipartite pure state $|\psi\rangle$ is entangled if, and only if, $r(|\psi\rangle) > 1$. This definition is generalized to the mixed states, leading to the so-called Schmidt number s of a mixed state, by means of the convex roof extension

[3] A problem belongs to the class of complexity NP-hard if any algorithm that solves it can be translated in polynomial time into one solving any problem in NP. Hence, an NP-hard problem is as hard as any problem in NP, although it might be harder.
NP stands for Nondeterministic Polynomial time and it consists of all problems whose solution can be verified in polynomial time by a deterministic Turing machine.

[TH00]:

$$s = \inf_{\{p_i, |\psi_i\rangle\}_i} \max_i r(|\psi_i\rangle), \tag{2.5}$$

i.e., the Schmidt number of ρ is the minimum over all ensembles that generate ρ (cf. Equation (2.1)) of the maximal Schmidt rank of the pure states in the ensemble. A mixed state ρ is separable if, and only if, $s = 1$; in such case, the decomposition in Equation (2.2) is given by the ensemble minimizing Equation (2.5). The Schmidt number constitutes a measure of entanglement and it is non-increasing under LOCC [Nie99; TH00]. Hence, it divides $\mathcal{D}(\mathcal{H}_{AB})$ into $d_1^2 d_2^2$ nested regions[4] according to s.

In what follows we present two operational criteria for deciding whether a state ρ belongs to the set of separable states, denoted $\mathcal{D}_{\text{sep}}$: the Positive under Partial Transposition (PPT) criterion and certification through an Entanglement Witness (EW).

Separability based on positive, but not completely positive, maps

A map $\Lambda : \mathcal{B}(\mathcal{H}_1) \longrightarrow \mathcal{B}(\mathcal{H}_2)$ is called positive if, for all $\rho \succeq 0$, $\Lambda[\rho] \succeq 0$. However, if ρ is the state of a composite quantum system and we apply Λ to one subsystem only, it may happen that the resulting state is not positive semi-definite; *i.e.*, not physical. Consequently, the positivity of a map is not sufficient to guarantee a physical operation. This caveat is solved through the notion of a completely positive map:

A positive map Λ is Completely Positive (CP) if, for any n and for any $\rho \succeq 0$, $(\mathbb{1}_n \otimes \Lambda)[\rho] \succeq 0$; *i.e.*, no matter what happens to the rest of the system, ρ is mapped onto a positive-semidefinite operator. If in addition Λ is Trace Preserving (TP), then Λ defines a physical operation: CPTP maps map quantum states onto quantum states. CPTP maps are also known as quantum channels.

Any positive map, however, is completely positive on separable states, and this is the idea behind the separability criteria based on positive, but not completely positive, maps: If we apply $(\mathbb{1}_n \otimes \Lambda)$ to a state of the form

[4] The upper bound $s \leq d_1^2 d_2^2$, stems from Carathodory's theorem [Car11]: Any state expressed as a convex combination like in Equation (2.2) can be re-expressed as another convex combination of no more than $\dim_{\mathbb{R}} \mathcal{D}(\mathcal{H}_{AB})$ terms, as $\mathcal{D}(\mathcal{H}_{AB})$ can be embedded into the $\mathbb{R}-$vector space of $d_1 d_2 \times d_1 d_2$ Hermitian matrices, which has dimension $d_1^2 d_2^2$.

(2.2), we also obtain a positive state

$$(\mathbb{1}_n \otimes \Lambda)[\rho] = \sum_i p_i \rho_A^{(i)} \otimes \Lambda(\rho_B^{(i)}) \succeq 0. \tag{2.6}$$

Hence, $(\mathbb{1}_n \otimes \Lambda)[\rho] \not\succeq 0$ indicates that ρ is not of the form (2.2) hence it must be entangled.

A necessary and sufficient condition for deciding if a bipartite ρ is separable is that ρ satisfies condition (2.6) for all positive, but not completely positive, maps [HHH96]. In practice, one cannot check this condition for all Λ, but there are maps that very well approximate $\mathcal{D}_{\text{sep}}$.

The PPT criterion

By picking $\Lambda = T$, where T is the transposition map with respect to a basis, defined as $T(|i\rangle\langle j|) = |j\rangle\langle i|$ and extended by linearity, one obtains the Peres criterion, a very strong necessary condition for separability [Per96]. In fact, it is also a sufficient condition for any $\rho \in \mathcal{D}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ or $\rho \in \mathcal{D}(\mathbb{C}^2 \otimes \mathbb{C}^3)$. This is because all positive maps $\Lambda : \mathcal{B}(\mathbb{C}^2 \otimes \mathbb{C}^d) \longrightarrow \mathcal{B}(\mathbb{C}^2 \otimes \mathbb{C}^d)$ are decomposable[5] for $d = 2$ [Stø63] and for $d = 3$ [Wor76] and if a decomposable map reveals entanglement, so does the transposition map [HHH96].

The Positive under Partial Transposition (PPT) criterion is known to be insufficient for any other bipartite case, as there are entangled states in $\rho \in \mathcal{D}(\mathbb{C}^2 \otimes \mathbb{C}^4)$ and in $\rho \in \mathcal{D}(\mathbb{C}^3 \otimes \mathbb{C}^3)$ for which $\rho^{T_B} \succeq 0$, where $\rho^{T_B} := (\mathbb{1} \otimes T)[\rho]$ is the state ρ partially transposed on Bob's side [Hor97].

The PPT criterion and, in general, any criterion of separability based on positive, but not completely positive, maps is straightforward to generalize to the multipartite scenario, for the case of fully separable states.

If a state $\rho_{\mathbf{A}}$ is $n-$separable, then for any bipartition $S|\overline{S}$ of $\mathbf{A}$, the application of Λ to every party in $\overline{S}$ does not change the positivity of the resulting state: $(\mathbb{1}_S \otimes \bigotimes_{A_i \in \overline{S}} \Lambda_{A_i})[\rho] \succeq 0$. A violation of this condition signals that there is entanglement across that bipartition.

[5] A decomposable map Λ can be written as $\Lambda = \Lambda_1 + \Lambda_2 \circ T$, where Λ_1 and Λ_2 are CP maps. This fact is intimately related to the decomposability of entanglement witnesses via the Choi-Jamiołkowski-Sudarshan isomorphism [Jam72; Cho75].

Entanglement Witnesses

The concept of Entanglement Witness (EW) was introduced in [HHH96] as a method to exploit the geometric properties of $\mathcal{D}_{\text{sep}}$. The set of separable states is closed and convex. It will be convenient to consider in this section unnormalized states, so that $\mathcal{D}_{\text{sep}}$ is a cone.

The Hahn-Banach theorem [Edw95] states that, given two convex closed sets A_1 and A_2, one of them being compact, there exists a continuous linear map f and a constant $\alpha \in \mathbb{R}$ such that $f(a_1) < \alpha \leq f(a_2)$ for all $a_i \in A_i$. In particular, it implies that a closed convex set in a Banach space is characterized by half-spaces whose normal vectors are non-positive semi-definite elements of the dual cone of $\mathcal{D}_{\text{sep}}$, denoted $\mathcal{P}$. $\mathcal{P}$ is, by definition, the set $\{W \in M_{d_A} \otimes M_{d_B} |\ \text{Tr}(W\rho) \geq 0,\ \forall\ \rho \in \mathcal{D}_{\text{sep}}\}$. Then, the set of elements $W \in \mathcal{P}$ such that $W \not\geq 0$ forms a non-convex set. Such an operator W is called Entanglement Witness [Ter00]. Note that we require that W has some negative eigenvalue, so that it can detect some entangled state. We denote by $\mathcal{W}$ the set of EWs. A necessary and sufficient condition for $\rho \in \mathcal{D}_{\text{sep}}$ is that $\text{Tr}W\rho \geq 0$ for all $W \in \mathcal{W}$ [HHH96].

Not all elements in $\mathcal{W}$ are necessary to characterize $\mathcal{D}_{\text{sep}}$ and the first attempt to find a minimal set of EWs that determine $\mathcal{D}_{\text{sep}}$ was done in [Lew+00], where the notion of optimal EW was defined. Let us briefly recall it. Given $W \in \mathcal{W}$, consider the sets

$$\Delta_W := \{\rho \in \mathcal{D}(\mathcal{H}) |\ \text{Tr}W\rho < 0\} \tag{2.7}$$

and

$$\Pi_W := \{|e, f\rangle \in \mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B} | \langle e, f|W|e, f\rangle = 0\}, \tag{2.8}$$

which are the set of states detected by W and the set of product states with zero expectation value[6] on W, respectively. Given two entanglement witnesses $W_1, W_2 \in \mathcal{W}$, W_1 is finer than W_2 if $\Delta_{W_2} \subset \Delta_{W_1}$; *i.e.*, if W_1 detects more entangled states than W_2. If there is no witness finer than W, then W is optimal. In terms of Π_W, optimal entanglement witnesses are those for which, for any $\varepsilon > 0$ and any operator $P \succeq 0$ with support orthogonal to Π_W, the operator $W - \lambda P \notin \mathcal{W}$; *i.e.*, there exists a product vector $|e', f'\rangle$ for which $\langle e', f'|W - \lambda P|e', f'\rangle < 0$, so $W - \lambda P$ is not an EW. Consequently,

[6] Note that Π_W does not form a subspace; in fact, it can be a finite set.

if Π_W spans the whole Hilbert space, then W is optimal [Lew+00]. We denote by $\mathrm{Opt}(\mathcal{W})$ the set of optimal entanglement witnesses.

There is a class of entanglement witnesses which is much easier to characterize: these are called decomposable witnesses. A decomposable EW $W \in \mathcal{W}$ has the form $W = P + Q^{T_B}$, where $P, Q \succeq 0$ (it is equivalent to take partial transposition on Alice instead of Bob). If this decomposition is not possible, the witness is called indecomposable. Notice the similarities with the notion of decomposable maps, first introduced in [Stø63; Wor76]. Decomposable EWs are those that are translated from decomposable maps via the Choi-Jamiołkowski-Sudarshan isomorphism [Jam72; Cho75].

Geometrically, one has the inclusions $\mathrm{Ext}(\mathcal{W}) \subsetneq \mathrm{Opt}(\mathcal{W}) \subsetneq \partial\mathcal{W}$ [SSŻ09], where $\partial\mathcal{W}$ is the boundary of $\mathcal{W}$ and $\mathrm{Ext}(\mathcal{W})$ is the set that generates extremal rays in $\mathcal{P}$. Each of these inclusions is strict[7]. Note, however that, although extremal (or even exposed[8]) EWs form proper subsets of $\mathrm{Opt}(\mathcal{W})$, they are sufficient to detect all entangled states [SSŻ09; HK11; CS14]. Nevertheless, the definition of optimal EWs is operational, in the sense that it can be recast into an efficient algorithm that brings any $W \in \mathcal{W}$ into an optimal one [Lew+00]. Hence, optimal EWs constitute a useful tool in entanglement theory.

Relating positive maps and EWs

The concepts defined for EWs can be recast in terms of positive maps via the Choi-Jamiołkowski-Sudarshan isomorphism [Jam72; Cho75], which relates the set $\mathcal{L}(M_d, M_{d'})$ of linear maps from M_d to $M_{d'}$ and the set $M_d \otimes M_{d'}$. Such isomorphism sends $\mathcal{P}$ to the cone of positive maps and

[7] As an example of $W \in \partial\mathcal{W} \setminus \mathrm{Opt}(\mathcal{W})$, consider the line segment $W(p) = pW_+ + (1-p)W_- \in M_2 \otimes M_2$ and consider the Bell basis $|\psi_\pm\rangle = (|00\rangle \pm |11\rangle)/\sqrt{2}$, $|\phi_\pm\rangle = (|01\rangle \pm |10\rangle)/\sqrt{2}$. Pick $W_\pm = |\psi_\pm\rangle\langle\psi_\pm|^{T_B} \in \mathrm{Ext}(\mathcal{W})$. For any $p \in [0, 1/2) \cup (1/2, 1]$, $W \in \mathcal{W}$, whereas $W(1/2) \succeq 0$. Consequently, $W(p) \notin \mathrm{Opt}(\mathcal{W})$ for any $0 < p < 1$. Hence, by moving to one of the extremes of the segment, $W(p)$ can be optimized. $W(p) \in \partial\mathcal{W}$ because for every $p \in [0, 1]$ and for any $\varepsilon > 0$, $\mathcal{W}(p) - \varepsilon|\phi_+\rangle\langle\phi_+|^{T_B} \notin \mathcal{W}$.

As an example of $W \in \mathrm{Opt}(\mathcal{W}) \setminus \mathrm{Ext}(\mathcal{W})$, a decomposable witness of the form $W = Q^{T_A}$ with $Q \in M_2 \otimes M_2$, $Q \succeq 0$ and $\mathrm{supp}(Q)$ being a Completely Entangled Subspace (CES) is optimal [Lew+00]; however it is not extremal if $\mathrm{rank}(Q) > 1$. A CES is a subspace containing no product vectors (see e.g. [ATL11]).

[8] Exposed EWs form a subset of $\mathrm{Ext}(\mathcal{W})$ [HK11]. All extremal decomposable EWs are exposed [CS14].

$\mathcal{W}$ to the set of positive, but not completely positive, maps. Interestingly, a positive map gives a more powerful necessary condition for separability than its corresponding EW[9]. On the other hand, entanglement witnesses correspond to quantum observables, whereas positive, but not completely positive, maps are unphysical. The Structural Physical Approximation (SPA) (see *e.g.* [HE02; Aug+14a]) allows one to overcome this difficulty by mixing a given positive map Λ with the completely depolarizing channel, until the result is a completely positive map: $\Lambda(p) = p\Lambda + (1-p)D$, where $D(X) = \mathrm{Tr}(X)\mathbb{1}_{\mathrm{d}}/d$ is the completely depolarizing channel and $0 \leq p \leq 1$. Clearly, there exists a largest p for which $\Lambda(p)$ is a CP map, denoted p^*. $\Lambda(p^*)$ is then called the SPA of Λ.

Via the Choi-Jamiołkowski-Sudarshan isomorphism one formulates the SPA in terms of EWs: the SPA to an EW $W \in \mathcal{W}$ is

$$W(p_*) = p_* W + (1-p_*)\frac{\mathbb{1}_{d_A d_B}}{d_A d_B}, \tag{2.9}$$

where $p_*^{-1} = 1 + d_A d_B |\lambda_{\min}|$ and $\lambda_{\min}$ is the minimal eigenvalue of W, which is negative.

2.2. Nonlocality

Nonlocality [Bru+14] is a central concept in quantum information theory. In 1964, Bell proved that some predictions of quantum theory cannot be explained through a Local Hidden Variable Model (LHVM) [Bel64], ruling out the possibility that quantum physics was an incomplete theory because of the existence of inaccessible (hidden) variables that would determine with certainty the outcome of measurements performed on a quantum system.

Local models are those that arise naturally within our everyday experience with the classical world. Physicists considered, after the formulation of the EPR paradox [EPR35], whether they could provide an alternative explanation to quantum physics which would be complete and more intuitive, until in 1964 Bell showed that the two of them were in contradiction.

[9] The typical example is the transposition map, which detects all $2 \otimes 2$ and $2 \otimes 3$ states, whereas its corresponding entanglement witness detects just a subset of them [HHH96].

Years after, Alain Aspect demonstrated, with an experiment in 1982, that Nature does not admit a LHVM [AGR82].

2.2.1. The device-independent formalism

Although a Bell experiment was inially designed to test a fundamental question (whether Nature is nonlocal), we typically present it as a game: a Bell experiment involves two or more parties, which may have interacted in the past, located in spacelike separated regions, each of them having access to their share of a physical system, for example, a source of entangled photons. Independently of the state of the system, each party chooses which measurement to perform on their subsystem and gets a result. Thus, each party can be treated as a black box with an input which corresponds to the choice of a measurement and an output that tells its result; nothing is assumed about the internal working of the device nor the object they are measuring.

We label the inputs of the n parties by $\vec{x} = (x_0, \ldots, x_{n-1})$ and the outputs by $\vec{a} = (a_0, \ldots, a_{n-1})$. The labelling of $\vec{x}$ encodes the different tunable parameters relevant for the experiment (*i.e.*, the measurement choice) and the labelling of $\vec{a}$ encodes the possible readouts of the experiment. The way that this labelling is assigned is irrellevant to the Bell's experiment and labels do not even have to correspond to physical quantities.

In the DI framework, one assumes that the parties have Independent and Identically Distributed (IID) preparations of the experiment, in the sense that after repeating it many times, they can infer the underlying conditional probabilites of the outputs given the inputs $P(\vec{a}|\vec{x})$ from the statistics collected from the experiment[10].

It is also required that the choice of inputs is independent of the state of the system, an assumption often referred to as *free will* assumption[11].

[10] There exist other frameworks in which can study nonlocality, such as the ones considered in Section 5.5.1. In this Thesis, we consider the typical framework in which parties perform a single measurement on a single copy of their resource and repeat the experiment in the same conditions.

[11] For instance, if Alice has to choose between measuring the spin of a electron in the direction x and measuring the spin in the direction z, her choice has to be independent on the state of the electron; in other words, the electron cannot know what Alice is going to measure. This situation is relevant in the framework of quantum cryptography tasks, where the manufacturer of the devices and/or the provider of entangled particles

Sometimes this assumption is partially fulfilled, but it can be remediated through a protocol called randomness amplification (see Chapter 6).

Depending on the physical principles that we take into consideration, some probability distributions $P(\vec{a}|\vec{x})$ may contradict them, so not every mathematically consistent P may be compatible with a given physical principle.

2.2.2. A geometric approach to correlations

In general, we will consider a scenario where n parties, each having acces to m measurements which have d outcomes, are performing a Bell experiment, and we denote this Bell scenario by (n, m, d). We denote by $\mathcal{M}_{x_i}^{(i)}$ the x_i-th measurement performed by i-th party. The object under consideration is then

$$P(a_0, \ldots, a_{n-1}|x_0, \ldots x_{n-1}), \quad 0 \leq a_i < d, \quad 0 \leq x_i < m. \tag{2.10}$$

Geometrically, one can think of (2.10) as a vector with $(md)^n$ coordinates, each corresponding to a possible combination of $a_0, \ldots, a_{n-1}|x_0, \ldots x_{n-1}$. Let us name such vector $\vec{P}$.

The problem of which probability distributions $\vec{P}$ are sound has been considered since more than a century ago; way before the genesis of modern probability, theory by George Boole, in his theory of *conditions of possible experience* [Boo62], but it was Froissart who reintroduced it in terms of nonlocality and physical principles from the geometric perspective [Fro81] that allows a systematic characterization of correlations in terms of convex sets.

Mathematical constraints

Since $\vec{P}$ has to be a valid probability distribution, it has to fulfill Kolmogórov's axioms of Probability Theory [Kol33]. Consequently, the elements of $\vec{P}$ have to be non-negative and normalized.

Hence, only $m^n(d^n - 1)$ components of $\vec{P}$ remain independent and the non-negativity constraints $P(a_0, \ldots, a_{n-1}|x_0, \ldots x_{n-1}) \geq 0$ define a region in space, which we denote $\mathbf{P}$.

is untrusted and can use this information to fake the statistics $P(\vec{a}|\vec{x})$, compromising security (see Section 6.3.2).

Note that $\mathbf{P}$ is a convex set. Recall that a set $\mathbf{P}$ is convex if, and only if, for all $\vec{P}_1, \vec{P}_2 \in \mathbf{P}$ the line segment $\vec{P}(\lambda) = \lambda\vec{P}_1 + (1-\lambda)\vec{P}_2$ (where $\lambda \in [0,1]$) belongs to $\mathbf{P}$. $\vec{P}(\lambda)$ is called a convex combination of $\vec{P}_1$ and $\vec{P}_2$. $\mathbf{P}$ is convex because it is the intersection of a number of half-spaces (non-negativity conditions) and a number of affine subspaces (normalization conditions). The intersection of convex sets is a convex set.

We shall name a set defined as a finite intersection of half-spaces a convex polyhedra. If, in addition, it is bounded, we shall call it a convex polytope; $\mathbf{P}$ is an example of a convex polytope.

Every convex polytope admits a dual description: On the one hand, it can be fully characterized either as the intersection of a minimal number of half-spaces (the intersection of the polytope with the hyperplane defining one of such half-spaces is called *facet*; the intersection of the polytope with a hyperplane defining any half-space which contains it is called *face*). On the other hand, it can be equivalently characterized by listing all its extreme points (the ones that cannot be written as convex combinations of others with $\lambda \in (0,1)$; such points are called *vertices*).

It is computationally a hard problem to go from one description to the other, especially in large dimension spaces[12]. Its complexity is $O(n^{\lfloor D/2 \rfloor} + n \log n)$, where n is the number of vertices (inequalities) and D the dimension of the affine space; $\lfloor \cdot \rfloor$ is the floor function [Cha93].

The no-signalling set

It is a natural postulate in a physical theory that the speed at which information travels is bounded; in particular, to be consistent with Einstein's relativity theory, information cannot travel faster than light. Therefore, two events happening at spacelike separated regions cannot instantaneously affect each other. This impossibility of instantaneous communication is known as the No-Signalling (NS) principle. In terms of $\vec{P}$, the NS principle has a simple formulation: the choice of measurement performed by one of the parties cannot influence the statistics observed by the rest; *i.e.*, for all

[12] A convex polyhedra admits this dual description as well, if we allow for vertices to be at infinity. Some programs avoid this by working in the Projective space instead of the Affine space, by treating points as rays, for example [Fuk14].

$x_i \neq x_i'$,

$$\sum_{a_i} P(\vec{a}|\vec{x}) = \sum_{a_i} P(\vec{a}|\vec{x}'), \tag{2.11}$$

where $\vec{x} = (x_0, \ldots, x_i, \ldots, x_{n-1})$ and $\vec{x}' = (x_0, \ldots, x_i', \ldots, x_{n-1})$. Note that when the NS holds, the marginal probability distribution

$$P(a_0, \ldots, \widehat{a_i}, \ldots, a_{n-1}|x_0, \ldots, \widehat{x_i}, \ldots, x_{n-1}) = \sum_{a_i} P(\vec{a}|\vec{x}) \tag{2.12}$$

is well defined (the notation $\widehat{\cdot}$ indicates that the element under the hat is missing). Observe that condition (2.11) can be applied recursively to any subset of parties.

The resulting region for which probabilities are no-signalling is also a convex polytope, as it is the intersection of $\mathbf{P}$ with the vector subspaces given by (2.11). This set is known as the no-signalling polytope and we denote it $\mathbf{P}_{NS}$. The number of independent components[13] of any $\vec{P} \in \mathbf{P}_{NS}$ is reduced to $(m(d-1)+1)^n - 1$. The facets of $\mathbf{P}_{NS}$ are easy to specify, as they are the non-negativity constraints subjected to normalization and NS constraints. Its vertices, known as PR-boxes [PR94], are hard to compute in general, and they are known only in few scenarios [Bar+05; Fri12].

The quantum set

When $\vec{P}$ is obtained from a quantum state on which local quantum measurements are performed, one obtains a different set of possible correlations, the quantum set of correlations fulfilling Quantum Theory (QT), which we denote by $\mathbf{Q}$.

Following the axioms of quantum physics, $\vec{P}$ has to be obtained via Born's

[13] This follows from a simple combinatorical argument: The number of independent components of $\vec{P} \in \mathbf{P}_{NS}$ is given by the normalization conditions of probabilities and the number of different marginals because of the NS principle: For every party, one can choose whether to measure it or not; if it is not measured, there are m possible measurements to perform, and for each measurement there are $d-1$ outcomes to specify (because the last outcome can always be recasted as a function of the rest by means of the normalization conditions). If nobody measures, there is no value needed to specify, so we rule out this possibility.

rule:

$$P(a_0,\ldots,a_{n-1}|x_0,\ldots,x_{n-1}) = \mathrm{Tr}\left(\rho \cdot \bigotimes_{i=0}^{n-1} \Pi^{(i)}_{a_i|x_i}\right), \tag{2.13}$$

where $\rho \in \mathcal{D}(\mathcal{H})$ for some Hilbert space $\mathcal{H}$ of unspecified dimension and $\{\Pi^{(i)}_{a_i|x_i}\}$ define a Positive-Operator Valued Measure (POVM) on the i-th party. A POVM fulfills that its POVM elements, $\Pi^{(i)}_{a_i|x_i}$, are positive semi-definite and they form a resolution of the identity: $\sum_{a_i} \Pi^{(i)}_{a_i|x_i} = \mathbb{1}^{(i)}$. Note that, since the dimension of $\mathcal{H}$ is unconstrained, one can assume, without loss of generality, that ρ is in a pure state and that the POVM is in fact a von Neumann (Projective Measurement (PM)) measurement; *i.e.*, the POVM elements are, in addition, pairwise orthogonal projectors.

Because $\dim_{\mathbb{C}} \mathcal{H}$ is unconstrained, $\mathbf{Q}$ forms a convex set. However, it is not a polytope and its boundary is unknown in practically all cases. Surprisingly, it turns out that $\mathbf{Q}$ is contained in $\mathbf{P}_{NS}$, a fact that follows directly from (2.13) fulfilling (2.11); however it is strictly smaller [PR94]. It remains today an open question *What should one require, in addition to the no-signalling principle, in order to recover quantum correlations?* To this aim, several operational principles have been proposed: Non-trivial communication complexity [Dam99; Bra+06], no advantadge for nonlocal computation [Lin+07], information causality [Paw+09], macroscopic locality [NW10], local orthogonality [Fri+13]. However, each of them defines a superset of $\mathbf{Q}$.

It is possible to approximate $\mathbf{Q}$ with a convergent hierarchy of spectrahedrons[14] $\mathbf{Q} \subseteq \ldots \subseteq \mathbf{Q}_2 \subseteq \mathbf{Q}_{1+AB} \subseteq \mathbf{Q}_1$ [NPA08]. Interestingly, it was recently shown that a generalization of the level of the Navascués-Pironio-Acín (NPA) Hierarchy $1 + AB$ to the multipartite case recovers all the operational principles mentioned above (except for information causality, which remains unknown) [Nav+15].

The LHVM set

Imagine a Bell experiment with $n = 2$ parties. In general, the obtained statistics $P(ab|xy)$ will not be of the form $P(a|x)P(b|y)$. This lack of inde-

[14] A spectrahedron is the feasible set of a Semi-Definite Program (SDP).

pendence is not surprising, nor does it imply an influence of one party to another; Alice and Bob may simply have established some correlation in the past, when they were allowed to interact or to agree on a common strategy. The idea behind a local theory, however, is that whatever interaction or factor relevant to both outcomes, described by a variable λ, must decouple the two probabilities, so that, if we know λ, they become independent: $P(ab|xy\lambda) = P(a|x\lambda)P(b|y\lambda)$.

Observe that, when λ is known, the outcome of Alice does not depend on the choice of input of Bob nor on his result, and vice-versa.

In general this λ may be inaccessible to us, and we call it *hidden variable*. In fact, λ may not be the same in every round of the Bell experiment, as it may include not fully controllable physical quantities, or the parties may agree to change their strategy at every round. Hence, it is natural to describe it via a probability distribution $p(\lambda)$.

This is what motivates the definition of a Local Hidden Variable Model (LHVM): We say that $\vec{P}$ admits a LHVM if it can be written in the form

$$P(\vec{a}|\vec{x}) = \int_\Lambda p(\lambda) \prod_{i=0}^{n-1} P(a_i|x_i\lambda)\mathrm{d}\lambda, \tag{2.14}$$

where Λ is the space of hidden variables, $p(\lambda) \geq 0$ and $\int_\Lambda p(\lambda)\mathrm{d}\lambda = 1$.

The set of probabilities admiting the form (2.14) is again a polytope, known as the local polytope and we denote it $\mathbf{P}_L$. The functions $P(a_i|x_i\lambda)$ are called local *response functions* and they need not be deterministic. However, every probability distribution can be expressed as a convex combination of deterministic events (one for each outcome and the weight of the convex combination corresponds to the probabilities of the events). These deterministic events are delta functions $\delta(a_i, f_i(x_i, \lambda))$, where f_i is some deterministic function that takes the information available to the i-th party, namely, x_i and λ, and produces an outcome in $\{0, \ldots, d-1\}$. Consequently, a LHVM admits also the form [Fin82]

$$P(\vec{a}|\vec{x}) = \int_\Lambda q(\lambda) \prod_{i=0}^{n-1} \delta(a_i, f_i(x_i, \lambda))\mathrm{d}\lambda, \tag{2.15}$$

for a (possibly different) probability distribution $q(\lambda)$.

Equation (2.15) already gives information on how to construct the vertices of $\mathbf{P}_L$, for they are the probability functions of the form $P(\vec{a}|\vec{x}) =$

$\prod_{i=0}^{n-1} \delta(a_i, \tilde{f}_i(x_i))$, with $\tilde{f}_i(x_i) \in \{0, \ldots, d-1\}$; *i.e.*, the ones that cannot be expressed as a convex combination of λ. Varying the possible choices of $\tilde{f}_i(x_i)$ we obtain the $(md)^n$ different vertices of $\mathbf{P}_L$.

$\mathbf{P}_L$ is a subset of $\mathbf{Q}$ because every probability of the form (2.14) can be constructed with a fully separable state; and it is a strictly smaller set because there are quantum states and measurements that produce $\vec{P}$'s which are outside $\mathbf{P}_L$ [Bel64]. These probability distributions are called nonlocal.

The half-spaces containing $\mathbf{P}_L$ are called *Bell inequalities*. If a Bell inequality corresponds to a facet of $\mathbf{P}_L$, we shall name it *tight* Bell inequality[15]. If a Bell inequality is violated by some $\vec{P} \in \mathbf{P}_{NS}$ we call it *non-trivial*. Finding all Bell inequalities is an extremely difficult task and only a few scenarios have been completely solved, none of them for more than 3 parties[16] [PS01; Pir14].

Since the labelling of parties, measurements and outcomes is arbitrary, the different sets of correlations obey some symmetries (*e.g.* shuffling the outcomes of a certain measurement in a Bell inequality will lead to another Bell inequality) and Bell inequalities can be grouped in classes[17] In the $(2, 2, 2)$ scenario, the only non-trivial class of Bell inequalities is the one derived by Clauser, Horne, Shimony and Holt [Cla+69] whereas in the $(3, 2, 2)$ scenario one finds 46 different classes [Śli03].

2.2.3. Multipartite nonlocality

Both the definition of a fully separable state (cf. Eq. (2.2)) and a LHVM (cf. Eq. 2.14) look similar. Analogously to the case of entanglement, in the multipartite scenario, various degrees of nonlocality are possible. However, the case of nonlocality is subtler, in the sense that one should specify what are the rules for the response functions of more than one party.

Genuine multipartite nonlocality was first introduced by Svetlichny in 1987 [Sve87]. Analogously to the biseparable case, Svetlichny defined a

[15] Note, however, that in polytope theory, a tight inequality is one which just touches the polytope.

[16] See also [Fri12] for an interesting duality relation between the vertices and facets of $\mathbf{P}_{NS}$ and $\mathbf{P}_L$ in the $(n, 2, 2)$ scenario. A repository of the currently known Bell inequalities can be found in [RBG14]

[17] The same argument applies to PR-boxes [Bar+05].

3-partite probability distribution to be bi-local if it was of the form

$$\begin{aligned} P(abc|xyz) &= \int_\Lambda p_{AB|C}(\lambda) P_{AB}(ab|xy\lambda) P_C(c|z\lambda) \mathrm{d}\lambda \\ &+ \int_\Lambda p_{AC|B}(\lambda) P_{AC}(ac|xz\lambda) P_B(b|y\lambda) \mathrm{d}\lambda \\ &+ \int_\Lambda p_{BC|A}(\lambda) P_{BC}(bc|yz\lambda) P_A(a|x\lambda) \mathrm{d}\lambda. \end{aligned} \tag{2.16}$$

Operationally, terms such as $P_{AB}(ab|xy\lambda)$ mean that Alice and Bob can exchange an arbitrary amount of communication between themselves, but not with Charlie. So, $P_{AB}(ab|xy\lambda)$ can be any mathematically sound probability distribution; in particular, a signalling one. This leads to grandfather-type paradoxes [Ban+13].

There are basically two possibilities to avoid these issues: one is to require that the probability distributions $P_{AB}(ab|xy\lambda)$ satisfy the no-signalling constraints (2.11) [Alm+10b]; such correlations are called No-Signalling Bi-Local (NSBL). Another one is to require that the correlations of the form $P_{AB}(ab|xy\lambda)$ appearing in (2.16) are time-ordered (*e.g.* Alice can signal to Bob or vice-versa, but not both at the same time); such correlations are called Time-Ordered Bi-Local (TOBL) [Gal+12]. All such constraints define convex polytopes and one has the chain of inclusions $\mathbf{P}_L \subsetneq \mathbf{P}_{NSBL} \subsetneq \mathbf{P}_{TOBL} \subsetneq \mathbf{P}_{\text{Svetlichny}} \subsetneq \mathbf{P}$ [Ban+13].

In the general case of n parties, having in mind the different flavors of multipartite locality stemming from the considerations mentioned above, one defines a probability distribution $P(\vec{a}|\vec{x})$ to be K-local if it is of the form

$$P(\vec{a}|\vec{x}) = \sum_{S \in \mathcal{S}_K} p_S \int_\Lambda p_S(\lambda) \prod_{k=1}^{K} p_k(\vec{a}_{|S_k}|\vec{x}_{|S_k}\lambda) \mathrm{d}\lambda. \tag{2.17}$$

Analogously to the case of (2.3), if $K = 2$ we will say that $\vec{P}$ is bi-local, whereas if $K = n$, we shall name it fully local. If $\vec{P}$ cannot be written as (2.17) with $K = 2$, then it is called Genuinely Multipartite Nonlocal (GMN).

Monogamy of correlations

A nonlocal probability distribution $\vec{P} \notin \mathbf{P}_L$ will violate some Bell inequality. Geometrically, the farther $\vec{P}$ is from $\mathbf{P}_L$, the higher its violation will be. The amount of violation (up to normalization) of a Bell inequality is often taken as a measure of nonlocality[18]. Physical principles (such as quantum mechanics or no-signalling theories) prevent nonlocality from being distributed arbitrarily between several parties. Entanglement does also display these kind of constraints, known as monogamy relations [CKW00]. In the case of nonlocal correlations, monogamies of correlations impose a tradeoff between the violation of a Bell inequality between two sets of parties, **A** and **B** and the same Bell inequality between the first set **A** and another one **C**.

As an example, let us consider 3 parties ABC and the Clauser-Horne-Shimony-Holt (CHSH) inequality [Cla+69]:

$$I_{AB} = \langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle, \tag{2.18}$$

where each correlator $\langle A_x B_y \rangle$ is defined as follows: $P(a = b|xy) - P(a \neq b|xy)$. The classical bound for which I_{AB} defines a facet of $\mathbf{P}_L$ for the $(2, 2, 2)$ scenario is $I_{AB} \leq 2$. If Alice, Bob and Charlie share arbitrary quantum resources, then $I_{AB}^2 + I_{AC}^2 \leq 8$ [TV06]. Even if they share a No-Signalling resource, a monogamy relation holds, namely $|I_{AB}| + |I_{AC}| \leq 4$ [Ton09].

2.2.4. Local models

Both entanglement and nonlocality are valuable resources for quantum information theory, although inequivalent ones. Because every separable quantum state produces local correlations, entanglement is necessary for nonlocality. In the case of pure states, Gisin showed that every entangled pure state can display nonlocal correlations [Gis91]. In the case of mixed states, there are bipartite states, known as Werner states, for which, no

[18] There is another formulation of measure of nonlocality formulated by Elitzur-Popescu-Rohrlich (EPR2) [EPR92], which measures the nonlocal content of $\vec{P}$ by decomposing it as a convex combination of a no-signalling distribution $\vec{P}_{NS} \in \mathbf{P}_{NS}$ and a local distribution $\vec{P}_L \in \mathbf{P}_L$ with maximal p: $\vec{P} = p\vec{P}_{NS} + (1-p)\vec{P}_L$.

matter what measurements are performed on them, its statistics are of the form (2.14) [Wer89]; *i.e.*, they admit a Local Hidden Variable Model.

In general, very little is known about which quantum states admit a local model [ADA14] essentially because one has to explicitly construct the response functions $P(a_i|x_i\lambda)$. In the multipartite case, even less is known: For example, when one considers GME states, even those pure, it is unknown whether all GME states are GMN [Bru+14]. In Chapter 5, we address this question and show that there exist GME states that do not display GMN.

2.3. Systems of indistinguishable particles

So far, we have considered entanglement and nonlocality in the setting of n spacelike separated particles belonging to Alice, Bob, Charlie, etc. One can as well consider the characterization of quantum correlations at short distances, where the particles involved (*e.g.* photons, electrons) have an indistinguishable character that has to be taken into account.

When one is given a system $\rho_{\mathbf{A}}$ of indistinguishable particles, then $\rho_{\mathbf{A}}$ remains invariant under any permutation of its subsystems; otherwise they could be distinguished.

Consider $\mathfrak{S}_n$, the group of permutations of n elements. Consider as well the n-partite Hilbert space $\mathcal{H} = (\mathbb{C}^d)^{\otimes n}$. $\mathfrak{S}_n$ acts on $\mathcal{H}$ by means of permuting each component of the computational basis of $\mathcal{H}$ and this action is extended by linearity to every element of $\mathcal{H}$. This action has a natural representation that assigns to each $\sigma \in \mathfrak{S}_n$ a permutation matrix Π_σ defined as

$$\Pi_\sigma |i_0\rangle \otimes \cdots \otimes |i_{n-1}\rangle = |i_{\sigma^{-1}(0)}\rangle \otimes \cdots \otimes |i_{\sigma^{-1}(n-1)}\rangle. \tag{2.19}$$

Definition 2.5. *A quantum state $\rho_{\mathbf{A}} \in \mathcal{D}(\mathcal{H})$ is Permutationally Invariant (PI) if, for any $\sigma \in \mathfrak{S}_n$*

$$\rho_{\mathbf{A}} = \Pi_\sigma \rho_{\mathbf{A}} \Pi_\sigma^\dagger. \tag{2.20}$$

2.3.1. The block decomposition of a Permutationally Invariant operator. Schur-Weyl duality

Given a permutationally invariant quantum state $\rho_{\mathbf{A}}$, it turns out that one can choose a basis of $(\mathbb{C}^d)^{\otimes n}$ such that its form is extremely simplified: In this basis, $\rho_{\mathbf{A}}$ is block-diagonal, and the size of each block is exponentially small compared to the $d^n \times d^n$ whole matrix $\rho_{\mathbf{A}}$ expressed in the computational basis. The reason for this simplification lies on a mathematical result known as Schur-Weyl duality, which says that $(\mathbb{C}^d)^{\otimes n}$ can be naturally decomposed in terms of irreducible representations of the groups $\mathfrak{S}_n$ and $\mathcal{U}_d$ (the group of $d \times d$ unitary matrices). This construction is explained in detail in Appendix A.

Given a PI quantum state $\rho_{\mathbf{A}}$, it decomposes $\mathcal{H}$ into the following direct sum (*cf.* Theorem A.9):

$$(\mathbb{C}^d)^{\otimes n} \cong \bigoplus_{\lambda \vdash (d,n)} \mathcal{K}_\lambda \otimes \mathcal{H}_\lambda, \tag{2.21}$$

where λ runs over all partitions of n with at most d elements and $\oplus$ denotes direct sum. $\mathcal{K}_\lambda$ is known as the multiplicity space. In the basis (2.21) $\rho_{\mathbf{A}}$ is block-diagonal.

The qubit case

If $d = 2$, the construction of (2.21) can be explicitly given and it corresponds to the case of n spin-$1/2$ particles. In this case, λ would run over the partitions of n with, at most, 2 elements, so one can translate (2.21) to a language closer to Physics:

$$(\mathbb{C}^2)^{\otimes n} \cong \bigoplus_{J=J_0}^{n/2} \mathcal{K}_J \otimes \mathcal{H}_J. \tag{2.22}$$

Usually, $\mathcal{H}_J$ are called the spin Hilbert spaces, as $\dim \mathcal{H}_J = 2J + 1$ and $\mathcal{K}_J$ the multiplicity spaces, which account for the different possibilities for the n qubits to obtain to a spin-J state. The multiplicity spaces are of dimension 1 if $J = n/2$ and

$$\dim \mathcal{K}_J = \binom{n}{n/2 - J} - \binom{n}{n/2 - J - 1} \tag{2.23}$$

otherwise.

A permutationally invariant n-qubit state $\rho_{\mathbf{A}}$, in the basis given by (2.21) takes the form

$$\rho_{\mathbf{A}} = \bigoplus_{J=J_0}^{n/2} \frac{p_J}{\dim \mathcal{K}_J} \mathbb{1}_J \otimes \rho_J, \tag{2.24}$$

where p_J forms a probability distribution and ρ_J are the so-called spin states, which can be viewed as density operators of $\mathcal{D}(\mathbb{C}^{2J+1})$.

Hence, a permutationally invariant n-qubit state $\rho_{\mathbf{A}}$ is uniquely determined by specifying its blocks ρ_J, an amount of information exponentially small compared to a general n-qubit state.

The following basis automatically gives a projection onto the $J-$th block (defining $m = n - 2J$; note that m is always an even number):

$$\{|D^k_{2J}\rangle \otimes |\psi^-\rangle^{\otimes m/2}\}_{k=0\ldots 2J}, \tag{2.25}$$

where $|D^k_{2J}\rangle$ is the $2J$ qubit Dicke state with k excitations (*cf.* Section 2.3.2 Eq. (2.27)) and $|\psi^-\rangle$ is the singlet state

$$|\psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}. \tag{2.26}$$

2.3.2. Symmetric states

The so-called symmetric states (or Dicke states) were first introduced by R. H. Dicke in 1954, when studying the emission of light from a cloud of atoms [Dic54]. He found that, when the atoms were in certain entangled states, the intensity of radiation scaled quadratically with the number of atoms, whereas if they were radiating independently, this intensity scaled linearly. Since then, Dicke states have been widely studied and they have been produced in experiments.

Dicke states can be defined either as the simultaneous eigenstates of the total angular momentum operators $J_z = 1/2 \sum_i \sigma_z^{(i)}$ and J^2, where $\sigma_z^{(i)}$ is the Pauli matrix acting on site i and $J^2 = J_x^2 + J_y^2 + J_z^2$, or as symmetric superpositions of states with the same number of excitations (throughout this Thesis we shall consider qubits, so that a Dicke state is defined by n qubits and k excitations and denoted $|D^k_n\rangle$):

$$|D_n^k\rangle = \binom{n}{k}^{-1/2} \sum_\sigma \sigma(|0\rangle^{\otimes n-k}|1\rangle^{\otimes k}). \tag{2.27}$$

Dicke states form an important subclass of permutationally invariant states, and they correspond to the first block in the decomposition 2.21; *i.e.*, the one corresponding to the partition $\lambda = (n)$. They span the so-called *symmetric space* and the symmetric space is closed[19] under the action of $U^{\otimes n}$ for any unitary U.

We shall denote the symmetric space by $\mathcal{S}(\mathcal{H}) := \mathrm{Span}\{|D_n^k\rangle\}_{k=0\ldots n}$ and we will call a density operator symmetric if $\rho_{\mathbf{A}} \in \mathcal{D}(\mathcal{S}(\mathcal{H}))$. In the case of n qubits, a symmetric state $\rho_{\mathbf{A}}$ cannot have rank greater than $n+1$, as these are the elements in (2.27).

PPT Entanglement in the Symmetric states

The multipartite PPT criterion and, in general, any entanglement criterion based on positive, but not completely positive maps, is hard to compute in systems of large n as, even if it is efficient to test on a single bipartition $S|\overline{S}$, the number of bipartitions scales as 2^n. However, for permutationally invariant states, this is greatly simplified: Now the condition n-separable implies $(\mathbb{1}_S \otimes \bigotimes_{a_i \in \overline{S}} \Lambda_{A_i})[\rho] \succeq 0$ will be the same, regardless of which particular parties are picked in S. Hence, it only depends on the number of parties in S, denoted $|S|$. Hence, if a PI state is n-separable, only $n-1$ conditions need to be checked. In the particular case $\Lambda = T$, only $\lfloor n/2 \rfloor$ are necessary, as global transposition preserves the positivity of the whole state. This motivates the definition of partial transposition for symmetric states as ρ^{Γ_k}, where $k = |\overline{S}|$ is the number of parties that have been transposed. A state which is PPT with respect to every bipartition will be called fully PPT.

The zoo of separability classes for symmetric states is also greatly simplified: Symmetric states are either n-separable, or GME, and there is no

[19] A nice way to see this is via the so-called Majorana representation [Maj32], which assigns a product state to every pure Dicke state; when taking a superposition of all permutations of this product state, one recovers the original Dicke state. For $d = 2$ this assignment is unique and it can be easily visualized in the Bloch sphere. Then, the action of $U^{\otimes n}$ is just a rotation of the Bloch sphere [Mar11].

other possibility. This makes them even more interesting, as proving that a general quantum state is GME might turn into a difficult task.

Applying Γ_k, transposition on k subsystems, breaks the symmetry of ρ: It is false in general that $\rho^{\Gamma_k} \in \mathcal{D}(\mathcal{S}(\mathcal{H}_{\mathbf{A}}))$. However, the symmetries in the partially transposed subsystems and the untouched ones are kept, so that $\rho^{\Gamma_k} \in \mathcal{D}(\mathcal{S}(\mathcal{H}_S) \otimes \mathcal{S}(\mathcal{H}_{\overline{S}}))$, for $k = |S|$. In the case of qubits, this means that the rank of ρ^{Γ_k} is $O(n^2)$, more precisely, bounded by $(n+1-k)(k+1)$, so it is possible to keep track of the transformation Γ_k efficiently. We shall denote by $\mathcal{D}_{\mathcal{S}}^{\mathrm{PPT}}(\mathcal{H})$ the set of density operators acting on $\mathcal{H}$ corresponding to symmetric states PPT with respect to every bipartition.

It was known that all PPT symmetric states of two and three qubits are fully separable [Eck+02]. The reason is that there is only one possible nontrivial bipartition to consider: $(1,1)$ and $(2,1)$, respectively, and then the sufficiency condition for the PPT criterion carries, as one can think of $\mathcal{S}(\mathbb{C}^2) \otimes \mathcal{S}(\mathbb{C}^2)$ as $\mathbb{C}^2 \otimes \mathbb{C}^2$ and of $\mathcal{S}(\mathbb{C}^2)^{\otimes 2} \otimes \mathcal{S}(\mathbb{C}^2)$ as $\mathbb{C}^3 \otimes \mathbb{C}^2$. However it was an open question whether this result would still be true for systems of 4 qubits or more.

In the case of 5 and 6 qubits, Tóth and Gühne found examples of GME symmetric states which are PPT with respect to the most balanced partition $\lfloor n/2 \rfloor, \lceil n/2 \rceil$, although they would break the PPT condition with respect to some other bipartitions [TG09].

Genuine multipartite entanglement is considered to be the strongest form of entanglement, whereas PPT states are considered the weakest[20]. Almost paradoxically, it turns out that one can find fully PPT states which are also GME for more than 3 qubits, as we study in Chapter 3.

[20] It was shown in [HHH98] that bipartite PPT states cannot be distilled; *i.e.*, no matter how many copies of a non-distillable state are available, there is no protocol that would produce a pure maximally entangled state $|\psi^+\rangle$. This is the reason why bound entanglement (*i.e.*, entanglement of undistillable states) is considered the weakest form of entanglement.

Interestingly, a conjecture by Peres related the concepts of nonlocality and bound entanglement, claiming that all bound entangled states admit a local model. The intuition that bound entanglement is too weak to violate a Bell inequality was proven to be false both in the multipartite [VB12] and the bipartite [VB14] scenarios very recently.

3. PPT Entangled Symmetric States

Characterization of entanglement in composite quantum systems is a difficult task. Already in the bipartite case, it was proven to be NP-hard [Gur03]. However, as we have alredy seen in Section 2.1.2, there exist several criteria which give sufficient conditions to certify that a state is entangled, of which the most celebrated one is the Positive under Partial Transposition (PPT) criterion. Nevertheless, the characterization of states which are both PPT and entangled remains elusive.

Some insight into the structure of the set of PPT entangled states has been gained over the years. For instance, methods have been developed that exploit the fact that PPT states form a convex set that contains the set of separable states, which is also convex [LMO07] (see also [Aug+10]). Consequently, to fully characterize the set of PPT states, it is sufficient to understand its extreme points. Recently, this property, although in an indirect way, allowed to disprove the Peres conjecture in the multipartite case [VB12] and, in what follows, we show how to use it to solve the open problem about the existence of four-qubit PPT entangled symmetric states [Tur+12].

In the multipartite case, the characterization of the PPT set becomes more complex. Although the set of states which are PPT with respect to every bipartition is still a convex set, its boundary becomes more complicated, as it stems from the intersection of an increasing number of sets of states that are PPT with respect to some bipartition. By restricting ourselves to an appropriate subclass of states; *i.e.*, states fulfilling some symmetry, this complexity can be vastly reduced[1]. In this chapter we focus on an important class of quantum states; the so-called Symmetric states, which we have introduced in Section 2.3.2.

The current chapter is devoted to the characterization of PPT entangled

[1] For instance, the full characterization of separability is possible if one only considers states which commute with the multilateral action of unitary [CK06a; EW01] or orthogonal [CK06b; VW01] groups.

symmetric states (PPTESS) of n qubits, and it is organized as follows: In Section 3.1, we give results concerning separability criteria, edgeness −with special emphasis to the most balanced bipartitions− and the Schmidt number of PPTESS. In Section 3.2, we study the set of PPTESS from a geometrical perspective, focusing on characterizing extremality, giving a criterion for entanglement of PPT symmetric states, and providing an algorithm that produces entangled symmetric states of n qubits which are PPT with respect to all bipartitions, also showing some numerical results. We conclude in Section 3.3, where we solve an open problem for the case of 4 qubits, in which we provide a half-analytical, half-numerical class of four-qubit PPTESS and we finish by discussing some methods and techniques that could be applied in future directions.

The results presented in this chapter are joint work with R. Augusiak, P. Hyllus, J. Samsonowicz, M. Kuś and M. Lewenstein [Tur+12; Aug+12].

3.1. Characterization

Through the whole chapter, we shall refer to the following object: the tuple formed by the rank of a quantum state and the ranks of its partial transpositions. This tuple of ranks will be our main tool to classify PPTESS. Such a classification is convenient for various reasons. First of all, not only groups a set of infinite elements into a finite number of classes, but it also gives an intuition on the complexity of a state. Loosely speaking we shall see that if a fully PPT symmetric state has ranks which are *too low*, then its simplicity allows for a decomposition as a separable state. However, if its ranks are *too high*, then it can be decomposed as a mixture of some separable part (which is useless from the information theoretic point of view) and some entangled part of lower ranks (which keeps the relevant information about the original state).

We begin by formulating separability criteria of PPT symmetric n-qubit states in Subsection 3.1.1, continue by studying the edge state decomposition in Subsection 3.1.2 and we conclude by commenting on the Schmidt number of symmetric states in Subsection 3.1.3.

3.1.1. Separability criteria

We begin by recalling a useful fact that greatly simplifies the analysis of entanglement in the symmetric states: Symmetric states are either n-separable or GME [Eck+02].

Theorem 3.1. *Let $\rho_{\mathbf{A}} \in \mathcal{D}(\mathcal{S}(\mathbb{C}^d)^{\otimes n})$. Then, only one of the following possibilities holds:*

$$\rho_{\mathbf{A}} = \sum_i p_i |e_i\rangle\langle e_i|^{\otimes n} \tag{3.1}$$

or

$$\rho_{\mathbf{A}} \neq \sum_{S|\overline{S}\in\mathcal{S}_2} p_{S|\overline{S}} \sum_i q^{(i)}_{S|\overline{S}} \rho^{(i)}_S \otimes \rho^{(i)}_{\overline{S}}, \tag{3.2}$$

where $|e_i\rangle \in (\mathbb{C}^d)^{\otimes n}$, p_i, $p_{S|\overline{S}}$ and $q^{(i)}_{S|\overline{S}}$ are valid probability distributions, and $\rho^{(i)}_S$ ($\rho^{(i)}_{\overline{S}}$) are pure states acting on the Symmetric Hilbert space of the parties contained in S ($\overline{S}$).

Proof. Assume that (3.2) is false. Then $\rho_{\mathbf{A}}$ can be expressed as

$$\rho_{\mathbf{A}} = \sum_{S|\overline{S}\in\mathcal{S}_2} p_{S|\overline{S}} \sum_i q^{(i)}_{S|\overline{S}} |e^{(i)}_S\rangle\langle e^{(i)}_S| \otimes |e^{(i)}_{\overline{S}}\rangle\langle e^{(i)}_{\overline{S}}|, \tag{3.3}$$

where the vectors $|e^{(i)}_S\rangle$ and $|e^{(i)}_{\overline{S}}\rangle$ are symmetric, as they belong to the range of $\rho_{\mathbf{A}}$. Now consider a permutation $\tau \in \mathfrak{S}_n$ which exchanges an element of S with an element of $\overline{S}$, say $a \in S, b \notin S$. Regarding S as a bipartite set $S = \{a\} \cup S \setminus \{a\}$ and the same for its complement $\overline{S} = \{b\} \cup \overline{S} \setminus \{b\}$, one can obtain the Schmidt decomposition of the symmetric vectors $|e^{(i)}_S\rangle$ and $|e^{(i)}_{\overline{S}}\rangle$, which reads

$$|e^{(i)}_S\rangle = \sum_j \sqrt{\mu_{S,a,i,j}} |e^{(j)}_{\{a\}}\rangle |e^{(j)}_{S\setminus\{a\}}\rangle \tag{3.4}$$

and

$$|e^{(i)}_{\overline{S}}\rangle = \sum_j \sqrt{\nu_{\overline{S},b,i,j}} |e^{(j)}_{\{b\}}\rangle |e^{(j)}_{\overline{S}\setminus\{b\}}\rangle, \tag{3.5}$$

with μ and ν being probability distributions.

Since, by hypothesis, $\Pi_\tau \rho_{\mathbf{A}} \Pi_\tau = \rho_{\mathbf{A}}$, one has that $\Pi_\tau |e_S^{(i)}\rangle |e_{\overline{S}}^{(i)}\rangle = |e_S^{(i)}\rangle |e_{\overline{S}}^{(i)}\rangle$, a condition which reads (we skip the subindices which are clear from the context for clarity)

$$\sum_{j,k} \sqrt{\mu_j \nu_k} |e_{\{b\}}^{(j)}\rangle |e_{S\setminus\{a\}}^{(j)}\rangle |e_{\{a\}}^{(k)}\rangle |e_{\overline{S}\setminus\{b\}}^{(k)}\rangle = \sum_{j,k} \sqrt{\mu_j \nu_k} |e_{\{a\}}^{(k)}\rangle |e_{S\setminus\{a\}}^{(j)}\rangle |e_{\{b\}}^{(j)}\rangle |e_{\overline{S}\setminus\{b\}}^{(k)}\rangle. \tag{3.6}$$

Note that we have ordered the Hilbert space in Eq. (3.6) as $\{a\},\ S\setminus\{a\},\ \{b\},\ \overline{S}\setminus\{b\}$. The orthogonality of the vectors in Eqs. (3.4,3.5) implies that $|e_{\{a\}}^{(j)}\rangle = |e_{\{b\}}^{(k)}\rangle$ for all pairs of indices (j,k). It is then well defined $|g\rangle := |e_{\{a\}}^{(j)}\rangle = |e_{\{b\}}^{(k)}\rangle$, which implies that every vector in the left hand side of (3.4, 3.5) is a pure product vector with respect to the bipartitions $\{a\}|S\setminus\{a\}$ or $\{b\}|\overline{S}\setminus\{b\}$, respectively.

Because, by hypothesis, $\rho_{\mathbf{A}} \in \mathcal{D}(\mathcal{S}(\mathbb{C}^d)^{\otimes n})$, one can choose any $\tau \in \mathfrak{S}_n$, in particular, any transposition between an element of S and an element of its complement, any vector in the decomposition (3.3) is fully product, so $\rho_{\mathbf{A}}$ has to be of the form (3.1); *i.e.*, fully separable. □

The set of symmetric states which are PPT with respect to every bipartition, which we denoted $\mathcal{D}_{\mathcal{S}}^{\mathrm{PPT}}(\mathcal{H})$, arises as the intersection of a number of sets. The boundary of the k-th set is defined as $\{\rho \in \mathcal{D}(\mathcal{S}(\mathcal{H})) :\ \rho^{\Gamma_k} \succeq 0,\ \det \rho^{\Gamma_k} = 0\}$; *i.e.*, at least one of the eigenvalues of the partially transposed states vanishes. In the following lemma we give some separability conditions in terms of the ranks of ρ and its partial transpositions. The idea behind Lemma 3.2 is that if a n-qubit symmetric state ρ is not supported in $\mathbb{C}^{|S|+1} \otimes \mathbb{C}^{n-|S|+1}$ with respect to any bipartition $S|\overline{S}$, its rank is upper bounded by the ranks of its subsystems. This result, although technical, will be used throughout all the section.

Lemma 3.2. *Let $\rho_{\mathbf{A}} \in \mathcal{D}_{\mathcal{S}}((\mathbb{C}^2)^{\otimes n})$ and let $S|\overline{S}$ be a bipartition of $\mathbf{A}$, with $|S| \leq |\overline{S}|$. Let us define $k_S := \dim \ker \rho_S$ and $r_S := \dim \mathrm{Im} \rho_S$ (analogously for $k_{\overline{S}}$, $r_{\overline{S}}$, $k_{\mathbf{A}}$ and $r_{\mathbf{A}}$). Then,*

- $k_{\overline{S}} > 0 \Rightarrow r_{\mathbf{A}} \leq r_{\overline{S}}$.
- $k_S > 0 \Rightarrow r_{\mathbf{A}} \leq r_S$.
- $k_{\overline{S}} > 0$ *and* $k_S > 0 \Rightarrow r_{\mathbf{A}} \leq \min\{r_S, r_{\overline{S}}\}$.

Proof. Clearly, every case follows from the previous ones, so we prove the first one.

As $k_{\overline{S}} > 0$, there are $k_{\overline{S}}$ linearly independent vectors belonging to $\ker \rho_{\overline{S}}$. Let us denote them $\{|\phi_i\rangle\}_{i=1\ldots k_{\overline{S}}}$. Then, for any pure $|S|-$qubit symmetric vector[2] $|\psi\rangle$, the projection of $|\psi\rangle|\phi_i\rangle$ to the symmetric space belongs to $\ker \rho_{\mathbf{A}}$: $P_{\mathbf{A}}(|\psi\rangle|\phi_i\rangle) \in \ker \rho_{\mathbf{A}}$, where $P_{\mathbf{A}}$ is the projector onto the Symmetric space, defined as

$$P_{\mathbf{A}} = \frac{1}{n!} \sum_{\sigma \in \mathfrak{S}_n} \Pi_\sigma, \tag{3.7}$$

and Π_σ is the permutation operator defined as in Eq. (2.19). If we find $n - r_{\overline{S}} + 1$ linearly independent vectors $P_{\mathbf{A}}(|\psi\rangle|\phi_i\rangle) \in \ker \rho_{\mathbf{A}}$ by appropriately choosing $|\psi\rangle$, the result follows (since $k_{\mathbf{A}} \geq n - r_{\overline{S}} + 1$ and $r_{\mathbf{A}} + k_{\mathbf{A}} = n + 1$ one has $r_{\mathbf{A}} \leq r_{\overline{S}}$).

To this end, we first prove the following observation: For any symmetric $|\psi\rangle$, the $k_{\overline{S}}$ vectors $P_{\mathbf{A}}(|\psi\rangle|\phi_i\rangle)$ are linearly independent. If this were not the case, there would exist a linear combination with coefficients $\alpha_i \in \mathbb{C}$ such that $\sum_i \alpha_i P_{\mathbf{A}}(|\psi\rangle|\phi_i\rangle) = 0$. But then $|\psi\rangle \otimes \sum_i \alpha_i |\phi_i\rangle \in \ker P_{\mathbf{A}}$. Since both $|\psi\rangle$ and $\sum_i \alpha_i |\phi_i\rangle$ are symmetric vectors, the only possibility[3] is that $\sum_i \alpha_i |\phi_i\rangle = 0$, which contradicts the fact that $|\phi_i\rangle$ were linearly independent.

Now we pick as a basis of $\mathcal{S}(\mathcal{H}_S)$ the Dicke states $|D^j_{|S|}\rangle$ defined in (2.27) and define the vectors

$$|\Phi^j_i\rangle := P_{\mathbf{A}}(|D^j_{|S|}\rangle|\phi_i\rangle), \tag{3.8}$$

where i ranges from 1 to $k_{\overline{S}} = |\overline{S}| - r_{\overline{S}} + 1$ and j from 0 to $|S|$. We already know that, for a fixed j, the vectors $|\Phi^j_i\rangle$ form a linearly independent set, so let us focus on the vectors $|\Phi^j_i\rangle$ by changing j.

On the one hand, $|\phi_i\rangle$ is a linear combination of elements of the computational basis with a number of ones ranging from 0 to $|\overline{S}|$. On the other

[2] Since, for any observable M, one has $\mathrm{Tr}[M\rho_{\overline{S}}] = \mathrm{Tr}[(\mathbb{1}_S \otimes M)\rho_{\mathbf{A}}]$, by taking $M = |\phi\rangle\langle\phi|$, with $|\phi\rangle \in \ker \rho_{\overline{S}}$, the following identity holds: $0 = \langle\phi|\rho_{\overline{S}}|\phi\rangle = \mathrm{Tr}[|\phi\rangle\langle\phi|\rho_{\overline{S}}] = \mathrm{Tr}[(\mathbb{1}_S \otimes |\phi\rangle\langle\phi|)\rho_{\mathbf{A}}] = \sum_i \mathrm{Tr}[|i\rangle\langle i| \otimes |\phi\rangle\langle\phi|\rho_{\mathbf{A}}]$. Hence, $\sum_i \langle i|\langle\phi|\rho_{\mathbf{A}}|i\rangle|\phi\rangle = 0$ and, because $\rho_{\mathbf{A}} \succeq 0$, every summand has to be zero. Hence, $|i\rangle|\phi\rangle \in \ker \rho_{\mathbf{A}}$ for every $|i\rangle$. By linearity, $|\psi\rangle|\phi\rangle \in \ker \rho_{\mathbf{A}}$ for any $|\psi\rangle \in \mathcal{H}_S$.

[3] A fact that is easily seen when expressing the vectors in the Dicke states basis defined in Eq. (2.27), where the identity $P_{\mathbf{A}}(|D^k_{|S|}\rangle|D^l_{|\overline{S}|}\rangle) = |D^{k+l}_n\rangle$ holds.

hand, $|D^j_{|S|}\rangle$ is a uniform linear superposition of all the elements of the computational basis with *exactly* j ones. Consequently, $|\Phi^j_i\rangle$ has a number of ones which ranges from j to $|\overline{S}|+j$. Equivalently, one has $\langle D^k_n|\Phi^j_i\rangle = 0$ if $k<j$ or $k>|\overline{S}|+j$.

Hence, for all j between 0 and $|\overline{S}|$, $\langle D^k_n|\Phi^j_i\rangle \neq 0$ at least on $k_{\overline{S}}$ indices k between j and $j+|\overline{S}|$ (because $k_{\overline{S}}$ is the dimension of the space spanned by $|\Phi^j_i\rangle = \sum_{k=j}^{|\overline{S}|+j} \beta^{i,j}_k |D^k_n\rangle$, for some $\beta^{i,j}_k \in \mathbb{C}$).

There will be one $|\Phi^0_i\rangle$, say $|\Phi^0_l\rangle$, for which $\langle D^{|\overline{S}|}_n|\Phi^0_l\rangle \neq 0$. If this were not the case, *i.e.*, if $\langle D^{|\overline{S}|}_n|\Phi^0_i\rangle = 0$ for all i, we pick the one for which $\langle D^{|\overline{S}|-1}_n|\Phi^0_i\rangle \neq 0$ and so on. Clearly, because $k_{\overline{S}}>0$, this procedure must terminate finding some $|\Phi^0_l\rangle$, otherwise $|\Phi^0_i\rangle = 0$ for all i, contradicting the fact that $|\Phi^0_i\rangle$ are linearly independent.

We assume then, for simplicity, that the vector $|\Phi^0_l\rangle$ is the one for which $\langle D^{|\overline{S}|}_n|\Phi^0_l\rangle \neq 0$. Hence $\langle \phi_l|1\rangle^{\otimes \overline{S}} \neq 0$. Hence, the rest of the vectors $|\Phi^j_l\rangle$ have nonzero overlap with $|D^k_n\rangle$, for $k \geq |\overline{S}|+1$, for any j from 1 to $|S|$ and thus they are linearly independent of the set $\{|\Phi^0_i\rangle\}_i$. Actually, by construction, they form a set of $|S|$ linearly independent vectors themselves. So, by joining the sets $\{|\Phi^0_i\rangle\}_{i=1,\ldots,|\overline{S}|-r_{\overline{S}}+1}$ and $\{\Phi^j_l\}_{j=1,\ldots,|S|}$, we have found the $n-r_{\overline{S}}+1$ set of vectors that we wanted in $\ker \rho_{\mathbf{A}}$. □

Lemma 3.2 implies, for example, that if $r_{\mathbf{A}} \geq n$, then $\rho_{\mathbf{A}}$ is supported on $\mathbb{C}^2 \otimes \mathbb{C}^n$ with respect to any one-vs-the rest partition.

In this way one can obtain a basic criterion for GME in symmetric states. Theorem 3.3 was already announced in [Eck+02], although a detailed proof was not provided.

Theorem 3.3. *Let $\rho_{\mathbf{A}} \in \mathcal{D}^{\mathrm{PPT}}_{\mathcal{S}}((\mathbb{C}^2)^{\otimes n})$. If $\rho_{\mathbf{A}}$ is entangled, its rank is maximal, i.e., $r_{\mathbf{A}} = n+1$.*

Proof. One can consider any one-vs-the rest partition, which we take, without loss of generality, to be $A_1|A_2\ldots A_n$, and see $\rho_{\mathbf{A}}$ as a bipartite state acting on $\mathbb{C}^2 \otimes \mathbb{C}^n$ (recall that $\mathcal{S}((\mathbb{C}^2)^{\otimes n-1}) \cong \mathbb{C}^n$). However, if $r_{\mathbf{A}} \leq n$ and $\rho_{\mathbf{A}}$ is supported on $\mathbb{C}^2 \otimes \mathbb{C}^n$, then it is separable [Kra+00], a fact which is guaranteed because, if $\rho_{\mathbf{A}}$ would not be supported on $\mathbb{C}^2 \otimes \mathbb{C}^n$, either $\ker \rho_{A_1}$ or $\ker \rho_{\mathbf{A}\setminus A_1}$ would be nontrivial. If $r_{A_1}=1$, Lemma 3.2 automatically implies that $r_{\mathbf{A}}=1$, so $\rho_{\mathbf{A}}$ is a pure product vector. If $r_{\mathbf{A}\setminus A_1} < n$,

then Lemma 3.2 implies that $r_{\mathbf{A}} < n$, and the results of [Kra+00] apply again, implying that $\rho_{\mathbf{A}}$ is separable. □

Theorem 3.3 provides a strong sufficient condition for GME in PPT fully symmetric qubit states, just by using the partition 1 vs $n-1$. Let us then explore what other partitions can tell us about the seprability of symmetric states. Specifically, Lemma 3.4 allows us to prove an analog of Theorem 3.3, but for the partial transpositions of ρ. We denote by ρ^{T_S}, where $S \subseteq \mathbf{A}$ the state ρ partially transposed in all parties belonging to S.

Lemma 3.4. *Let $\rho_{\mathbf{A}} \in \mathcal{D}_{\mathcal{S}}^{\mathrm{PPT}}((\mathbb{C}^2)^{\otimes n})$ and consider an arbitrary partition $S|\overline{S}$ of $\mathbf{A}$. Let us define $k := |S|$. If $\rho_{\mathbf{A}}$ is entangled, then ρ^{T_S} is supported on the bipartitie Symmetric Hilbert space corresponding to $S|\overline{S}$, i.e., $\mathbb{C}^{k+1} \otimes \mathbb{C}^{n-k+1}$.*

Proof. If $\rho_{\mathbf{A}}$ entangled and ρ^{T_S} is not supported on the Hilbert Space that corresponds to the bipartition $S|\overline{S}$, one can find in one of its subsystems, *e.g.* $\overline{S}$, a $(n-k)-$qubit symmetric vector $|\phi\rangle \in \ker \rho_{\overline{S}}$. But then, for any symmetric k-qubit vector $|\psi\rangle$, $\rho_{\mathbf{A}}^{T_S}|\psi\rangle|\phi\rangle = 0$ or, equivalently, $\rho|\psi^*\rangle|\phi\rangle = 0$. It suffices to choose $|\psi\rangle = |D_k^0\rangle = |0\rangle^{\otimes k}$ to find a vector in the kernel of $\rho_{\mathbf{A}}$, namely, the symmetrized vector $P_{\mathbf{A}}(|0\rangle^{\otimes k}|\psi\rangle) \in \ker \rho_{\mathbf{A}}$. Hence, $r_{\mathbf{A}} \leq n$ and Theorem 3.3 implies that $\rho_{\mathbf{A}}$ is separable, which is a contradiction. □

Lemma 3.4 tells us that if $\rho_{\mathbf{A}}^{T_S}$ is not supported in $\mathbb{C}^{k+1} \otimes \mathbb{C}^{n-k+1}$ for some k, then it is fully separable. This implies that the ranks of the partial transpositions of $\rho_{\mathbf{A}}$ cannot be too low. Concretely, Theorem 3.5 quantifies this statement:

Theorem 3.5. *Let $\rho_{\mathbf{A}} \in \mathcal{D}_{\mathcal{S}}^{\mathrm{PPT}}((\mathbb{C}^2)^{\otimes n})$ and consider an arbitrary bipartition $S|\overline{S}$ of $\mathbf{A}$, with $|S| = k \leq n-k$. Let us define $r_{\mathbf{A}}^S := \mathrm{rank}(\rho_{\mathbf{A}}^{T_S})$. If $\rho_{\mathbf{A}}$ is entangled, then $r_{\mathbf{A}}^S > n-k+1$.*

Proof. Lemma 3.4 allows us to assume that $\rho_{\mathbf{A}}$ is supported on $\mathbb{C}^{k+1} \otimes \mathbb{C}^{n-k+1}$, otherwise it is separable. It then follows from the results of [Hor+00] that $\rho_{\mathbf{A}}$ is separable if $r_{\mathbf{A}}^S \leq n-k+1$. To complete the proof it is enough to notice that the reasoning above does not depend on the bipartition. □

So far, we have derived a separability criterion for n-qubit PPT symmetric states which can be stated as: if $r^S_{\mathbf{A}} \leq n-k+1$ for some bipartition, then $\rho_{\mathbf{A}}$ is separable. However, more tricky bipartitions can provide further separability conditions for generic[4] symmetric states, also in term of the ranks.

Theorem 3.6. *Let $\rho_{\mathbf{A}} \in \mathcal{D}_S^{\mathrm{PPT}}((\mathbb{C}^2)^{\otimes n})$ and let $S|\overline{S}$ be a bipartition of $\mathbf{A}$ with $k = |S|$. Then, if $r^S_{\mathbf{A}} \leq (k+1)(n-k)$, then $\rho_{\mathbf{A}}$ is generically separable.*

Proof. Since $\rho_{\mathbf{A}}$ is fully PPT, the n-qubit state $\sigma := \rho_{\mathbf{A}}^{T_S}$ is another valid quantum state, although it is no longer symmetric. Now we consider a party A_i from $\overline{S}$. We can assume, without loss of generality that this party is A_n. One can see σ as a bipartite state which acts on $\mathbb{C}^{(k+1)(n-k)} \otimes \mathbb{C}^2$. $\rho_{\mathbf{A}}$ is fully PPT, so it follows that $\sigma^{T_{A_n}} \succeq 0$. This fact, together with the hypotesis that $\operatorname{rank} \sigma \leq (k+1)(n-k)$ implies that σ is biseparable with respect to the bipartition $(\mathbf{A} \setminus A_n)|A_n$ [Kra+00]:

$$\sigma = \sum_i p_i |\psi_i\rangle\langle\psi_i|_{\mathbf{A}\setminus A_n} \otimes |e_i\rangle\langle e_i|_{A_n}, \tag{3.9}$$

where p_i forms a probability distribution.

Note that the result of [Kra+00] holds if σ is supported on $\mathbb{C}^{(k+1)(n-k)} \otimes \mathbb{C}^2$, which is generically the case.

We are now going to exploit the fact that σ is still symmetric with respect to the subsystem $\overline{S}$, a condition which we can write as $P_{\overline{S}}\sigma P_{\overline{S}} = \sigma$. Consequently, all the vectors $|\psi_i\rangle|e_i\rangle$ which appear in the decomposition (3.9) are also symmetric with respect to the $\overline{S}$ subsystem, as they belong to the range of σ. Hence, we have that $P_{\overline{S}}|\psi_i\rangle|e_i\rangle = |\psi_i\rangle|e_i\rangle$ for every i. This symmetry in the $\overline{S}$ subsystem imposes (*c.f.* Lemma 3.7) that $|\psi_i\rangle|e_i\rangle$ must be of the form $|\tilde{\psi}_i\rangle|e_i\rangle^{\otimes(n-k)}$ where $|\tilde{\psi}_i\rangle$ corresponds to the parties in S and the parties in $\overline{S}$ share the fully product state $|e_i\rangle^{\otimes(n-k)}$. So we obtain a new form for σ, which is

$$\sigma = \sum_i p_i |\tilde{\psi}_i\rangle\langle\tilde{\psi}_i|_S \otimes (|e_i\rangle\langle e_i|^{\otimes(n-k)})_{\overline{S}}. \tag{3.10}$$

[4] A *generic* property in mathematics is one that holds for *typical* examples. From the point of view of measure theory, a generic property is one that holds almost everywhere, or with probability 1. Topologically, or from the point of view of algebraic geometry, a generic property holds on a dense open set. Equivalently, it does not hold in a nowhere dense set (a set whose closure has empty interior).

One can now partially transpose σ with respect to all the parties in S, which will correspond to conjugation only of the vectors $|\tilde{\psi}_i\rangle$ and we obtain a form of $\rho_{\mathbf{A}}$ (since $\sigma^{T_S} = \rho_{\mathbf{A}}$)

$$\rho_{\mathbf{A}} = \sum_i p_i |\tilde{\psi}_i^*\rangle\langle\tilde{\psi}_i^*|_S \otimes (|e_i\rangle\langle e_i|^{\otimes(n-k)})_{\overline{S}}. \tag{3.11}$$

Because $\rho_{\mathbf{A}}$ is symmetric, the form of Eq. (3.11), which shows it is biseparable, implies it is fully separable. □

Lemma 3.7. *Consider a bipartition $S|\overline{S}$ of $\mathbf{A}$, and let $A \in \overline{S}$. Let $|e\rangle$ be a qubit of A and $|\psi\rangle$ be a n-qubit pure state acting on $\mathbf{A} \setminus A$. If $P_{\overline{S}}|\psi\rangle|e\rangle = |\psi\rangle|e\rangle$, then $|\psi\rangle$ has to be of the form $|\psi\rangle = |\tilde{\psi}\rangle_S(|e\rangle^{\otimes(|\overline{S}|-1)})_{\overline{S}\setminus A}$.*

Proof. The methods of the proof are similar to those used in Theorem 3.1.

We start by decomposing $|\psi\rangle$ in the bipartition $S|(\overline{S} \setminus A)$ via the Schmidt decomposition, which reads

$$|\psi\rangle|e\rangle = \sum_i \sqrt{\mu_i}|i\rangle_S|\phi_i\rangle_{\overline{S}\setminus A}|e\rangle_A, \tag{3.12}$$

where $\{|i\rangle\}_i$ can be completed, if necessary, to an orthonormal basis of the Hilbert space associated to the subsystem S and μ_i forms a probability distribution. Because $\Pi_\sigma P_{\overline{S}} = P_{\overline{S}}$ for any permutation $\sigma \in \mathfrak{S}_{n-k}$, we have that $\Pi_\sigma|\psi\rangle|e\rangle = |\psi\rangle|e\rangle$. In particular, this is true for any swap of A with a party $B \notin \overline{S}$. Hence, we have that

$$\sum_i \sqrt{\mu_i}|i\rangle_S \Pi_\sigma(|\phi_i\rangle_{\overline{S}\setminus A}|e\rangle_A) = \sum_i \sqrt{\mu_i}|i\rangle_S|\phi_i\rangle_{\overline{S}\setminus A}|e\rangle_A. \tag{3.13}$$

By projecting the parties of S onto $\langle i|$, and by picking σ to be the swap between parties A and B, denoted $\sigma = (A, B)$, the following equality is obtained:

$$|\phi_i\rangle_{\overline{S}\setminus B}|e\rangle_B = |\phi_i\rangle_{\overline{S}\setminus A}|e\rangle_A. \tag{3.14}$$

This holds for any permutation σ, so by repeating the argument over all the possible pairs of A with an element of $\overline{S}$, we conclude that $|\phi_i\rangle = |e\rangle^{\otimes(|\overline{S}|-1)}$. The proof is concluded by defining $|\tilde{\psi}\rangle_S = \sum_i \sqrt{\mu_i}|i\rangle_S$. □

The above criteria motivate that we work with the following object

$$\vec{r}_{\mathbf{A}} := (r_{\mathbf{A}}, r_{\mathbf{A}}^{A_1}, \ldots, r_{\mathbf{A}}^{A_1 \ldots A_{\lfloor n/2 \rfloor}}); \tag{3.15}$$

i.e., a $(1+\lfloor n/2 \rfloor)-$tuple of the ranks of the state and its partial transpositions with respect to $1, 2$ until $\lfloor n/2 \rfloor$ subsystems (we do not consider partial transpositions of more subsystems as transposition of the whole state does not change its separability properties). The maximal rank of $\rho_{\mathbf{A}}^{T_S}$ is $(|S|+1)(n-|S|+1)$ so, in principle (taking into account that Theorem 3.3 allows us to assume that $r_{\mathbf{A}} = n+1$ otherwise $\rho_{\mathbf{A}}$ is separable), there are

$$\prod_{k=1}^{\lfloor n/2 \rfloor} (k+1)(n-k+1) = n!(n/2+1)^{2(\lfloor n/2 \rfloor - n/2)+1} \tag{3.16}$$

possible configurations or relevant ranks $\vec{r}_{\mathbf{A}}$ that may correspond to a symmetric n-qubit state. However, Theorems 3.5 and 3.6 imply that, for a bipartition $S|\overline{S}$ of $\mathbf{A}$, the states for which $r_{\mathbf{A}}^S \leq (|S|+1)(n-|S|)$ correspond to states that are separable or generically separable, leaving a small portion of ranks to consider, namely, $|S|+1$ per partition. The total number of configurations of $\vec{r}_{\mathbf{A}}$ which are relevant for generically PPT symmetric entangled n-qubit states is then reduced to $(\lfloor n/2 \rfloor + 1)!$. This represents just a fraction of (3.15), which vanishes to 0 superexponentially, more percisely, as $2^{-2k}\sqrt{\pi k}/k!$, where $n = 2k$.

For a low number of qubits, this gives a treatable number of cases to analyze: *e.g.* for $n = 4,\ 5$ there are 6 cases to consider (out of the respective 72 or 120) and for $n = 6,\ 7,\ 24$ possibilities (out of the respective 2880 or 5040). In Section 3.1.2 we shall see how to further reduce these numbers, with the aid of edgeness.

3.1.2. Symmetric edge states

An important class of PPT states are the so-called *edge* states [LS98; Lew+00; KL01]. The importance of edge states stems from the fact that every PPT state can be decomposed as a mixture of a fully separable and an edge state [LS98]. Their definition is somewhat inspired in the range criterion for separability [Hor97].

Definition 3.8. *A state $\rho_{\mathbf{A}} \in \mathcal{D}^{PPT}(\mathcal{H}_{\mathbf{A}})$ is edge if there does not exist a product vector $|e_1\rangle \otimes \ldots \otimes |e_n\rangle$ belonging to the range of $\rho_{\mathbf{A}}$ such that, for all bipartition $S|\overline{S}$ of $\mathbf{A}$, the state $(|e_1\rangle \otimes \ldots \otimes |e_n\rangle)^{C_S}$ belongs to the range of $\rho_{\mathbf{A}}^{T_S}$, where C_S denotes conjugation of the vectors corresponding to the systems in S.*

Definition 3.8 can also be interpreted as follows: one cannot subtract a fully product vector without losing the PPT property from an edge state. Hence, they lay on the boundary of the set of PPT states. The set of PPT states is convex, as we shall see in Section 3.2, thus it is completely determined by its extreme points. Every extremal state is also edge.

As Definition 3.8 suggests, the general method to prove that a state $\rho_{\mathbf{A}} \in \mathcal{D}_{\mathcal{S}}^{\mathrm{PPT}}((\mathbb{C}^2)^{\otimes n})$ is not an edge state is to find a vector $|e\rangle \in \mathbb{C}^2$ such that $|e\rangle^{\otimes n} \in \operatorname{Im} \rho_{\mathbf{A}}$ and $(|e\rangle^{\otimes n})^{C_S} \in \operatorname{Im} \rho_{\mathbf{A}}^{T_S}$ for all bipartitions $S|\overline{S}$ of $\mathbf{A}$. We note that, as we work with symmetric states, any product vector in the range of $\rho_{\mathbf{A}}$ enjoys the same symmetries as $\rho_{\mathbf{A}}$, hence it has to be of the form $|e\rangle^{\otimes n}$. As $\ker \rho_{\mathbf{A}}$ and $\operatorname{Im} \rho_{\mathbf{A}}$ define orthogonal subspaces, finding such $|e\rangle$ amounts to solving a system of $\sum_{k=1}^{\lfloor n/2 \rfloor} \dim \ker \rho_{\mathbf{A}}^{T_S}$ equations (we assumed that $r_{\mathbf{A}}$ is maximal; *i.e.*, $n+1$)

$$(\langle e|^{\otimes n})^{C_S} |\Psi_i^S\rangle = 0, \tag{3.17}$$

where $|\Psi_i^S\rangle \in \ker \rho_{\mathbf{A}}^{T_S}$. As one does not need to take normalized solutions $|e\rangle$ in order to parametrize the solutions of Eq. (3.17) and there is an irrelevant global phase, $|e\rangle$ can be parametrized, without loss of generality, as $|e\rangle = (1, \alpha)$, for $\alpha \in \mathbb{C} \cup \{\infty\}$. This allows us to express Eq. (3.17) as a system of polynomial equations in α and its conjugate α^*, which we name $P_i(\alpha, \alpha^*) = 0$. Solving the resulting system of polynomial equations is, in general, a very hard task (see, *e.g.* the discussion in [Kra+00]). We shall exploit a method introduced in [SKL07] in order to prove that it is possible to find a solution to a single equation of that type in Theorem 3.10.

We start with Lemma 3.9, in which we give a sufficient condition for a polynomial in α and α^* to have a solution.

Lemma 3.9. *Let $P \in \mathbb{C}[x, y]$ be a polynomial in two variables with complex coefficients. Let us write the equation $P(\alpha, \alpha^*) = 0$ as*

$$\sum_{i=0}^{k} (\alpha^*)^i Q_i(\alpha) = 0, \qquad \alpha \in \mathbb{C}, \tag{3.18}$$

where Q_i are single-variable polynomials of degree $\deg Q_i$. Let us denote $n := \deg Q_k$ and $m := \deg Q_0$.

If $\max_i \deg Q_i = n > k$ and $m > k$, then Eq. (3.18) has at least one solution.

Proof. Generically, the number of complex solutions of Eq. (3.18) is upper bounded by $2^{k-1}(k + n(n - k + 1))$ [Kra+00]. Here we provide a method to find one. First of all, we substitute $\alpha = rs$ and $\alpha^* = r/s$, with $r \in \mathbb{R}$ and $s \in \mathbb{C}$ and we treat r as a parameter and s as a variable. Thus, we obtain

$$\sum_{i=0}^{k} \left(\frac{r}{s}\right)^i Q_i(rs) = 0. \tag{3.19}$$

We want to show that there is a pair $(r, s) \in \mathbb{R} \times \mathbb{C}$ such that $|s| = 1$ solving Eq. (3.19) and thus Eq. (3.18) (because in this case simply $r = |\alpha|$ and $s = e^{\mathrm{i} \arg \alpha}$). To more comfortably deal with the argument of Q_i we further reparametrize $s = x/r$ for $x \in \mathbb{C}$, leading to the following equation

$$\sum_{i=0}^{k} \left(\frac{r^2}{x}\right)^i Q_i(x) = 0. \tag{3.20}$$

In the limit when $r \to \infty$, the l. h. s. of Eq. (3.20) is dominated by the $i = k-$th term, approaching $Q_k(x)$. $Q_k(x) = 0$ has n complex solutions by virtue of the fundamental theorem of algebra, which we denote x_i^∞. Since $s = x/r$, as r grows, $s_i^\infty \to 0$.
On the other hand, the limit when $r \to 0$ shows that the l. h. s. of Eq. (3.20) goes to $Q_0(x)$, which has m complex solutions x_i^0. Hence, $s_i^0 \to \infty$.
Since Eq. (3.19), as an equation in s, has, at most, $n + k$ solutions (just multiply its l. h. s. by s^k and it becomes a polynomial of degree at most $n + k$). As a consequence, when $r \to \infty$ ($r \to 0$), Eq. (3.19) may have up to k additional roots s_i^∞ (up to $n + k - m$ roots s_i^0) wihch can remain unspecified.
By varying continuously r from 0 to ∞, roots s_i^0 also continuously go to s_j^∞.
Since we have assumed[5] that $m > k$, at least one of the m roots $s_i^0 \to \infty$

[5] This assumption is crucial; otherwise we could not discard that all the m roots that are close to infinity for small r go to the unspecified roots for large r and that the n roots that are close to zero for large r go to the unspecified roots for small r, thus never crossing the unit circle.

must go to one of the n roots $s_i^\infty \to 0$. Hence, there must be at least a pair (r, s) for which $|s| = 1$, solving Eq. (3.19) and Eq. (3.18). □

Theorem 3.10. *Consider $\rho_{\mathbf{A}} \in \mathcal{D}_S^{\mathrm{PPT}}((\mathbb{C}^2)^{\otimes n})$ with $r_{\mathbf{A}}^S$ being maximal in all subsystems S of size $|S| \neq k$ with $1 \leq |S| \leq \lceil n/2 \rceil - 1$ (i.e., $r_{\mathbf{A}}^S = (|S|+1)(n-|S|+1)$) and for all subsystems X such that $|X| = k$, $r_{\mathbf{A}}^X = (k+1)(n-k+1)-1$, where $\lceil \cdot \rceil$ is the ceiling function. Generically, such $\rho_{\mathbf{A}}$ is not edge.*

Proof. We shall prove that it is possible to find $|e\rangle^{\otimes n} \in \operatorname{Im} \rho_{\mathbf{A}}$ and $(|e\rangle^{\otimes n})^{C_S} \in \operatorname{Im} \rho_{\mathbf{A}}^{C_S}$ for all subsystems S of size not k. Since all the $r_{\mathbf{A}}^S$ are maximal except for the subsystems X, for which the rank is maximal minus one, let us denote by $|\Psi\rangle$ the unique vector $|\Psi\rangle \in \ker \rho_{\mathbf{A}}^{T_X}$, which leads to a single equation (3.17) $\langle \Psi | (|e^*\rangle^{\otimes k} |e\rangle^{\otimes (n-k)}) = 0$. By parametrizing $|e\rangle = (1, \alpha)$, the latter can be written as

$$\sum_{i=0}^{k} (\alpha^*)^i Q_i(\alpha) = 0, \tag{3.21}$$

with $Q_i(\alpha)$ being polynomials of degree no larger than $n-k$ (generically, $\deg Q_i(\alpha) = n-k$). The assumptions guarantee that $n-k > k$ holds, so Lemma 3.9 applies, implying that Eq. (3.21) has, at least, one solution and a $\rho_{\mathbf{A}}$ with the above ranks is generically not edge. □

Remark 3.11. The form of the upper bound on $|S|$ in Theorem 3.10 might result intriguing. Indeed, the theorem does not work for even n and $k = n/2$, as Eq. (3.18) is generically an equation with the same order in both α and α^*. For instance, the equation $\alpha^* \alpha + 1 = 0$ has no solution in $\mathbb{C}$.

Balanced bipartitions

In order to complete our classification (*c.f.* Remark 3.11), we shall prove an analogous fact to Theorem 3.10 for $n = 4$ and $n = 6$ qubits.

Theorem 3.12. *Four-qubit PPT symmetric states of ranks $\vec{r}_{A\ldots D} = (5, 8, 8)$ and six-qubit PPT symmetric states of ranks $\vec{r}_{A\ldots F} = (7, 12, 15, 15)$ are not edge.*

Proof. We shall proceed in proving Theorem 3.12 for a general even n and in Remark 3.13 we shall see why it no longer works for $n \geq 8$.

Let $n = 2k$ and let S be a subset of $\mathbf{A}$ of size k. By hypothesis, $r^S_{\mathbf{A}} = (k+1)^2 - 1$; *i.e.*, maximal minus one, so that there is a single vector $|\Psi\rangle \in \ker \rho^{T_S}_{\mathbf{A}}$. Hence, $\rho_{\mathbf{A}}$ is not edge if, and only if, the equation

$$\langle e|^{\otimes k} \langle e^*|^{\otimes k} |\Psi\rangle = 0 \tag{3.22}$$

has a solution $|e\rangle \in \mathbb{C}^2$. To this end, one observes that the swapping subsystems S and $\overline{S}$ is well behaved with respect to complex conjugation in balanced bipartitions of symmetric states; *i.e.*,

$$\Pi_\tau \rho^{T_S}_{\mathbf{A}} \Pi^\dagger_\tau = (\rho^*_{\mathbf{A}})^{T_S}, \tag{3.23}$$

where $\tau \in \mathfrak{S}_n$ swaps S and $\overline{S}$.

Since $|\Psi\rangle$ is the unique vector in $\ker \rho^{T_S}_{\mathbf{A}}$, it has to enjoy the same symmetry, namely $\Pi_\tau |\Psi\rangle = |\Psi^*\rangle$. As the bipartition $S|\overline{S}$ does not break the symmetry within each element of the bipartition, it is convenient to represent $|\Psi\rangle$ in the product[6] Dicke basis $|D^i_k\rangle|D^j_k\rangle \in \mathcal{S}(\mathbb{C}^2)^{\otimes k} \otimes \mathcal{S}(\mathbb{C}^2)^{\otimes k}$. Let us arrange its coefficients in a matrix which we denote M_Ψ. The above symmetry implies that M_Ψ is Hermitian: $M_\Psi = M^\dagger_\Psi$, thus it can be diagonalized with real eigenvalues and its eigenvectors form an orthonormal basis. We can then write

$$|\Psi\rangle = \sum_{l=0}^{k} \lambda_l |\omega^*_l\rangle |\omega_l\rangle \tag{3.24}$$

with $\lambda_l \in \mathbb{R}$ and $|\omega_l\rangle \in \mathcal{S}(\mathbb{C}^2)^{\otimes k}$.

As $|\Psi\rangle \in \ker \rho^{T_S}_{\mathbf{A}}$, the following holds for any pair of vectors $|x\rangle,\ |y\rangle \in \mathcal{S}(\mathbb{C}^2)^{\otimes k}$: $0 = \langle x^*|\langle y|\rho^{T_S}_{\mathbf{A}}|\Psi\rangle$, which, after applying Eq. (3.24) transforms to $\sum_l \lambda_l \langle x^*|\langle y|\rho^{T_S}_{\mathbf{A}}|\omega^*_l\rangle|\omega_l\rangle = 0$.
By moving the partial transposition to the vectors (*i.e.*, using the identity $\mathrm{Tr}(\rho^{T_S}\sigma) = \mathrm{Tr}(\rho\sigma^{T_S})$) we get $\sum_l \lambda_l \langle \omega_l|\langle y|\rho_{\mathbf{A}}|x\rangle|\omega_l\rangle = 0$. And, because $\Pi_\tau \rho_{\mathbf{A}} = \rho_{\mathbf{A}}$, we finally obtain $\sum_l \lambda_l \langle \omega_l|\langle y|\rho_{\mathbf{A}}|\omega_l\rangle|x\rangle = 0$.

Defining the operator $W := \sum_l \lambda_l |\omega_l\rangle\langle\omega_l|$, we then have that the identity

$$\mathrm{Tr}[(W \otimes |x\rangle\langle y|)\rho_{\mathbf{A}}] = 0 \tag{3.25}$$

[6] For finite-dimensional spaces, since $\mathcal{H}^* \otimes \mathcal{K} \cong \hom(\mathcal{H}, \mathcal{K})$, where $\mathcal{H}^*$ is the dual space of $\mathcal{H}$; that implies we can arrange the coefficients of $|\Phi\rangle$ in a $(k+1) \times (k+1)$ matrix.

holds for all $|x\rangle, |y\rangle \in \mathcal{S}(\mathbb{C}^2)^{\otimes k}$.

Observe that Eq. (3.22) is equivalent to

$$\langle e|^{\otimes k} W |e\rangle^{\otimes k} = 0 \tag{3.26}$$

because of Eq. (3.24). If Eq. (3.26) did not have any solution, for any $|e\rangle \in \mathbb{C}^2$, the l. h. s. of Eq. (3.26) would have the same sign, say positive. Hence, W is an entanglement witness supported on the symmetric space $\mathcal{S}(\mathbb{C}^2)^{\otimes k}$. Because there are no PPT entangled states of two and three symmetric qubits (*c.f.* [Stø63; Wor76; HHH96; Eck+02]), for $n = 4$ and $n = 6$, W must be a decomposable EW; *i.e.*, of the form

- $W = P + Q^{T_A}$ for $n = 4$, where $P, Q \succeq 0$ act on the Hilbert space $(\mathbb{C}^2)^{\otimes 2}$, or
- $W = \tilde{P} + \tilde{Q}^{T_A} + \tilde{R}^{T_{AB}}$ for $n = 6$, where $\tilde{P}, \tilde{Q}, \tilde{R} \succeq 0$ act on the Hilbert space $(\mathbb{C}^2)^{\otimes 3}$.

Then, Eq. (3.26) implies the following conditions hold for any $|x\rangle \in \mathcal{S}(\mathbb{C}^2)^{\otimes k}$:

- $\mathrm{Tr}[(P \otimes |x\rangle\langle x|)\rho_{\mathbf{A}}] = \mathrm{Tr}[(Q \otimes |x\rangle\langle x|)\rho_{\mathbf{A}}^{T_A}] = 0$ for $n = 4$, or
- $\mathrm{Tr}[(\tilde{P} \otimes |x\rangle\langle x|)\rho_{\mathbf{A}}] = \mathrm{Tr}[(\tilde{Q} \otimes |x\rangle\langle x|)\rho_{\mathbf{A}}^{T_A}] = \mathrm{Tr}[(\tilde{R} \otimes |x\rangle\langle x|)\rho_{\mathbf{A}}^{T_{AB}}] = 0$ for $n = 6$.

Hence, either $\rho_{\mathbf{A}}$, $\rho_{\mathbf{A}}^{T_A}$ or $\rho_{\mathbf{A}}^{T_{AB}}$ is rank deficient, contradicting the assumptions. Then, Eq. (3.26) and thus Eq. (3.22) must have a solution, implying that $\rho_{\mathbf{A}}$ is not edge. □

Remark 3.13. Even for $n = 8$ the above method does not apply, for there exist examples of PPT entangled symmetric states consisting of more than 3 qubits [Tur+12; TG09]. Thus, there exist indecomposable entanglement witnesses detecting them.

Nevertheless, it is worth noticing that if $\rho_{\mathbf{A}}$ is indeed an edge state, then the entanglement witness W constructed in the proof of Theorem 3.12 must be indecomposable.

We shall see now that, for the case of $n = 4$ qubits, one can go one step further, namely, when r_{ABCD}^{AB} is two less than maximal, a fact that we prove in Theorem 3.14:

Theorem 3.14. *Any $\rho_{\mathbf{A}} \in \mathcal{D}_S^{\mathrm{PPT}}(\mathbb{C}^2)^{\otimes 4}$ of ranks $\vec{r}_{\mathbf{A}} = (5, 8, 7)$ is generically not edge.*

Proof. We have that $\rho_{\mathbf{A}}$ and $\rho_{\mathbf{A}}^{T_A}$ are of full rank, whereas $\ker \rho_{\mathbf{A}}^{T_{AB}}$ is two-dimensional. As a consequence, $\rho_{\mathbf{A}}$ will not be edge if we can find a vector $|e\rangle \in \mathbb{C}^2$ such that $|e\rangle^{\otimes 4} \in \operatorname{Im} \rho_{\mathbf{A}}$, $|e^*\rangle|e\rangle^{\otimes 3} \in \operatorname{Im} \rho_{\mathbf{A}}^{T_A}$ and $|e^*\rangle^{\otimes 2}|e\rangle^{\otimes 2} \in \operatorname{Im} \rho_{\mathbf{A}}^{T_{AB}}$. The first two conditions are automatically satisfied by hypothesis (any vector belongs to the range of a full-rank operator). Hence, we have to solve a system of two equations

$$\langle e^*|^{\otimes 2}\langle e|^{\otimes 2}|\Psi_i\rangle = 0, \qquad i = 1, 2, \tag{3.27}$$

where $|\Psi_i\rangle$ span $\ker \rho_{\mathbf{A}}^{T_{AB}}$. We consider now the unitary operator Π_τ, where $\tau \in \mathfrak{S}_4$ swaps subsystems AB and CD. Then, we have the identity $\rho_{\mathbf{A}}^{T_{AB}} = \Pi_\tau (\rho_{\mathbf{A}}^*)^{T_{AB}} \Pi_\tau$ which enables us to write the following Schmidt decomposition:

$$|\Psi_1\rangle = \sum_{k=1}^{r_1} \lambda_k |e_k\rangle|f_k^*\rangle, \qquad |\Psi_2\rangle = \sum_{k=1}^{r_2} \lambda_k |f_k\rangle|e_k^*\rangle, \tag{3.28}$$

where r_i is the Schmidt rank of $|\Psi_i\rangle$. Our aim is now to show that $r_1 = r_2 = 2$.

Notice that the largest subspace of $\mathbb{C}^3 \otimes \mathbb{C}^3$ that contains only vectors of Schmidt rank three is one-dimensional [CMW08], so if $r_1 = r_2 = 3$, $|\Psi_1\rangle$ and $|\Psi_2\rangle$ cannot be linearly independent. On the other hand, if $r_1 = 1$ or $r_2 = 1$, it is product with respect to the bipartition $AB|CD$, implying $0 = \langle e|\langle f^*|\rho_{\mathbf{A}}^{T_{AB}}|e\rangle|f^*\rangle = \langle e^*|\langle f^*|\rho_{\mathbf{A}}|e^*\rangle|f^*\rangle$, implying that $P_4(|e^*\rangle|f^*\rangle) \in \ker \rho_{\mathbf{A}}$, so that $r_{\mathbf{A}} = 4$, contradicting the assumption that $r_{\mathbf{A}} = 5$.

So either r_1 or r_2 must be 2. We can assume, without loss of generality that $r_1 = 2$. Then, we consider $\Pi_\tau|\Psi_1\rangle$. If $|\Psi_1\rangle$ and $\Pi_\tau|\Psi_1^*\rangle$ are linearly independent, this is the case of Eq. (3.28) with $r_2 = 2$ by choosing $|\Psi_2\rangle := \Pi_\tau|\Psi_1^*\rangle$. If not, then necessarily $\Pi_\tau|\Psi_1^*\rangle = \zeta|\Psi_1\rangle$ for some $\zeta \in \mathbb{C}$. But then short algebra proves that $|\Psi_1\rangle$ and $|\Psi_2\rangle$ are linearly dependent, contradicting the fact that $\dim \ker \rho_{\mathbf{A}}^{T_{AB}} = 2$.

Hence, we have proved that $r_1 = r_2 = 2$. Eqs. (3.27), by parametrizing $|e\rangle = (1, \alpha)$, with $\alpha \in \mathbb{C}$ can be recasted as

$$P(\alpha^*)Q(\alpha) + \tilde{P}(\alpha^*)\tilde{Q}(\alpha) = 0 \tag{3.29}$$

having solution both for α and for α^*, where $P, Q, \tilde{P}$ and $\tilde{Q}$ are polynomials of degree generically 2.

Such α exists if, and only if, there exists a $z \in \mathbb{C}$ for which $P(\alpha^*) = z\tilde{P}(\alpha^*)$ and $\tilde{Q}(\alpha) = -zQ(\alpha)$. The equation in P allow us to find α^* as a function of z. Because P and $\tilde{P}$ are of degree at most 2, there are generically 2 solutions which we put to the equation in Q, so that we get

$$(z^*)^2 Q_4(z) + z^* Q_4'(z) + Q_4''(z) = 0, \tag{3.30}$$

where Q_4, Q_4' and Q_4'' are polynomials of degree generically 4. Since z and its conjugate appear with different degrees in Eq. (3.30) Lemma 3.9 applies, providing the existence of a solution z, allowing us to find α. □

Remark 3.15. The method of Theorem 3.14 can only be applied in the case of $n = 4$ qubits, as, for $n = 6$, there would be 3 terms in the l. h. s. of Eq. (3.29) and the factorization in terms of z could not be done. As we shall see in Section 3.2, numerics suggest that there are no edge generic states of such ranks.

So far, the analysis of PPT entangled symmetric states with respect to edgeness has allowed us to further reduce the configuration of ranks that PPTESS can have. This is because any PPT state which is not edge can be written as a convex combination of a pure product state and another PPT state of lower ranks.

3.1.3. Schmidt number

In this section we discuss some facts about the Schmidt number of the symmetric states (*cf.* Eq. (2.5)). We shall see that any entangled state in $\mathcal{D}_{\mathcal{S}}^{\mathrm{PPT}}((\mathbb{C}^2)^{\otimes n})$ has Schmidt number two for 4 qubits and, at most, three, for 5 qubits. We also make some considerations with respect to systems with larger n. In this section, we shall use the linear algebra insted of the bra-ket notation $(a, b) \equiv a|0\rangle + b|1\rangle$ in order to simplify the expressions.

Let us first introduce the ingredients of our method: Consider the transformations $F_n : (\mathbb{C}^2)^{\otimes n} \longrightarrow \mathbb{C}^2$, defined as the projection $F_n(1, \alpha)^{\otimes n} = (1, \alpha^n)$, and $G_n : (\mathbb{C}^2)^{\otimes (n+1)} \longrightarrow (\mathbb{C}^2)^{\otimes (2n+1)}$, defined as $(1, \alpha^{n+1}) \otimes (1, \alpha)^{\otimes n} \mapsto (1, \alpha)^{\otimes (2n+1)}$. Both maps are extended by linearity (they simply

pick and/or duplicate coordinates accordingly). Let $\hat{F}_n$ and $\hat{G}_n$ be the adjoint actions of F_n and G_n, respectively, defined as $\hat{F}_n(X) := F_n X F_n^\dagger$ and $\hat{G}_n(X) := G_n X G_n^\dagger$, respectively.

Let us analyze now how F_n and G_n behave on symmetric states. Take a symmetric vector of n qubits $|\psi\rangle \in \mathcal{S}((\mathbb{C}^2)^{\otimes n})$ and apply $F_{\lceil n/2 \rceil}$ to the first $\lceil n/2 \rceil$ qubits of $|\psi\rangle$; then, we get a $(\lfloor n/2 \rfloor + 1)$-qubit vector $|\psi'\rangle \in \mathbb{C}^2 \otimes \mathcal{S}((\mathbb{C}^2)^{\otimes n})$. The inverse of this transformation is given by applying $G_{n/2-1}$ to the first $n/2$ qubits of $|\psi'\rangle$ (if $n \equiv 0 \mod 2$) or $G_{\lceil n/2 \rceil - 1}$ to the whole $|\psi'\rangle$ (if $n \equiv 1 \mod 2$), returning the original $|\psi\rangle$.

In the case of mixed states, the use of adjoint actions gives an analogous procedure: By applying $\hat{F}_{\lceil n/2 \rceil}$ to the first $\lceil n/2 \rceil$ qubits of $\rho_{\mathbf{A}}$ one obtains a state $\sigma_{\mathbf{B}'}$, were we have denoted $\mathbf{A} = A_1 \dots A_{\lceil n/2 \rceil} B_1 \dots B_{\lfloor n/2 \rfloor}$, $\mathbf{B} = B_1 \dots B_{\lfloor n/2 \rfloor}$ and $\mathbf{B}' = C\mathbf{B}$. The parties in $\mathbf{B}$ are still symmetric, so that $\sigma_{\mathbf{B}'}$ can be regarded as a state acting on $\mathbb{C}^2 \otimes \mathbb{C}^{\lfloor n/2 \rfloor + 1}$. Hence, $\hat{F}$ can be seen as a *compression* operation that preserves the rank: $\operatorname{rank} \rho_{\mathbf{A}} = \operatorname{rank} \sigma_{\mathbf{B}'}$. The reason for that is twofold. First, $\operatorname{Im} \rho_{\mathbf{A}}$ is spanned by the symmetric product vectors $(1, \alpha)^{\otimes n}$, by varying[7] $\alpha \in \mathbb{C}$. Second, such vectors are mapped as $F_{\lceil n/2 \rceil} : (1, \alpha)_{\mathbf{A}}^{\otimes n} \mapsto (1, \alpha^{\lceil n/2 \rceil})_C \otimes (1, \alpha)_{\mathbf{B}}^{\otimes \lfloor n/2 \rfloor}$. Because all the powers of α, from α^0 to α^n appear in the projected vectors, the whole information of $\rho_{\mathbf{A}}$ is still encoded in $\sigma_{\mathbf{B}'}$. This information is decoded by applying $\hat{G}$. Precisely, applying either $\hat{G}_{n/2}$ to $\mathbf{B}$ if n is even, or $\hat{G}_{\lceil n/2 \rceil - 1}$ to $\mathbf{B}'$ if n is odd, $\rho_{\mathbf{A}}$ is recovered.

With the following theorem we shall see how this compression procedure is useful to give an upper bound on the Schmidt number of a PPT entangled symmetric state:

Theorem 3.16. *Let $\rho_{\mathbf{A}} \in \mathcal{D}_{\mathcal{S}}^{\mathrm{PPT}}(\mathbb{C}^2)^{\otimes n}$. Let $\sigma_{\mathbf{B}'} := \hat{F}_{\lceil n/2 \rceil}(\rho_{\mathbf{A}})$, where $\hat{F}_{\lceil n/2 \rceil}$ is applied to the first $\lceil n/2 \rceil$ qubits. If $\sigma_{\mathbf{B}'}$ is separable with respect to the $C|\mathbf{B}$ bipartition, then $\rho_{\mathbf{A}}$ admits the following decomposition*

$$\rho_{\mathbf{A}} = \sum_{i=1}^{K} \left[\sum_{j=1}^{\lceil n/2 \rceil} A_j^{(i)} (1, \alpha_j^{(i)})^{\otimes n} \right], \tag{3.31}$$

where $K \in \mathbb{N}$, $A_j^{(i)}, \alpha_j^{(i)} \in \mathbb{C}$ and $[\psi] := |\psi\rangle\langle\psi|$.

[7] It suffices to take n different values of α, denoted α_i, because the determinant of a $n \times n$ Vandermonde matrix is $\prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)$.

Proof. Because of Theorem 3.3 we can assume that $\rho_{\mathbf{A}}$ has full rank: $r_{\mathbf{A}} = n+1$. Since $\sigma_{\mathbf{B}'}$ is biseparable with respect to the bipartition $C|\mathbf{B}$, there is the following decomposition

$$\sigma_{\mathbf{B}'} = \sum_{i=1}^{K} p_i |e_i\rangle\langle e_i| \otimes |f_i\rangle\langle f_i|, \tag{3.32}$$

where $|e_i\rangle \in \mathbb{C}^2$, $|f_i\rangle \in \mathbb{C}^{\lfloor n/2 \rfloor + 1}$, $K \in \mathbb{N}$ and p_i constitutes a probability distribution: $p_i \geq 0$ and $\sum_i p_i = 1$.

Since $\hat{F}_{\lceil n/2 \rceil}$ preserves the rank of $\rho_{\mathbf{A}}$ and $\sigma_{\mathbf{B}'}$, then $\operatorname{rank} \sigma_{\mathbf{B}'} = n+1$. However, $\sigma_{\mathbf{B}'}$ acts on $\mathbb{C}^2 \otimes \mathbb{C}^{\lfloor n/2 \rfloor + 1}$, so its maximal rank can be $2(\lfloor n/2 \rfloor + 1)$. Hence, for odd n, $\sigma_{\mathbf{B}'}$ has full rank, whereas for even n, there is a single vector in $\ker \sigma_{\mathbf{B}'}$, which we denote $|\phi\rangle :\propto |1\rangle|0\rangle - |0\rangle|n/2\rangle$. Now we distinguish several cases:

- $n \equiv 0 \mod 2$. Since $|\phi\rangle \in \ker \sigma_{\mathbf{B}'}$, putting $|e_i\rangle \propto (1, \alpha_i^{n/2})$ with $\alpha_i \in \mathbb{C}$ imposes a constraint on $|f_i\rangle$, which can be written as $\langle n/2|f_i\rangle = \langle 0|f_i\rangle \alpha_i^{n/2}$. Hence $|f_i\rangle$ has $n/2$ degrees of freedom and $|f_i\rangle \in \mathbb{C}^{n/2}$ instead of $\mathbb{C}^{n/2+1}$, but by exploiting the following isomorphism, $\mathbb{C}^{n/2} \cong \mathcal{S}((\mathbb{C}^2)^{\otimes n/2-1})$, we can rewrite in the computational basis

$$|f_i\rangle = \sum_{j=1}^{n/2} A_j^{(i)} (1, e^{\mathrm{i}\varphi_j} \alpha_i)^{\otimes n/2}, \tag{3.33}$$

  with $\varphi_j := 2\pi j/(n/2) = 4\pi j/n$ and $A_j^{(i)} \in \mathbb{C}$. Applying $\hat{G}_{n/2-1}$ to $\sigma_{\mathbf{B}'}$ one recovers Eq. (3.31).

- $n \equiv 1 \mod 2$. In this case, we choose $|e_i\rangle \propto (1, \alpha_i^{\lceil n/2 \rceil})$ and, because $|f_i\rangle \in \mathbb{C}^{\lfloor n/2 \rfloor + 1}$ and we have the isomorphism $\mathbb{C}^{\lfloor n/2 \rfloor + 1} \cong \mathcal{S}((\mathbb{C}^2)^{\otimes \lfloor n/2 \rfloor})$, we can expand $|f_i\rangle$ in the product computational basis, as a sum of product symmetric vectors:

$$|f_i\rangle = \sum_{j=1}^{\lfloor n/2 \rfloor + 1} A_j^{(i)} (1, e^{\mathrm{i}\varphi_j} \alpha_i)^{\otimes \lfloor n/2 \rfloor}, \tag{3.34}$$

  where $\varphi_j := 2\pi j/\lceil n/2 \rceil$ and $A_j^{(i)} \in \mathbb{C}$. As in the previous case, applying $G_{\lceil n/2 \rceil - 1}|e_i\rangle|f_i\rangle$ gives $\sum_{j=1}^{\lfloor n/2 \rfloor + 1} A_j^{(i)} (1, e^{\mathrm{i}\varphi_j} \alpha_i)^{\otimes n}$, leading to the form in Eq. (3.31).

A final comment is in order: we have chosen that symmetric product vectors in which to expand the $|f_i\rangle$ to be of the form $(1, e^{\mathrm{i}\varphi_j}\alpha_i)^{\otimes\lfloor n/2\rfloor}$, where the phases next to α_i are chosen to be $\lceil n/2\rceil-$th roots of unity. Such vectors span a $\lceil n/2\rceil-$dimensional vector space. □

As a consequence, Theorem 3.16 implies that PPT entangled states of $n = 4$ or $n = 5$ have Schmidt number 2 or, at most 3, respectively, as precisely stated in Corollary 3.17, in which we also give a bound in the number of terms K needed in the mixture.

Corollary 3.17. *Any entangled $\rho_{\mathbf{A}} \in \mathcal{D}_{\mathcal{S}}^{\mathrm{PPT}}(\mathbb{C}^2)^{\otimes 4}$ can be written as*

$$\rho_{\mathbf{A}} \propto \sum_{i=1}^{K} \left[A_1^{(i)}(1, \alpha_i)^{\otimes 4} + A_2^{(i)}(1, -\alpha_i)^{\otimes 4} \right], \tag{3.35}$$

whereas any entangled $\rho_{\mathbf{A}} \in \mathcal{D}_{\mathcal{S}}^{\mathrm{PPT}}(\mathbb{C}^2)^{\otimes 5}$ can be written as

$$\rho_{\mathbf{A}} \propto \sum_{i=1}^{K} \left[A_1^{(i)}(1, \alpha_i)^{\otimes 5} + A_2^{(i)}(1, e^{\mathrm{i}2\pi/3}\alpha_i)^{\otimes 5} + A_3^{(i)}(1, e^{-\mathrm{i}2\pi/3}\alpha_i)^{\otimes 5} \right], \tag{3.36}$$

with $K \leq 6$, where $A_j^{(i)}, \alpha_i \in \mathbb{C}$ and $[\psi] := |\psi\rangle\langle\psi|$.

Proof. We get a state that acts on $\mathbb{C}^2 \otimes \mathbb{C}^3$ by application of $\hat{F}_2$ ($\hat{F}_3$) to the first two (three) qubits of $\rho_{\mathbf{A}}$ for $n = 4$ ($n = 5$) qubits. The obtained $\sigma_{\mathbf{B}'}$ is PPT, hence it is also separable [Kra+00]. We can apply Theorem 3.16 and Eq. (3.31) particularizes to Eq. (3.35) or (3.36). Because every qubit-qutrit separable state can be written as a convex combination of, at most, six product vectors [SKL07], the bound $K \leq 6$ follows. □

Interestingly, by using the methods introduced in [SKL07], one can obtain a slightly different and simpler form of Eq. (3.35), in which the terms $(1, -\alpha_i)^{\otimes 4}$ are replaced either by $|0000\rangle$ or $|1111\rangle$.

Theorem 3.18. *Any entangled $\rho_{\mathbf{A}} \in \mathcal{D}_{\mathcal{S}}^{\mathrm{PPT}}(\mathbb{C}^2)^{\otimes 4}$ can be written as*

$$\rho_{\mathbf{A}} \propto \sum_{i=1}^{K} \left[A^{(i)}(1, \alpha_i)^{\otimes 4} + B^{(i)}(0, 1)^{\otimes 4} \right], \tag{3.37}$$

with $K \leq 6$, where α_i, $A^{(i)}$ and $B^{(i)} \in \mathbb{C}$ and $[\psi]$ is the projector onto $|\psi\rangle$.

Proof. We exploit the methods introduced in [SKL07]. To begin with, we note that any $\rho_{\mathbf{A}}$ admits two forms of decompositions: it can be expressed as a sum of rank-one matrices

$$\rho_{\mathbf{A}} = \sum_{i=1}^{K} |\Psi_i\rangle\langle\Psi_i|, \tag{3.38}$$

where $|\Psi_i\rangle$ may have norm smaller than 1. A particular case of decomposition (3.38) is the eigendecomposition of $\rho_{\mathbf{A}}$. Because of Corollary 3.17, $K \leq 6$.

On the other hand, one can express $\rho_{\mathbf{A}}$ in the Dicke basis and obtain its elements as a 5×5 matrix:

$$\rho_{\mathbf{A}} = \sum_{\mu,\nu=0}^{4} (\rho_{\mathbf{A}})^{\mu}_{\nu} |D_4^{\mu}\rangle\langle D_4^{\nu}|, \tag{3.39}$$

where $(\rho_{\mathbf{A}})^{\mu}_{\nu}$ is matrix element of $\rho_{\mathbf{A}}$ appearing on the $\mu-$th row, $\nu-$th column in the basis $\{|D_4^i\rangle\}_{i=0\ldots4}$ of $\mathcal{S}(\mathbb{C}^2)^{\otimes 4}$ (which can be unnormalized, although for convenience one tends to choose the Dicke basis defined in (2.27)).

Both decompositions (3.38) and (3.39) are related via the Gram system of $\rho_{\mathbf{A}}$, which is a collection of K-dimensional vectors $\{|v_i\rangle\}_{i=0\ldots4}$ defined as

$$|v_i\rangle := \frac{1}{\langle D_4^i | D_4^i\rangle}(\langle\Psi_1|D_4^i\rangle, \ldots, \langle\Psi_K|D_4^i\rangle). \tag{3.40}$$

Then $(\rho_{\mathbf{A}})^{\mu}_{\nu}$ is given by $\langle v_\mu | v_\nu\rangle$. In this way, one goes from Eq. (3.39) to Eq. (3.38).

Now we project the last party onto $|0\rangle$, which leads to a three-qubit symmetric PPT state $\tilde{\rho}_{\mathbf{A}\setminus D}$. Note that $\tilde{\rho}_{\mathbf{A}\setminus D}$ is separable. Then, there exists a diagonal matrix $M = \mathrm{diag}(\alpha_1^*, \ldots, \alpha_K^*)$ such that $|v_\mu\rangle = M^\mu |v_0\rangle$ for $0 \leq \mu < 4$ and $|v_4\rangle = M^4|v_0\rangle + |\tilde{v}\rangle$, for some $|\tilde{v}\rangle \in \mathbb{C}^K$ [SKL07]. Let us explicitly write the coordinates of $|v_0\rangle$ and $|\tilde{v}\rangle$ as $|v_0\rangle = (A_1^*, \ldots, A_K^*)$ and $|\tilde{v}\rangle = (B_1^*, \ldots, B_K^*)$. Then, $|\Psi_i\rangle$ has the following expression:

$$|\Psi_i\rangle = \sum_{\mu=0}^{4} \frac{\langle D_4^\mu|\Psi_i\rangle}{\langle D_4^\mu|D_4^\mu\rangle}|D_4^\mu\rangle = A_i \sum_{\mu=0}^{4} \alpha_i^\mu |D_4^\mu\rangle + B_i|D_4^4\rangle = A_i(1,\alpha_i)^{\otimes 4} + B_i|D_4^4\rangle. \tag{3.41}$$

Substituting Eq. (3.41) into Eq. (3.38) gives the form of Eq. (3.37), finisihing the proof. □

Remark 3.19. In order to obtain an expression as in Eq. (3.37) but with $(0,1)^{\otimes 4}$ replaced by $(1,0)^{\otimes 4}$, one simply projects party D of $\rho_{\mathbf{A}}$ onto $|1\rangle$ instead of $|0\rangle$ in the proof of Theorem 3.18.

3.2. The Geometry of the set of PPTESS

The polynomial equations appearing in Section 3.1.2 involve both a complex variable and its conjugate and we have seen that they are not easy to solve in general. In this section we exploit the geometrical properties of the set of PPT entangled symmetric states in order to obtain separability criteria for extremal PPT symmetric states, as we do in Section 3.2.1. Then, in Section 3.2.2, we provide an algorithm to produce such kind of states.

In Chapter 2 we have defined the set of quantum states $\mathcal{D}(\mathcal{H})$ and the set of separable states $\mathcal{D}_{\text{sep}}(\mathcal{H})$. $\mathcal{D}(\mathcal{H})$ is a convex set: $\forall \rho_1, \rho_2 \in \mathcal{D}(\mathcal{H})$, $\rho(\lambda) \in \mathcal{D}(\mathcal{H})$ for all $0 \leq \lambda \leq 1$, where $\rho(\lambda) := \lambda\rho_1 + (1-\lambda)\rho_2$. The states $\rho(\lambda)$ which cannot be written as a convex combination of any $\rho_1, \rho_2 \neq \rho$ with $0 < \lambda < 1$ are called extremal and they form the set $\text{Ext}(\mathcal{D}(\mathcal{H}))$, which consists of all the rank-one projectors; *i.e.*, pure vectors.

Similarly, $\mathcal{D}_{\text{sep}}(\mathcal{H})$ is also a convex set, because Definition 2.1 shows that the mixture of separable states leads to a separable state. The same holds for k-separable states (*cf.* Definition 2.2). Although deciding membership in the set $\mathcal{D}_{\text{k}-\text{sep}}(\mathcal{H})$ is NP-hard [Gur03], the elements in $\text{Ext}(\mathcal{D}_{\text{k}-\text{sep}}(\mathcal{H}))$ are easy to characterize, as they are the pure product vectors (product with respect to any k-partition). For the case of fully separable states, its extremal elements are the fully product pure states. In the case of symmetric states, $\text{Ext}(\mathcal{D}_{\text{n}-\text{sep}}(\mathcal{S}(\mathcal{H})))$ is the set of all pure product vectors of the form $|e\rangle^{\otimes n}$.

Let us now take a glance at the set of PPT states. Let us denote as $\mathcal{D}^{\text{PPT},S}(\mathcal{H})$ the set of states $\rho \in \mathcal{D}(\mathcal{H})$ that are PPT with respect to the bipartition $S|\overline{S}$; *i.e.*, $\rho^{T_S} \succeq 0$. This set is also convex, for any S: for any pair of states ρ_1 and ρ_2 such that $\rho_1^{T_S} \succeq 0$ and $\rho_2^{T_S} \succeq 0$, any convex combination of them fulfills $(\lambda\rho_1 + (1-\lambda)\rho_2)^{T_S} \succeq 0$. Because the intersection of convex sets is also a convex set, the set of states PPT with respect to every

bipartition, denoted

$$\mathcal{D}^{\mathrm{PPT}}(\mathcal{H}) = \cap_{S\subseteq\mathbf{A}}\mathcal{D}^{\mathrm{PPT},S}(\mathcal{H}). \tag{3.42}$$

When we refer to symmetric states, this set will be denoted $\mathcal{D}_{\mathcal{S}}^{\mathrm{PPT}}(\mathcal{H})$, as in Section 3.1.

As we have discussed, deciding membership in the set of fully separable states is a hard problem, whereas its extremal points are easy to characterize. On the other hand, deciding membership in the set of PPT states is easy for the case of symmetric states[8]. The characterization of its extremal points will be discussed in Section 3.2.1. We have indirectly addressed this issue in Section 3.1.2 for edge states, although it is unknown whether being edge implies being extremal (edge states certainly lie on the boundary of $\mathcal{D}_{\mathcal{S}}^{\mathrm{PPT}}(\mathcal{H})$, but this condition is not sufficient to guarantee extremality).

Criterion for Entanglement

In order to certify that a PPT entangled state is indeed an entangled state, one needs of course, another separability criterion independent of the positivity under partial transposition.

The criterion we provide here is in the spirit of [LMO07] (see also [Aug+10]): Because the set of separable states is included in the set of PPT states, the extremal points of the set of PPT states which are not extremal in the set of separable states must be entangled.

Formally, one has the following inclusions: $\mathcal{D}_{\mathrm{sep}} \subseteq \mathcal{D}^{\mathrm{PPT}}$. Since $\mathcal{D}_{\mathrm{sep}} \cap \mathrm{Ext}(\mathcal{D}^{\mathrm{PPT}}) \subseteq \mathrm{Ext}(\mathcal{D}_{\mathrm{sep}})$, the states in $\mathrm{Ext}(\mathcal{D}^{\mathrm{PPT}}) \setminus \mathrm{Ext}(\mathcal{D}_{\mathrm{sep}})$ must be entangled, because $(\mathrm{Ext}(\mathcal{D}^{\mathrm{PPT}})\setminus\mathrm{Ext}(\mathcal{D}_{\mathrm{sep}}))\cap\mathcal{D}_{\mathrm{sep}} = \mathrm{Ext}(\mathcal{D}^{\mathrm{PPT}})\cap\overline{\mathrm{Ext}(\mathcal{D}_{\mathrm{sep}})}\cap \mathcal{D}_{\mathrm{sep}} = (\mathrm{Ext}(\mathcal{D}^{\mathrm{PPT}}) \cap \mathcal{D}_{\mathrm{sep}}) \cap \overline{\mathrm{Ext}(\mathcal{D}_{\mathrm{sep}})} = \mathrm{Ext}(\mathcal{D}_{\mathrm{sep}}) \cap \overline{\mathrm{Ext}(\mathcal{D}_{\mathrm{sep}})} = \emptyset$.

Our aim is to show that $\mathrm{Ext}(\mathcal{D}^{\mathrm{PPT}}) \setminus \mathrm{Ext}(\mathcal{D}_{\mathrm{sep}}) \neq \emptyset$ for the symmetric case and $n > 3$ qubits.

Remark 3.20. Note that $\vec{r}_{\mathbf{A}} = (1, 1, 1, \ldots, 1)$ for any $\rho_{\mathbf{A}} \in \mathrm{Ext}(\mathcal{D}_{n-\mathrm{sep}})$, since $\rho_{\mathbf{A}}$ must be a pure product vector. Thus, a state $\rho_{\mathbf{A}} \in \mathrm{Ext}(\mathcal{D}_{\mathcal{S}}^{\mathrm{PPT}})$ with $\vec{r}_{\mathbf{A}} \neq (1, 1, 1, \ldots, 1)$ must be entangled.

[8] It is sufficient to check the sign of the minimal eigenvalue of a $O(n)$ number of matrices that have size $O(n^2)$, where n is the number of qubits, as we shall see in Remark 3.26.

3.2.1. Extremal PPT States

In this section we consider a multipartite Hilbert space $\mathcal{H} = \bigotimes_{i=0}^{n-1} \mathbb{C}^{d_i}$. Given a state $\rho \in \mathcal{D}^{\mathrm{PPT}}(\mathcal{H})$ which is not extremal, it admits a convex decomposition in terms of $\rho_1, \rho_2 \in \mathcal{D}^{\mathrm{PPT}}(\mathcal{H}) \setminus \{\rho\}$ of the form

$$\rho = \lambda\rho_1 + (1-\lambda)\rho_2, \qquad 0 < \lambda < 1. \tag{3.43}$$

Eq. (3.43) implies that $\mathrm{Im}\,\rho_i \subseteq \mathrm{Im}\,\rho$ and, by taking a partial transposition with respect to a bipartition $S|\overline{S}$ of $\mathbf{A}$ in Eq. (3.43), it also implies $\mathrm{Im}\,\rho_i^{T_S} \subseteq \mathrm{Im}\,\rho^{T_S}$. Hence, if ρ is not extremal, there exists another PPT state $\sigma \neq \rho$ such that

$$\mathrm{Im}\,\sigma \subseteq \mathrm{Im}\,\rho \text{ and } \mathrm{Im}\,\sigma^{T_S} \subseteq \mathrm{Im}\,\rho^{T_S}\ \forall S \subset \mathbf{A}. \tag{3.44}$$

If there is a σ fulfilling Eqs. (3.44) then one can indeed construct a convex decomposition for ρ: It suffices to see that there exists a scalar $x > 0$ such that $\rho(x) := (1+x)\rho - x\sigma$ is a PPT state (by moving along the direction defined by $\rho - \sigma$ without leaving the set of PPT states). Then, $\rho = (\rho(x) + x\sigma)/(1+x)$. Hence, we arrive at a simple criterion for deciding membership in $\mathrm{Ext}(\mathcal{D}^{\mathrm{PPT}}(\mathcal{H}))$: ρ is extremal if, and only if, any solution σ of Eqs. (3.44) must be $\sigma \propto \rho$.

Remark 3.21. One can relax the assumption of σ being PPT to just being a Hermitian matrix h satisfying the following set of equations [Aug+10]

$$P_S h^{T_S} P_S = h^{T_S}, \tag{3.45}$$

where P_S is a projection onto $\mathrm{Im}\,\rho^{T_S}$ and we allow S to be $\emptyset$.

Proof. If there exist an h fulfilling 3.45, then one can move along the direction of $h - \rho$ or $\rho - h$ without leaving the PPT set: consider the family of states[9] parametrized by x: $\rho(x) := (1 + x\mathrm{Tr}h)\rho - xh$. One can find then $x_1 < 0 < x_2$ such that $\rho(x) \in \mathcal{D}^{\mathrm{PPT}}(\mathcal{H})$ for any $x \in [x_1, x_2]$. In particular, a convex decomposition of ρ is given by x_1 and x_2:

$$\rho = \frac{1}{x_2 - x_1}(x_2\rho(x_1) - x_1\rho(x_2)), \tag{3.46}$$

which implies that ρ is not extremal. □

[9] The correction $\mathrm{Tr}h$ is added just to impose $\mathrm{Tr}\rho(x) = 1$ for all x.

Remark 3.22. The system of equations (3.45) can be recast into a single equation, by *vectorizing*[10] h as an element of the $\mathbb{R}$-vector space of Hermitian matrices; *i.e.*,

$$\hat{P}_M \circ \ldots \circ \hat{P}_1 \circ \hat{P}_\emptyset(h) = h, \tag{3.47}$$

where $\hat{P}_i(X) := (P_{S_i} X^{T_{S_i}} P_{S_i})^{T_{S_i}}$ and $M+1$ is the number of equations in (3.45); $\emptyset$ simply indicates the case for which there is no partial transposition to be applied.

Proof. Clearly, if (3.45) holds for all S and some h, then (3.47) also holds. Conversely, if there is an h satisfying (3.47) and one of the conditions (3.45) would not hold, comparing the norms of both sides of every equation shows that neither could be satisfied. □

Let us formally state the separability criterion we have just proved:

Theorem 3.23. *A state $\rho \in \mathrm{Ext}(\mathcal{D}^{\mathrm{PPT}}(\mathcal{H}))$ if, and only if, Eq. (3.45) has no Hermitian solution linearly independent of ρ.*

Since we are interested in criteria in terms of $\vec{r}_{\mathbf{A}}$, by counting the number equations and unknowns appearing in Eq. (3.45) we can obtain necessary conditions for extremality in terms of the ranks of the partial transpositions of ρ, which we denoted as $r^S_{\mathbf{A}}$.

We notice that every equation in (3.45) imposes $(\dim \mathcal{H})^2 - (r^S_{\mathbf{A}})^2$ linear constraints on h. The maximal number of independent constraints is then given by the sum $(M+1)(\dim \mathcal{H})^2 - \sum_S (r^S_{\mathbf{A}})^2$. Since any Hermitian matrix acting on $\mathcal{H}$ is specified by $(\dim \mathcal{H})^2$ real parameters, taking into account normalization, we obtain that the number of equations is smaller than the number of free parameters (*i.e.*, Eq. (3.45) has a solution) if

$$\sum_S (r^S_{\mathbf{A}})^2 \geq M(\dim \mathcal{H})^2 + 1, \tag{3.48}$$

in which case ρ is not extremal.

[10] Here we use the identity $A \otimes B\mathrm{vec(X)} = \mathrm{vec}(AXB^T)$, where the vectorization operator acts as $\mathrm{vec}|a\rangle\langle b| = |a\rangle|b\rangle$ and it is extended by linearity. The partial transposition acts just as a permutation of the components of h.

Extremal PPTESS

Here we particularize the above considerations to the case of symmetric states. The first difference is that Eq. (3.48) does not take into account that the partial transpositions of ρ act now on Hilbert spaces of different dimensions[11]. The condition for h in (3.48) for a bipartition S of size k now gives $((k+1)(n-k+1))^2 - (r_{\mathbf{A}}^S)^2$ linear constraints. Hence, condition (3.48) becomes

$$\sum_{k=0}^{\lfloor n/2 \rfloor} (r_{\mathbf{A}}^k)^2 \geq 1 - (n+1)^2 + \sum_{k=0}^{\lfloor n/2 \rfloor} (k+1)^2 (n-k+1)^2. \tag{3.49}$$

The second difference is that Theorem 3.3 guarantees that only symmetric states of full rank $r_{\mathbf{A}} = n+1$ can be entangled, so inequality (3.49) can be recasted as

$$\sum_{k=1}^{\lfloor n/2 \rfloor} (r_{\mathbf{A}}^k)^2 \geq 1 - (n+1)^2 + \sum_{k=1}^{\lfloor n/2 \rfloor} (k+1)^2 (n-k+1)^2. \tag{3.50}$$

Example 3.24. *To better illustrate how inequality (3.50) is useful to discard tuples of ranks $\vec{r}_{\mathbf{A}}$, in Table 3.1 we present, for $n \in \{4,5,6\}$ qubits, the configurations that are ruled out by this criteria.*

3.2.2. Algorithm to produce Extremal PPT States

The discussion provided in Section 3.2.1 almost gives a step-by-step recipe on how to construct extremal elements in $\mathcal{D}^{\mathrm{PPT}}$: One simply needs to keep adding constraints to (3.45) until only one solution remains [LMO07; Tur+12; Aug+12].

Given a PPT state ρ and a linearly independent solution h of (3.45) we construct $\rho(x) := (1 + x\mathrm{Tr}h)\rho - xh$, as in Remark 3.21. By moving x until $\rho(x)$ hits the boundary of the PPT set[12], we find an $x = x_*$ for which $\rho(x_*) \in \mathcal{D}^{\mathrm{PPT}}$ but $\operatorname{rank} \rho(x_*)^{T_S} = \operatorname{rank} \rho^{T_S} - 1$ for some bipartition $S|\overline{S}$ of

[11] The case of four qubits was studied in detail in [Aug+10]

[12] Because $\mathcal{D}^{\mathrm{PPT}}$ arises as the intersection of $\mathcal{D}^{PPT,S}$ for all the considered bipartitions $S|\overline{S}$ of $\mathbf{A}$, x_* corresponds to the smallest x such that the one of the eigenvalues of $\rho_{\mathbf{A}}^{T_S}$ changes its sign for the first bipartition $S|\overline{S}$ that this sign change happens.

n	Inequality (3.50)	$\vec{r}_{\mathbf{A}}$ excluded with (3.50)
4	$(r^1_{A\ldots D})^2 + (r^2_{A\ldots D})^2 \geq 121$	$(5,7,9),(5,8,8),(5,8,9)$
5	$(r^1_{A\ldots E})^2 + (r^2_{A\ldots E})^2 \geq 209$	$(6,9,12),(6,10,11),(6,10,12)$
6	$\sum_{i=1}^{3}(r^i_{A\ldots F})^2 \geq 577$	$(7,10,15,16),(7,11,15,16),$ $(7,12,14,16),(7,12,15,15),$ $(7,12,15,16)$

Table 3.1.: Inequality (3.50) (second column) for the cases of $4 \leq n \leq 6$ together with the ranks (third column) excluded with its aid for which there are no extremal PPTESS. We have not listed the configuration of ranks $\vec{r}_{\mathbf{A}}$ for which each component is maximal, as the fact that there are no extremal states of maximal ranks can be inferred without the aid of inequality (3.50).

A. Let us define $\rho_1 := \rho(x_*)$. Observe that (at least) one of the ranks of ρ_1 is diminished by one with respect to the ranks of ρ.

Now the iteration is clear: We look again for the system of equations (3.45) but now the projectors P_S correspond to the projectors on the ranges of the partial transpositions of ρ_1. If there is only the trivial solution $h \propto \rho_1$, ρ_1 is extremal and the algorithm is finished. Otherwise, at least one of the ranks of ρ_1 can be lowered while keeping the PPT property. Hence, we find another x_* and we define $\rho_2 := \rho_1(x_*)$ and so on. The ranks $\vec{r}_{\mathbf{A}}$ keep lowering (and the number of constraints imposed by (3.45) increasing) until we arrive at an extremal state. If the final $\vec{r}_{\mathbf{A}} = (1,1,\ldots 1)$ (which will be eventually reached in a finite number of steps because $\dim \mathcal{H} < \infty$), then the state is separable; otherwise it is entangled.

Remark 3.25. If at step t, ρ_t is not extremal, the solution h of (3.45) can be chosen in a non-unique fashion. One can always pick a solution randomly, but clearly, picking h in a particular way may lead to different families of extremal PPTESS.

Algorithm to produce Extremal PPTESS

The above algorithm can be adjusted to deal with fully PPT symmetric states and highly improve its performance. The partial transposition of ρ is

very easily implemented in the computational basis, however $\dim((\mathbb{C}^2)^{\otimes n})$ is exponential in n, so it takes a lot of resources, especially because the states under consideration act on a subspace which grows linearly with n (and its partial transpositions, at most, quadratically). Hence, the key is to represent the partial transpositions of ρ without having to do the intermediate step of representing it in the computational basis and then projecting it back.

To this purpose, let us denote as ρ_{red} the $(n+1)\times(n+1)$ representation of $\rho \in \mathcal{D}_{\mathcal{S}}^{\mathrm{PPT}}((\mathbb{C}^2)^{\otimes n})$ in the symmetric space. In order to go from the representation in $\mathcal{S}(\mathbb{C}^2)^{\otimes n}$ to $\mathbb{C}^{n+1}$ let us define the $(n+1)\times 2^n$ matrix given by

$$B_n := \sum_{m=0}^{n} |m\rangle\langle D_n^m|, \tag{3.51}$$

where $|D_n^m\rangle$ are the Dicke states defined in (2.27). Note that we have $\rho_{\mathrm{red}} = B_n \rho B_n^T$. It is straightforward to check $B_n^T B_n = P_{\mathcal{S}}$ and $B_n B_n^T = \mathbb{1}_{n+1}$, where $P_{\mathcal{S}}$ is the projector onto the symmetric space defined in (3.7).

When k parties are transposed, ρ^{T_k} acts on $\mathcal{S}(\mathbb{C}^2)^{\otimes k} \otimes \mathcal{S}(\mathbb{C}^2)^{\otimes(n-k)}$; *i.e.*, its partial transposition can be represented as a $(k+1)(n-k+1)\times(k+1)(n-k+1)$ square matrix acting on $\mathbb{C}^{k+1}\otimes\mathbb{C}^{n-k+1}$, which we denote $\rho_{\mathrm{red}}^{T_k}$.

The projection from the whole Hilbert space to the space which $\rho_{\mathrm{red}}^{T_k}$ acts on is given by the matrix $\tilde{B}_k := (B_k \otimes B_{n-k})B_n^T$.

Remark 3.26. The relation between ρ_{red} and $\rho_{\mathrm{red}}^{T_k}$ is given by

$$\rho_{\mathrm{red}}^{T_k} = (\tilde{B}_k \rho_{\mathrm{red}} \tilde{B}_k^T)^{T_k} \tag{3.52}$$

Proof. The proof is a simple calculation:

$$\begin{aligned}
\rho_{\mathrm{red}}^{T_k} &= [(B_k \otimes B_{n-k})\rho(B_k^T \otimes B_{n-k}^T)]^{T_k} \\
&= [(B_k \otimes B_{n-k})B_n^T \rho_{\mathrm{red}} B_n (B_k^T \otimes B_{n-k}^T)]^{T_k} \\
&= (\tilde{B}_k \rho_{\mathrm{red}} \tilde{B}_k^T)^{T_k}.
\end{aligned}$$

□

The elements of $\tilde{B}_k$ are given by

$$\langle i,j|\tilde{B}_k|m\rangle = \sqrt{\binom{n}{i}\binom{n}{j}\Big/\binom{n}{m}}\,\delta_{i+j=n}, \tag{3.53}$$

where $0 \leq i \leq k$, $0 \leq j \leq n-k$ and $0 \leq m \leq n$.

Hence, an efficient implementation of the partial transposition of a symmetric state is done by expanding the $(n+1)\times(n+1)$ matrix ρ_{red} by means of $\tilde{B}_k$ to the $(k+1)(n-k+1)\times(k+1)(n-k+1)$ square matrix $\tilde{B}_k\rho_{\rm red}\tilde{B}_k^T$ and partially transposing it, as a bipartite $\mathbb{C}^{k+1}\otimes\mathbb{C}^{n-k+1}$ system. The matrices h appearing in Eq. (3.45) can be treated in the same way, allowing us to reduce the algorithm complexity from exponential to polynomial, both in time and in memory. The complexity of our approach amounts to $O(n^6)$.

Numerical results

We have applied the algorithm presented in Section 3.2.2 to PPT symmetric states with a number of qubits from $n=4$ up to $n=23$. We have taken as an initial state the projector onto the PPT symmetric space $P_{\mathcal{S}}/(n+1)$ (*cf.* Eq. 3.7), whose ranks are maximal. It is also separable, because it is the projection of the white noise $\mathbb{1}/2^n$ onto the Symmetric space. Note that $\vec{r}_{\mathbf{A}}$ being maximal guarantees that any extremal PPT state can be reached, as if it were not the case (*c.f.* Theorems 3.3 3.6), the algorithm could not produce any PPT entangled state by means of lowering ranks.

The solution of the system of equations (3.45) has been picked randomly within the subspace of all their solutions. Other configurations, however, may not be excluded by the analysis performed in previous sections and yet not be reached through a random search. In this case, one can design the matrices h in such a way that a specific rank is lowered. In Table 3.2 we have collected the obtained ranks. We see an interesting effect: numerics suggests that at most three configurations of $\vec{r}_{\mathbf{A}}$ are possible for even number of parties, and this number is not increasing with n. In the case of odd number of parties, we only see one configuration of ranks, and it corresponds to the $\vec{r}_{\mathbf{A}}$ for which $r_S=(n/2+1)^2-2$, for any partition $S|\overline{S}$ such that $|S|=|\overline{S}|$; *i.e.*, the rank of the most balanced partial transposition is maximal minus 2.

Interestingly, in the case of higher dimensional Hilbert spaces, one can find PPT entangled states of lower ranks than those which are extremal (by using PPT extremal entangled states supported on lower-dimensional Hilbert spaces) [LMS10]. However, this cannot happen for symmetric qubits, as they would always be separable.

As a case study, let us consider $n=4$ symmetric qubits, with $\vec{r}_{\mathbf{A}}=$

$(r_\emptyset, r_A, r_{AB})$. Theorems 3.3 and 3.6 imply that all states for which $\vec{r}_{\mathbf{A}} = (5, r_A, r_{AB})$ with $r_A, r_{AB} \leq 6$ are either separable or generically separable. On the other hand, Theorem 3.14 implies that the states with $\vec{r}_{\mathbf{A}} = (5, 8, 7)$ are generically not edge hence generically not extremal. The criterion for extremality given in inequality (3.50) implies that the cases $(5, 7, 9)$, $(5, 8, 8)$ and $(5, 8, 9)$ are ruled out because they cannot be extremal. There are only two candidates left: $\vec{r}_{\mathbf{A}} = (5, 7, 8)$ and $\vec{r}_{\mathbf{A}} = (5, 7, 7)$.

We made 30.000 runs of the algorithm and 19.2% of the generated states were extremal of ranks $(5, 7, 8)$, so they were entangled. The remaining $80, 8\%$ of the cases led to states of ranks $(5, 7, 7)$ all of which turned out to be separable. Furthermore, we observed a branching during the exploration: starting from the initial state $P_{\mathcal{S}}/(n+1)$ with maximal ranks $(5, 8, 9)$, $99, 4\%$ of the times we obtained an intermediate $(5, 8, 8)$ state, whereas the rest $(0, 6\%)$ of the time a $(5, 7, 9)$ state was found. This is in agreement with the data in Table 3.2, in which the most balanced partition is shown to be the most restrictive, hence the boundary of $\mathcal{D}_{\mathcal{S}}^{\mathrm{PPT},S}$ with $|S| = \lfloor n/2 \rfloor$ is the most likely to be found. Numerics also suggest that PPT states of ranks $(5, 7, 7)$ are generically separable, a fact that we discuss in Section 3.3.1.

3.3. Particular considerations

In this section we focus on the particular cases of 4, 5 and 6-qubit PPT symmetric states. We analyze which configurations of ranks the study and characterization of PPT entangled symmetric states reduces to.

- $n = 4$.

  In virtue of Theorem 3.5 4-qubit PPT symmetric states are separable if one of the following conditions holds: $r_\emptyset \leq 4$, $r_A \leq 4$ or $r_{AB} \leq 3$. Then, Theorem 3.6 generically guarantees the separability if $r_A \leq 6$ or $r_{AB} \leq 6$. Assuming that $r_\emptyset = 5$, there remain 6 out of 72 configurations of ranks which are still not ruled out: $(5, 7, 7)$, $(5, 7, 8)$, $(5, 7, 9)$, $(5, 8, 8)$ and $(5, 8, 9)$.

  However, the analysis on edgeness shows that states of full ranks; *i.e.*, of ranks $(5, 8, 9)$ can never be edge. Theorem 3.12 shows that states of ranks $(5, 8, 8)$ cannot be edge. Then, Theorems 3.14 and 3.10 show that, generically, states of ranks $(5, 8, 7)$ or $(5, 7, 9)$ are

not edge, respectively. Hence, a typical PPTESS with one of these four configuration of ranks can always be expressed, by subtracting appropriate symmetric product vectors, as a PPTESS of ranks either $(5,7,7)$ or $(5,7,8)$.

With the numerical studies carried out (*cf.* Section 3.2.2) we have found extremal states of ranks $(5,7,8)$, whereas all the states of ranks $(5,7,7)$ we found were separable. This is a strong indication (See also Section 3.3.1) that states of ranks $(5,7,7)$ are generically separable. If so, the analysis of entanglement in fully PPT $4-$qubit symmetric states is reduced to the caracterization of states with ranks $(5,7,8)$.

- $n=5$.

  For the case of $5-$qubit PPT symmetric states, Theorem 3.5 already implies that states with a configuration of ranks $\vec{r}_{\mathbf{A}}=(r_\emptyset, r_A, r_{AB})$ are separable if one of the following conditions hold: $r_\emptyset \leq 5$, $r_A \leq 5$ or $r_{AB} \leq 4$. Then, Theorem 3.6 implies that separability, in the generic sense, is guaranteed if either $r_A \leq 8$ or $r_{AB} \leq 9$. The six configurations of ranks (out of the 120 possible ones assuming $r_\emptyset = 6$) for which typical PPT symmetric states may not be separable are $(6,9,10)$, $(6,9,11)$, $(6,9,12)$, $(6,10,10)$, $(6,10,11)$ and $(6,10,12)$.

  With respect to edgeness, three of these configurations are not possible. Precisely, due to Theorem 3.10, states of ranks $(6,9,12)$, $(6,10,11)$ or $(6,10,12)$ cannot be edge. Note that these cannot be extremal either, due to Ineq. (3.50), as it is shown in Table 3.1. Finally, numerics suggest that only the $(6,10,10)$ configuration leads to an entangled extremal state, as it is shown in Table 3.2.

- $n=6$.

  This case is more intrincate. After applying Theorem 3.5, a sufficient condition for separability is that $r_\emptyset \leq 6$ or $r_A \leq 6$ or $r_{AB} \leq 5$ or $r_{ABC} \leq 4$. Generically, Theorem 3.6 guarantees a sufficient condition for separability, which is $r_A \leq 10$ or $r_{AB} \leq 12$ or $r_{ABC} \leq 12$. Thus, there are 24 configurations of ranks which are not ruled out. Theorem 3.12 says that configurations $(7,12,15,15)$ do not correspond to edge states and Theorem 3.10 implies that the configuration $(7,12,14,16)$ or $(7,11,15,16)$ are never generically edge. Finally, the configuration

of maximal ranks $(7, 12, 15, 16)$ never corresponds to an edge state. These are the same configurations of ranks which are excluded for extremality by Ineq. (3.50), as it is shown in Table 3.1. However, numerical studies indicate that only two out of the remaining 20 configurations of ranks correspond to extremal PPTESS (*cf.* Table 3.2).

3.3.1. Special constructions

In this section we analyze two particular constructions. We first give a half-analytical−half-numerical class of PPTESS of 4 qubits, starting from a generalization of the $2 \otimes 4$ bound entangled state introduced by Horodecki [Hor97]. Then, we discuss some directions in which the conjecture we posed in Section 3.3; *i.e.*; that all $4-$qubit PPT symmetric states of ranks $(5, 7, 7)$ are generically separable, can be addressed.

Constructing four-qubit PPT entangled symmetric states

Definition 3.27. *The $2 \otimes 4$ bound entangled state introduced by Horodecki is given by [Hor97]*

$$\rho_b := \frac{1}{7b+1} \begin{pmatrix} b & \cdot & \cdot & \cdot & \cdot & b & \cdot & \cdot \\ \cdot & b & \cdot & \cdot & \cdot & \cdot & b & \cdot \\ \cdot & \cdot & b & \cdot & \cdot & \cdot & \cdot & b \\ \cdot & \cdot & \cdot & b & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \frac{1+b}{2} & \cdot & \cdot & \frac{\sqrt{1-b^2}}{2} \\ b & \cdot & \cdot & \cdot & \cdot & b & \cdot & \cdot \\ \cdot & b & \cdot & \cdot & \cdot & \cdot & b & \cdot \\ \cdot & \cdot & b & \cdot & \frac{\sqrt{1-b^2}}{2} & \cdot & \cdot & \frac{1+b}{2} \end{pmatrix}, \tag{3.54}$$

where, for clarity, zeroes are denoted by $\cdot$ and b is a real parameter ranging from $0 \leq b \leq 1$.

Let us first briefly recall the motivation of Definition 3.27:
Consider the vectors

$$|\Psi_i\rangle := \frac{1}{\sqrt{2}} \left(|0\rangle|i\rangle + |1\rangle|i+1\rangle \right), \quad i = 0 \ldots 2 \tag{3.55}$$

and

$$|\Phi_b\rangle := \frac{1}{\sqrt{2}}|1\rangle\left(\sqrt{1-b}|0\rangle + \sqrt{1+b}|3\rangle\right). \tag{3.56}$$

It is easy to see that the state $\rho_{\text{insep}} := \frac{2}{7}\sum_{i=0}^{2}|\Psi_i\rangle\langle\Psi_i| + \frac{1}{7}|0,3\rangle\langle 0,3|$ does not have positive partial transposition, so it is clearly not separable. Now we mix it with a projector on $|\Phi_b\rangle$ to obtain the family of states

$$\rho_b := \frac{7b}{7b+1}\rho_{\text{insep}} + \frac{1}{7b+1}|\Phi_b\rangle\langle\Phi_b|. \tag{3.57}$$

It is easily seen that ρ_b is a PPT state, and the way to see it is to observe that $\rho_b^T = (\mathbb{1}_2 \otimes U)\rho_b(\mathbb{1}_2 \otimes U)^\dagger$, where U is a unitary matrix only with ones in the antidiagonal. Using the range criterion, Horodecki showed that ρ_b is entangled for $b \in (0,1)$.

Let us now generalize this construction to the $2 \otimes d$ case. We consider the vectors

$$|\Psi_i\rangle := \frac{1}{\sqrt{2}}\left(|0\rangle|i\rangle + |1\rangle|i+1\rangle\right), \quad i = 0 \ldots d-2 \tag{3.58}$$

and

$$|\Phi_b\rangle := \frac{1}{\sqrt{2}}|1\rangle\left(\sqrt{1-b}|0\rangle + \sqrt{1+b}|d-1\rangle\right), \tag{3.59}$$

so we can define the families of states

$$\rho_{\text{insep}}^d := \frac{2}{2d-1}\sum_{i=0}^{d-2}|\Psi_i\rangle\langle\Psi_i| + \frac{1}{2d-1}|0,d-1\rangle\langle 0,d-1| \tag{3.60}$$

and

$$\rho_{d,b} := \frac{b}{b+1}\rho_{\text{insep}}^d + \frac{1}{(2d-1)b+1}|\Phi_b\rangle\langle\Phi_b|. \tag{3.61}$$

Clearly, for $d = 4$ we recover the states introduced in [Hor97].

Theorem 3.28. *The states $\rho_{d,b} \in \mathcal{D}(\mathbb{C}^2 \otimes \mathbb{C}^d)$ defined in Eq. (3.61) are PPT for $d \geq 2$ and $b \in [0,1]$.*

Proof. In matrix form, Eq. (3.61) reads

$$\rho_{d,b} = \frac{1}{(2d-1)b+1}\begin{pmatrix} b\mathbb{1}_d & bD_{\text{upper}} \\ D_{\text{lower}} & C \end{pmatrix}, \tag{3.62}$$

where D_{upper} and D_{lower} are $d \times d$ dimensional matrices, with just ones in its upper or lower diagonal, respectively, and $C \in M_d$ is given by

$$C = \frac{1}{2}\begin{pmatrix} 1+b & 0 & \dots & 0 & \sqrt{1-b^2} \\ 0 & 2b & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 2b & 0 \\ \sqrt{1-b^2} & 0 & \dots & 0 & 1+b \end{pmatrix}. \tag{3.63}$$

The partial transposition of $\rho_{d,b}$ with respect to $\mathbb{C}^2$ reads

$$\rho_{d,b}^{T_A} = \frac{1}{(2d-1)b+1}\begin{pmatrix} b\mathbb{1}_d & bD_{\text{lower}} \\ D_{\text{upper}} & C \end{pmatrix}. \tag{3.64}$$

Consider now the unitary matrix U formed just by ones in its antidiagonal. It is immediate to check that $UD_{\text{upper}}U^\dagger = D_{\text{lower}}$, $UD_{\text{lower}}U^\dagger = D_{\text{upper}}$ and $UCU^\dagger = C$. Hence, the identity

$$\rho_{d,b}^{T_A} = (\mathbb{1}_2 \otimes U)\rho_{d,b}(\mathbb{1}_2 \otimes U)^\dagger \tag{3.65}$$

holds, which means that $\rho_{d,b}^{T_A} \succeq 0$ if, and only if, $\rho_{d,b} \succeq 0$. □

Theorem 3.29. *The states $\rho_{d,b} \in \mathcal{D}(\mathbb{C}^2 \otimes \mathbb{C}^d)$ defined in Eq. (3.61) are entangled for $d \geq 4$ and $b \in (0,1)$. They are separable for $d = 2, 3$, as well as for $b = 0$ or $b = 1$.*

Proof. Let us start by proving that for $d \geq 4$ and $b \in (0,1)$, the states in Eq. (3.61) are entangled. To this purpose, we also use the range criterion introduced in [Hor97]. We briefly recall it in order to use it in the proof:

If ρ is separable, then there is a set of product vectors $\{|e_i, f_i\rangle\}_i$ spanning $\operatorname{Im}\rho$ such that $\{|e_i^*, f_i\rangle\}_i$ span $\operatorname{Im}\rho^{T_A}$.

All the product vectors in $\operatorname{Im}\rho_{d,b}$ are given by the uni-parametric family

$$(1,\alpha) \otimes (\alpha^{d-1} + y, \alpha^{d-2}, \dots, \alpha, 1), \qquad \alpha \in \mathbb{C} \cup \{\infty\}, \tag{3.66}$$

where $y := \sqrt{(1-b)/(1+b)}$. Let us remark that when $\alpha = \infty$ the state (3.66) corresponds to the product vector $(0,1) \otimes (1,0,\dots,0)$, which is also in the range of $\rho_{d,b}$. The vectors in Eq. (3.66) span $\operatorname{Im}\rho_{d,b}$.

On the other hand, all the vectors in $\mathrm{Im}\,\rho_{d,b}^{T_A}$ are given by the family

$$(a_1, \ldots, a_{d-1}, ya_1 + a_d; a_2, a_3, \ldots, a_d, a) \tag{3.67}$$

with a, a_i being complex numbers. Hence, we have to study if, when partially conjugating a vector from (3.66) it belongs to $\mathrm{Im}\,\rho_{d,b}^{T_A}$ (*i.e.*, it takes the form (3.67)). This is equivalent to solving the system of equations

$$\begin{aligned} \alpha(1-|\alpha|^2) &= 0 && (3.68)\\ \alpha^*(\alpha^{d-1}+y) &= \alpha^{d-2} && (3.69)\\ y(y+\alpha^{d-1}) &= 1+|\alpha|^2. && (3.70) \end{aligned}$$

However, this system is incompatible: if $\alpha = 0$, the third equation is not fulfilled, because $y \neq 1$ and, if $|\alpha|^2 = 1$, the second equation is not fulfilled, because $y \neq 0$. The argument for $(0,1) \otimes (1,0,\ldots,0)$ goes along the same lines. Hence, $\rho_{d,b}$ is entangled for $d \geq 4$ and $b \in (0,1)$.

Let us now prove the separability of the remaining cases. If $d = 2$ or 3, then $\rho_{d,b}$ acts on $\mathbb{C}^2 \otimes \mathbb{C}^2$ or $\mathbb{C}^2 \otimes \mathbb{C}^3$. Since Theorem 3.28 guarantees that $\rho_{d,b}$ is PPT and the PPT criterion is necessary and sufficient in this case, $\rho_{d,b}$ is separable.

If $b = 0$, then Eq. (3.61) says that $\rho_{d,0} = |\Phi_0\rangle\langle\Phi_0|$, which is separable. Finally, if $b = 1$, $\rho_{d,1}$ can be written in the following form [Hor97]:

$$\rho_{d,1} = \frac{1}{16\pi}\int_0^{2\pi} P_\varphi \otimes Q_\varphi \mathrm{d}\varphi, \tag{3.71}$$

where P_φ is the projector onto $|0\rangle + e^{\mathbb{i}\varphi}|1\rangle$ and Q_φ is the projector onto $\sum_{k=0}^{d-1} e^{-\mathbb{i}k\varphi}|k\rangle$, so it is separable as well. □

Remark 3.30. It follows from the proof of Theorem 3.29 that $\rho_{d,b}$ are edge states for $d \geq 0$ and $b \in (0,1)$.

Finally, we point out that the action of $(\mathbb{1}_2 \otimes U)$ does not change the rank of the state, which is $d+1$, so there are $d-1$ vectors in the kernel of the state:

Theorem 3.31. $\mathrm{rank}\rho_{d,b} = \mathrm{rank}\rho_{d,b}^{T_A} = d+1$.

Proof. The following vectors belong to $\ker \rho_{d,b}$ and are given by

$$|\Phi_i\rangle \propto |0,i\rangle - |1,i+1\rangle, \quad i = 1,\ldots,d-2 \tag{3.72}$$

$$|\Phi_{d-1}\rangle \propto -\sqrt{1+b}|00\rangle + \sqrt{1-b}|0,d-1\rangle + \sqrt{1+b}|11\rangle. \tag{3.73}$$

These vectors span a $d-1$ dimensional subspace. On the other hand, as pointed out in the proof of Theorem 3.29, the product vectors defined in Eq. (3.66) span a $d+1$-dimensional subspace. Hence, the rank of $\rho_{d,b}$ is $d+1$. Since the relation $\rho_{d,b}^{T_A} = (\mathbb{1}_2 \otimes U)\rho_{d,b}(\mathbb{1}_2 \otimes U)^\dagger$ holds, both of them have the same rank. □

We have now characterized and studied the properties of the states $\rho_{d,b}$ defined in Eq. (3.61). We shall show now how they can be used to generate PPT symmetric entangled states. We start by applying a full-rank transformation given by $F = \mathbb{1}_d - y|0\rangle\langle d-1|$ to the $\mathbb{C}^d$ subsystem. The resulting state is the unnormalized positive semi-definite operator

$$\rho'_{d,b} = (\mathbb{1}_2 \otimes F)\rho_{d,b}(\mathbb{1}_2 \otimes F^\dagger). \tag{3.74}$$

The product vectors in the range of $\rho'_{d,b}$ are almost the same as in Eq. (3.61):

$$(1,\alpha) \otimes (\alpha^{d-1}, \alpha^{d-2}, \ldots, \alpha, 1), \qquad \alpha \in \mathbb{C} \cup \{\infty\}. \tag{3.75}$$

This particular form of the product vectors in Eq. (3.75) allows us to map $\rho'_{d,b}$ to a symmetric n-qubit state in a simple way: In order to introduce extra parameters while keeping the PPT property, we map the state $\rho'_{d,b}$ to a smaller space $\mathbb{C}^2 \otimes \mathbb{C}^{d'}$. By considering the non-singular $d' \times d$ matrix (with $d' < d$)

$$F_2 := \sum_{i=0}^{d'} \sum_{j=0}^{d-d'} \gamma_j |i\rangle\langle i+j|, \tag{3.76}$$

where $\gamma_j \in \mathbb{C}$. Thus, the state $\rho''_{d,b} := (\mathbb{1}_2 \otimes F_2)\rho'_{d,b}(\mathbb{1}_2 \otimes F_2)^\dagger$ have $d - d' + 1$ additional parameters. The particular form of (3.76) is such that new parameters γ_j are introduced, although the product vectors in $\operatorname{Im} \rho''_{d,b}$ have the form (3.75). Because F and F_2 are local operations edgeness is preserved.

In the spirit of the transformations F_n and G_n defined in Section 3.1.3, we apply another local operation on the second subsystem, which we denote V, such that $V : (\alpha^{d-1}, \ldots, \alpha, 1) \mapsto (1, \alpha)^{\otimes(d-1)}$. V has full rank because all powers of α appear, so it can be inverted. This is how a $(n = d')$-qubit symmetric state is obtained: $\omega_n := (\mathbb{1}_2 \otimes V)\rho''_{d,b}(\mathbb{1}_2 \otimes V)^\dagger \in \mathcal{D}_{\mathcal{S}}^{\mathrm{PPT,A}}(\mathbb{C}^2)^{\otimes n}$. Note that, by construction, all one-vs-rest partial transpositions are positive.

As a result of the application of the three filters F, F_2 and V, we get a PPT symmetric state with respect to the $1|n-1$ partition. However, it needs not be the case for other partitions. To ensure full PPT-ness we add a fully PPT state such as $P_{\mathbf{A}}/(n+1)$; *i.e.*, the projector onto the symmetric space defined in Eq. (3.7). This way, we find a fully PPT state $\omega_{n,\lambda} :\propto \omega_n + \lambda P_{\mathbf{A}}$ for λ sufficiently large. Clearly, there exists the smallest $\lambda \geq 0$ for which $\omega_{n,\lambda}$ is PPT, which we denote λ_*. Although the rank of the state is preserved, in this way one could destroy the entanglement present in ω_n, as we increase all the ranks $\vec{r}_{\mathbf{A}}$. To lower them, we search for product vectors $|e\rangle^{\otimes n} \in \mathcal{D}(\mathbb{C}^2)^{\otimes n}$ such that its partial conjugations C_S fulfill $(|e\rangle^{\otimes n})^{C_S} \in \operatorname{Im} \omega_{n,\lambda_*}^{T_S}$ for all $S \subseteq \mathbf{A}$. If this $|e\rangle$ exists, we consider a state $\tilde{\omega}_{n,\lambda_*} :\propto \omega_{n,\lambda_*} - \mu|e\rangle\langle e|^{\otimes n}$. Clearly, there exists a smallest μ for which one of the ranks of $\tilde{\omega}_{n,\lambda}$ is lower than those of ω_{n,λ_*}, and we denote it μ_*. This procedure is repeated until such $|e\rangle$ is not found, the resulting state is edge.

In particular, we apply the provided method to obtain a family of PPTESS for $n = 4$. To this end, we introduce $\rho'_{5,b} = (\mathbb{1}_2 \otimes F)\rho_{5,b}(\mathbb{1}_2 \otimes F)^\dagger$ and we add two extra parameters γ_1 and γ_2 by means of the local filter F_2, which is a 4×5 matrix and afterwards we apply the filter V. The particular choice of parameters $b = 1/2$, $\gamma_1 = \gamma_2^{-1} = 1/\sqrt{2}$ leads to a state ω_4 which is PPT with respect to the $A|BCD$ bipartition, wereas $\omega_4^{T_{AB}} \not\geq 0$. To cover the negative eigenvlues of $\omega_4^{T_{AB}}$ we add P_4, the projector onto the symmetric space of 4 qubits and consider $\omega_{4,\lambda} \propto \omega_4 + \lambda P_4$. The smallest λ for which $\omega_4^{T_{AB}} \succeq 0$ has to be found with the aid of numerics, and it is $\lambda_* \approx 0.94842$. For ω_{4,λ_*}, its $\vec{r}_{\mathbf{A}}$ is $(5, 8, 8)$. Again, by using numerics, we are able to find a qubit vector $|e\rangle \propto (1, \alpha)$ with $\alpha \approx 7 + 38.52091\mathbb{i}$ (there are infinitely many α's) such that $|e\rangle^{\otimes 4} \in \operatorname{Im} \omega_{4,\lambda_*}$, $|e^*\rangle|e\rangle^{\otimes 3} \in \operatorname{Im} \omega_{4,\lambda_*}^{T_A}$ and $|e^*\rangle^{\otimes 2}|e\rangle^{\otimes 2} \in \operatorname{Im} \omega_{4,\lambda_*}^{T_{AB}}$. For this state, we subtract a projector onto $|e\rangle^{\otimes 4}$ and arrive at $\tilde{\omega}_{4,\lambda_*,\mu_*} \propto \omega_{4,\lambda_*} - \mu_*|e\rangle\langle e|^{\otimes 4}$ with $\mu_* \approx 0.64625$. The state $\tilde{\omega}_{4,\lambda_*,\mu_*}$ has ranks $\vec{r}_{\mathbf{A}} = (5, 7, 8)$ and with the aid of the algorithm

described in Section 3.2.2 we check that it is extremal, so it is both edge and entangled. Let us just point out that the choice of parameters (b, γ_1, γ_2) was completely arbitrary and other choices also lead to PPTESS, such as $(b, \gamma_1, \gamma_2) = (1/6, 3/8, 11/23)$.

The $(5, 7, 7)$ case

In this last section we analyze the case of four-qubit PPT symmetric states with $\vec{r}_{\mathbf{A}} = (5, 7, 7)$ and provide directions in which one might prove that such states are generically separable, as numerics suggest (*c.f.* Table 3.2). The approach we present is based on the methodology introduced in [SKL07].

We start by noting that any $\rho \in \mathcal{D}(\mathcal{H})$ can be written as

$$\rho = \sum_{k=1}^{l} |\psi_k\rangle\langle\psi_k|, \tag{3.77}$$

where $|\psi_k\rangle$ have norm at most 1. A particular decomposition of the form (3.77) is the eigendecomposition, but we are not assuming that $|\psi_k\rangle$ are orthogonal vectors.

Let us denote by $|e_k\rangle$ an orthonormal basis of $\mathcal{H}$. Every element of ρ, in the basis e is written, in terms of the ψ_k, as

$$\langle e_i|\rho|e_j\rangle = \sum_{k=1}^{l} \langle e_i|\psi_k\rangle\langle\psi_k|e_j\rangle, \tag{3.78}$$

and can be rewritten as the scalar product of two vectors $|v_i\rangle$, $|v_j\rangle$ which are defined as

$$|v_i\rangle := \left(\langle\psi_1|e_i\rangle, \ldots, \langle\psi_l|e_i\rangle\right)^T, \qquad 1 \leq i \leq \dim \mathcal{H}. \tag{3.79}$$

Hence, a quantum state ρ is just the Gram matrix of the set of vectors $|v_i\rangle$, also called a Gram system of ρ. This decomposition is not unique, as the set of vectors $U|v_i\rangle$ for any unitary U leads to the same ρ.

We proceed now to finding a Gram system of a PPT symmetric state ρ of ranks $(5, 7, 7)$ and study the relation within the Gram systems of ρ^{T_A}, ρ^{T_B}

and $\rho^{T_{AB}}$. Due to the fact that $r_A = 7$, ρ^{T_A} can be decomposed into seven rank-one components, namely

$$\rho^{T_A} = \sum_{k=1}^{7} |\Psi_k\rangle\langle\Psi_k|, \tag{3.80}$$

where $\langle\Psi_k|\Psi_k\rangle < 1$. Because each of the $|\Psi_k\rangle$ acts on $\mathbb{C}^2 \otimes \mathcal{S}((\mathbb{C}^2)^{\otimes 3})$, any Gram system of ρ^{T_A} consists of eight seven-dimensional vectors which we denote $|a\rangle \ldots |d\rangle, |\tilde{a}\rangle, \cdots |\tilde{d}\rangle \in \mathbb{C}^7$, whose explicit form is

$$a_k = \langle\Psi_k|0000\rangle,\ d_k = \langle\Psi_k|0111\rangle,\ \tilde{a}_k = \langle\Psi_k|1000\rangle,\ \tilde{d}_k = \langle\Psi_k|1111\rangle,$$

$$\begin{aligned} b_k &= \langle\Psi_k|0001\rangle = \langle\Psi_k|0010\rangle = \langle\Psi_k|0100\rangle \\ \tilde{b}_k &= \langle\Psi_k|1001\rangle = \langle\Psi_k|1010\rangle = \langle\Psi_k|1100\rangle \\ c_k &= \langle\Psi_k|0011\rangle = \langle\Psi_k|0110\rangle = \langle\Psi_k|0101\rangle \\ \tilde{c}_k &= \langle\Psi_k|1011\rangle = \langle\Psi_k|1110\rangle = \langle\Psi_k|1101\rangle. \end{aligned}$$

In matrix form, ρ^{T_A} can be written as

$$\rho^{T_A} = \begin{pmatrix} A^\dagger & B^\dagger & \tilde{B}^\dagger & \tilde{C}^\dagger \end{pmatrix} \begin{pmatrix} A \\ B \\ \tilde{B} \\ \tilde{C} \end{pmatrix} = \begin{pmatrix} A^\dagger A & A^\dagger B & A^\dagger \tilde{B} & A^\dagger \tilde{C} \\ B^\dagger A & B^\dagger B & B^\dagger \tilde{B} & B^\dagger \tilde{C} \\ \tilde{B}^\dagger A & \tilde{B}^\dagger B & \tilde{B}^\dagger \tilde{B} & \tilde{B}^\dagger \tilde{C} \\ \tilde{C}^\dagger A & \tilde{C}^\dagger B & \tilde{C}^\dagger \tilde{B} & \tilde{C}^\dagger \tilde{C} \end{pmatrix}, \tag{3.81}$$

where A is a a 7×4 matrix whose columns are $|a\rangle, |b\rangle, |b\rangle$ and $|c\rangle$, and similarly $B = (|b\rangle, |c\rangle, |c\rangle, |d\rangle)$, $\tilde{B} = (|\tilde{a}\rangle, |\tilde{b}\rangle, |\tilde{b}\rangle, |\tilde{c}\rangle)$ and $\tilde{C} = (|\tilde{b}\rangle, |\tilde{c}\rangle, |\tilde{c}\rangle, |\tilde{d}\rangle)$. Note that each block in Eq. (3.81) is a 4×4 matrix. For short, we denote $\rho^{T_A} = [A, B, \tilde{B}, \tilde{C}]$.

The same construction can be applied to ρ and we will get a decomposition of the form $\rho = [A', B', B', C]$, because ρ is fully symmetric. If we now project the first subsystem of ρ and ρ^{T_A}, we shall get the same $3-$qubit matrices ($\langle 0|_A \rho |0\rangle_A = \langle 0|_A \rho^{T_A} |0\rangle_A$), so that they will have the same Gram systems. Hence, there exists a unitary U that relates both Gram systems: $A' = UA$ and $B' = UB$. As we have previously argued, Gram systems are related by unitaries, so we can assume, without loss of generality, that $A' = A$ and $B' = B$. Now, by projecting the first subsystem onto $|1\rangle$ (*i.e.*,

$\langle 1|_A \rho |1\rangle_A = \langle 1|_A \rho^{T_A} |1\rangle_A$) we obtain additional relations, namely $\tilde{B} = UB$ and $\tilde{C} = UC$ for some unitary U. Therefore, we can relate the two Gram decompositions as

$$\rho = [A, B, B, C] \iff \rho^{T_A} = [A, B, UB, UC]. \tag{3.82}$$

The previous equation implies the following relations which restrict which U can be used:

$$A^\dagger UB - B^\dagger A = A^\dagger C - B^\dagger B = B^\dagger UB - C^\dagger A = B^\dagger UC - C^\dagger B = 0, \tag{3.83}$$

where $0 \in M_4$ is the zero matrix.

A similar reasoning applies to ρ^{T_B} and $\rho^{T_{AB}}$, which can be represented as

$$\rho^{T_B} = [A, UB, B, UC], \quad \rho^{T_{AB}} = [A, UB, VB, VUC], \tag{3.84}$$

where $U, V \in \mathcal{U}_7$ fulfill $UB = VB$. Then, by comparing the representations of ρ^{T_B} and $\rho^{T_{AB}}$ with the partial transposition with respect to A, further conditions are obtained:

$$\begin{aligned} A^\dagger VB - B^\dagger A = A^\dagger VUC - B^\dagger UB \\ = B^\dagger U^\dagger VB - C^\dagger U^\dagger A = B^\dagger U^\dagger VUC - C^\dagger B = 0. \end{aligned} \tag{3.85}$$

Having the Gram systems of ρ and its partial transpositions, let $|\Psi_k\rangle$ and $|\Phi_k\rangle$ be the Gram decompositions of ρ^{T_B} and $\rho^{T_{AB}}$, respectively. Adding an additional ancillary system, denoted a, we introduce the following Q matrix:

$$Q :\propto \sum_{k=1}^{7} (|0\rangle|\Psi_k\rangle + |1\rangle|\Phi_k\rangle)(\langle 0|\langle \Psi_k| + \langle 1|\langle \Phi_k|), \tag{3.86}$$

which, in terms of the Gram systems introduced above, takes the form

$$Q = [A, UB, B, UC; A, UB, VB, VUC]. \tag{3.87}$$

The Q matrix effectively acts on $\mathbb{C}^7 \otimes \mathbb{C}^3$, with respect to the bipartition $aAB|CD$ (it suffices to count dimensions: CD act on the symmetric space of 2 qubits, which is three-dimensional). By definition, Q has rank 7. Hence, if it were supported on $\mathbb{C}^7 \otimes \mathbb{C}^3$ and $Q^{T_{aAB}} \succeq 0$, it would be separable with respect to the $aAB|CD$ bipartition, as implied by the results in

[Hor+00]. We cannot prove this condition for any ρ, although, generically, Q is supported on $\mathbb{C}^7 \otimes \mathbb{C}^3$.

After some algebra, one checks that a sufficient condition for $Q^{T_{aAB}} \succeq 0$ is that

$$B^\dagger VUC - C^\dagger UB = C^\dagger U^\dagger VUC - C^\dagger UC = 0, \tag{3.88}$$

where $0 \in M_4$ is the zero matrix. The explicit form of B and C helps in simplifying the former conditions, which lead to a set of equations for the scalar product of vectors that compose the Gram system of ρ. Some of them are automatically satisfied by virtue of Eqs. (3.83) and (3.85). If the remaining equations hold, then $Q^{T_{aAB}} \succeq 0$, so Q is generically separable.

The original ρ is recovered by projecting the auxiliary qubit a onto $|0\rangle$. Hence, if Q is separable across the $aAB|CD$ bipartition, ρ is also separable across the $AB|CD$ bipartition and, because $\rho \in \mathcal{D}_{\mathcal{S}}^{\mathrm{PPT}}(\mathbb{C}^2)^{\otimes 4}$, Theorem 3.1 implies it is fully separable.

n	r_0	r_1	r_2	r_3	r_4	r_5	r_6	r_7	r_8	r_9	r_{10}	r_{11}
4	5	7 (-1)	8 (-1)									
5	6	10	10 (-2)									
6	7	12	14 (-1) 14 (-1)	14 (-2) 13 (-3)								
7	8	14	18	18 (-2)								
8	9	16	21	23 (-1) 23 (-1)	23 (-2) 22 (-3)							
9	10	18	24	28	28 (-2)							
10	11	20	27	32	34 (-1) 34 (-1) 35 (+0)	33 (-3) 34 (-2) 32 (-4)						
11	12	22	30	36	40	40 (-2)						
12	13	24	33	40	45	47 (-1) 47 (-1) 48 (+0)	47 (-2) 46 (-3) 45 (-4)					
13	14	26	36	44	50	54	54 (-2)					
14	15	28	39	48	55	60	62 (-1) 62 (-1) 63 (+0)	62 (-2) 61 (-3) 60 (-4)				
15	16	30	42	52	60	66	70	70 (-2)				
16	17	32	45	56	65	72	77	79 (-1) 79 (-1) 80 (+0)	79 (-2) 78 (-3) 77 (-4)			
17	18	34	48	60	70	78	84	88	88 (-2)			
18	19	36	51	64	75	84	91	96	98 (-1) 98 (-1) 99 (+0)	98 (-2) 97 (-3) 96 (-4)		
19	20	38	54	68	80	90	98	104	108	108 (-2)		
20	21	40	57	72	85	96	105	112	117	119 (-1) 119 (-1) 120 (+0)	119 (-2) 118 (-3) 117 (-4)	
21	22	42	60	76	90	102	112	120	126	130	130 (-2)	
22	23	44	63	80	95	108	119	128	135	140	142 (-1) 142 (-1) 143 (+0)	142 (-2) 141 (-3) 140 (-4)
23	24	46	66	84	100	114	126	136	144	150	154	154 (-2)

Table 3.2.: Here we collect the ranks of extremal states found by using the algorithm described in Sec. 3.2.2. The first column contains the number of qubits, while the next columns correspond to the ranks of $\rho_{\mathbf{A}}$ and its partial transpositions $r_i := r_{|\mathbf{A}|=i}$ $(i = 1, \ldots, \lfloor n/2 \rfloor)$. Notice that there are no PPT entangled states with $n < 4$ [Eck+02] (cf. Sec. 3.1.1). The negative numbers in parentheses denote the difference between the given rank and its maximal value (the lack of parentheses stands for the maximal rank). For $n \equiv 0 \mod 2$ we have found, at most, three possible configurations of ranks, and, interestingly, in the case of $n \equiv 1 \mod 2$ we have found only one such configuration.

4. Nonlocality in Multipartite Quantum States

Correlations that go beyond the paradigm of local realism (*i.e.*, those that do not admit a Local Hidden Variable Model (LHVM)[1]) are referred to as nonlocal. Bell's theorem [Bel64] shows that correlations between the outcomes of certain measurements performed to some quantum states can be nonlocal[2]. Bell's nonlocality is detected *via* the so-called Bell's inequalities, which serve as certificates that correlations do not admit a LHVM. These are -often linear- inequalities that are formulated in terms of the probabilities that arise from performing local measurements on a shared resource, such as a quantum state. Violation of a single Bell inequality, the typical example being the Clauser-Horne-Shimony-Holt (CHSH) inequality [Cla+69], signals that those correlations do not admit a LHVM.

Bell nonlocality has three interesting aspects that are worth highlighting. First, it is a *resource* for several Quantum Information Processing (QIP) tasks [Bar+05]. Examples of them are Device-Independent Quantum Key Distribution (DIQKD) [Pir+13], Certified Quantum Random Number Generation (CQRNG) [Pir+10], Randomness Amplification (RA) [CR12], Dimensionality Witnessing (DW) [Gal+10], and many other tasks that fall into the Device-Independent (DI) paradigm (see Section 2.2.1). Hence, being able to reveal the nonlocality of a composite quantum system is a central problem in QIP, and it is going to be one of the crucial problems of future quantum technologies.

Second, it is tightly related to a more philosophical aspect of quantum physics [Bel04; Gis14]. For instance, the *free will* problem is of relevance, as

[1] These correlations are often referred to as classical, local or Einstein-Podolsky-Rosen (EPR) [EPR35]. Throughout this Thesis, we use these terms indistinctively to indicate that correlations can be explained *via* a LHVM.

[2] The term nonlocal is often used in many-body systems to refer to, *e.g.*, the range of interactions. In this Thesis, the term nonlocal will refer to Bell's nonlocality, unless stated otherwise.

the measurement settings that should be used in a Bell experiment should be chosen freely[3]; however, the only way we have to certify the existence of intrinsic randomness -assuming the No-Signalling (NS) principle- is through nonlocal correlations, so that we need to perform another Bell experiment in the first place in order to guarantee that the choice of measurement settings is indeed *free*. We can think that we -as entities that possess free will to some extent[4]- can freely choose the measurements in the first place; however one can never rule out a super-deterministic scenario in which there is no randomness whatsoever and everything is predetermined[5].

Thus, guaranteeing the LHVM assumptions is not as simple as it might look like. A definitive Bell experiment has not yet been performed in the laboratory, for one has to be careful with the so-called loopholes. One can violate Bell inequalities with classical resources if loopholes are left open. The most relevant of them are the detection loophole and the locality loophole. The problem with the detection loophole is as follows: If one has an imperfect detector, like a photon counter that may give dark counts, may not click when it receives a photon, etc., one can exploit it to *not give an answer* when it does not like the question that it has been asked (when the measurement settings are inconvenient for violating a Bell inequality). In this way, one can fake a Bell inequality violation. The locality loophole appears when the parties are not enough far apart (space-like separated) to ensure that there could not be any form of communication between them in the process of measuring. There are many physical systems in which only one of these two loopholes can be easily closed. Since systems such as trapped ions have high detection efficiency, but low separation, the first loophole is closed, but the second is left open. On the other hand, since systems such as photons have low detection efficiency, although they can be

[3] Or, at least, they should be independent from the state of the system, which we describe with a *hidden variable* λ.

[4] As we shall see in Section 6.3.2, *free will* (what we mathematically quantify as the degree of independence between measurement settings and the state of the system) can be amplified; *i.e.*, one can increase the quality of the randomness used in a Bell experiment, provided that the initial randomness is good enough.

[5] In that case, one can never escape the circular argument that, in order to obtain certified randomness by violating a Bell inequality, one would need certified randomness in the first place to run the Bell experiment and choose the measurements. This choice could be done *via* another Bell experiment, that would need certified randomness to choose its inputs, etc.

sent very far apart, the first loophole is open, although the second is closed. Closing both at the same time is an extremely challenging task, although very recent advances, using Nitrogen-Vacancy (NV)-centers in diamond, show that this goal might be reached in the coming months [Pfa+14].

Third, the mathematical complexity of characterization of quantum nonlocality makes it an extremely challenging task. Deciding membership in the set of local (also called EPR) correlations is an NP-complete task [BFL91; Bru+14]. Even worse, finding all Bell inequalities for a given Bell scenario (n, m, d) with n parties, m measurements and d outcomes is NP-hard; a task of doubly exponential complexity [Cha93], see also Section 2.2.2.

Bell nonlocality is deeply related with entanglement, a connection that we address in Chapter 5. The most general result between these two concepts says that any quantum state that violates a Bell inequality must necessarily be entangled. However, the converse is not true in general. In [Gis91] it was proven that any pure bipartite entangled state violates a Bell inequality, a result that was generalized to the multipartite case [PR92]. However, for the case of mixed states, the connection is much more subtle, as there are bipartite entangled mixed states that will never violate a Bell inequality, both when using projective measurements [Wer89] or POVMs [Bar02]. We shall see in Chapter 5 that entanglement and nonlocality are inequivalent for any number of parties, in the sense that there exist Genuinely Multipartite Entangled (GME) states that do not display Genuinely Multipartite Nonlocal (GMN).

In spite of being a weaker property than nonlocality, during the last decade entanglement has been a very useful tool to characterize properties of many-body systems, as well as to identify when a Quantum Phase Transition (QPT) occurs and its properties[6].

[6] Take, for instance, lattice spin models that are described by local (here *local* stands for finite interaction range, or interactions that decay rapidly with the distance) Hamiltonians. In the ground states of such models (the states with the lowest energy), the following properties are true (see [Tur+15a; Tur+15b] and references therein, such as [ECP10]):

1. The reduced density matrix of two spins typically displays entanglement if the spins are close in distance, even at criticality. However, entanglement measures still show signatures of QPTs.

2. One can also try to perform optimized measurements on the rest of the system, in

It is then natural to wonder about the role of nonlocality in many-body systems. More specifically, whether it also plays an important role in characterizing correlations in them. This is a question that has interest *per se*; however, apart from its fundamental interest, it has hardly been explored. Although every ground state of a generic many-body Hamiltonian is pure and entangled and, because every pure entangled state violates a Bell inequality, it is also a nonlocal state, its nonlocality is almost impossible to verify in an experiment: the Bell inequalities that are known for that [Aol+12; BGP10; ŻB02] typically include correlation functions involving products of observables from all parties. Although performing a Bell experiment with one of these inequalities is, in principle, possible, in practice it turns out to be a Herculean task, for it presents several technical challenges: first, parties must be addressed individually and one has to prepare a different measurement for each party, so that a high degree of individual control is required; second, the number of correlators appearing in such inequalities can be exponentially large, $O(m^n)$, so that one would have to estimate the probabilities of an exponentially big number of events, severely maiming the possibility to investigate this issue in a many-body

order to concentrate entanglement in two chosen spins. This is the idea behind the concept of *localizable entanglement*. At standard QPTs, the entanglement length diverges as the correlation length diverges. However, there exist critical systems for which the correlation length remains finite, whereas the entanglement localization length diverges to infinity.

3. For systems that are not at criticality, the low energy states -ground states- exhibit area laws: the entropy (von Neumann or, more generally, Rényi) of the reduced density matrix corresponding to a block scales as the length of the boundary of the block. At criticality, one often needs to apply a logarithmic correction to the growth. If the system is 1-dimensional, these are well studied results; however higher-dimensional cases are full of open questions.

4. Ground states and states that appear as low energy states of physical Hamiltonians can be efficiently described with Matrix Product States (MPS) and, more generally, tensor network techniques.

5. The spectrum of the logarithm of a reduced density matrix of a block is typically referred to as *entanglement spectrum*. Topological order is typically exhibited in its properties for gapped one- and two-dimensional systems; in 2D, the appearance of the so-called *topological entropy* gives a negative constant correction to the area laws.

Most of these results also hold for lattice Bose and Fermi models; even for quantum field theories.

system with large n. Instead, the typical quantities that one has access to in a many-body experiment are few-body correlations; often one- and two-body. Hence, the question that is physically relevant is whether nonlocality detection in many-body systems is even possible using one and two-body correlations.

This problem poses several technical challenges. First, the mathematical complexity does not allow for finding all Bell inequalities for more than 3 parties in the simplest scenario [Śli03]. Second, one expects that, the higher the order (the number of parties involved) of the correlator, the more information it contains. Hence, it is easier to reveal nonlocality with Bell inequalities that involve correlators among many (or all) parties, as they are the strongest ones [BGP10; ŻB02]. There exist already Bell inequalities that do not involve full-body correlators; for example, all-except-for-one [WNŻ12] correlator Bell inequalities have been constructed. Nevertheless, we must here address a much more demanding question, namely, whether nonlocality detection is possible from the smallest amount of information[7] that is available in a Bell test: two-body correlators.

Although the answer we are going to provide is positive [Tur+14a], it is worth highlighting that we can construct states that are physically relevant (they appear as ground states of typical many-body Hamiltonians) with this property. On the other hand, such inequalities are not able to detect nonlocality in all pure entangled states. For instance, *graph states* have two-body reduced density matrices compatible with the reduced density matrices of a separable state, hence entanglement cannot be detected with two-body correlators [GHG10] (neither nonlocality can, as this is a more stringent condition). This proves that finding and classifying such quantum states is *per se* an interesting task.

In this chapter we introduce techniques for the detection of nonlocality in many-body quantum states. We focus on the derivation of Bell inequalities with one and two-body correlators which are either translationally or permutationally invariant.

The chapter is organized as follows: In Section 4.1 we characterize the structure and the construction of the local polytope of two-body correlations that are invariant under the action of a given symmetry group. In Section 4.2 we derive in detail an analytical class of permutationally sym-

[7] One can never violate a Bell inequality with one-body correlators only.

metric Bell Inequalities. In Section 4.3 we propose an analytical class of quantum states and measurements that maximally violates the inequalities described in Section 4.2. In Section 4.4, we propose an analytical class that detects the nonlocality of every entangled Dicke state. In Section 4.5 we introduce the tools to generalize the techniques used in this chapter to obtain permutationally symmetric Bell Inequalities for any scenario with k-body correlators. In Section 4.6 we study the case for translationally invariant Bell inequalities with 2-body correlators and in Section 4.7 we give some considerations from the experimental point of view.

The results presented in this Chapter are joint work with R. Augusiak, A. B. Sainz, T. Vértesi, A. Acín and M. Lewenstein [Tur+14a; Tur+14b; Tur+15b] (see also [Tur+15a]). The results of Section 4.5 are new and they have not been published yet.

4.1. The structure of the local polytope

In Section 2.2 we have already introduced the basics of nonlocality. In particular, the local polytope, which we denoted $\mathbf{P}_L$, and we analysed its complexity, which depended on the Bell scenario (n, m, d) under consideration. The aim of this section is to study the geometry of certain projections of $\mathbf{P}_L$, which will lead to Bell inequalities with some desired properties.

Description in terms of correlators

When working in a Bell scenario (n, m, d) in which the measurements have binary outcomes, *i.e.*, $d = 2$, it is more comfortable to work with correlation functions instead of the vector of probabilities $P(a_0, \ldots, a_{n-1}|x_0, \ldots, x_{n-1})$ introduced in Eq. (2.10). In such case, we name the outcomes of the observables ± 1. The expectation value of the x_i-th measurement performed by the i-th party is then given by

$$\langle \mathcal{M}_{x_i}^{(i)} \rangle := P(a_i = 1|x_i) - P(a_i = -1|x_i). \tag{4.1}$$

Similarly, for two-body correlators, one has

$$\langle \mathcal{M}_{x_i}^{(i)} \mathcal{M}_{x_j}^{(j)} \rangle := P(a_i = a_j|x_i x_j) - P(a_i \neq a_j|x_i x_j). \tag{4.2}$$

This generalizes to higher order correlators, just by taking the expectation value of the product of all the involved outcomes.

When $\vec{P}$ is no-signalling, one can express it in terms of all the marginals of the form $P_{i_1\ldots i_k}(0\ldots 0|x_{i_1}\ldots x_{i_k})$ by repeatedly using the fact that the marginals are normalized probability distributions. Equivalently, there is a one-to-one correspondence between $P(a_0,\ldots,a_{n-1}|x_0,\ldots,x_{n-1})$ and $\langle \mathcal{M}_{x_1}^{(i_1)}\cdots\mathcal{M}_{x_k}^{(i_k)}\rangle$, which is given by

$$P(a_0\ldots a_{n-1}|x_0\ldots x_{n-1}) = \frac{1}{2^n}\sum_{k=0}^{n}\sum_{0\leq i_1<\ldots<i_k<n} a_{i_1}\cdots a_{i_k}\langle \mathcal{M}_{x_{i_1}}^{(i_1)}\cdots\mathcal{M}_{x_{i_k}}^{(i_k)}\rangle, \tag{4.3}$$

where we have defined $\langle\emptyset\rangle := 1$.

Thus, in the $(n,m,2)$ scenario there is no information loss when working with correlators instead of probabilities. As Eq. (4.3) is a linear and invertible change of variables, it does not modify the geometrical properties (*e.g.* convexity, number of facets, face lattice) of $\mathbf{P}_L$.

The vertices of $\mathbf{P}_L$ now satisfy the relations

$$\langle \mathcal{M}_{x_{i_1}}^{(i_1)}\cdots\mathcal{M}_{x_{i_k}}^{(i_k)}\rangle = \langle \mathcal{M}_{x_{i_1}}^{(i_1)}\rangle\cdots\langle \mathcal{M}_{x_{i_k}}^{(i_k)}\rangle, \tag{4.4}$$

with $\langle \mathcal{M}_{x_i}^{(i)}\rangle = \pm 1$ for all i.

4.1.1. Going to a lower order correlations local polytope

As discussed in Section 2.2, both the dimension of the space in which $\mathbf{P}_L$ is embedded and its number of vertices are exponential in n, making its characterization an intractable task. By projecting it onto a much smaller dimensional affine space, we aim at obtaining a simpler object, easier to characterize. However, such simplification does not come for free, for the Bell inequalities we shall obtain will be weaker in general.

When one applies a projection π to a polytope $\mathbb{P}$, a point $\vec{P}$ can either be projected inside or outside of $\pi(\mathbb{P})$. However, if $\pi(\vec{P})$ is not inside of $\pi(\mathbb{P})$, then it must have come from some $\vec{P}$ outside of $\mathbb{P}$[8]. Hence, violating

[8] The reason is that if $\vec{P} = \sum_i \lambda_i \vec{Q}_i$, where λ_i form a convex combination and $\vec{Q}_i \in \mathbb{P}$, then $\pi(\vec{P}) = \sum_i \lambda_i \pi(\vec{Q}_i)$, where $\pi(\vec{Q}_i) \in \pi(\mathbb{P})$.

a Bell inequality for $\pi(\mathbf{P}_L)$ certifies nonlocality, whereas the correlations that can be expressed as a convex combination of the vertices of $\pi(\mathbf{P}_L)$ are left inconclusive.

There is clearly a compromise between the degree of simplification given by the projection π and the strength of the Bell inequalities that characterize $\pi(\mathbf{P}_L)$. The projections to apply will be chosen with the objective of obtaining Bell inequalities that one can readily test in an experiment. But also, for a more fundamental study, we shall tackle the question of what is the minimal amount of information needed, in terms of correlators (the simplest measurements), that can reveal nonlocality. We will be interested in two basic kinds of projections: (i) reducing the order of the correlators $\langle \mathcal{M}_{x_{i_1}}^{(i_1)} \cdots \mathcal{M}_{x_{i_k}}^{(i_k)} \rangle$ that appear in the Bell Inequality, so that measurements involving less parties need to be performed, and (ii) applying a symmetry group G such that the Bell inequality remains invariant under the action of G.

One can reduce the order of correlators to K-body: if $d = 2$, this can be done by including only those of the form $\langle \mathcal{M}_{x_{i_1}}^{(i_1)} \cdots \mathcal{M}_{x_{i_k}}^{(i_k)} \rangle$, with $k \leq K$. For a general (n, m, d) Bell scenario, this corresponds to the marginals $P_{i_1 \ldots i_k}(a_{i_1}, \ldots a_{i_k} | x_{i_1} \ldots x_{i_k})$, also for $k \leq K$. The dimension of $\mathbf{P}_L$ is reduced from $(m(d-1)+1)^n - 1$ to[9]

$$\sum_{k=1}^{K} \binom{n}{k} m^k (d-1)^k, \tag{4.5}$$

and the number of vertices is kept the same, as we shall prove in Lemma 4.1, adapting the proof of [BGP10; Tur+14b]. We denote by $\mathbb{P}_K$ the local polytope obtained by *not* including the correlators of order higher than K.

Lemma 4.1. *Let π_K be the projection that restricts $\vec{P}$ to, at most, K-body correlators. Then, for any $\vec{P} \in \mathrm{Ext}(\mathbf{P}_L)$, $\pi_K(\vec{P}) \in \mathrm{Ext}(\mathbb{P}_K)$. Moreover, $|\mathrm{Ext}(\mathbf{P}_L)| = |\mathrm{Ext}(\mathbb{P}_K)|$.*

[9] Eq. (4.5) follows from a counting argument. For a fixed correlator length k, there are $\binom{n}{k}$ ways to choose the parties involved in the correlator; then, one has to choose k measurements to perform out of m, which can be repeated as they correspond to different parties, and k times $d-1$ outcomes, because of the normalization condition that makes the last outcome redundant. When $K = n$, one recovers the general bound $(m(d-1)+1)^n - 1$.

Proof. We begin by observing that one can group the components of $\vec{P}$ in k-body marginals or correlators: $\vec{P} = \bigoplus_{k=1}^{n} \vec{P}_k$. Each $\vec{P}_k$ has dimension $\binom{n}{k} m^k (d-1)^k$ (*cf.* Eq. (4.5)). Now, π_K acts as follows: $\pi_K(\vec{P}) = \bigoplus_{k=1}^{K} \vec{P}_k$.

We shall now see how every vertex of $\mathbf{P}_L$ gets uniquely mapped to a vertex of $\mathbb{P}_K$, by explicitly constructing, for any $\vec{Q} \in \mathrm{Ext}(\mathbb{P}_K)$, a $\vec{P} \in \mathrm{Ext}(\mathbf{P}_L)$ for which $\vec{Q} = \pi_K(\vec{P})$. Such $\vec{P}$ can always be constructed, for any $K \geq 1$, because many-body probability distributions or correlators factorize at the vertices of $\mathbf{P}_L$ (*cf.* Section 2.2.2). Hence, they can always be reconstructed [BGP10] from the information present in one-body correlators, which are always present, as $K \geq 1$.

It remains to see that, for any $\vec{P} \in \mathrm{Ext}(\mathbf{P}_L)$, $\pi_K(\vec{P}) \in \mathrm{Ext}(\mathbb{P}_K)$. It is sufficient to show that, if this were not the case, then $\pi_K(\vec{P}) = \sum_i p_i \vec{Q}_i$, with $\vec{Q}_i$ being different elements of $\mathrm{Ext}(\mathbb{P}_K)$. As all coordinates of $\vec{Q}_i$ are either 0 or 1 (if we work with probabilities) or ± 1 (if $d = 2$ and we work with correlators), then there must exist at least one coordinate which is different than 0 or 1 (or -1 or 1). This contradicts the assumption that $\vec{P} \in \mathrm{Ext}(\mathbf{P}_L)$.

As a result, $\pi_K(\vec{P}) \in \mathrm{Ext}(\mathbb{P}_K) \iff \vec{P} \in \mathrm{Ext}(\mathbf{P}_L)$. It is straightforward to see, by looking at one-body correlators, that different vertices correspond to different mapped vertices; *i.e.*, $\vec{P} \neq \vec{P}' \iff \pi_K(\vec{P}) \neq \pi_K(\vec{P}')$. Hence, we arrive at $|\mathrm{Ext}(\mathbf{P}_L)| = |\mathrm{Ext}(\mathbb{P}_K)| = d^{mn}$. □

On the other hand, one can consider a group G of symmetry[10] such that the vertices of $\pi(\mathbb{P}_K)$ remain invariant under the action of G, and so will the facets. We denote this projected polytope $\mathbb{P}_K^G$. The motivation for this kind of symmetry is two-fold: first, not only further reduces de dimension in which the polytope can be embedded, but it also reduces the number of its vertices; second, by choosing G which contains a symmetry present in a physical system, it produces Bell inequalities which exploit this symmetry and greatly simplify its experimental realization. In the next section we study in detail $\mathbb{P}_K^G$.

[10] This group can be seen as a subgroup of the symmetric group of n elements $\mathfrak{S}_n$, denoted $G \leq \mathfrak{S}_n$, as it applies a subset of all possible permutations to the parties.

4.1.2. The symmetrized polytope

Let G be a group, seen as a subgroup of the group of permutations of n elements, $\mathfrak{S}_n$. We denote it $G \leq \mathfrak{S}_n$. Let us denote by $\mathcal{P}_K$ the set of K-body probabilities:

$$\mathcal{P}_K := \bigcup_{k=1}^{K} \{P_{i_1 \dots i_k}(a_{i_1} \dots a_{i_k} | x_{i_1} \dots x_{i_k})\}, \tag{4.6}$$

with $0 \leq i_1 < \dots < i_k < n$, $0 \leq a_j < d-1$ and $0 \leq x_j < m$. The action of G on the set $\mathcal{P}_K$ is defined through the permutation of the parties $i_1 \dots i_k$. Formally, we have an action g given by

$$\begin{array}{rll} g: & G \times \mathcal{P}_K & \longrightarrow \mathcal{P}_K \\ & (\sigma \ , \ P_{i_1 \dots i_k}(a_{i_1} \dots a_{i_k} | x_{i_1} \dots x_{i_k})) & \mapsto \ P_{\sigma(i_1 \dots i_k)}(a_{i_1} \dots a_{i_k} | x_{i_1} \dots x_{i_k}). \end{array} \tag{4.7}$$

Since the action of a group on a set induces a partition of such set into different orbits, given a correlator $P \in \mathcal{P}_K$, let us denote the corresponding orbit induced by g as $[P] := \{g(\sigma, P), \sigma \in G\}$. The set of orbits is denoted $\mathcal{P}_K/G$. Observe that a correlator P can only belong to one orbit; this is why we say that orbits constitute a partition of the set $\mathcal{P}_K$. Thus, we can express $\mathcal{P}_K$ as the disjoint union, denoted $\sqcup$, of all its orbits; *i.e.*,

$$\mathcal{P}_K = \bigsqcup_{[P] \in \mathcal{P}_K/G} [P]. \tag{4.8}$$

By construction, now we have an equality between sets: $g([P]) = [P]$. In particular, the sum of all the elements in $[P]$ remains invariant under the action of any $\sigma \in G$. This motivates the definition of a G-invariant correlator $S_{[P]}$:

$$S_{[P]} :\propto \sum_{P \in [P]} P \qquad \forall [P] \in \mathcal{P}_K/G. \tag{4.9}$$

Observe that there are as many G-invariant correlators as elements in $\mathcal{P}_K/G$. We have used the proportionality symbol in Eq. (4.9) to indicate that the property of G-invariance does not depend on this proportionality factor. We shall choose it to our convenience in the next sections.

Since Eq. (4.9) defines a linear projection, we can define the G-symmetric polytope of at most K-body correlations, which we denote $\mathbb{P}_K^G$, as the

image of $\mathbf{P}_L$ by Eq. (4.9). Its dimension is simply given by the number of G-symmetric correlators that one can obtain via Eq. (4.9); *i.e.*; $\sum_{k=1}^{K} |\mathcal{P}_k/G|$. Note that the proportionality constant implicit in Eq. (4.9) corresponds to a stretching in the corresponding dimension and thus it does not change the relevant geometrical properties of $\mathbb{P}_K^G$.

The G-symmetric K-body polytope $\mathbb{P}_K^G$ can be completely characterized by listing its vertices. They can be readily obtained from the projection of the vertices of $\mathbf{P}_L$ via Eq. (4.9). However, this procedure turns out to be inefficient in practice, as there is a number of vertices d^{mn} exponential in n. We shall now see how to bound the number of vertices of $\mathbb{P}_K^G$ and how to generate them directly, without having to consider any of $\mathrm{Ext}(\mathbf{P}_L)$.

Bounding the number of vertices of the G-symmetric K-body correlations polytope

By virtue of Eq. (4.9), which is a linear projection, every vertex of $\mathbb{P}_K^G$ is the image of some vertex of $\mathbf{P}_L$. The converse is not true in general, as a vertex of $\mathbf{P}_L$ may get mapped to the interior of $\mathbb{P}_K^G$, which happens to be the case in most situations. We will identify this behavior by looking at the deterministic local strategies (which are in one-to-one correspondence with the vertices of $\mathbf{P}_L$). Every set of deterministic local strategies that gives the same values in Eq. (4.9) is a candidate for a vertex, so counting this set will give an upper bound on the cardinality of $\mathrm{Ext}(\mathbb{P}_K^G)$. To this end, we shall make use of the Redfield-Pólya's enumeration theorem [Red27; Pól37].

A Deterministic Local Strategy (DLS) is just an assignment of a list of a predetermined outcomes for every measurement for every party. Thus, it can be thought of as a function $f : X \longrightarrow Y$, where $X = \{0, \ldots, n-1\}$ indexes the parties and $Y = \{(y_0, \ldots, y_{m-1}), \quad 0 \leq y_i < d\}$ indexes the set of tuples that indicate the outcomes of each of the m measurements. We denote[11] the set of all DLSs Y^X. Analogously to Eq. (4.8), it is possible to partition Y^X, thus grouping strategies that give the same values in all Eqs. (4.9). We will say that f_1 and f_2 are equivalent (or they belong to the same element in Y^X/G) if, and only if, there exists a permutation $\sigma \in G$ such that it brings f_1 to f_2 (See Figure 4.1). The Redfield-Pólya enumeration

[11] By simple analogy to the cardinality of the set of functions from X to Y, since $|Y^X| = |Y|^{|X|}$ in the finite case.

theorem counts the number of orbits, which is given by

$$|Y^X/G| = \frac{1}{|G|}\sum_{\sigma\in G}|Y|^{c(\sigma)}, \tag{4.10}$$

where $c(\sigma)$ denotes the function that, for each permutation σ, outputs the number of disjoint cycles[12] of σ.

It is now clear from Eqs. (4.9) and (4.10) that both the dimensions of $\mathbb{P}_K^G$ and its number of vertices depend on the chosen symmetry group G. There is a trade-off between the order of the group and the complexity of $\mathbb{P}_K^G$: the bigger the symmetry group, the smaller the dimensions and number of vertices of $\mathbb{P}_K^G$, as well as the chances to obtain useful Bell inequalities for nonlocality detection in many-body systems.

4.1.3. The permutationally invariant K-body correlations polytope

In this section we consider the case of the biggest symmetry group $G = \mathfrak{S}_n$. The polytope $P_K^{\mathfrak{S}_n}$ is described by Bell inequalities which are invariant under any permutation of the parties. For the case $K = n$, with $n \leq 5$, inequalities of these kind were considered in [BGP10].

Let us start by upper bounding $|\mathrm{Ext}(\mathbb{P}_K^{\mathfrak{S}_n})|$, by an explicit computation of (4.10). It is useful to recall that the number of permutations of n elements with k disjoint cycles is given by the unsigned[13] Stirling number of the first kind, denoted $\left[\begin{array}{c} n \\ k \end{array}\right]$. This has the following property [AS65]:

$$\sum_{k=1}^{n}\left[\begin{array}{c} n \\ k \end{array}\right] x^k = x(x+1)\cdots(x+n-1) = \frac{(x+n-1)!}{(x-1)!}. \tag{4.11}$$

[12] This is a well-defined quantity, as every permutation decomposes uniquely into a product of disjoint cycles (*modulo* a permutation of the cycles).

[13] The signed Stirling number of the first kind has an additional factor $(-1)^{n-k}$ in front, and it corresponds to the coefficients of the falling factorial $x(x-1)\cdots(x-n+1)$ [AS65].

With the aid of (4.11), Eq. (4.10) can be directly calculated, since

$$\begin{aligned} |Y^X/\mathfrak{S}_n| &= \frac{1}{n!}\sum_{\sigma\in\mathfrak{S}_n}(d^m)^{c(\sigma)} = \frac{1}{n!}\sum_{k=1}^{n}\left[\begin{array}{c} n \\ k \end{array}\right](d^m)^k \\ &= \frac{1}{n!}\frac{(n+d^m-1)!}{(d^m-1)!} = \binom{n+d^m-1}{d^m-1}. \end{aligned} \tag{4.12}$$

We shall see in Sections 4.1.4 and 4.6.1 that the bound $|\mathrm{Ext}(\mathbb{P}_K^{\mathfrak{S}_n})| \leq |Y^X/G|$ is not tight in general and it can be further refined.

Let us now see a simpler argument for deriving Eq. (4.12), without having to use the Redfield-Pólya theorem. This will allow us to parametrize the vertices of $\mathbb{P}_K^{\mathfrak{S}_n}$ with d^m-1 integer parameters. The combinatorical interpretation of Eq. (4.12) is that the number of $\mathfrak{S}_n$-equivalent DLSs is nothing else than the number of ways to partition a set of n elements into d^m possibly empty subsets. In other words, the number of ways to color n indistinguishable parties with d^m colors (*cf.* Figure 4.1). Or, in a language closer to nonlocality, the different sets of instructions that are given to the parties *prior* to the experiment that determine the outcome of the measurements; since the inequality is permutationally invariant, it does not matter the order in which such sets of instructions are given. The key idea is to identify a DLS $f : X \longrightarrow Y$ as a coloring of a hypergraph, which has the elements of X (the parties) as its nodes and the k-body correlators as its hyperedges; the colors are the elements of Y. If the colors of the nodes are permuted according to an element of G, then all the correlators (4.9) keep the same values, so they correspond to the same point in $\mathbb{P}_K^G$.

However, as we are currently considering $G = \mathfrak{S}_n$, this happens for any permutation. Thus, the values of (4.9) only depend on the amount of parties assigned to each color; *i.e.*, the amount of parties sharing the same DLS. There are $|Y| = d^m$ possible DLSs, so one has to consider the number of partitions of n into d^m (some possibly empty) subgroups. Eq. (4.12) follows from a simple combinatorical argument: arrange the n parties in a line, add d^m-1 more and then choose, out of the $n+d^m-1$, d^m-1 to act as a separator.

Dichotomic observables

From now on, for simplicity, let us focus on the particular case $d = 2$, where all observables can take two values, ± 1 and let us work in the correlation functions framework introduced in Section 4.1. Recall that there is no loss of generality in this switch for $d = 2$. We are now interested in characterizing $\dim \mathbb{P}_K^{\mathfrak{S}_n} = |\mathcal{P}_K/\mathfrak{S}_n|$. A direct look at Eq. (4.9) shows that $S_{[\mathcal{M}]}$, where $\mathcal{M}$ is a k-body expectation value with $1 \leq k \leq K$, only depends on the choice of k out of the m possible measurements available. For instance, one would have $S_{[A_2B_2C_0]} = S_{[B_2D_0E_2]} = \ldots$, which suggests to take as a canonical representative the lexicographically lowest element, that in this particular example would be $A_0B_2C_2$, and simply denote the correlator as $\mathcal{S}_{022}$. This step greatly simplifies the task of finding $\dim \mathbb{P}_K^{\mathfrak{S}_n}$, which is the number of ordered sequences $0 \leq x_1 \leq x_2 \leq \ldots \leq x_k < m$, for k going from 1 to K. Hence,

$$|\mathcal{P}_K/\mathfrak{S}_n| = \sum_{k=1}^{K} \binom{k+m-1}{m-1} = \binom{m+K}{K} - 1. \tag{4.13}$$

Observe that Eq. (4.13) shows that the dimension of $\mathbb{P}_K^{\mathfrak{S}_n}$ does not depend on n, which is an essential step towards the many-body regime; *i.e.*, for large n.

The symmetric polytope of 2-body correlations

The simplest element from the family of polytopes $\mathbb{P}_K^{\mathfrak{S}_n}$ is for $K = 2$ and 2 dichotomic measurements, which has dimension 5. We are now in position to define the symmetric correlators we will be working with, throughout most of this chapter:

$$\mathcal{S}_k := \sum_{i=0}^{n-1} \mathcal{M}_k^{(i)}, \quad 0 \leq k \leq 1, \tag{4.14}$$

$$\mathcal{S}_{kl} := \sum_{i=0}^{n-1} \sum_{j=0, j\neq i}^{n-1} \mathcal{M}_k^{(i)} \mathcal{M}_l^{(j)}, \quad 0 \leq k \leq l \leq 1. \tag{4.15}$$

It is easy to check that Eqs. (4.14) and (4.15) do correspond to Eq. (4.9) with the appropriate proportionality factor. As it is shown in Figure 4.1,

single-body correlators can also be obtained by summing the black circles and subtracting the red ones, and two-body correlators are given by adding the black edges and subtracting the red ones. Hence, to make explicit calculations in what follows, it is convenient to introduce the variables below:

$$\begin{aligned} a_f &:= |f^{-1}(+,+)|, \qquad & b_f &:= |f^{-1}(+,-)|, \\ c_f &:= |f^{-1}(-,+)|, \qquad & d_f &:= |f^{-1}(-,-)|, \end{aligned} \tag{4.16}$$

where f^{-1} denotes the preimage of the map $f : X \longrightarrow Y$. The variable a_f counts the number of parties for which its predetermined outcomes are $\mathcal{M}_0 = +, \mathcal{M}_1 = +$ for a given f, and so on for b_f, c_f and d_f. In the particular example of Fig. 4.1 we have $a_f = 2, b_f = 1, c_f = 1$ and $d_f = 0$. Because there are no other possibilities, one always has, for all $f \in Y^X$, $a_f + b_f + c_f + d_f = n$. Interestingly, the values of the symmetric correlators (4.14, 4.15) can be inferred just from these four numbers. As one can directly check, for a given f,

$$\mathcal{S}_0 = a_f + b_f - c_f - d_f \tag{4.17}$$

and

$$\mathcal{S}_1 = a_f - b_f + c_f - d_f. \tag{4.18}$$

The two-body correlators (4.15) are found using the fact that correlators factorize on the vertices of $\mathbf{P}_L$; hence, for any f,

$$\mathcal{S}_{kl} = \mathcal{S}_k \mathcal{S}_l - \sum_{i=0}^{n-1} \mathcal{M}_k^{(i)} \mathcal{M}_l^{(i)}. \tag{4.19}$$

The subtracted amount in Eq. (4.19) is well defined on vertices, and it amounts to either n if $k = l$, or the sum of the product of the k-th and the l-th observables over all the parties if $k \neq l$, a term which we shall define as $\mathcal{Z}$:

$$\mathcal{Z} := \sum_{i=0}^{n-1} \mathcal{M}_0^{(i)} \mathcal{M}_1^{(i)} = a_f - b_f - c_f + d_f. \tag{4.20}$$

Eq. (4.15) now reads $\mathcal{S}_{00} = (\mathcal{S}_0)^2 - n$, $\mathcal{S}_{01} = \mathcal{S}_0 \mathcal{S}_1 - \mathcal{Z}$ and $\mathcal{S}_{11} = (\mathcal{S}_1)^2 - n$. In the forthcoming sections, we shall skip the subindex f when it is clear from the context.

Permutationally invariant Bell inequalities

The Bell inequalities that constrain[14] the polytope $\mathbb{P}_2$, for the $(n,2,2)$ scenario, in terms of correlation functions, are given by

$$\begin{aligned}\beta_c + \sum_{i=0}^{n-1}\left(\alpha_i\langle\mathcal{M}_0^{(i)}\rangle + \beta_i\langle\mathcal{M}_1^{(i)}\rangle\right) + \sum_{0\leq i<j<n}\gamma_{ij}\langle\mathcal{M}_0^{(i)}\mathcal{M}_0^{(j)}\rangle \\ + \sum_{0\leq i\neq j<n}\delta_{ij}\langle\mathcal{M}_0^{(i)}\mathcal{M}_1^{(j)}\rangle + \sum_{0\leq i<j<n}\varepsilon_{ij}\langle\mathcal{M}_1^{(i)}\mathcal{M}_1^{(j)}\rangle \quad \geq \quad 0,\end{aligned} \tag{4.21}$$

for some $\alpha_i, \beta_i, \gamma_{ij}, \delta_{ij}, \varepsilon_{ij} \in \mathbb{R}$ and $\beta_c \in \mathbb{R}$. The constant term β_c is the so-called classical bound, and it is found by optimizing (4.21) over all LHVM or, equivalently, over all deterministic local strategies $f \in Y^X$. The number of degrees of freedom in a general 2-body correlators Bell inequality is $2n^2$ (*cf.* Eq. (4.5) for $d = m = K = 2$).

After symmetrization by $\mathfrak{S}_n$, the Bell inequalities obtained will have all the coefficients equal: $\alpha_i = \alpha$, $\beta_i = \beta$, $\gamma_i = \gamma$, $\delta_i = \delta$ and $\varepsilon_i = \varepsilon$, because the Bell inequalities that define $\mathbb{P}_2^{\mathfrak{S}_n}$ are of the form

$$\beta_c + \alpha\mathcal{S}_0 + \beta\mathcal{S}_1 + \frac{\gamma}{2}\mathcal{S}_{00} + \delta\mathcal{S}_{01} + \frac{\varepsilon}{2}\mathcal{S}_{11} \geq 0, \tag{4.22}$$

with $\alpha, \beta, \gamma, \delta, \varepsilon \in \mathbb{R}$ and $\beta_c \in \mathbb{R}$ being the corresponding classical bound.

4.1.4. Characterization of the vertices of the permutationally invariant polytope

The dimension of the space in which $\mathbb{P}_2^{\mathfrak{S}_n}$ is embedded for the $(n,2,2)$ scenario is 5, as it has coordinates $\mathcal{S}_0, \mathcal{S}_1, \mathcal{S}_{00}, \mathcal{S}_{01}$ and $\mathcal{S}_{11}$. However, a point in this space that corresponds to a DLS, namely f, only 4 parameters are needed in order to completely describe it: either (a,b,c,d) or $(n,\mathcal{S}_1,\mathcal{S}_0,\mathcal{Z})$. These two sets of variables are related via a (proportional to) orthogonal transformation, given by a Hadamard matrix:

$$\begin{pmatrix} n \\ \mathcal{S}_1 \\ \mathcal{S}_0 \\ \mathcal{Z} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = H^{\otimes 2} \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}. \tag{4.23}$$

[14] In particular, those inequalities that correspond to facets.

We shall further study this relation in Section 4.5, where it will be generalized to the (n, m, d) scenario with K-body correlators, both in the framework of probabilities and the framework of expectation values.

As we have argued in Section 4.1.3, in order to explore all the vertices of $\mathbb{P}_2^{\mathfrak{S}_n}$, it is enough to consider all the partitions of n in 4 non-negative integers. To this end, let us define the set of all such partitions:

$$\mathbb{T}_n = \{(a, b, c, d) \in \mathbb{Z}^4 : \ a, b, c, d \geq 0, \ a + b + c + d = n\}. \tag{4.24}$$

Note that Eq. (4.24) has a clear geometrical interpretation: $\mathbb{T}_n$ is the set of points of a simplex with integer coordinates. In the particular case $(n, 2, 2)$, it can be viewed as the integer-coordinates points of a tetrahedron. In order to conveniently describe all the candidates for vertices of $\mathbb{P}_2^{\mathfrak{S}_n}$, let us introduce the following map:

$$\begin{array}{rccc} \varphi : & \mathbb{T}_n & \longrightarrow & \mathbb{P}_2^{\mathfrak{S}_n} \\ & (a, b, c, d) & \mapsto & (\mathcal{S}_0, \mathcal{S}_1, \mathcal{S}_{00}, \mathcal{S}_{01}, \mathcal{S}_{11}), \end{array} \tag{4.25}$$

Then $\mathbb{P}_2^{\mathfrak{S}_n}$ is the convex hull[15] of $\varphi(\mathbb{T}_n)$, which we shall denote $\mathbb{P}_2^{\mathfrak{S}_n} = \mathrm{CH}(\varphi(\mathbb{T}_n))$.

In the following theorem, we show how one can discard most of the points in $\mathbb{T}_n$, namely, those with no coordinate equal to zero. This is why we need to introduce the following set

$$\partial\mathbb{T}_n := \{(a, b, c, d) \in \mathbb{Z}^4 : \ a, b, c, d \geq 0, \ a + b + c + d = n, \ abcd = 0\}. \tag{4.26}$$

Theorem 4.2. *For all $p = (a, b, c, d) \in \mathbb{T}_n$, the following equivalence holds:*

$$p \in \partial\mathbb{T}_n \iff \varphi(p) \in \mathrm{Ext}(\mathbb{P}_2^{\mathfrak{S}_n}). \tag{4.27}$$

Proof. Let us start with the *if* part. Suppose that $p \in \mathbb{T}_n \setminus \partial\mathbb{T}_n$, so that all the coordinates of p are strictly positive; *i.e.*, $a, b, c, d \geq 1$. We have to show that p is not a vertex of $\mathbb{P}_2^{\mathfrak{S}_n}$ and we will do so by explicitly giving a convex

[15] The convex hull of a set S is the smallest convex set containing S. If the convex hull is a closed set, then it can be defined as the intersection of all closed half-spaces containing S. This happens when S is compact. In particular, in our case, when S is finite.

decomposition. Let us consider a vector v from $\mathbb{T}_n$: $v = (1, -1, -1, 1)$. Note that v is the fourth row of the Hadamard matrix in (4.23). Since a Hadamard matrix is orthogonal, all its rows are pairwise orthogonal. Consequently, for any λ, $p + \lambda v$ has the same value for any n, $\mathcal{S}_0$ and $\mathcal{S}_1$, whereas $\mathcal{Z}(p + \lambda v) = \mathcal{Z}(p) + 4\lambda$. Hence, the only coordinate that can change is $\mathcal{S}_{01}$. After short algebra, one finds that $\mathcal{S}_{01}(p + \lambda v) = \mathcal{S}_{01}(p) - 4\lambda$. Observe that for any μ_1, μ_2, we have

$$\mu_1 \varphi(p + \mu_2 v) + \mu_2 \varphi(p - \mu_1 v) = (\mu_1 + \mu_2)\varphi(p). \tag{4.28}$$

If $\mu_1, \mu_2 > 0$, we have found a convex decomposition of $\varphi(p)$:

$$\varphi(p) = \frac{\mu_1}{\mu_1 + \mu_2}\varphi(p + \mu_2 v) + \frac{\mu_2}{\mu_1 + \mu_2}\varphi(p - \mu_1 v) \tag{4.29}$$

Notice that if we pick $\mu_1 = \min\{a, d\}$ and $\mu_2 = \min\{b, c\}$, then $p + \mu_2 v \in \partial\mathbb{T}_n$ and $p - \mu_1 v \in \partial\mathbb{T}_n$ hold. Since $\mu_1, \mu_2 > 0$, this ensures that Eq. (4.29) is a proper convex decomposition, so $\varphi(p) \notin \mathrm{Ext}(\mathbb{P}_2^{\mathfrak{S}_n})$.

Conversely, for the *only if* part, let $p \in \partial\mathbb{T}_n$. If $\varphi(p)$ were not a vertex of $\mathbb{P}_2^{\mathfrak{S}_n}$, there would exist a convex combination of different elements from $\mathrm{Ext}(\mathbb{P}_2^{\mathfrak{S}_n})$, namely $\{q_i\}_{i=1\ldots k}$, for some $k > 1$, that would give $\varphi(p)$. Since φ, when restricted to DLSs, is an invertible transformation, for every q_i there is a unique $p_i \in \mathbb{T}_n$ such that $\varphi(p_i) = q_i$.

To see that φ is indeed invertible in any DLS, it suffices to observe that $(\mathcal{S}_0, \mathcal{S}_1, \mathcal{S}_{00}, \mathcal{S}_{01}, \mathcal{S}_{11}) = (\mathcal{S}_0, \mathcal{S}_1, (\mathcal{S}_0)^2 - n, \mathcal{S}_0\mathcal{S}_1 - \mathcal{Z}, (\mathcal{S}_1)^2 - n)$, from which one can trivially obtain $n, \mathcal{S}_1, \mathcal{S}_0, \mathcal{Z}$ and, via Eq. (4.23), a, b, c and d. Let us then label the different coordinates of p_i, $p_i = (a_i, b_i, c_i, d_i)$. Then, $\varphi(p)$ has then the following decomposition:

$$\varphi(p) = \sum_{i=1}^{k} \lambda_i \varphi(p_i), \tag{4.30}$$

where $0 < \lambda_i < 1$ and the sum of the λ_i is 1.

By looking at the third coordinate of the vectors in Eq. (4.30), the fact that $\mathcal{S}_{00}(r) = (\mathcal{S}_0(r))^2 - n$ for all $r \in \mathbb{T}_n$ implies the following:

$$\begin{aligned} (\mathcal{S}_0(p))^2 - n &= \sum_{i=1}^{k} \lambda_i [(\mathcal{S}_0(p_i))^2 - n] \\ \left(\sum_{i=1}^{k} \lambda_i \mathcal{S}_0(p_i)\right)^2 &= \sum_{i=0}^{k} \lambda_i (\mathcal{S}_0(p_i))^2. \end{aligned} \tag{4.31}$$

Treating Equation (4.31) as a quadratic function in $\mathcal{S}_0(p_m)$, for some $1 \leq m \leq k$ we can collect terms and obtain a degree two polynomial equation in $\mathcal{S}_0(p_m)$:

$$\lambda_m(\lambda_m - 1)(\mathcal{S}_0(p_m))^2 + 2\lambda_m \mathcal{S}_0(p_m) \sum_{i \neq m} \lambda_i \mathcal{S}_0(p_i) + \left(\sum_{i \neq m} \lambda_i \mathcal{S}_0(p_i) \right)^2 - \sum_{i \neq m} \lambda_i (\mathcal{S}_0(p_i))^2 = 0. \tag{4.32}$$

Eq. (4.32) has a real solution $\mathcal{S}_0(p_m) \in \mathbb{R}$ if, and only if, its discriminant is non-negative, which is equivalent to

$$-4\lambda_m \sum_{i<j:\ i,j \neq m} \lambda_i \lambda_j (\mathcal{S}_0(p_i) - \mathcal{S}_0(p_j))^2 \geq 0. \tag{4.33}$$

Because all $\lambda_i > 0$, Eq. (4.33) is fulfilled if, and only if, for all $i, j \neq m$, $\mathcal{S}_0(p_i) = \mathcal{S}_0(p_j)$. However, Eq. (4.33) holds for each m, which allows us to conclude that it must necessarily be the case that, for all i, $\mathcal{S}_0(p_i) = \mathcal{S}_0(p)$. By applying the same reasoning to $\mathcal{S}_1$, we can conclude

$$\mathcal{S}_x(p_i) = \mathcal{S}_x(p), \qquad 0 \leq x \leq 1, \quad 1 \leq i \leq k. \tag{4.34}$$

The assumption that $\varphi(p) \notin \mathrm{Ext}(\mathbb{P}_2^{\mathfrak{S}_n})$ only leaves the possibility that every $\mathcal{S}_{01}(p_i)$ must be different. Since in any DLS one has $\mathcal{S}_{01}(r) = \mathcal{S}_0(r)\mathcal{S}_1(r) - \mathcal{Z}(r)$, Ea. (4.34) implies that every $\mathcal{Z}(p_i)$ must be different. The fourth coordinate of Eq. (4.30) then reads

$$a - b - c + d = \sum_{i=1}^{k} \lambda_i (a_i - b_i - c_i + d_i). \tag{4.35}$$

By appropriately adding and subtracting Eqs. (4.35, 4.34), and using the fact that $a + b + c + d = a_i + b_i + c_i + d_i = n$, one shows that:

$$a = \sum_{i=1}^{k} \lambda_i a_i, \quad b = \sum_{i=1}^{k} \lambda_i b_i, \quad c = \sum_{i=1}^{k} \lambda_i c_i, \quad d = \sum_{i=1}^{k} \lambda_i d_i, \tag{4.36}$$

which is equivalent to $p = \sum_{i=1}^{k} \lambda_i p_i$. That is, p is a convex combination of elements of $\mathbb{T}_n$ with the same weights as the convex combination of $\varphi(p)$.

Finally, if $p \in \partial\mathbb{T}_n$, by definition one of its coordinates is zero. However, if any of its coordinates were 0, Eqs. (4.34), (4.35) and $a+b+c+d = a_i+b_i+c_i+d_i$ would imply that, for every i, $p = p_i$, contradicting the fact that Eq. (4.29) was a proper convex decomposition. This contradiction comes from the assumption that $\varphi(p)$ was not a vertex of $\mathbb{P}_2^{\mathfrak{S}_n}$. Hence, $\varphi(p) \in \mathrm{Ext}(\mathbb{P}_2^{\mathfrak{S}_n})$. □

Remark 4.3. Theorem 4.2 enables us to construct $\mathbb{P}_2^{\mathfrak{S}_n}$ as the convex hull of $\varphi(\partial\mathbb{T}_n)$, instead of the convex hull of $\varphi(\mathbb{T}_n)$. In addition, we have completely characterized the vertices of $\mathbb{P}_2^{\mathfrak{S}_n}$, and we can count how many there are:

$$\begin{aligned} |\mathrm{Ext}(\mathbb{P}_2^{\mathfrak{S}_n})| &= |\partial\mathbb{T}_n| = |\mathbb{T}_n| - |\mathbb{T}_n \setminus \partial\mathbb{T}_n| = |\mathbb{T}_n| - |\mathbb{T}_{n-4}| \\ &= \binom{n+3}{3} - \binom{n-1}{3} = 2(n^2+1), \end{aligned} \tag{4.37}$$

which is an improvement from $O(n^3)$ to $O(n^2)$. Due to Theorem 4.2 and the fact that φ is invertible on DLSs, every vertex of $\mathbb{P}_2^{\mathfrak{S}_n}$ is generated from a unique tuple $(a,b,c,d) \in \partial\mathbb{T}_n$.

In terms of the coloring introduced in Fig. 4.1, the interpretation is that a coloring $f : X \longrightarrow Y$ in which all colors appear cannot correspond to an element in $\mathrm{Ext}(\mathbb{P}_2^{\mathfrak{S}_n})$.

4.2. Classes of Bell Inequalities

As we have discussed in Remark 4.3, the coordinates $(\mathcal{S}_0, \mathcal{S}_1, \mathcal{S}_{00}, \mathcal{S}_{01}, \mathcal{S}_{11})$ of the vertices of $\mathbb{P}_2^{\mathfrak{S}_n} = \mathrm{CH}(\varphi(\partial\mathbb{T}_n))$ are of the form

$$\mathcal{S}_0 = a + b - c - d \tag{4.38}$$
$$\mathcal{S}_1 = a - b + c - d \tag{4.39}$$
$$\mathcal{S}_{00} = (\mathcal{S}_0)^2 - n \tag{4.40}$$
$$\mathcal{S}_{01} = \mathcal{S}_0\mathcal{S}_1 - \mathcal{Z} \tag{4.41}$$
$$\mathcal{S}_{11} = (\mathcal{S}_1)^2 - n, \tag{4.42}$$

for $(a,b,c,d) \in \partial\mathbb{T}_n$. We will exploit this parametrization to derive classes of Bell inequalities for $\mathbb{P}_2^{\mathfrak{S}_n}$. Note that if two sets S_1 and S_2 fulfill $S_1 \subseteq S_2$, then

its convex hulls are also included one into the other: $\mathrm{CH}(S_1) \subseteq \mathrm{CH}(S_2)$. Thus, if we relax the condition that the parameters (a, b, c, d) are integers to being real numbers, we shall obtain a larger object, which is convex and does not need to be a polytope, that contains $\mathbb{P}_2^{\mathfrak{S}_n}$. Hence, a Bell inequality valid for this object will also be valid for $\mathbb{P}_2^{\mathfrak{S}_n}$. To this end, let us define the following sets:

$$\mathbf{T}_n = \{(a, b, c, d) \in \mathbb{R}^4 : \ a, b, c, d \geq 0, \ a + b + c + d = n\} \tag{4.43}$$

$$\partial\mathbf{T}_n = \{(a, b, c, d) \in \mathbb{R}^4 : \ a, b, c, d \geq 0, \ a + b + c + d = n, \ abcd = 0\} \tag{4.44}$$

What we gain doing this relaxation is that now $\mathrm{CH}(\partial\mathbf{T}_n)$ can be easier to characterize, as new tools such as differential calculus can be applied to it. As we shall see later on, the price to pay in doing so is not that high, as the inequalities we shall obtain will be *optimizable*; *i.e.*, we can bring them back to $\mathbb{P}_2^{\mathfrak{S}_n}$.

Let us define $\mathbf{P}_2^{\mathfrak{S}_n} := \mathrm{CH}(\partial\mathbf{T}_n)$. As the proof of Theorem 4.2 applies to the continuous case as well, then $\mathrm{CH}(\varphi(\mathbf{T}_n)) = \mathrm{CH}(\varphi(\partial\mathbf{T}_n))$. As $\partial\mathbb{T}_n \subset \partial\mathbf{T}_n$, then $\mathbb{P}_2^{\mathfrak{S}_n} \subseteq \mathbf{P}_2^{\mathfrak{S}_n}$, as we discussed, so that a Bell inequality valid for $\mathbf{P}_2^{\mathfrak{S}_n}$ is also a Bell inequality valid for $\mathbb{P}_2^{\mathfrak{S}_n}$. The characterization of Bell inequalities on $\mathbf{P}_2^{\mathfrak{S}_n}$ is an easier task[16] than finding the ones corresponding to $\mathbb{P}_2^{\mathfrak{S}_n}$.

Before formally stating Theorem 4.4, let us take a look at the idea behind the derivation of the class of Bell inequalities we present. Eqs. (4.38-4.42) are polynomials of degree 1 or 2 in the variables a, b, c and d. Thus,

[16] The sets $\varphi(\partial\mathbf{T}_n)$ and $\varphi(\mathbf{T}_n)$ are defined through polynomial equalities and inequalities. We say that they are semialgebraic. The characterization of convex hulls of semialgebraic sets is a well studied subject [GT]. Although its exact characterization is an NP-hard problem [BPT], there exist efficient approximations with semi-definite programming techniques in terms of the so-called theta bodies. As we shall discuss in Section 4.5, these techniques can be directly applied to any (n, m, d) scenario with K-body correlators when the symmetry group G is $\mathfrak{S}_n$.

The Navascués-Pironio-Acín (NPA) hierarchy [NPA08] mentioned in Section 2.2.2 is also in the spirit of such approximations, although for the case of non-commutative variables. When the NPA hierarchy gives a certificate that a set of correlations is outside $\mathbf{Q}_k$ for some k, then such correlations cannot be realized with quantum resources. In our case, a characterization of $\mathbf{P}_2^{\mathfrak{S}_n}$ through theta bodies produces also a hierarchy of sets $\mathbf{P}_2^{\mathfrak{S}_n} \subseteq \ldots \subseteq \Theta_2 \subseteq \Theta_1$ that can certify if a set of correlations which is outside of Θ_k for some k; in such case, the correlations under study cannot be simulated through shared randomness and they must be necessarily nonlocal. To our knowledge, this technique has never been used in order to decide between local and non-local correlations.

they define a manifold in a 5-dimensional space, and this manifold is 3-dimensional, because of the normalization constraint $a+b+c+d=n$. By finding a tangent hyperplane to it, we might obtain a good candidate for a Bell inequality. Hence, we have to determine a plane of the form

$$\alpha\mathcal{S}_0+\beta\mathcal{S}_1+\frac{\gamma}{2}\mathcal{S}_{00}+\delta\mathcal{S}_{01}+\frac{\varepsilon}{2}\mathcal{S}_{11}+\beta_c=0, \tag{4.45}$$

and then prove that the l. h. s. of Eq. (4.45) is positive on all elements of $\varphi(\mathbf{T}_n)$. This will give us constraints on the coefficients $\alpha,\beta,\gamma,\delta,\varepsilon$ and the classical bound β_c that will define a *good* Bell inequality. Theorem 4.2 already gives us a hint on how to start the search: since the extremal points of $\mathbf{P}_2^{\mathfrak{S}_n}$ satisfy $abcd=0$ in $\mathbf{T}_n$, an option is to look in a single facet of $\mathbf{T}_n$; *e.g.*, those for which $a=0$. Not all Bell inequalities need to be tight (in the sense of fulfilling Eq. (4.45)) on the same facet of $\mathbf{T}_n$, as $a=0$ implies $abcd=0$ but the converse is not true in general. However, for simplicity, we are looking for a class of Bell inequalities that displays this feature.

Let us introduce the following Lagrangian function, with λ and μ being Lagrange multipliers:

$$\mathcal{L}=\alpha\mathcal{S}_0+\beta\mathcal{S}_1+\frac{\gamma}{2}\mathcal{S}_{00}+\delta\mathcal{S}_{01}+\frac{\varepsilon}{2}\mathcal{S}_{11}+\lambda(a+b+c+d-n)+\mu a, \tag{4.46}$$

from which we wish to find its minimum $-\beta_c:=\min_{a,b,c,d,\lambda,\mu\in\mathbb{R}}\mathcal{L}$. Because we are dealing with two-body correlators, the necessary condition for an extremum to exist reduces to an inhomogeneous system of linear equations. Thus, we can look for a solution of it, denoted $(a^*,b^*,c^*,d^*,\lambda^*,\mu^*)$, corresponding to a zero of the differential application $D\mathcal{L}$. To this end, swe have to solve

$$\begin{pmatrix} \xi_+ & \zeta & -\zeta & -\xi_+ & 1 & 1\\ \zeta & \xi_- & -\xi_- & -\zeta & 1 & 0\\ -\zeta & -\xi_- & \xi_- & \zeta & 1 & 0\\ -\xi_+ & -\zeta & \zeta & \xi_+ & 1 & 0\\ 1 & 1 & 1 & 1 & 0 & 0\\ 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}\begin{pmatrix} a^*\\ b^*\\ c^*\\ d^*\\ \lambda^*\\ \mu^* \end{pmatrix}=\begin{pmatrix} -\alpha-\beta+\xi_+/2\\ -\alpha+\beta+\xi_-/2\\ \alpha-\beta+\xi_-/2\\ \alpha+\beta+\xi_+/2\\ 0\\ 0 \end{pmatrix}, \tag{4.47}$$

where $\xi_\pm:=\gamma\pm2\delta+\varepsilon$ and $\zeta:=\gamma-\varepsilon$.

Generically, the matrix appearing in Eq. (4.47) is non-singular. This means that for almost any $\xi_\pm$ and ζ, it is invertible, which leads to a

unique solution (a^*, b^*, c^*, d^*); *i.e.*, a Bell inequality which is tangent only to one point. Our task is to *tilt* the Bell inequality by properly choosing its coefficients, so that it becomes tangent to as many points as possible in $\mathbf{P}_2^{\mathfrak{S}_n}$. The number of solutions of Eq. (4.47) is given by Rouché-Frobenius theorem, a basic linear algebra result[17]. Since we are not interested in having a unique solution, the first condition we impose on the coefficients of Eq. (4.45) is that $\det A = 0$, where A is the matrix appearing on the l. h. s. of Eq. (4.47). After simple algebra, this condition simplifies to

$$\delta^2 - \gamma\varepsilon = 0. \tag{4.48}$$

When Eq. (4.48) is enforced, the rank of A is not greater than 5. If we further impose $\gamma\delta\epsilon \neq 0$, a condition we can always assume (otherwise the Bell inequality in Eq. (4.45) becomes trivial, it is exactly 5. It only remains to ensure that $A|\vec{c}$ has rank 5 as well, which is equivalent to having all its 5×5 minors vanishing, a condition that reads

$$\delta(\beta + \delta) = \varepsilon(\alpha + \delta). \tag{4.49}$$

When Conditions (4.48) and (4.49) are imposed, one can find the corresponding local minimum, which equals the classical bound provided that this minimum is global:

$$\beta_c = -\mathcal{L}(a^*, b^*, c^*, d^*, \lambda^*, \mu^*) = \frac{(\beta + \delta)^2 + n(\delta - \varepsilon)^2}{2\varepsilon}. \tag{4.50}$$

One can repeat the same argument and come up with similar expressions by exploring the facets $b = 0$, $c = 0$ or $d = 0$. Only permutations of parameters and sign changes would appear. It turns out that we can prove that the minimum in Eq. (4.50) is indeed global in $\mathbf{P}_2^{\mathfrak{S}_n}$, and we can apply a small correction to it to make Eq. (4.45) tangent to $\mathbb{P}_2^{\mathfrak{S}_n}$, as we do in Theorem 4.4. Furthermore, in Theorem 4.5 we give a necessary and sufficient criteria for counting in how many vertices of $\mathbb{P}_2^{\mathfrak{S}_n}$ it is tangent, and when is it tight.

[17] It states that, for a square matrix A, a linear system of equations $A\vec{b} = \vec{c}$ has some solution(s) (is compatible) if, and only if, the rank of A is the same as the rank of the extended matrix $A|\vec{c}$. This solution is unique, if and only if, $\det A \neq 0$.

Theorem 4.4. *For any $\sigma \in \{-1, 1\}$ and $x, y, \mu \in \mathbb{N}$ such that μ has opposite parity to x (y) if n is even (odd), define the parameters of (4.22) as*

$$\alpha_{\pm} = x[\sigma\mu \pm (x+y)], \quad \beta = \mu y, \quad \gamma = x^2, \quad \delta = \sigma xy, \quad \varepsilon = y^2. \tag{4.51}$$

Then, the classical bound of the resulting Bell inequality, for which it is tangent to $\mathbb{P}_2^{\mathfrak{S}_n}$, is

$$\beta_c = \frac{1}{2}[n(x+y)^2 + (\sigma\mu \pm x)^2 - 1]. \tag{4.52}$$

Proof. Let I be the function defined as

$$\begin{aligned} I &= \frac{1}{2}[n(x+y)^2 + (\sigma\mu \pm x)^2 - 1] + x[\sigma\mu \pm (x+y)]\mathcal{S}_0 + \mu y \mathcal{S}_1 \\ &\quad + \frac{x^2}{2}\mathcal{S}_{00} + \sigma xy \mathcal{S}_{01} + \frac{y^2}{2}\mathcal{S}_{11} \end{aligned} \tag{4.53}$$

We will show that $\min_{\mathbb{P}_2^{\mathfrak{S}_n}} I = 0$. For this purpose, we notice that for all DLSs, I takes the following form

$$\begin{aligned} I &= \frac{1}{2}[n(x+y)^2 + (\sigma\mu \pm x)^2 - 1] + x[\sigma\mu \pm (x+y)]\mathcal{S}_0 + \mu y \mathcal{S}_1 \\ &\quad + \frac{x^2}{2}\left(\mathcal{S}_0^2 - n\right) + \sigma xy\left(\mathcal{S}_0\mathcal{S}_1 - \mathcal{Z}\right) + \frac{y^2}{2}\left(\mathcal{S}_1^2 - n\right) \\ &= \frac{1}{2}\left(x^2\mathcal{S}_0^2 + 2\sigma xy\mathcal{S}_0\mathcal{S}_1 + y^2\mathcal{S}_1^2\right) + xyn - \sigma xy\mathcal{Z} + \frac{1}{2}(\sigma\mu \pm x)^2 \\ &\quad + (\sigma\mu \pm x)x\mathcal{S}_0 \pm xy\mathcal{S}_0 + \mu y\mathcal{S}_1 - \frac{1}{2} \\ &= \frac{1}{2}\left(x\mathcal{S}_0 + \sigma y\mathcal{S}_1\right)^2 + \frac{1}{2}\left[(\sigma\mu \pm x)^2 + 2(\sigma\mu \pm x)x\mathcal{S}_0 + 2(\sigma\mu \pm x)\sigma y\mathcal{S}_1\right] \\ &\quad \mp \sigma xy\mathcal{S}_1 \pm xy\mathcal{S}_0 - \sigma xy\mathcal{Z} + xyn - \frac{1}{2} \\ &= \frac{1}{2}\left(x\mathcal{S}_0 + \sigma y\mathcal{S}_1 + \sigma\mu \pm x\right)^2 + xy\left(\pm\mathcal{S}_0 \mp \sigma\mathcal{S}_1 - \sigma\mathcal{Z} + n\right) - \frac{1}{2}. \end{aligned}$$

The condition $I \geq 0$ can be reexpressed as

$$\left(x\mathcal{S}_0 + \sigma y\mathcal{S}_1 + \sigma\mu \pm x\right)^2 + 8xyr \geq 1, \tag{4.54}$$

where $r := (\pm\mathcal{S}_0 \mp \sigma\mathcal{S}_1 - \sigma\mathcal{Z} + n)/4$. Observe that r always amounts to one of the variables a, b, c or d, depending on the choice of the signs $\sigma, \pm$

we perform. One has the following values for r:

$\sigma\backslash\pm$	$+$	$-$
$+$	b	c
$-$	a	d

(4.55)

Let $\tilde{I}$ denote the l. h. s. of Eq. (4.54). $\tilde{I}$ is always non-negative, because $x, y \in \mathbb{N}$ and $r \geq 0$. However, we need to show that 0 cannot be achieved, thus proving that I is indeed tangent to $\mathbb{P}_2^{\mathfrak{S}_n}$. Note that if $r > 0$ or $x\mathcal{S}_0 + \sigma y\mathcal{S}_1 + \sigma\mu \pm x \neq 0$, the inequality (4.54) is trivially satisfied. Thus, the set of points for which $\tilde{I} = 0$ could be possible needs to be a subset of $\tilde{I}_0$, where $\tilde{I}_0$ is defined as

$$\tilde{I}_0 := \{(a, b, c, d) \in \mathbb{T}_n : \ r = 0, \ x\mathcal{S}_0 + \sigma y\mathcal{S}_1 + \sigma\mu \pm x = 0\}. \tag{4.56}$$

Observe that when (a, b, c, d) are taken to be continuous, $\tilde{I}_0$ is a line lying on a facet of $\partial\mathbf{T}_n$. We shall now see how the conditions of Theorem 4.4 ensure that $\tilde{I}_0 = \emptyset$. It will be sufficient to discuss the parity of $x\mathcal{S}_0 + \sigma y\mathcal{S}_1 + \sigma\mu \pm x$. Recall that, for any $m \in \mathbb{Z}$, $m \equiv m^2 \equiv -m \mod 2$. Then, it follows that $\mathcal{S}_0 \equiv \mathcal{S}_1 \equiv n \mod 2$. If n is even, then $x\mathcal{S}_0 + \sigma y\mathcal{S}_1 + \sigma\mu \pm x \equiv \mu + x \mod 2$. But this can not be the case, since $\mu + x \equiv 1 \mod 2$ by hypothesis. Otherwise, if n is odd, then $x\mathcal{S}_0 + \sigma y\mathcal{S}_1 + \sigma\mu \pm x \equiv x + y + \mu + x \equiv \mu + y \mod 2$ and, in this case, $\mu + y \equiv 1 \mod 2$ again by hypothesis. Hence, $\tilde{I}_0 = \emptyset$, which implies Eq. (4.54), which in turn proves that (4.51, 4.52) constitutes a valid Bell inequality, tangent to $\mathbb{P}_2^{\mathfrak{S}_n}$ for any n. □

Every Bell inequality constructed from Theorem 4.4 is tangent to $\mathbb{P}_2^{\mathfrak{S}_n}$. However, the optimal Bell inequalities are those which are *tight*; *i.e.*, in this case, those tangent in a set of points spanning a 4-dimensional affine subspace. Before stating Theorem 4.5, which will allow us to count on how many vertices of $\mathbb{P}_2^{\mathfrak{S}_n}$ an inequality I (constructed from Theorem 4.4) is tangent to, let us introduce a bit of notation to reduce the number of cases.

We begin by renaming the faces of the tetrahedron $\mathbb{T}_n$ according to the

choice of the independent signs σ and $\pm$.

$$\begin{array}{c|cccc} \sigma & + & + & - & - \\ \pm & + & - & + & - \\ \hline r & b & c & a & d \\ s & a & d & b & c \\ t & d & a & c & b \\ u & c & b & d & a \end{array} . \tag{4.57}$$

Note now that Eq. (4.23) is further generalized to

$$\begin{pmatrix} n \\ \mathcal{S}_1 \\ \mathcal{S}_0 \\ \mathcal{Z} \end{pmatrix} = \begin{pmatrix} 1 & & & \\ & \mp\sigma & & \\ & & \pm & \\ & & & -\sigma \end{pmatrix} \cdot H^{\otimes 2} \cdot \begin{pmatrix} r \\ s \\ t \\ u \end{pmatrix},$$

or, equivalently,

$$\begin{pmatrix} n \\ \mathcal{S}_1 \\ \mathcal{S}_0 \\ \mathcal{Z} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ \mp\sigma & \pm\sigma & \mp\sigma & \pm\sigma \\ \pm & \pm & \mp & \mp \\ -\sigma & \sigma & \sigma & -\sigma \end{pmatrix} \begin{pmatrix} r \\ s \\ t \\ u \end{pmatrix}. \tag{4.58}$$

Theorem 4.5. *Let I be defined as in Theorem 4.4. Let us further assume that x and y are coprimes and let the following quantities be defined as follows:*

$$\begin{array}{rcl} K'_r(\tau) & := & (\pm n(y-x) + \sigma\mu \pm x + \tau)/2, \\ t_0(\tau) & := & \pm y^{-1} K'_r(\tau) \mod x, \\ u_0(\tau) & := & (nx \pm K'_r(\tau) - (x+y)t_0(\tau))/x, \\ s_0(\tau) & := & (\mp K'_r(\tau) + y t_0(\tau))/x, \end{array} \tag{4.59}$$

where $\tau \in \{-1, 1\}$. If a vertex of $\mathbb{P}_2^{\mathfrak{S}_n}$ saturates (4.51, 4.52), then it is of the form $\varphi([r,s,t,u])$, where

$$[r,s,t,u] := [0, s_0(\tau), t_0(\tau), u_0(\tau)] + k[0, x, y, -(x+y)], \qquad k \in \mathbb{Z}. \tag{4.60}$$

Furthermore, the number of vertices of $\mathbb{P}_2^{\mathfrak{S}_n}$ for which (4.51, 4.52) is saturated is given by

$$N_S := \sum_{\tau=\pm 1} \max\left\{0, \left\lfloor \frac{u_0(\tau)}{x+y} \right\rfloor - \max\left\{0, \left\lceil \frac{-s_0(\tau)}{y} \right\rceil\right\} + 1\right\}. \tag{4.61}$$

Proof. We start by explicitly solving the Diophantine equation

$$\frac{1}{2}(n(x+y)^2+(\sigma\mu\pm x)^2-1)+x(\sigma\mu\pm(x+y))\mathcal{S}_0+\mu y\mathcal{S}_1 \\ +\frac{x^2}{2}\mathcal{S}_{00}+\sigma xy\mathcal{S}_{01}+\frac{y^2}{2}\mathcal{S}_{11}=0 \qquad (4.62)$$

over the integers. As discussed in the proof of Theorem 4.4, Eq. (4.62) is saturated on $r=0$ and $(x\mathcal{S}_0+\sigma y\mathcal{S}_1+\sigma\mu\pm x)^2=1$. This last condition can be rewritten as $x\mathcal{S}_0+\sigma y\mathcal{S}_1+\sigma\mu\pm x+\tau=0$, where $\tau\in\{-1,1\}$. With the notation introduced in Eq. (4.60) it reads $K_r(\tau)\pm 2(xs-yt)=0$, where $K_r(\tau)$ is defined as $K_r(\tau):=\pm n(y-x)+\sigma\mu\pm x+\tau$.

Notice how the assumptions of Theorem 4.4 guarantee that $K_r(\tau)$ is even: Indeed, if $n\equiv 0 \mod 2$, then $K_r(\tau)\equiv\mu+x+1\equiv 0 \mod 2$ (because the assumptions on Theorem 4.4 are that μ has opposite parity to x when n is even); otherwise, if $n\equiv 1 \mod 2$ then $K_r(\tau)\equiv y+\mu+1\equiv 0 \mod 2$ (because in this case μ has opposite parity to y when n is odd). Hence, we can define $K'_r(\tau):=K_r(\tau)/2$ and we just showed that $K'_r(\tau)\in\mathbb{Z}$.

Now, the condition $K_r(\tau)\pm 2(xs-yt)=0$ is equivalent to $K'_r(\tau)\pm(xs-yt)=0$, which we can solve for t: $yt=\pm K'_r(\tau)+xs$. This equation, when taken *modulo* x, reads $yt\equiv\pm K'_r(\tau) \mod x$. Since $\gcd(x,y)=1$ by hypothesis, this equation has a solution $t\equiv\pm y^{-1}K'_r(\tau) \mod x$, where y^{-1} is the inverse of y in the group of integers *modulo* x, typically denoted $\mathbb{Z}_x$, (such an inverse exists if, and only if, $\gcd(x,y)=1$). In practice, computation of y^{-1} is done via the Bézout identity, which says that for any pair of integers $x,y\in\mathbb{Z}$ there exist (not unique) $p,q\in\mathbb{Z}$ such that $px+qy=\gcd(x,y)$. In the case that $\gcd(x,y)=1$ when taking Bézout's identity *modulo* x we obtain $qy\equiv 1 \mod x$; because of the assumption $\gcd(x,y)=1$ of the theorem, the inverse of y *modulo* x is well defined and we can write $q\equiv y^{-1} \mod x$.

Let us now solve Eq. (4.62) for the other variables s,u, but we will keep the following form for t, to keep track of the total number of solutions: $t(\tau)=t_0(\tau)+kx$, where $k\in\mathbb{Z}$ and $0\leq t_0(\tau)<x$. Then, solving $K'_r(\tau)\pm(xs-yt)=0$ for s we obtain $s(\tau)=s_0(\tau)+ky$, where $s_0(\tau):=(\mp K'_r(\tau)+yt_0(\tau))/x$. Note that $s_0(\tau)$ is a well defined integer number, a fact that can be shown by directly solving $xs(\tau)=(\mp K'_r(\tau)+yt_0(\tau))+kxy$, because $yt(\tau)\equiv yt_0(\tau)\equiv\pm K'_r(\tau) \mod x$. The last variable u is directly obtained from the normalization condition $n=r+s+t+u$ (*cf.* Eq. (4.57)). Then,

we write $u = n - s - t$ as $u(\tau) = u_0(\tau) - k(x+y)$, where $u_0(\tau) := (nx + K'_r(\tau) - (x+y)t_0(\tau))/x$, which is integer by the same argument as $s_0(\tau)$.

To sum up, the family of points $(r,s,t,u) \in \mathbb{Z}^4$ for which (4.62) is fulfilled is

$$\bigcup_{\tau\in\{-1,1\}} \{[0, s_0(\tau), t_0(\tau), u_0(\tau)] + k[0, x, y, -(x+y)] : \ k \in \mathbb{Z}\} \qquad (4.63)$$

Geometrically, this corresponds to alternating points in a *zig-zag* pattern along two parallel lines which lie on the *facet* $r = 0$ of $\mathbb{T}_n$.

Conversely, let us now study and count which solutions really belong to $\mathbb{T}_n$; *i.e.* those for which $r, s, t, u \geq 0$. Since we have the family of solutions indexed by k, we just have to count how many k's are available. The condition $t \geq 0$ leads to $t_0 + kx \geq 0$, which for $k \in \mathbb{Z}$ means $k \geq \lceil -t_0/x \rceil$. Now, taking into account that t_0 is, by definition, chosen to be $0 \leq t_0 < x$, which is equivalent to $0 \geq -t_0/x > -1$; equivalently $\lceil -t_0/x \rceil = 0$. Thus, $k \geq 0$. The condition $s \geq 0$ becomes $s_0 + ky \geq 0$, which for $k \in \mathbb{Z}$ is $k \geq \lceil -s_0/y \rceil$. Finally, the condition $u \geq 0$ is equivalent to $u_0 - k(x+y) \geq 0$, which for $k \in \mathbb{Z}$ reads $k \leq \lfloor u_0/(x+y) \rfloor$.

Hence, for each $\tau \in \{-1, 1\}$, the number of solutions belonging to $\mathbb{T}_n$ is given by $|\{k \in \mathbb{Z} : k \geq \max\{0, \lceil -s_0(\tau)/y \rceil\}, k \leq \lfloor u_0(\tau)/(x+y) \rfloor\}|$; *i.e.*, $\max\{0, \lfloor u_0(\tau)/(x+y) \rfloor - \max\{0, \lceil -s_0(\tau)/y \rceil\} + 1\}$. Note that we put the first maximum just to ensure that there is always a non-negative number of solutions, denoted N_S. Finally, we can define N_S by summing this expression over the possible values for τ:

$$N_S := \sum_{\tau=\pm 1} \max\left\{0, \left\lfloor \frac{u_0(\tau)}{x+y} \right\rfloor - \max\left\{0, \left\lceil \frac{-s_0(\tau)}{y} \right\rceil\right\} + 1\right\}. \qquad (4.64)$$

□

If an inequality of the form (4.51, 4.52) is tight, then $N_S \geq 5$, because a 4-dimensional affine subspace is spanned by 5 points or more. Numerically, we could solve for $n \leq 33$ all facets of $\mathbb{P}_2^{\mathfrak{S}_n}$ and we saw that this condition was, not only necessary, but also sufficient. It is possible to prove this property analytically, by observing that 3 or more different points, with the same τ, are always linearly dependent. Nevertheless, the proof consists of a

n	# Bell inequalities in the class	Total # of tight Bell inequalities
5	16	152
10	272	2018
15	1208	7744
20	3592	21274
25	8248	46496
30	16688	90370

Table 4.1.: The second column shows the number of facets of $\mathbb{P}_2^{\mathfrak{S}_n}$ that belong to the class introduced in Theorem 4.4. The third column shows the total number of facets of $\mathbb{P}_2^{\mathfrak{S}_n}$, which are obtained by brute-force solving the polytope using the C-library Double Description method (CDD) algorithm [Fuk14]. Remarkably, the ratio between the second and the third columns grows with n.

tedious calculation that does not provide any particularly valuable insight, so we do not include it.

In Table 4.1 we have counted how many facets of $\mathbb{P}_2^{\mathfrak{S}_n}$ have the form of Theorem 4.4. Interestingly, already for $n = 30$ parties, we recover 18.5% of the total number of facets. In Appendix C we have collected the classes of inequalities for low n (see Tables C.1, C.2, C.3 and C.4).

4.3. Quantum Violation

In this section we shall analyze the form of the Bell operator corresponding to a Bell inequality for $\mathbb{P}_2^{\mathfrak{S}_n}$; *i.e.*, Bell inequalities of the form (4.22). When the l. h. s. of (4.22) is smaller than zero for some quantum states and measurements, then it signals nonlocality. A possible approach to show that quantum physics violates such an inequality is to fix the dimension D of $\mathcal{H}$ and find a quantum state and a set of POVMs such that the correlations obtained violate (4.22). In order to find the maximal quantum violation, one has to increase the dimension D in which the states are defined and the measurements are performed (*e.g.* the case for the CGLMP inequality [Col+02]). Fortunately, for the $(n, 2, 2)$ scenario, the maximal quantum violation is always obtained for $D = 2$ [TV06]. In this case, Toner and Verstraete showed that it is sufficient to perform traceless real observables

on qubits.

Let $\vec{\boldsymbol{\sigma}} := [\sigma_x, \sigma_y, \sigma_z]$ be the vector of Pauli matrices, and we will use the notation $\vec{\sigma}^{(i)}$ to indicate that they act on the i-th subsystem. Any traceless qubit observable with eigenvalues ± 1 can be expressed as $\hat{\mathbf{n}}\cdot\vec{\boldsymbol{\sigma}}$, where $\hat{\mathbf{n}} := [x, y, z]$ is a unit vector; *i.e.*, $\hat{\mathbf{n}}\cdot\vec{\boldsymbol{\sigma}} = x\sigma_x + y\sigma_y + z\sigma_z$, with $x^2+y^2+z^2 = 1$. Equivalently, x, y and z can be expressed in spherical coordinates in terms of sine and cosine functions. When restricting $\hat{\mathbf{n}}\cdot\vec{\boldsymbol{\sigma}}$ to be a real observable, this parametrization is simplified and it reads

$$\mathcal{M}_{x_i}^{(i)} = \cos\theta_{x_i}^{(i)}\sigma_z^{(i)} + \sin\theta_{x_i}^{(i)}\sigma_x^{(i)}, \tag{4.65}$$

where $\theta_{x_i}^{(i)} \in [0, 2\pi)$. For a simpler notation (since we will be working with two observables per site), we shall denote $\theta_{x_i}^{(i)}$ as φ_i when $x_i = 0$ or as θ_i when $x_i = 1$.

When all observables $\mathcal{M}_{x_i}^{(i)}$ have been fixed, the l. h. s. of (4.22) becomes the so-called Bell Operator, which we denote $\mathcal{B}(\{\varphi_i, \theta_i\})$. The eigenvector corresponding to the lowest eigenvalue (if this is negative) is the quantum state giving the maximal quantum violation for the measurements determined by $\{\varphi_i, \theta_i\}$. Hence, by optimizing over $\{\varphi_i, \theta_i\}$, one finds the overall maximal quantum violation, as well as which state to prepare and which measurements to perform in order to achieve it.

Even if a Bell Inequality displays some kind of symmetry with respect to exchange of parties (*i.e.*, it consists of G-invariant correlators 4.9 for some group $G \subseteq \mathfrak{S}_n$), the pure state for which this maximal quantum violation is achieved does not need to be G-invariant (In Sec. 4.6 we shall see an example of this), because the optimal observables $\{\varphi_i^*, \theta_i^*\}$ need not be the same at each site. As described in Sect. 4.6, at the expense of increasing $D = \dim\mathcal{H}$, one can construct a mixed state ρ and extended measurements with the aid of some ancillas, for which ρ is $G-$invariant and the extended measurements are the same for each party.

Nevertheless, for the current section, we focus on $G = \mathfrak{S}_n$, where numerics indicate that the maximal quantum violation is already achieved with a permutationally invariant quantum state and the same set of measurements at every site. This greatly simplifies our analysis, since the techniques introduced in Appendix A can be applied: The Bell Operator can be block-diagonalized, because by picking $\{\varphi_i, \theta_i\}$ independent of i, it becomes permutationally invariant. Hence, only 2 parameters, say $\{\varphi, \theta\}$ suffice

to describe all the measurements. Furthermore, (4.22) contains only 2-body correlators, which enables us to prove that $\mathcal{B}(\varphi,\theta)$ is a pentadiagonal operator in the Schur basis; sometimes tridiagonal.

As the proofs of the theorems in this section are rather long and technical, they have been moved to Appendix B.

4.3.1. Block-diagonalization of the Bell operator

The idea behind Schur-Weyl duality (*cf.* Theorem A.9) is that the Hilbert space splits into blocks, on which the representations of the symmetric group $\mathfrak{S}_n$ and the unitary group $\mathcal{U}$ commute. These blocks are easily found for the qubit case, by projecting onto the elements of Eq. (A.18).

In the following theorem, we give the analytical form of each of these blocks, when the same set of traceless real observables is performed by every party:

$$\mathcal{M}_0^{(i)} = \cos\varphi\sigma_z^{(i)} + \sin\varphi\sigma_x^{(i)}, \qquad \mathcal{M}_1^{(i)} = \cos\theta\sigma_z^{(i)} + \sin\theta\sigma_x^{(i)}. \tag{4.66}$$

Theorem 4.6. *The J-th Block $\mathcal{B}_J(\varphi,\theta)$ of the Bell operator corresponding to a 2-body symmetric Bell inequality (4.22), with measurements given by (4.66), has elements $(\mathcal{B}_J(\varphi,\theta))_l^k$ (k-th row, l-th column), where $0 \leq k,l, \leq 2J$; those elements are given by*

$$(\mathcal{B}_J(\varphi,\theta))_l^k = d_k\delta_{k,l} + u_k\delta_{k,l-1} + u_l\delta_{k-1,l} + v_k\delta_{k,l-2} + v_l\delta_{k-2,l}, \tag{4.67}$$

where d_k ($0 \leq k \leq 2J$) stand for the elements of the diagonal, u_k ($0 \leq k \leq 2J-1$) correspond to the elements of the upper (lower) diagonal and v_k ($0 \leq k \leq 2J-2$) stand for the elements of the second upper (lower) diagonal and $\delta_{k,l}$ is the Kronecker delta function ($\delta_{k,l} = 1 \iff k = l$, otherwise $\delta_{k,l} = 0$). The values of the coefficients d_k, u_k, v_k are given by

$$\begin{aligned} d_k &:= \beta_c + (2J-2k)A + ((2J-2k)^2 - n)B/2 + (2k(2J-k) - m)C/2, \\ u_k &:= (A' + (2J-1-2k)D)\sqrt{(2J-k)(k+1)}, \\ v_k &:= C\sqrt{(2J-k)(2J-k-1)(k+1)(k+2)}/2, \end{aligned}$$

where the parameters A, A', B, C, D depend only on the Bell Inequality coeffi-

cients and the measurements' angles:

$$\begin{aligned} A &:= \alpha\cos\varphi + \beta\cos\theta, \\ A' &:= \alpha\sin\varphi + \beta\sin\theta, \\ B &:= \gamma\cos^2\varphi + 2\delta\cos\varphi\cos\theta + \varepsilon\cos^2\theta, \\ C &:= \gamma\sin^2\varphi + 2\delta\sin\varphi\sin\theta + \varepsilon\sin^2\theta, \\ D &:= \gamma\cos\varphi\sin\varphi + \delta\cos\varphi\sin\theta + \delta\cos\theta\sin\varphi + \varepsilon\cos\theta\sin\theta. \end{aligned} \tag{4.68}$$

Let us notice that Eq. (4.67) ensures that ever block $\mathcal{B}_J$ of the Bell operator is pentadiagonal, because we are considering a permutationally invariant Bell inequality with, at most, 2-body correlators. If it included 3-body correlators, it would be heptadiagonal, and so on. It is now immediate to see that some entangled states cannot be detected by few-body Bell inequalities[18]. However, there exist other classes of states, some of them experimentally realizable, that show nonlocality in a robust way, as we shall introduce in this section and in Section 4.4.

Eq. (4.67) has important numerical implications, because it allows to store the whole Bell operator in a sparse matrix. This way, one can easily show nonlocality of GME states comprising more than 10^4 qubits. This optimization is carried by varying φ and θ and looking at the smallest eigenvalue of each of the blocks $\mathcal{B}_J(\varphi,\theta)$, and one needs to check $\lfloor n/2 \rfloor$ of them. In fact, this optimization depends only on one parameter: the difference between θ and φ, as we state in Theorem 4.7:

Theorem 4.7. *Let $\mathcal{B}(\varphi,\theta)$ denote the Bell operator corresponding to the measurements described in (4.66). Then, the expectation value $\langle\mathcal{B}(\varphi,\theta)\rangle_\rho := \mathrm{Tr}\mathcal{B}(\varphi,\theta)\rho$ depends only on $\theta-\varphi$. More precisely,*

$$\forall c\in\mathbb{R},\ \langle\mathcal{B}(\varphi,\theta)\rangle_\rho = \langle\mathcal{B}(\varphi+c,\theta+c)\rangle_{\rho'},$$

where $\rho' = \mathcal{U}\rho\mathcal{U}^\dagger$ and $\mathcal{U}$ is a unitary transformation given by $\mathcal{U} := U^{\otimes n}$,

[18] Take, for example, the Greenberger-Horne-Zeilinger (GHZ) state $2^{-n/2}(|0\rangle^{\otimes n} + |1\rangle^{\otimes n})$, which is supported on the last block $J = n/2$ of the decomposition (A.16). The density matrix of the state has only four terms; two of them in the diagonal, and the remaining ones are the coherences $|D_n^n\rangle\langle D_n^0|$ and $|D_n^0\rangle\langle D_n^n|$, which can be reached only a full-body correlator. Hence, to a not-full-body correlations symmetric Bell inequality, the GHZ state is indistinguishable from the separable mixture $|0\rangle\langle 0|^{\otimes n}/2 + |1\rangle\langle 1|^{\otimes n}/2$.

where U is the unitary matrix

$$U = \begin{pmatrix} \cos(c/2) & -\sin(c/2) \\ \sin(c/2) & \cos(c/2) \end{pmatrix}. \tag{4.69}$$

Furthermore, $\mathcal{B}(\varphi + c, \theta + c) = \mathcal{U}\mathcal{B}(\varphi, \theta)\mathcal{U}^\dagger$.

Observe that Theorem 4.7 can be interpreted as follows: by rotating the state and the measurements accordingly, the spectrum of the Bell operator remains invariant. We can use this fact in order to simplify our analysis of the maximal quantum violation. First of all, the constant C defined in Eq. (4.68) can be taken to be zero by an appropriate choice of $\theta - \varphi$. With this choice, $\mathcal{B}$ becomes tridiagonal; *i.e.*, even simpler. The dependency between θ and $\kappa := \theta - \varphi$ can be found analytically:

Theorem 4.8. *The Bell operator $\mathcal{B}(\varphi, \theta)$ is tridiagonal when*

$$\theta_\pm = \arctan\left(\frac{\gamma \sin\kappa}{\gamma\cos\kappa + \delta \pm \sqrt{\delta^2 - \gamma\varepsilon}}\right). \tag{4.70}$$

4.3.2. Analytical class of states

Here we introduce a new class of states, which has an analytical expression, that violates the Bell inequalities belonging to the class of Theorem 4.4. In Section 4.3.3 we show that this class asymptotically converges to the state giving maximal quantum violation as n grows. Such class of states is unitarily equivalent to a Gaussian superposition of Dicke states with variance growing as $O(\sqrt{n})$, centered at $\min_k d_k$ (*cf.* Theorem 4.6). We have found that the maximal quantum violation is achieved in the symmetric block $J = n/2$, although other blocks also have quantum violation (decreasing in magnitude as J decreases)[19].

Theorem 4.9. *Let $|\psi_n\rangle = \sum_{k=0}^{n} \psi_k^{(n)} |D_n^k\rangle$ be a symmetric n-qubit state with the following coefficients, expressed in the Dicke basis:*

$$\psi_k^{(n)} = \frac{e^{-(k-\mu)^2/4\sigma}}{\sqrt[4]{2\pi\sigma}}, \tag{4.71}$$

[19] In other scenarios, such as $(n, 3, 2)$, we have also found other classes of Bell inequalities maximally violated with states supported on the lowest J blocks.

where $\mu = \frac{n}{2} + \frac{A}{2B-C}$ *and* $e^{-1}/2\pi \ll \sigma \ll n$ *and the constants are taken from the definition of Theorem 4.6. Let* $\varphi(\theta)$ *be the choice of* φ *such that* $C = 0$*, as in Theorems 4.7, 4.8. Then, the value of* $\langle\psi_n|\mathcal{B}_{n/2}(\varphi(\theta),\theta)|\psi_n\rangle$ *is given by*

$$\left(\frac{\beta_c}{n} - \frac{B}{2} + E\right) n + \left(2B\sigma - \frac{A^2}{2B} + E\right) + o(\sigma n^{-1}), \tag{4.72}$$

where $E := e^{-1/8\sigma}\left(A' - \frac{AD}{B}\right)$.

Let us briefly comment on the choice of the parameters μ and σ. Because d_k is a quadratic function in k, it has an extremum, which is $k = \mu$. If $\mathcal{B}$ were diagonal, then $d_{[\mu]}$, where $[\cdot]$ is the rounding function, would be its minimal eigenvalue. However, $d_k \geq 0$ for the inequalities of Theorem 4.4, so that a superposition of Dicke states is necessary to violate them. The parameter σ has to be in a range in such the off-diagonal elements u_k play a role in this, and such range is limited to the approximations used in the proof remaining valid.

Example 4.10. *Let us illustrate Theorem 4.9 with an example. We take the Bell inequality used in [Tur+14a] and show how the class of states (4.9) violates it robustly for large* n*. This Bell inequality is the one of Theorem 4.4 for the particular parameters* $x = y = 1$*,* $\sigma = \pm = -1$ *and* $\mu = 0$*, which has the expression*

$$-2\mathcal{S}_0 + \frac{1}{2}\mathcal{S}_{00} - \mathcal{S}_{01} + \frac{1}{2}\mathcal{S}_{11} + 2n \geq 0, \tag{4.73}$$

for which $C = (\sin\varphi - \sin\theta)^2$.

In order to make $C = 0$ *(and* $\mathcal{M}_0 \neq \pm\mathcal{M}_1$*) we pick* $\varphi = \pi - \theta$*. This already defines the value of the constants* A, A', B, C *and* D*:*

$$\begin{aligned} A &= 2\cos\theta, \\ A' &= -2\sin\theta, \\ B &= 4\cos^2\theta, \\ C &= 0, \\ D &= 0. \end{aligned}$$

The form of the Bell operator $\mathcal{B}_{n/2}(\pi-\theta,\theta)$ is the following:

$$\begin{aligned} d_k &= 2n(1+\cos\theta+(n-1)\cos^2\theta)-[4\cos\theta(1+2n\cos\theta)]k+[8\cos^2\theta]k^2, \\ u_k &= -2\sin\theta\sqrt{(n-k)(k+1)}, \\ v_k &= 0. \end{aligned}$$

We are now ready to calculate the parameters of the class in Theorem 4.9 are

$$\mu_n = \frac{n}{2}+\frac{1}{4\cos\theta}, \tag{4.74}$$

and $\sigma_n \in \Theta(\sqrt{n})$, which fulfills the requirements for the validity of the approximations of Theorem 4.9.

Theorem 4.9 gives the asymptotic expectation value:

$$\begin{aligned} & \langle\varphi_n|\mathcal{B}_{n/2}(\pi-\theta,\theta)|\varphi_n\rangle \\ \simeq\ & \left(\frac{\beta_c}{n}-\frac{B}{2}+e^{-1/8\sigma}A'\right)n+\left(2B\sigma-\frac{A^2}{2B}+e^{-1/8\sigma}A'\right)+o(\sigma n^{-1}). \end{aligned}$$

And we obtain the optimal θ, denoted θ^*, by optimizing over the leading term:

$$\frac{\beta_c}{n}-\frac{B}{2}+e^{-1/8\sigma}A' \simeq \frac{\beta_c}{n}-\frac{B}{2}+A' = 2(1-\cos^2\theta-\sin\theta) \Rightarrow \theta^* \in \{\pi/6, 5\pi/6\}.$$

As a result, the quantum violation relative to the classical bound reads (taking $\sigma=\sqrt{n}$ for simplicity)

$$\langle\varphi_n|\mathcal{B}_{n/2}(\pi/6,5\pi/6)|\varphi_n\rangle/\beta_c \simeq -\frac{1}{4}+3n^{-1/2}-\frac{3}{4}n^{-1}+o(n^{-3/2}),$$

which shows that quantum violation exists for large n and it tends to $-1/4$ when compared to the classical bound as $n \longrightarrow \infty$.

4.3.3. Accuracy of analytical results

In the current section, we show how the class of states of Theorem 4.9 performs in practice; *i.e.*, when we compare it with the values given by numerical optimization. In all comparisons we take the particular Bell inequality given in the previous example, (4.73). The state maximally

violating it, as we have discussed, is a superposition of Dicke states. We denote it $|\psi_n^{\min}\rangle$ and it has the form

$$|\psi_n^{\min}\rangle = \sum_{k=0}^{n} c_k^{(n)} |D_n^k\rangle, \tag{4.75}$$

where $c_k^{(n)}$ are real coefficients, a direct consequence of the Bell operator being a real symmetric matrix. In Figure 4.2 one can see that an interesting regularity appears as n grows in the $c_k^{(n)}$, when seen as a function of k. Figure 4.2 displays the coefficients of the optimal state for $\mathcal{B}(0, \theta^* - \varphi^*)$, where $\theta - \varphi$ has been optimized numerically. However, if φ^* is chosen such that $C = 0$, then the form of the $c_k^{(n)}$, which we denote $\alpha_k^{(n)}$ for this case; *i.e.*, the coefficients of the eigenstate corresponding to the lowest eigenvalue of $\mathcal{B}(\varphi^*, \theta^*)$, changes. The $\alpha_k^{(n)}$ are represented in Figure 4.3, where they are compared to the analytical state which is proposed in Theorem 4.9, where a good agreement is found. The relative difference between the optimal numerical and the optimal analytical state is compared in Figure 4.4. Observe that, by virtue of Theorem 4.7, both $c_k^{(n)}$ and $\alpha_k^{(n)}$ lead to the same quantum violation as long as the parties rotate the measurements accordingly.

4.3.4. The two-body reduced density matrix

There are basically two ways to operate with a Bell inequality of the form (4.22). One is the one we have been using, which deals with the block-diagonalization of the Bell operator $\mathcal{B}$, where exact diagonalization can be performed inexpensively on the different blocks $\mathcal{B}_J$. The other uses the fact that, when a number of subsystems is traced out of a permutationally invariant quantum state, it does not matter which subsystems are chosen, that the reduced density matrix is always the same. Hence, by knowing the reduced 2-body density matrix of a quantum state, it contains enough information to know whether it can violate (4.22).

Let us denote by ρ_2 the two-body reduced density matrix of $|\psi\rangle$ and let $\mathcal{M}_0$ and $\mathcal{M}_1$ be the pair of measurements that the parties perform. Then, the collection of expectation values $\{\langle \mathcal{M}_k \otimes \mathcal{M}_l \rangle_{\rho_2}\}_{kl}$ and $\{\langle \mathcal{M}_k \otimes \mathbb{1}_2 \rangle_{\rho_2}\}_k$ is sufficient to calculate the quantum expecation value of $\mathcal{B}$. One simply

has to multiply them by the number of times that they appear in $\mathcal{S}_{kl}$ and $\mathcal{S}_k$:

$$\beta_c + n\left(\alpha\langle\mathcal{M}_0\otimes\mathbb{1}_2\rangle_{\rho_2} + \beta\langle\mathcal{M}_1\otimes\mathbb{1}_2\rangle_{\rho_2}\right) + n(n-1)\left(\frac{\gamma}{2}\langle\mathcal{M}_0\otimes\mathcal{M}_0\rangle_{\rho_2} + \delta\langle\mathcal{M}_0\otimes\mathcal{M}_1\rangle_{\rho_2} + \frac{\varepsilon}{2}\langle\mathcal{M}_1\otimes\mathcal{M}_1\rangle_{\rho_2}\right) \quad (4.76)$$

If (4.76) is negative, then nonlocality is detected.

In the following theorem, we show how to compute such reduced state:

Theorem 4.11. *Let ρ be the density matrix of an n-qubit state supported on the symmetric space. Let $\rho_{\mathcal{S}}$ be the representation of ρ in the symmetric space. Let us denote by $\mathrm{Tr}_{n-d}(\rho)$ the density matrix of ρ after tracing out $n-d$ subsystems. This reduced density matrix is given by*

$$\left(\mathrm{Tr}_{n-d}(\rho)\right)^{\mathbf{i}'}_{\mathbf{j}'} = \sum_{k=0}^{n-d} \frac{\binom{n-d}{k}(\rho_{\mathcal{S}})^{k+|\mathbf{i}'|}_{k+|\mathbf{j}'|}}{\sqrt{\binom{n}{k+|\mathbf{i}'|}\binom{n}{k+|\mathbf{j}'|}}}, \quad (4.77)$$

where $0 \leq \mathbf{i}', \mathbf{j}' < 2^d$, $\mathbf{i}' = i_0 \ldots i_{d-1}$ and $\mathbf{j}' = j_0 \ldots j_{d-1}$ are represented in binary and $|\mathbf{i}'|, |\mathbf{j}'|$ is their number of ones in this binary representation. Columns are indexed by $\mathbf{i}'$ and rows are indexed by $\mathbf{j}'$.

As we are mostly interested in the limit for large n, it is convenient to take a closer look at the $\binom{n-d}{k}\left[\binom{n}{k+|\mathbf{i}'|}\binom{n}{k+|\mathbf{j}'|}\right]^{-1/2}$ factor appearing in Eq. (4.77). As binomial numbers grow very rapidly, from the point of view of numerics, formula (4.77) can be affected if they are not handled carefully. In particular, for $n \gtrsim 650$, they can take values greater than 10^{308}, which is the storage limit for 64-bit floating point arithmetic. It is therefore necessary to simplify this expression. Hence, let us define

$$f(n,k,d,|\mathbf{i}'|,|\mathbf{j}'|) := \binom{n-d}{k}\left[\binom{n}{k+|\mathbf{i}'|}\binom{n}{k+|\mathbf{j}'|}\right]^{-1/2}. \quad (4.78)$$

Observe that f is a symmetric function in $|\mathbf{i}'|$ and $|\mathbf{j}'|$. Furthermore, it fulfills the geometric mean property

$$f(n,k,d,|\mathbf{i}'|,|\mathbf{j}'|) = \sqrt{f(n,k,d,|\mathbf{i}'|,|\mathbf{i}'|)f(n,k,d,|\mathbf{j}'|,|\mathbf{j}'|)}. \quad (4.79)$$

In the present context, we shall be interested in the $d = 1, 2$ case, which we introduce below (by means of Eq. (4.79) one can derive the rest of the values).

$$f(n,k,1,0,0) = \frac{n-k}{n}, \qquad f(n,k,1,1,1) = \frac{k+1}{n}. \tag{4.80}$$

$$f(n,k,2,0,0) = \frac{n-k}{n}\cdot\frac{n-k-1}{n-1}, \quad f(n,k,2,1,1) = \frac{n-k-1}{n}\cdot\frac{k+1}{n-1},$$

$$f(n,k,2,2,2) = \frac{k+1}{n}\cdot\frac{k+2}{n-1}. \tag{4.81}$$

In the spirit of Theorem 4.9, we can now study the asymptotic behavior of the reduced 2-body state ρ_2.

Theorem 4.12. *Let $|\psi\rangle$ be the state introduced in Theorem 4.9. Its two-body reduced state ρ_2 can be well approximated for large n as*

$$\rho_2 = \frac{1}{n(n-1)}\left(n^2 P_{++} + n\begin{pmatrix} -(1+2c)/2 & -c/2 & -c/2 & 1/2 \\ -c/2 & 0 & 0 & c/2 \\ -c/2 & 0 & 0 & c/2 \\ 1/2 & c/2 & c/2 & (2c-1)/2 \end{pmatrix} + o(n)\right), \tag{4.82}$$

where $c = \mu - n/2$ and P_{++} is the projector onto the state $[(|0\rangle + |1\rangle)/\sqrt{2}]^{\otimes 2}$.

Let us remark on Theorem 4.12. ρ_2 tends to a separable state P_{++}, which is clear by monogamy of entanglement (also from a de Finetti argument). Let us point out that, on the one hand, in Theorem 4.9 we observe that the quantum violation increases linearly with n, whereas Theorem 4.12 indicates that ρ_2 goes to a separable state. The reason for this apparent contradiction is that the coefficients of the inequalities defined in Theorem 4.4 are picked in such a way that the state P_{++} has expectation value exactly zero on them. Hence, the quantum violation comes from the second order term in Eq. (4.82).

4.3.5. Robustness

Let us discuss the robustness against different types of noises of the Bell inequalities introduced so far. To this end, we concentrate on the Bell inequality (4.73).

Misalignments

As Fig. 4.5 shows, the quantum violation relative to the classical bound of Inequality (4.73) is more robust as n grows. Moreover, the Bell inequality is very insensitive to the relative misalignment between the two measurements that are performed, which is measured by $\theta - \varphi$ (*cf.* Eq. (4.66)). As Theorem 4.7 shows, the only relevant parameter is the difference between θ and φ; however, the state that should be measured does depend both on θ and ϕ (see Figs. 4.2 and 4.3).

White noise

Let $|\psi_n\rangle$ be defined as in (4.71). Assuming that, due to interaction with the environment, we actually have a partially depolarized mixture with white noise

$$\rho_n(p) = (1-p)|\psi_n\rangle\langle\psi_n| + p\frac{\mathbb{1}_{2^n}}{2^n}, \tag{4.83}$$

where p is a mixing parameter. By a continuity argument, there always exists a range $0 \leq p < p_n^{\text{cr}}$ for which $\rho_n(p)$ still violates (4.73) with the same measurement settings as $|\psi_n\rangle$. The critical value p_n^{cr} is the minimal amount of noise that has to be added so that one can simulate the observed correlations with a local hidden variable model. The behavior of p_n^{cr} with n is shown in Fig. 4.6, where we see that the tolerance to noise increases with n, asymptotically tending to

$$\lim_{n\to\infty} p_n^{\text{cr}} = \frac{1}{5}. \tag{4.84}$$

Particle losses

Now we propose the following situation: in an experiment in which the maximal violation of (4.73) is tested, n' out of the original n particles that constitute the state $|\psi_n\rangle$ described in Theorem 4.9 have been lost. The remaining $n-n'$ particles form a mixed state, described by a density matrix which we denote $\rho_{n,n'}$. Notice that, as $|\psi_n\rangle \in \mathcal{S}(\mathcal{D}(\mathbb{C}^2)^{\otimes n})$, tracing out any set of n' particles results into $\rho_{n,n'}$. Theorem 4.11 tells us how to explicitly find the expression for $\rho_{n,n'}$.

n	n'_{cr}	$n - n'_{\text{cr}}$
10	0	10
10^2	23	77
10^3	301	699
10^4	3232	6768

Table 4.2.: The maximal number of particles that can be lost, n'_{cr}, such that the Bell inequality (4.73) remains violated by the reduced state$\rho_{n,n'_{\text{cr}}}$ of $|\psi_n\rangle$. A few values of n are shown. The ratio between the second and the first column shows that the robustness grows with n.

We plan to study the quantum violation of (4.73) with the state $\rho_{n,n'}$ and, in particular, to find which is the critical n', denoted n'_{cr}, such that nonlocality is still detected. To this end, we take the same measurements and adjust the classical bound $\beta_c(n)$ to the one of $n-n'$ particles: $\beta_c(n-n')$. We report the results in Table 4.2, where we see that the tolerance to particle losses grows with n, achieving a ratio of almost $1/3$ for $n = 10^4$, showing that inequalities of the type (4.73) are quite robust to this kind of losses.

4.4. Inequalities for the Dicke States

The class of states introduced in Theorem 4.9 are the ones which work best for detecting nonlocality in $\mathbb{P}_2^{\mathfrak{S}_n}$, via the class of Bell inequalities introduced in Theorem 4.4[20]. However, it may be difficult to prepare a Gaussian superposition of Dicke states like the one of Theorem 4.9 in an experiment. This is why, in this section, we look for nonlocality of more physical states, such as ground states of physical Hamiltonians, that is revealed by $\mathbb{P}_2^{\mathfrak{S}_n}$. The Dicke states (2.27) constitute an example of these states, as they appear as ground states of the isotropic Lipkin-Meshkov-Glick

[20] Since numerically we could easily solve the polytope $\mathbb{P}_2^{\mathfrak{S}_n}$ for $n \leq 33$, the best inequalities (in terms of the maximal quantum violation over the classical bound) were found to be those from Theorem 4.4.

(LMG) Hamiltonian [LMG65]:

$$H = -\frac{\lambda}{n}\sum_{i<j}\left(\sigma_x^{(i)}\sigma_x^{(j)} + \sigma_y^{(i)}\sigma_y^{(j)}\right) - h\sum_{i=1}^{n}\sigma_z^{(i)}. \tag{4.85}$$

The LMG Hamiltonian describes n spins which interact through the ferromagnetic coupling ($\lambda > 0$) under a magnetic field in the z direction of intensity h. By tuning the value of h, the ground state of (4.85) sweeps over all Dicke states $|D_n^k\rangle$. This is easily seen by representing H in the Schur-Weyl basis (*cf.* Theorem B.1).

The interactions in (4.85) occur over all possible pairs. However, it is also possible to engineer a good approximation of this Hamiltonian for low n as a ground state of a one-dimensional ferromagnetic spin-$1/2$ XXZ Hamiltonian with nearest-neighbor interactions [Zho+11]. Recall that every n-qubit symmetric state (either pure or mixed) is entangled if, and only if, it is genuinely multipartite entangled [Eck+02; Aug+12]. Hence, every Dicke state $|D_n^k\rangle$ is entangled for $k > 0$ and $k < n$. Interestingly, entangled n-qubit symmetric states have been shown to be genuinely multipartite nonlocal [Che+14]. The experimental realization of Dicke states is already within reach of current technologies, and we discuss the state-of-the-art in Section 4.7.

In this section, we present two new classes of Bell inequalties from $\mathbb{P}_2^{\mathfrak{S}_n}$ that detect the nonlocality of every Dicke state $|D_n^k\rangle$ for $0 < k < n$. Obviously, they do not apply to the cases $k \in \{0, n\}$ since $|D_n^0\rangle = |0\rangle^{\otimes n}$ and $|D_n^n\rangle = |1\rangle^{\otimes n}$ are both fully separable. The first class we present, in Theorem 4.13, covers those Dicke states for which $0 < k \lesssim 3n/10$ (or $7n/10 \lesssim k < n$ by an appropriate symmetry[21] of the Bell inequality). The second class is presented in Theorem 4.14 and it detects the rest of Dicke states; those which are closer to the most balanced one $3n/10 \lesssim k \lesssim 7n/10$, which corresponds to a weak magnetic field in (4.85). The limits $3n/10$ and $7n/10$ have been taken in a conservative manner, as the Dicke states nearby are detected by both classes (*cf.* the overlap in Figure reffig:dickeviol). The analysis of the quantum violation of Dicke states $|D_n^k\rangle$ is very simplified thanks to Theorem 4.6, which is $\langle D_n^k|\mathcal{B}|D_n^k\rangle = d_k$.

[21] One simply renames the outcomes of all the observables

Theorem 4.13. *The inequality (4.22) defined through the parameters*

$$\beta_c = (1+2k)((n-2k-1)^2+n-1),$$
$$\alpha = \beta = (1+2k)(n-1-2k), \qquad \gamma = \varepsilon = k, \quad \delta = k+1, \tag{4.86}$$

where $0 \leq k \leq (n-1)/2$*, is a valid Bell inequality for* $\mathbb{P}_2^{\mathfrak{S}_n}$ *for any* n*.*

Theorem 4.14. *Let* $\nu = \lfloor n/2 \rfloor - k$*. The inequality (4.22) defined through the parameters*

- *If* $n \equiv 0 \bmod 2$*:*

$$\beta_c = \binom{n}{2}(n+2(2\nu^2+1)),$$
$$\alpha = 2\nu n(n-1),\ \beta = \alpha/n, \qquad \gamma = n(n-1),\ \delta = n,\ \varepsilon = -2. \tag{4.87}$$

- *If* $n \equiv 1 \bmod 2$*:*

$$\beta_c = \binom{n}{2}(n+3+4\nu(\nu+1)),$$
$$\alpha = (1+2\nu)n(n-1),\ \beta = \alpha/n, \quad \gamma = n(n-1),\ \delta = n,\ \varepsilon = -2. \tag{4.88}$$

where $0 \leq \nu \leq \lfloor n/2 \rfloor - 1$*, is a valid Bell inequality for* $\mathbb{P}_2^{\mathfrak{S}_n}$ *for any* n*.*

4.4.1. Quantum violation of the Dicke states

Let us now find which are the best measurements that one can perform on the Dicke states $|D_n^k\rangle$ in order to detect nonlocality with either (4.86) or (4.87, 4.88). In virtue of Theorem 4.6, the expectation value $\langle D_n^k|\mathcal{B}(\varphi,\theta)|D_n^k\rangle$ is already given by d_k. However, the main difference with Section 4.3 is that the quantum state is now fixed. Hence, the result of Toner and Verstraete [TV06] does not apply and we cannot suppose that we can achieve the maximal violation of the Bell inequalities (4.86) nor (4.87, 4.88)[22]. Theorem 4.6 can be easily generalized to arbitrary qubit measurements

[22] We have numerically checked that the inequalities presented are optimal (with respect to the quantum violation relative to the classical bound) for the Dicke states. But the Dicke states need not be the optimal states for such inequalities; in general, they are not.

$\mathcal{M}_0 = \hat{\mathbf{n}}_0 \cdot \vec{\sigma}$, $\mathcal{M}_1 = \hat{\mathbf{n}}_1 \cdot \vec{\sigma}$, by using the results of Theorem B.1. Let us denote by $\mathcal{B}(\hat{\mathbf{n}}_0, \hat{\mathbf{n}}_1)$ the Bell Operator corresponding to such measurements. It is possible to prove that the expectation value $\langle D_n^k | \mathcal{B}(\hat{\mathbf{n}}_0, \hat{\mathbf{n}}_1) | D_n^k \rangle$ only depends on the difference between the azimuthal angles (taking spherical coordinates) that $\hat{\mathbf{n}}_0$ and $\hat{\mathbf{n}}_1$ define in the Bloch Sphere. This expectation value is minimal when such difference is zero. Hence, there is no loss of generality in considering real observables, implying that the expression for d_k given in Theorem 4.6 applies.

Let us begin with considering the class of Bell inequalities (4.86). In this case, because of the symmetry in the coefficients, the expectation value $\langle D_n^k | \mathcal{B}(\varphi, \theta) | D_n^k \rangle$ is a symmetric function of φ and θ. Numerically we observe that its minimum is obtained at $\varphi = -\theta$. With this ansatz, our analysis is greatly simplified, and we can get an analytically closed form for the optimal $\langle D_n^k | \mathcal{B}(-\theta^*, \theta^*) | D_n^k \rangle$. Indeed, after some algebra, solving

$$\frac{\partial}{\partial \theta} d_k(-\theta, \theta) = 0 \tag{4.89}$$

leads to the following non-trivial solutions:

$$\theta^* = \pm 2 \arccos \pm \sqrt{\frac{C_1}{C_2}}, \tag{4.90}$$

where $C_1 = k(n - (1 + 3k))$ and $C_2 = n^2(2k + 1) - n(8k^2 + 4k + 1) + 2k^2(1 + 4k)$; the two $\pm$ signs are independent. Using this optimal angle θ^*, the maximal quantum violation $\langle D_n^k | \mathcal{B}(-\theta^*, \theta^*) | D_n^k \rangle$ is given by

$$d_k(-\theta^*, \theta^*) = -\frac{4C_1^2}{C_2}. \tag{4.91}$$

For the other class of Bell inequalities (4.87, 4.88), the proof of existence of quantum violation goes along the same lines. In [Tur+14a] it was proved for $k = \lceil n/2 \rceil$, where $\mathcal{M}_0 = \sigma_z$ was assumed for simplification. Its numerical optimization is discussed in the Supplemental material of [Tur+14a].

We report below the numerical results obtained for the maximal quantum violation of the inequalities of Theorems 4.13 and 4.14, for $n = 2^{10}$, in Fig. 4.7.

4.5. Generalization

In this section, we discuss how the methodology introduced in Section 4.1 can be generalized to any Bell scenario (n, m, d) with n parties having m d-outcomed measurements, and to obtain Bell inequalities with, at most, K-body correlators.

The main goal is to generalize Eq. (4.23), so that one can construct, from a space of parameters which will be the set of points of a simplex with integer coordinates (*cf.* Eq. (4.24)), all vertices of $\mathbb{P}_K^{\mathfrak{S}_n}$ for any scenario. Moreover, as the main ingredient in the proof of Theorem 4.2 is the orthogonality of $\mathcal{Z}$ with $\mathcal{S}_0$, $\mathcal{S}_1$ and n (*cf.* Eq. (4.23)), finding new $\mathcal{Z}$'s will indicate in which points of the generalized $\mathbb{T}_n$ to look for, in order to discard vertices of $\mathbf{P}_L$ that get projected to the interior of $\mathbb{P}_K^{\mathfrak{S}_n}$, hence lowering the bound (4.12), as in Remark 4.3.

Let us begin by defining the set of basic variables, which were named a, b, c and d in Section 4.1 (*cf.* Eq. 4.16). In this case, we shall use a vector, denoted $\mathbf{y} \in Y := [0, d-1]^m \cap \mathbb{Z}^m$; *i.e.*, $\mathbf{y}$ is an m-dimensional vector of integer coordinates between 0 and $d-1$. Hence, any DLS $f : X \longrightarrow Y$ is such that, to every party in X, it assigns a color $\mathbf{y}$. We have the constraint that $\sum_{\mathbf{y}\in Y} |f^{-1}(\mathbf{y})| = n$. When the DLS f is clear from the context, we shall use the shorter notation $c_{\mathbf{y}} := |f^{-1}(\mathbf{y})|$.

Hence, we have a generalized tetrahedron

$$\mathbb{T}_{n,m,d} := \{(c_{\mathbf{y}})_{\mathbf{y}} \in \mathbb{Z}^{d^m} : c_{\mathbf{y}} \geq 0, \sum_{\mathbf{y}} c_{\mathbf{y}} = n\}. \tag{4.92}$$

Let us first introduce the symmetric correlators in terms of the no-signalling probabilities $P(a_0, \ldots, a_{n-1}|x_0, \ldots, x_{n-1})$, which, for short, we denote $P(\mathbf{a}|\mathbf{x})$. For identifying the marginal probability distributions of $P(\mathbf{a}|\mathbf{x})$ we shall add a subindex $i_1, \ldots, i_k$ to P to indicate to which parties does the marginal probability distribution correspond to, and we denote it as $P_{i_1,\ldots,i_k}(a_{i_1}, \ldots, a_{i_k}|x_{i_1}, \ldots, x_{i_k})$. Unless stated otherwise, we allow for any configuration $i_1, \ldots, i_k$ such that $i_j \neq i_k$ for any $j \neq k$; *i.e.*, we do not restrict ourselves to the case where the parties in the marginal are ordered: $i_1 < \ldots < i_k$. For a shorter notation, we shall use $P_{\mathbf{i}}(\mathbf{a}|\mathbf{x}) := P_{i_1,\ldots,i_k}(a_{i_1}, \ldots, a_{i_k}|x_{i_1}, \ldots, x_{i_k})$, whenever k is clear from the context and understanding that we do a slight abuse of notation because $\mathbf{a}$ and $\mathbf{x}$ have k components, instead of n.

Then, the K-th order Symmetric correlator corresponding to the $\mathbf{a}$-th outcomes of the $\mathbf{x}$-th measurements is defined as

$$P^{\mathbf{a}}_{\mathbf{x}} := \sum_{\substack{i_1,\dots,i_K \\ i_x \neq i_y}} P_{\mathbf{i}}(\mathbf{a}|\mathbf{x}). \tag{4.93}$$

For instance, the first and second order symmetric correlators would be $P^a_x = \sum_{i=0}^{n-1} P_i(a|x)$ and $P^{ab}_{xy} = \sum_{i\neq j} P_{ij}(ab|xy)$, respectively. Observe that $P^{ab}_{xy} = P^{ba}_{yx}$. In fact, for any permutation $\sigma \in \mathfrak{S}_K$, one has that $P^{\sigma(\mathbf{a})}_{\sigma(\mathbf{x})} = P^{\mathbf{a}}_{\mathbf{x}}$. Hence, we can suppose, without loss of generality, that the elements in $\mathbf{x}$ are lexicographically ordered.

Let us now introduce an auxiliary quantity, $Q^{\mathbf{a}}_{\mathbf{x}}$, where the length of $\mathbf{x}$ is k:

$$Q^{\mathbf{a}}_{\mathbf{x}} := \sum_{i=0}^{n-1} \prod_{l=1}^{k} P_i(a_l|x_l). \tag{4.94}$$

Our goal is to see that, for any DLS, $P^{\mathbf{a}}_{\mathbf{x}}$ can always be expressed in terms of one-body $P^{a'}_{x'}$'s and in terms of $Q^{\mathbf{a}}_{\mathbf{x}}$'s.

Let us illustrate it with a simple example: Consider any DLS $f : X \longrightarrow Y$. Then, $P^{ab}_{xy} = \sum_{i\neq j} P_{ij}(ab|xy) = \sum_{i,j} P_{ij}(ab|xy) - \sum_{i=j} P_{ij}(ab|xy)$. As probabilities factorize in every f, we obtain $\sum_i P_i(a|x) \sum_j P_j(b|y) - \sum_i P_i(a|x)P_i(b|y)$, which automatically leads to $P^{ab}_{xy} = P^a_x \cdot P^b_y - Q^{ab}_{xy}$.

Observe that, in DLSs, the expression of $Q^{\mathbf{a}}_{\mathbf{x}}$ can be simplified in many cases. This is because, whenever a product of $P_i(a|x)$ with $P_i(a'|x)$ appears (with $a \neq a'$), that term in the sum (4.94) has to be zero; also $P_i(a|x)^2 = P_i(a|x)$ is a useful property. Thus, we obtain a simplification rule for Q:

- If two of measurements in $\mathbf{x}$ are the same, say the g-th and the h-th; *i.e.*, $x_g = x_h$, then

$$Q^{a_1\dots a_g\dots a_h\dots a_k}_{x_1\dots x_g\dots x_h\dots x_k} = \delta(a_g - a_h) Q^{a_1\dots a_g\dots \widehat{a_h}\dots a_k}_{x_1\dots x_g\dots \widehat{x_h}\dots x_k}, \tag{4.95}$$

  where $\widehat{\cdot}$ denotes that this element is missing.

- If this happens for $k = 2$, then Q is simplified either to zero or to a one-body P:

$$Q^{ab}_{xx} = \delta(a - b) P^a_x. \tag{4.96}$$

For example, in the $(n,3,d)$ scenario with 3-body correlators, in terms of the variables describing $\mathbb{T}_{n,3,d}$, one would have expressions like $Q^{abc}_{xyz} = c_{abc}$, $Q^{ab}_{01} = \sum_{j=0}^{d-1} c_{abj}$, $Q^{ab}_{02} = \sum_{j=0}^{d-1} c_{ajb}$, $Q^{ab}_{12} = \sum_{j=0}^{d-1} c_{jab}$, $Q^{a}_{0} = \sum_{i,j=0}^{d-1} c_{aij}$, etc. Now it is clear that $Q^{\mathbf{a}}_{\mathbf{x}}$ counts how many parties have outcome a_1 for the observable x_1, outcome a_2 for the observable x_2, and so on. Hence, the simplification rule (4.95) ensures consistency between $\mathbf{a}$ and $\mathbf{x}$ (we can't ask that an observable has two different outcomes) and, when Q is expressed in terms of $c_{\mathbf{y}}$, we see that we sum over all those observables upon which no condition was imposed.

The recipe to calculate $P^{\mathbf{a}}_{\mathbf{x}}$ on a DLS is quite simple: One just has to add and subtract the same amount of terms in order to obtain factorizations of the kind $\sum_{ij} Pij(ab|xy) = P^a_x P^b_y$, as in the previous example. For higher-order correlators, however, this process becomes more complex.

A further change of notation is necessary, in order to find a shorter expression for a general $P^{\mathbf{a}}_{\mathbf{x}}$: Let us see the reason by giving the explicit expression of a DLS for $k \leq 4$:

P^a_x	P^a_x
P^{ab}_{xy}	$P^a_x P^b_y - Q^{ab}_{xy}$
P^{abc}_{xyz}	$P^a_x P^b_y P^c_z - [P^a_x Q^{bc}_{yz} + P^b_y Q^{ac}_{xz} + P^c_z Q^{ab}_{xy}] + 2Q^{abc}_{xyz}$
P^{abcd}_{xyzu}	$P^a_x P^b_y P^c_z P^d_u$ $-[P^a_x P^b_y Q^{cd}_{zu} + P^a_x P^c_z Q^{bd}_{yu} + P^a_x P^d_u Q^{bc}_{yz}$ $+P^b_y P^c_z Q^{ad}_{xu} + P^b_y P^d_u Q^{ac}_{xz} + P^c_z P^d_u Q^{ab}_{xy}]$ $+[Q^{ab}_{xy} Q^{cd}_{zu} + Q^{ac}_{xz} Q^{bd}_{yu} + Q^{ad}_{xu} Q^{bc}_{yz}]$ $+2[P^a_x Q^{bcd}_{yzu} + P^b_y Q^{acd}_{xzu} + P^c_z Q^{abd}_{xyu} + P^d_u Q^{abc}_{xyz}]$ $-6Q^{abcd}_{xyzu}$

(4.97)

It is easy to observe that every of the expressions in brackets in (4.97) is highly symmetric. In fact, it can be generated from $\mathbf{a}$ and $\mathbf{x}$ just by knowing how to split the terms, with a certain coefficient in front. Let $\lambda \vdash K$ be a partition of K: $\lambda = (\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_K)$, where $\lambda_i \geq 0$ and $\sum_{k=1}^{K} \lambda_k = K$. Let us introduce the notation $a^b_{(\lambda_1,\ldots,\lambda_K)}$ (we can omit those $\lambda_k = 0$), where λ identifies a bracket in (4.97), a is the number in front of the coefficient and b just keeps track of the number of terms inside the bracket. In this new notation, $P^{\mathbf{a}}_{\mathbf{x}}$ takes the following form (we denote this conversion with an arrow $\leftarrow$):

K	$P^{\mathbf{a}}_{\mathbf{x}} \leftarrow \sum_{\lambda \vdash K} a^b_\lambda$
1	$1^1_{(1)}$
2	$1^1_{(1,1)} - 1^1_{(2)}$
3	$1^1_{(1,1,1)} - 1^3_{(2,1)} + 2^1_{(3)}$
4	$1^1_{(1,1,1,1)} - 1^6_{(2,1,1)} + 1^3_{(2,2)} + 2^4_{(3,1)} - 6^1_{(4)}$
5	$1^1_{(1,1,1,1,1)} - 1^{10}_{(2,1,1,1)} + 1^{15}_{(2,2,1)} + 2^{10}_{(3,1,1)} - 2^{10}_{(3,2)} - 6^5_{(4,1)} + 24^1_{(5)}$
6	$1^1_{(1,1,1,1,1,1)} - 1^{15}_{(2,1,1,1,1)} + 1^{45}_{(2,2,1,1)} - 1^{15}_{(2,2,2)} + 2^{20}_{(3,1,1,1)} - 2^{60}_{(3,2,1)}$ $+4^{10}_{(3,3)} - 6^{15}_{(4,1,1)} + 6^{15}_{(4,2)} + 24^6_{(5,1)} - 120^1_{(6)}$

(4.98)

Let us enumerate a few properties:

- Every time there is a $\lambda_k = 1$ in the partition, this corresponds to a 1-body P. If $\lambda_k > 1$, then this corresponds to a Q.

- The sign of a depends only on the parity of the number of elements in the partition which are zero: $\mathrm{sgn}(a) = (-1)^{|\{\lambda_k = 0\}|}$. This is a consequence of the simplification rule (4.95) that we use: The original indices in the sum that defines $P^{\mathbf{a}}_{\mathbf{x}}$ are $i_1 \dots i_K$, which are all different. To have a factorization into lower order P's, one must add and subtract Q's, and every time this is done, a minus sign is carried over.

- By taking a partition of K with exactly k elements, $\lambda \vdash (k, K)$, one has the identity $\sum_{\lambda \vdash (k,K)} ab = (-1)^{K-k} \left[\begin{array}{c} K \\ k \end{array} \right]$, where $\left[\begin{array}{c} \cdot \\ \cdot \end{array} \right]$ denotes the unsigned Stirling number of the first kind [AS65]. This formula is a direct consequence of its definition, as the unsigned Stirling number of the first kind counts how many permutations of K elements into k disjoint cycles exist and, for every permutation, we have a term in the corresponding bracket. However, we have to make a difference, and take into account, not only the number of cycles, but its length[23].

[23] Take, for instance, $K = 4$. There are two partitions of 4 with 2 elements: $(2,2)$ and $(3,1)$. For the $(2,2)$ partition, there are 3 permutations of 4 elements of the form $(\cdot\cdot)(\cdot\cdot)$ (recall that disjoint cycles commute) and, for the $(3,1)$ partition, one finds 8 permutations of the form $(\cdot\cdot\cdot)(\cdot)$. Hence, $\left[\begin{array}{c} 4 \\ 2 \end{array} \right] = 3 + 8 = 11$.

- The absolute value of a is given by $\prod_{\lambda_k>0}(\lambda_k-1)!$. This is, again, a consequence of the simplification rule (4.95). Let us illustrate this fact with an example, in which we are going to calculate P^{abc}_{xyz} explicitly.

$$P^{abc}_{xyz} = \sum_{\substack{i,j,k \\ i\neq j, j\neq k, i\neq k}} P_{ijk}(abc|xyz)$$
$$= \sum_{i=0}^{n-1}\sum_{j=0,j\neq i}^{n-1}\left(\sum_{k=0}^{n-1} P_{ijk}(abc|xyz) - \sum_{k\in\{i,j\}} P_{ijk}(abc|xyz)\right) \quad (4.99)$$

  It is important to notice that we have added and subtracted the values $\{i,j\}$ for the index k; the set $\{i,j\}$ contains 2 elements ($K-1$ in the general case). Now we can start factorizing:

$$P^{abc}_{xyz} = P^{ab}_{xy}\cdot P^{c}_{z} - \sum_{i\neq j}\left(P_{iji}(abc|xyz) + P_{ijj}(abc|xyz)\right). \quad (4.100)$$

  Applying this rule again (adding and subtracting the value $\{i\}$ for the index j) leads to the 2 equal terms $P_{iii}(abc|xyz)$ that give the factor 2 (because the previous step generated 2 elements P_{iji} and P_{ijj} that have led to P_{iii} when $i=j$, which corresponds to Q^{abc}_{xyz} when summed over i). This way we obtain the expression (4.97) and we see the way the coefficient $|a|$ in (4.98) is generated.

Hence, it is necessary to be able to count how many permutations of K elements exist into cycles of lengths $\lambda=(\lambda_1,\lambda_2,\ldots,\lambda_K)$: To this end, let us re-express $\lambda=(1^{\mu_1},2^{\mu_2},\ldots,r^{\mu_r})$, where μ_i denotes the multiplicity of i; *i.e.*, we have made an equivalence $(2,2,1,1,1)\equiv(1^3,2^2)$. As there are μ_k cycles of length k, which permute as they are disjoint, we gain a factor $\mu_k!$. Within each k-cycle, one has k cyclic permutations; this can be done μ_k times independently, one for each k-cycle, thus gaining a factor k^{μ_k}. We can now calculate, for a given $\lambda\vdash K$, the corresponding value $|a|b$, which is

$$|a|b = \frac{K!}{\prod_{k=1}^{r}\mu_k!\cdot\prod_{k=1}^{r}k^{\mu_k}}. \quad (4.101)$$

So, the number of elements b inside a bracket corresponding to a $\lambda\vdash K$ is

$$b = \frac{K!}{\prod_{k=1}^{r}\mu_k!\cdot\prod_{k=1}^{r}k^{\mu_k}\prod_{\lambda_k>0}(\lambda_k-1)!}. \quad (4.102)$$

Generating the vertices

With this procedure, one can efficiently generate the vertices of $\mathbb{P}_K^{\mathfrak{S}_n}$ for a general Bell Scenario (n, m, d). The only necessary ingredients are the functions P_x^a and $Q_{\mathbf{x}}^{\mathbf{a}}$, which can be easily obtained from the variables $c_{\mathbf{y}}$ describing $\mathbb{T}_{n,m,d}$:

It is convenient, at this point, to introduce the normalization constraints in terms of the correlators $P_{\mathbf{x}}^{\mathbf{a}}$. Because $\vec{P}$ is no-signalling, every time that one of the components of $\mathbf{a}$ is $d-1$, it can be re-expressed as a function of n and some $P_{\mathbf{x}}^{\mathbf{a}}$ which do not have any $d-1$. For instance, the 1-body correlators fulfill

$$P_x^{d-1} = n - \sum_{a=0}^{d-2} P_x^a, \tag{4.103}$$

for the 2-body we have the relations

$$P_{xy}^{a,d-1} = (n-1)P_x^a - \sum_{b=0}^{d-2} P_{xy}^{ab} \tag{4.104}$$

$$P_{xy}^{d-1,b} = (n-1)P_y^b - \sum_{a=0}^{d-2} P_{xy}^{ab} \tag{4.105}$$

$$P_{xy}^{d-1,d-1} = n(n-1) - (n-1)\sum_{c=0}^{d-2}(P_x^c + P_y^c) + \sum_{a,b=0}^{d-2} P_{xy}^{ab}, \tag{4.106}$$

and so on.

Let us start by arranging the P_x^a and $Q_{\mathbf{x}}^{\mathbf{a}}$ in an appropriate way. To this end, consider the vector $\vec{\mathfrak{P}}$ with the following d^m components. The simplest way to describe its ordering is to take its entries indexed in base d; *i.e.*, from $d^m - 1$ to 0: $\vec{\mathfrak{P}} = (\mathfrak{P}_{d-1,d-1,\ldots,d-1}, \ldots, \mathfrak{P}_{00\ldots1}, \mathfrak{P}_{00\ldots0})$. Now we apply the following rule:

- Whenever the m values on the index are $d-1$, we put $\mathfrak{P}_{d-1,d-1,\ldots,d-1} := n$.
- Whenever there are $m-1$ values on the index that are $d-1$, we put a single P. Let us suppose that the x-th index is $a \neq d-1$; then we set $\mathfrak{P}_{d-1,\ldots,a,\ldots,d-1} := P_x^{d-2-a}$.

- If there are less than $m-1$ values on the index equal to $d-1$, say m', then we put a Q with indices of length m'; *e.g.*, we set $\mathfrak{P}_{a,b,c,d-1,\ldots,d-1} := Q_{012}^{d-2-a,d-2-b,d-2-c}$.

We have written the general form of $\vec{\mathfrak{P}}$ in Eq. (4.107), where its recursive form is more explicit.

$$\begin{aligned}
\vec{\mathfrak{P}} \;=\; & [n, P_{m-1}^{0}, \ldots, P_{m-1}^{d-2}; \\
& P_{m-2}^{0}, Q_{m-2,m-1}^{00}, \ldots Q_{m-2,m-1}^{0,d-2}; \ldots; P_{m-2}^{d-2}, Q_{m-2,m-1}^{d-2,0}, \ldots, Q_{m-2,m-1}^{d-2,d-2}; \\
& P_{m-3}^{0}, Q_{m-3,m-1}^{00}, \ldots, Q_{m-3,m-1}^{0,d-2}; \\
& Q_{m-3,m-2}^{00}, Q_{m-3,m-2,m-1}^{000}, \ldots, Q_{m-3,m-2,m-1}^{0,0,d-2}; \\
& \ldots \\
& Q_{m-3,m-2}^{d-2,d-2}, Q_{m-3,m-2,m-1}^{d-2,d-2,0} \ldots Q_{m-3,m-2,m-1}^{d-2,d-2,d-2}; \\
& \vdots \\
& \ldots\ldots\ldots\ldots Q_{0,1,\cdots,m-1}^{d-2,d-2,\cdots,d-2}].
\end{aligned} \tag{4.107}$$

This suggests that some kind of tensor structure can be exploited to find $\vec{\mathfrak{P}}$, as in the spirit of Eq. (4.23). Indeed, let us define the following $d \times d$ matrix M:

$$M := \begin{pmatrix} 1 & 1 & \cdots & 1 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ & & \ddots & & \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix} \tag{4.108}$$

Then, we have that M brings $\vec{c_{\mathbf{y}}}$ to $\vec{\mathfrak{P}}$:

$$\vec{\mathfrak{P}} = M^{\otimes m} \cdot \vec{c_{\mathbf{y}}}. \tag{4.109}$$

Example 4.15. *Consider the* $(n, 3, 2)$ *Bell scenario with* $K = 3$*-body correla-*

tors. Then, Eq. (4.109) becomes

$$\begin{pmatrix} n \\ P_2^0 \\ P_1^0 \\ Q_{12}^{00} \\ P_0^0 \\ Q_{02}^{00} \\ Q_{01}^{00} \\ Q_{012}^{000} \end{pmatrix} = M^{\otimes 3} \begin{pmatrix} c_{000} \\ c_{001} \\ c_{010} \\ c_{011} \\ c_{100} \\ c_{101} \\ c_{110} \\ c_{111} \end{pmatrix}, \qquad M = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}. \tag{4.110}$$

Example 4.16. *Consider now the* $(n, 2, 3)$ *Bell scenario with* $K = 2$*-body correlators. Eq. (4.109) has the form*

$$\begin{pmatrix} n \\ P_1^0 \\ P_1^1 \\ P_0^0 \\ Q_{01}^{00} \\ Q_{01}^{01} \\ P_0^1 \\ Q_{01}^{10} \\ Q_{01}^{11} \end{pmatrix} = M^{\otimes 2} \begin{pmatrix} c_{00} \\ c_{01} \\ c_{02} \\ c_{10} \\ c_{11} \\ c_{12} \\ c_{20} \\ c_{21} \\ c_{22} \end{pmatrix}, \qquad M = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}. \tag{4.111}$$

4.5.1. Expectation values

A similar argument can be presented for expectation values instead of probabilities, leading to an equivalent result to Eq. (4.109). Eq. (4.23) is a particular example of this. Working in the ± 1 expectation value framework is most usual when $d = 2$, where one uses Eq. (4.3) as a change of variables. If we want to generalize that to any d, then it is convenient to work with complex correlators; *i.e.*, to take as outcomes the d-th roots of unity [Arn12].

Let us define

$$\mathcal{S}_x^{\alpha} := \sum_{a=0}^{d-1} \omega^{-a\alpha} P_x^a, \qquad \mathcal{S}_{xy}^{\alpha\beta} := \sum_{a,b=0}^{d-1} \omega^{-a\alpha - b\beta} P_{xy}^{ab}, \tag{4.112}$$

and, in general,

$$\mathcal{S}^{\boldsymbol{\alpha}}_{\mathbf{x}} := \sum_{\mathbf{a}} \omega^{-\mathbf{a}\cdot\boldsymbol{\alpha}} P^{\mathbf{a}}_{\mathbf{x}}, \tag{4.113}$$

where ω is a primitive root of the unity. When $\omega = -1$, Eq. (4.112) coincides with Eqs. (4.14) and (4.15).

The inverse transformation is given by the inverse discrete Fourier transform: If the length of $\boldsymbol{\alpha}$ is m, then

$$P^{\mathbf{a}}_{\mathbf{x}} = d^{-m} \sum_{\boldsymbol{\alpha}} \omega^{\mathbf{a}\cdot\boldsymbol{\alpha}} \mathcal{S}^{\boldsymbol{\alpha}}_{\mathbf{x}}, \tag{4.114}$$

In the case of correlators, the normalization (plus the no-signalling) conditions imply that every time that there is a 0 in $\boldsymbol{\alpha}$, the corresponding measurement can be taken out and a function of function of n appears multiplying: $\mathcal{S}^{0}_{x} = n$, $\mathcal{S}^{0\beta}_{xy} = (n-1)\mathcal{S}^{\beta}_{y}$, $\mathcal{S}^{\alpha 0}_{xy} = (n-1)\mathcal{S}^{\alpha}_{x}$, $\mathcal{S}^{00}_{xy} = n(n-1)$ and so on.

As an analogy to the Q functions defined in Eq. (4.94), one has the functions $\mathcal{Z}$:

$$\mathcal{Z}^{\boldsymbol{\alpha}}_{\mathbf{x}} := \sum_{\mathbf{y}} \omega^{-\mathbf{y}\cdot\boldsymbol{\alpha}} c_{\mathbf{y}}. \tag{4.115}$$

Example 4.17. *For the $(n, 2, 2)$ scenario, we recover Eq. (4.23).*

Example 4.18. *For the $(n, 2, 3)$ scenario, we have a similar relation to Eq. (4.111), which is*

$$\begin{pmatrix} n \\ \mathcal{S}^1_1 \\ \mathcal{S}^2_1 \\ \mathcal{S}^1_0 \\ \mathcal{Z}^{11}_{01} \\ \mathcal{Z}^{12}_{01} \\ \mathcal{S}^2_0 \\ \mathcal{Z}^{21}_{01} \\ \mathcal{Z}^{22}_{01} \end{pmatrix} = H^{\otimes 2} \begin{pmatrix} c_{00} \\ c_{01} \\ c_{02} \\ c_{10} \\ c_{11} \\ c_{12} \\ c_{20} \\ c_{21} \\ c_{22} \end{pmatrix}, \qquad H = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega^{-1} & \omega \\ 1 & \omega & \omega^{-1} \end{pmatrix}, \tag{4.116}$$

where ω is a primitive third-root of unity.

Let us remark that the orthogonality of the rows of H, which is a Discrete Fourier Transform matrix, is the key property that is used in proving Theorem 4.2. Thus, an analogous result, to reduce the bound (4.12), could be derived; one would have to find convex combinations (in the space spanned by the $\mathcal{Z}$'s) of parameters $c_{\mathbf{y}}$ in $\mathbb{T}_{n,m,d}$ that would be preserved as projected vertices of $\mathbf{P}_L$ in $\mathbb{P}_K^{\mathfrak{S}_n}$.

Consequently, we have given a method that generalizes the construction of $\mathbb{P}_K^{\mathfrak{S}_n}$ to any Bell scenario in an efficient manner. When the $c_{\mathbf{y}}$ variables are taken as continuous, we obtain a relaxation $\mathbf{P}_k^{\mathfrak{S}_n}$ of $\mathbb{P}_k^{\mathfrak{S}_n}$, which is the convex hull of a semialgebraic set which consists of the polynomial equations $\varphi(c_{\mathrm{y}})$ given by Eq. (4.98) with variables in the domain $\mathbf{T}_{n,m,d}$, (*cf.* Eq. (4.43)); *i.e.*, $\mathbf{P}_k^{\mathfrak{S}_n} := \mathrm{CH}(\varphi(\mathbf{T}_{n,m,d}))$ for which efficient SDP relaxations exist [BPT; GT].

4.6. Translationally Invariant Bell Inequalities

In this section we look for 2-body Bell inequalities that obey a less restrictive symmetry: translational invariance. We fully classify all 3- and 4-partite Bell inequalities of this kind for the $(n, 2, 2)$ scenario and classify them into equivalence classes. Their quantum violation is checked and give an example of a 5-partite 2-body correlator Bell inequality that involves only nearest neighbors, which is violated by a genuinely multipartite entangled quantum state. Finally, we show how any translationally invariant Bell inequality can be maximally violated by a translationaly invariant state, with all parties using the same collection of observables.

The symmetry group which is considered in this section is the one generated by the full cycle: the permutation $\tau \in \mathfrak{S}_n$ such that $\tau : 0 \mapsto 1 \mapsto 2 \mapsto \ldots \mapsto n-1 \mapsto 0$; *i.e.*, the cyclic group, which we denote $\mathbb{Z}_n$.

4.6.1. The Translationally Invariant Polytope

Here we analyze the relevant properties of the local polytope $\mathbb{P}_2^{\mathbb{Z}_n}$. The Bell Inequalities we are looking for are a particular subclass of (4.21), which can be expressed in terms of the $\mathbb{Z}_n$-symmetric correlators (4.9). For the $(n, 2, 2)$ scenario, these correlators correspond to

$$\mathcal{S}_k = \sum_{i=0}^{n-1} \langle \mathcal{M}_k^{(i)} \rangle, \qquad k \in \{0,1\}, \tag{4.117}$$

which coincides with Eq. (4.14), and

$$\mathcal{T}_{kl}^{(r)} = \sum_{i=0}^{n-1} \langle \mathcal{M}_k^{(i)} \mathcal{M}_l^{(i+r)} \rangle \qquad k \leq l \in \{0,1\}, \tag{4.118}$$

with $r = 1, \ldots, \lfloor n/2 \rfloor$ for $k = l$ and $r = 1, \ldots, n-1$ for $k < l$. The parameter r can be seen as an interaction range. The party indices are taken *modulo* n.

Hence, any 2-body translationally invariant Bell inequality reads

$$\beta_c + \alpha \mathcal{S}_0 + \beta \mathcal{S}_1 + \sum_{r=1}^{\lfloor n/2 \rfloor} \left(\gamma_r \mathcal{T}_{00}^{(r)} + \epsilon_r \mathcal{T}_{11}^{(r)} \right) + \sum_{r=1}^{n-1} \delta_r \mathcal{T}_{01}^{(r)} \geq 0. \tag{4.119}$$

The number of vertices of $\mathbb{P}_2^{\mathbb{Z}_n}$ can be upper bounded with the Redfield-Pólya's theorem [Red27; Pól37] by identifying $\mathbb{Z}_n$-equivalent DLSs. The explicit bound needs a slightly different mathematical machinery than the one used in (4.12):

The elements of the cyclic group of order n generated by τ are of the form τ^k, where $1 \leq k \leq n$ and τ^n is the identity permutation. Let us recall the fact that the number of cycles of τ^k is the greatest common divisor between n and k, denoted $\gcd(n,k)$. This allows us to rewrite Eq. (4.10) as

$$|Y^X/\mathbb{Z}_n| = \frac{1}{n} \sum_{k=1}^{n} |Y|^{\gcd(n,k)}. \tag{4.120}$$

Let us now observe that, for any k, $d' := \gcd(n,k)$ is, by construction, a divisor of n; *i.e.*, $d'|n$. This allow us to group the terms of the sum in Eq. (4.120) in those who have the same greatest common divisor with n. Since the sets $\{k \in \{1,\ldots,n\} : \gcd(n,k) = d'\}$ and $\{l \in \{1,\ldots,n/d'\} : \gcd(n/d', l) = 1\}$ have the same cardinality, and the cardinality of the latter is, by definition, Euler's totient function $\varphi(n/d')$, a well-known funcion in number theory, we can re-express Eq. (4.120) as

$$|Y^X/\mathbb{Z}_n| = \frac{1}{n} \sum_{d'|n} \varphi(n/d') |Y|^{d'}. \tag{4.121}$$

Let us introduce the change of variables $d = n/d'$, which is well defined because only those $d'|n$ are considered. Also, for the $(n, 2, 2)$ scenario we are interested in, we have that $|Y| = 4$. Hence, we arrive at the most simplified expression to upper bound the amount of vertices of $\mathbb{P}_2^{\mathbb{Z}_n}$:

$$\mathrm{Ext}(\mathbb{P}_2^{\mathbb{Z}_n}) \leq |Y^X/\mathbb{Z}_n| = \frac{1}{n}\sum_{d|n}\varphi(d)\sqrt[d]{4^n} \tag{4.122}$$

The bound (4.122) is not always tight. As we shall see, $n = 4$ constitutes a counterexample[24]; it is tight, however, for $n = 3, 5$.

4.6.2. Equivalent Bell inequalities

The inherent symmetry of the local polytope $\mathbf{P}_L$ is best understood from an operational point of view: the naming of parties, observables and outcomes is totally arbitrary, and this is reflected in the structure of the local polytope. Hence, if we rename or permute the parties, measurements and/or outcomes of a Bell inequality for $\mathbf{P}_L$, we obtain another valid Bell inequality. Although with these procedure we generate geometrically different half-spaces, they are equivalent in the operational sense; thus it is significantly meaningful to group Bell inequalities into equivalence classes.

By the same principle, the translationally invariant local polytope $\mathbb{P}_2^{\mathbb{Z}_n}$ enjoys similar symmetries, which we used to classify the facets of $\mathbb{P}_2^{\mathbb{Z}_3}$ and $\mathbb{P}_2^{\mathbb{Z}_4}$ in Appendix C. We consider the following symmetries

- A renaming of the parties in a cyclical way: $\mathcal{M}_k^{(i)} \mapsto \mathcal{M}_k^{(i+1)}$ for all $0 \leq i < n$ and $k \in \{0, 1\}$. This, by construction, leaves $\mathbb{P}_2^{\mathbb{Z}_n}$ invariant.
- A renaming of the observables $\mathcal{M}_0^{(i)} \leftrightarrow \mathcal{M}_1^{(i)}$ for $0 \leq i < n$. At the level of inequality (4.119), this corresponds tot he changes $\alpha \leftrightarrow \beta$, $\gamma_r \leftrightarrow \varepsilon_r$ and $\delta_r \leftrightarrow \delta_{n-r}$ for $1 \leq r \leq \lfloor n/2 \rfloor$.

[24] According to Eq. (4.122), for the $(4, 2, 2)$ scenario we should have $|Y^X/\mathbb{Z}_4| = (1 \times 4^4 + 1 \times 4^2 + 2 \times 4)/4 = 70$ candidates to vertex. However, explicitly solving the polytope with, for example, the CDD algorithm [Fuk14], gives that $|\mathrm{Ext}(\mathbb{P}_2^{\mathbb{Z}_4})| = 68$. This is because the DLSs $f : A \mapsto (+,+),\ B \mapsto (-,+),\ C \mapsto (+,-),\ D \mapsto (-,-)$ and $\tilde{f} : A \mapsto (+,+),\ B \mapsto (-,-),\ C \mapsto (+,-),\ D \mapsto (-,+)$ give exactly the same values on the translationally invariant correlators (4.117, 4.118). The same happens for $g : A \mapsto (+,+),\ B \mapsto (+,-),\ C \mapsto (-,+),\ D \mapsto (-,-)$ and $\tilde{g} : A \mapsto (+,+),\ B \mapsto (-,-),\ C \mapsto (-,+),\ D \mapsto (+,-)$. Thus, f and $\tilde{f}$ (as well as g and $\tilde{g}$) are projected to the same element in $\mathrm{Ext}(\mathbb{P}_2^{\mathbb{Z}_4})$.

- A renaming of the $k-$th observable's outcomes at all sites; *i.e.*, $\mathcal{M}_k^{(i)} \leftrightarrow -\mathcal{M}_k^{(i)}$ for $0 \leq i < n$. The effect on inequality (4.119) is the following: If $k = 0$, it exchanges $\alpha \leftrightarrow -\alpha$ and $\delta_r \leftrightarrow -\delta_r$ for $1 \leq r \leq n-1$; if $k = 1$, then it swaps the sign of $\beta \leftrightarrow -\beta$ and $\delta_r \leftrightarrow -\delta_r$ for $1 \leq r \leq n-1$.
- A renaming of the parties following the *reflection* $\mathcal{M}_k^{(i)} \leftrightarrow \mathcal{M}_k^{(n-i-1)}$ for all i and k. This exchanges $\delta_r \leftrightarrow \delta_{n-r}$ for $1 \leq r \leq \lfloor n/2 \rfloor$ in (4.119).

These symmetries can be composed, leading to new ones. Let us point out that the four types of symmetries introduced, although clearly inspired by the fact that we have translational invariance, constitute only a subset of those considered in $\mathbf{P}_L$. It may happen that a the composition of several more general symmetries, which break translational invariance in general, change the class of the Bell inequality, when some of the coefficients are zero. Let us illustrate this fact with an example. Suppose that $\alpha = \beta = 0$ in (4.119) and $n \equiv 0 \bmod 2$. Applying $\mathcal{M}_k^{(i)} \leftrightarrow -\mathcal{M}_k^{(i)}$ for all odd i and for all k exchanges $\gamma_r \leftrightarrow -\gamma_r$, $\delta_r \leftrightarrow -\delta_r$ and $\varepsilon_r \leftrightarrow -\varepsilon_r$ for all odd r.

4.6.3. Numerical results

The three-partite case

In the case of $n = 3$, the Bell inequalities of the form (4.119) take the form

$$\beta_c + \alpha\mathcal{S}_0 + \beta\mathcal{S}_1 + \gamma_1\mathcal{T}_{00}^{(1)} + \varepsilon_1\mathcal{T}_{11}^{(1)} + \delta_1\mathcal{T}_{01}^{(1)} + \delta_2\mathcal{T}_{01}^{(2)} \geq 0. \tag{4.123}$$

Since $\mathcal{T}_{01}^{(1)} + \mathcal{T}_{01}^{(2)}$ and the rest of correlators appearing in (4.123) are permutationally invariant, by imposing $\delta_1 = \delta_2$ in (4.123), we obtain an inequality of the form (4.22) as a particular case. Inequality (4.123) shows that $\mathbb{P}_2^{\mathbb{Z}_3}$ is 6-dimensional. The CDD algorithm [Fuk14] shows that $\mathbb{P}_2^{\mathbb{Z}_3}$ can be minimally described with 38 facets. These, under the symmetries introduced in Section 4.6.2, are grouped into 6 classes, which are listed in Table C.5. Linear programming shows that $|\mathrm{Ext}(\mathbb{P}_2^{\mathbb{Z}_3})| = 24$, meaning that the bound (4.122) is tight.

Only the last inequality in Table C.5 is violated by quantum states. Let us introduce the constants β_Q and β_N, which, if substituted for β_c in Ineq.

(4.123), correspond to the quantum bound and the non-signalling bound, respectively, of the corresponding Bell inequality. The rest of the inequalities in Table C.5 are trivial, in the sense that $\beta_c = \beta_Q = \beta_N$.

For the 6-th inequality in Table C.5, we have $(\beta_c, \beta_Q, \beta_N) = (9, 10.02, 13)$; the maximal quantum violation is realized with the following pure state:

$$|\psi\rangle = -0.08(|000\rangle + |111\rangle) - 0.5628(|001\rangle + |010\rangle + |100\rangle) + 0.1108(|011\rangle + |110\rangle + |101\rangle), \quad (4.124)$$

with the same measurements at each site, which are given by $\varphi = -1.1946$ and $\theta = 0.0957$ (*cf.* Eq. (4.66)). These angles have been chosen so that the coefficients in front of $|000\rangle$ and $|111\rangle$ are equal. The state $|\psi\rangle$ has some relevant properties: it is symmetric, so it is genuinely multipartite entangled [Aug+12]. All its bipartite reductions are local, as they do not violate the CHSH inequality [Cla+69]. The closest Dicke state $|D_3^k\rangle$ to $|\psi\rangle$ is for $k = 1$; *i.e.*, the so-called $|W\rangle$ state, which suggests that it also violates this inequality. Indeed, the corresponding β_Q for the $|W\rangle$ state is 9.85, with the same measurements at each site, given by $\varphi = 5.2556$ and $\theta = 0.2285$.

The state $|\psi\rangle$ is less entangled than $|W\rangle$ with respect to the geometric measure of entanglement E_G[25]. Since, for symmetric states, the maximum of E_G is obtained through a fully symmetric separable state $|e\rangle^{\otimes n}$ [Hüb+09], one easily obtains $E_G(|\psi\rangle) = 0.2726$ and $E_G(|W\rangle) = 1/3$. Interestingly, although $E_G(|\psi\rangle) < E_G(|W\rangle)$, the quantum violation given by $|\psi\rangle$ is stronger than the one obtainable by $|W\rangle$.

The four-partite case

For the $(4, 2, 2)$ scenario, the CDD algorithm [Fuk14] shows that $\mathbb{P}_2^{\mathbb{Z}_4}$ has 1038 facets. We grouped them into 103 equivalence classes, collected in Table C.6. The dimension of $\mathbb{P}_2^{\mathbb{Z}_4}$ is 9, as the general 2-body translationally invariant Bell inequalities for this scenario can be written in the following form:

$$\begin{aligned}\beta_c + \alpha\mathcal{S}_0 + \beta\mathcal{S}_1 + \gamma_1\mathcal{T}_{00}^{(1)} + \gamma_2\mathcal{T}_{00}^{(2)} + \varepsilon_1\mathcal{T}_{11}^{(1)} + \varepsilon_2\mathcal{T}_{11}^{(2)} \\ + \delta_1\mathcal{T}_{01}^{(1)} + \delta_2\mathcal{T}_{01}^{(2)} + \delta_3\mathcal{T}_{01}^{(3)} \geq 0. \quad (4.125)\end{aligned}$$

[25] Let us recall that for n-partite states $|\varphi\rangle$ in $\mathcal{H} = (\mathbb{C}^d)^{\otimes n}$, the geometric measure of entanglement is defined as $E_G(|\varphi\rangle) = 1 - \max_{|\phi_{\text{prod}}\rangle} |\langle\phi_{\text{prod}}|\varphi\rangle|^2$, where $|\varphi_{\text{prod}}\rangle = |e_1\rangle \cdots |e_n\rangle$ [WG03].

Let us comment on the different properties of the inequalities listed in Table C.6: Inequalities 1 to 20 are trivial, as $\beta_c = \beta_Q = \beta_N$. Inequalities 21 to 24 have no quantum violation ($\beta_c = \beta_Q$), but they do have non-signalling violation[26] ($\beta_Q < \beta_N$). All the remaining Bell inequalities, from 25 to 103, are violated by quantum states ($\beta_c < \beta_Q$). However, we have further classified them into those for which the same pair of qubit observables at all sites achieves its maximal violation (25 to 63) and those for which this is not the case (64 to 103). Interestingly, in the first group, we find inequality 27 which is the only one not maximally violated by a genuinely multipartite quantum state. This is because the 27th inequality can be regarded as a sum of CHSH between parties A and C and between B and D, so it can be maximally violated by a product of two maximally entangled 2-qubit states. Let us point out that the optimal state corresponding to inequalities 26 to 63 is translationally invariant, whereas for inequality 25 the state is orthogonal to the space of translationally invariant vectors[27]. On the other hand, inequalities 27 and 64 to 103 are maximally violated by states that are separable across some bipartition. If the Bell inequality does not clearly split as a sum of other two (like in the 27th), this can happen because we need to remove the constraint that the same set of observables must be used at all sites in order to improve the quantum violation. In particular, if the same set of qubit measurements is used in inequalities 64 to 69, then, one does not find any quantum violation.

There are some Bell inequalities in Table C.6 for which their corresponding optimal quantum state has all its reduced bipartite systems local (25, 73, 81, 87 and 88). Hence, no bipartite Bell inequality can reveal nonlocality in these subsystems. This implies that some of the quantum violations are purely multipartite, even if they are obtained only from bipartite correlations.

Geometrically, some of the inequalities of Table C.6 already constitute

[26] Noticeably, such inequalities have some similarity with the Guess-Your-Neighbor-Input (GYNI) Bell inequalities [Alm+10a]. Operationally, they can be regarded as distributed tasks for which the aid of quantum resources does not provide any advantadge over classical ones. However, there exist no-signalling correlations which are beyond the quantum set of correlations $\mathbf{Q}$ that perform better at such task. From the geometrical point of view, GYNI inequalities constitute facets of $\mathbf{P}_L$; however only the 21st inequality has this property for $\mathbb{P}_2^{\mathbb{Z}_4}$.

[27] A translationally invariant n-qubit state $|\psi\rangle$ is such that, for any k, $\tau^k(|\psi\rangle) = |\psi\rangle$, where $\tau \in \mathfrak{S}_n$ is the permutation that shifts to the right.

facets of $\mathbb{P}_2$; these are 4, 10, 17, 20, 21, 25, 28, 36, 38, 43, 51, 54, 57, 69, 81, 84, 89 and 94.

The five-partite case

In this case, we have that $\mathbb{P}_2^{\mathbb{Z}_5}$ is described by 10 translationally invariant correlators constructed as in Eq. (4.9), and the number of vertices is 208, which makes the upper bound (4.122) tight, since $208 = (1 \times 4^5 + 4 \times 4)/5$. The CDD algorithm [Fuk14] shows how the minimal description of $\mathbb{P}_2^{\mathbb{Z}_5}$ in terms of half-spaces has $34,484$ facets which can be grouped into 4198 different classes by virtue of the symmetries in Section 4.6.2. This number is already too large to explicitly list them. The case $n = 6$ is already intractable.

An additional simplification that one can use is to restrict the range of the parameter r in (4.119); *i.e.*, to work just with nearest neighbor correlations. In the $(5, 2, 2)$ the projected local polytope would have dimension 6 and the form of its defining Bell inequalities would be

$$\beta_c + \alpha\mathcal{S}_0 + \beta\mathcal{S}_1 + \gamma_1\mathcal{T}_{00}^{(1)} + \delta_1\mathcal{T}_{01}^{(1)} + \delta_{n-1}\mathcal{T}_{01}^{(n-1)} + \varepsilon_1\mathcal{T}_{11}^{(1)} \geq 0. \quad (4.126)$$

Let us illustrate (4.126) with a particular example, for the $(5, 2, 2)$ scenario:

$$35 - 2\mathcal{S}_0 - 6\mathcal{S}_1 - 2\mathcal{T}_{00}^{(1)} + 2\mathcal{T}_{01}^{(1)} + 4\mathcal{T}_{01}^{(4)} + 5\mathcal{T}_{11}^{(1)} \geq 0. \quad (4.127)$$

Inequality (4.127) can indeed detect nonlocality in multipartite quantum states. If we impose the same set of qubit observables to be used at each site, then we find that $\beta_Q = 35.29$, which is greater than $\beta_c = 35$, and the translationally invariant quantum state

$$\begin{aligned} |\psi\rangle \quad = \quad & -0.3710(|00000\rangle + |11111\rangle) \\ & -0.1817|T_{00001}\rangle + 0.1260|T_{00011}\rangle - 0.1418|T_{00101}\rangle \\ & +0.2645|T_{00111}\rangle - 0.0603|T_{01011}\rangle + 0.0486|T_{01111}\rangle \end{aligned} \quad (4.128)$$

achieves this bound, where the translationally invariant vectors $|T_{abcde}\rangle$ are defined as

$$|T_{abcde}\rangle := \sum_{k=0}^{4} \tau^k(|abcde\rangle), \quad (4.129)$$

where $\tau \in \mathfrak{S}_5$ is the shift operator. The measurements corresponding to (4.128) are given by $\varphi = 1.2967$ and $\theta = 1.9866$ (*cf.*, Eq. (4.66)), and are chosen so that $|00000\rangle$ and $|11111\rangle$ have the same coefficient in front. The state introduced in (4.128) is genuinely multipartite entangled, and none of its two-body subsystems violate the CHSH inequality, so they are local, as CHSH is the only non-trivial inequality in the $(2, 2, 2)$ scenario [Cla+69]. Its geometrical measure of entanglement reads $E_G(|\psi\rangle) = 0.4980$.

Inequality (4.126) can be maximally violated with qubits and traceless real observables [TV06]; however, even if the Bell inequality has translationally invariant symmetry, this does not imply that the same set of measurements can be taken at each site. Indeed, if we unrestrict this constraint, we can obtain better results in general; *e.g.* $\beta_Q = 36.21$ for inequality (4.127). However, the state that achieves this β_Q is almost fully product: $|\psi'\rangle = |0\rangle|0\rangle|1\rangle \otimes (0.7312|00\rangle - 0.3775|01\rangle + 0.2674|10\rangle + 0.5013|11\rangle)$; *i.e.*, entangled across DE only. The corresponding measurements are $\varphi_i = 0$ for all i, and $\theta_i = 0$ for $0 \leq i < 3$, $\theta_3 = 4.7378$ and $\theta_4 = 1.2083$. Nevertheless, in Section 4.6.4 we show that, at the price of increasing the dimension of the Hilbert space of the quantum state, we can achieve the same maximal β_Q with a translationally invariant qudit state and the same set of observables at each site.

4.6.4. Quantum violation with translationally invariant qudit states

In this section we show that the β_Q corresponding to any translationally invariant Bell inequality with M measurements per site with binary outcomes can always be achieved with a translationally invariant state and the same set of measurements per site, which we shall refer to as symmetric measurement settings. If the local dimension of the optimal state (not necessarily obeying any translational invariant kind of symmetry) is d, then a Hilbert space of local dimension $d \cdot n$ is sufficient to accomodate a translationally invariant state achieving the same optimal violation.

We also introduce a numerical method that enables one to find such states and observables, often showing that the upper bound $d \cdot n$ is not tight, as we have checked for the inequalities listed in Table C.6.

A general translationally invariant Bell inequality written in terms of

correlators can be expressed as

$$\beta_c + \sum_{k=1}^{n} \sum_{\substack{0\leq i_1<\ldots<i_k<n \\ 0\leq x_{i_1},\ldots,x_{i_k}\leq 1}} \alpha^{i_1,\ldots,i_k}_{x_{i_1},\ldots,x_{i_k}} \left\langle \mathcal{M}^{(i_1)}_{x_{i_1}} \cdots \mathcal{M}^{(i_k)}_{x_{i_k}} \right\rangle \geq 0, \tag{4.130}$$

where the $\alpha^{i_1,\ldots,i_k}_{x_{i_1},\ldots,x_{i_k}}$ coefficients obey the following inequalities for all $1 \leq k \leq n$, $0 \leq i_1 < \ldots < i_k < n$ and $0 \leq x_{i_1}, \ldots, x_{i_k} \leq 1$:

$$\alpha^{i_1,\ldots,i_k}_{x_{i_1},\ldots,x_{i_k}} = \alpha^{i_1+1,\ldots,i_k+1}_{x_{i_1},\ldots,x_{i_k}}, \tag{4.131}$$

with the convention that, whenever $i_k = n-1$,

$$\alpha^{i_1+1,\ldots,i_k+1}_{x_{i_1},\ldots,x_{i_k}} = \alpha^{i_1+1,\ldots,n}_{x_{i_1},\ldots,x_{i_k}} = \alpha^{0,i_1+1,\ldots,i_{k-1}+1}_{x_{i_k},x_{i_1},\ldots,x_{i_k-1}}. \tag{4.132}$$

Let $|\psi\rangle \in \mathcal{H} = (\mathbb{C}^d)^{\otimes n}$ be the state giving the optimal violation, and let $\{\mathcal{M}^{(i)}_{x_i}\}_i$ be the corresponding set of measurements. By attaching an ancillary system of n dimensions to every site, let us construct the following state $\rho^{TI} \in \mathcal{D}((\mathbb{C}^d \otimes \mathbb{C}^n)^{\otimes n})$, which is translationally invariant by definition:

$$\rho^{TI} := \frac{1}{n} \sum_{i=0}^{n-1} (\Pi_{\tau,d})^i |\psi\rangle\langle\psi| (\Pi^\dagger_{\tau,d})^i \otimes (\Pi_{\tau,n})^i |0,\ldots,n-1\rangle\langle 0,\ldots,n-1| (\Pi^\dagger_{\tau,n})^i, \tag{4.133}$$

where $\Pi_{\tau,d}$ is the representation of the shift permutation in $(\mathbb{C}^d)^{\otimes n}$ (*cf.* Eq. (A.5)). The corresponding dichotomic observables now act and $\mathbb{C}^d \otimes \mathbb{C}^n$ and are taken to be the same at all sites.

$$\widetilde{\mathcal{M}^{(i)}_k} := \sum_{j=0}^{n-1} \mathcal{M}^{(i)}_k \otimes |i\rangle\langle i|, \tag{4.134}$$

where $0 \leq k < M$. With the aid of Eq. (4.131) one checks that the state (4.133) and the measurements (4.134) produce the maximal quantum violation.

We have proved that by extending the local Hilbert space dimension d to $d \cdot n$ one can always maximally violate a translationally invariant Bell inequality with a quantum state fulfilling the same symmetry, and the same set of measurements at each site. In particular, for the Bell inequalities in

Table C.5, $n = 3$, states with local dimension at most 6 are sufficient; and for those in Table C.6, states with local dimension at most 8 suffice.

The construction that we have presented above is fully general, but it is numerically expensive to increase the local dimension of the particles we are working with, and sometimes it is not necessary to invest so many resources: in the following section we present a numerical see-saw algorithm that allows to perform the search for translationally invariant states and identical measurements in a fixed dimension in an efficient manner.

Numerical techniques

Here we shall assume that the local dimension of the Hilbert space is fixed to D and we shall look for the best translationally invariant and measurement settings for a given Bell inequality. This way we naturally obtain an upper bound $d_{\min}$ on the minimal local dimension of the Hilbert space for which such state and symmetric settings exist. We conjecture [Tur+14b] that for a small number of parties $N \lesssim 6$ and low dimensions $D \lesssim 7$ the algorithm outputs the maximal quantum violation for these constraints, impliying that $d_{\min}$ (the minimal D for which β_Q is achieved) is tight. Actually, the $d_{\min}$ we find generally improve the $d \cdot n$ upper bound introduced in the previous section.

The numerical technique is a variation of the *see-saw* iterative type introduced in [WW01] (see also [PV10]), and it consists of the following steps:

1. We start by generating M random unitary matrices $U_k \in \mathcal{U}_D$, for $0 \leq k < M$ (A simple parametrization of U_D can be found in [SHH10]) and we take the first party's dichotomic observables as

$$\mathcal{M}_k^{(0)} := U_k \Lambda U_k^\dagger, \tag{4.135}$$

   with Λ being a $D \times D$ diagonal matrix with entries ± 1 chosen uniformly at the diagonal.

2. We set the observables of the remaining parties to be the same as the first one:

$$\mathcal{M}_k^{(i)} := \mathcal{M}_k^{(0)}, \tag{4.136}$$

   for $1 \leq i < n$ and $0 \leq k < M$.

3. We construct the Bell operator $\mathcal{B}$:

$$\mathcal{B} := \sum_{k=1}^{n} \sum_{\substack{0\leq i_1<\ldots<i_k<n \\ 0\leq x_{i_1},\ldots,x_{i_k}\leq 1}} \alpha^{i_1,\ldots,i_k}_{x_{i_1},\ldots,x_{i_k}} \mathcal{M}^{(i_1)}_{x_{i_1}} \otimes \cdots \otimes \mathcal{M}^{(i_k)}_{x_{i_k}}, \quad (4.137)$$

and we minimize $\mathrm{Tr}\mathcal{B}\rho$ subject to the constraints $\rho \succeq 0$ and $\mathrm{Tr}\rho = 1$. This optimization corresponds to a semi-definite program; however, it is equivalent to finding the eigenvector $|\psi\rangle$ corresponding to the minimal eigenvalue of $\mathcal{B}$. This way, we find the current quantum bound $\beta := -\langle\psi|\mathcal{B}|\psi\rangle$.

4. We generate the translationally invariant state

$$\rho^{TI} := \frac{1}{n}\sum_{i=0}^{n-1} \Pi^i_{\tau,D}|\psi\rangle\langle\psi|(\Pi^\dagger_{\tau,D})^i, \quad (4.138)$$

where $\Pi_{\tau,D}$ represents the shift operator in $\mathbb{C}^D$ (*cf.* Eq. (A.5)). Notice that $\mathrm{Tr}(\mathcal{B}\rho^{TI}) = \langle\psi|\mathcal{B}|\psi\rangle = -\beta$.

5. And now we optimize the measurements. We do so by fixing the measurements of all but one parties (we can choose, without loss of generality, the first one) and optimizing the free one's; this way we obtain a semi-definite program which can be addressed efficiently. Let us define the F_k operators:

$$F_k := \sum_{j=1}^{n} \sum_{0\leq i_1<\ldots<i_j<n} \sum_{0\leq x_{i_1},\ldots,x_{i_j}\leq 1} \alpha^{0,i_2-i_1,\ldots,i_j-i_1}_{k,x_{i_2},\ldots,x_{i_j}} \times \mathrm{Tr}_{2\ldots n}\left(\mathbb{1}^{(0)}_D \otimes \mathcal{M}^{(i_2-i_1)}_{x_{i_2}} \otimes \cdots \otimes \mathcal{M}^{(i_j-i_1)}_{x_{i_j}} \rho^{TI}\right). \quad (4.139)$$

Then, we only need to observe that $\mathrm{Tr}(\mathcal{B}\rho^{TI}) = \sum_{k=0}^{M-1}\mathrm{Tr}(\mathcal{M}^{(0)}_k F_k)$, subject to the constraints $-\mathbb{1}_D \preceq \mathcal{M}^{(i)}_k \preceq \mathbb{1}_D$, is the expression to minimize, from which semi-definite programming can be applied, obtaining a minimum $\widetilde{\beta}$. Alternatively, one can use the spectral decomposition of F_k, which reads $F_k = \sum_i \lambda^{(k)}_i |\phi^{(i)}_k\rangle\langle\phi^{(i)}_k|$ to directly obtain the optimal measurements, which are given by

$$\mathcal{M}^{(0)}_k := -\sum_i \mathrm{sgn}(\lambda^{(k)}_i)|\phi^{(k)}_i\rangle\langle\phi^{(k)}_i|, \quad (4.140)$$

for $0 \leq k < M$. Observe that now the measurements are no longer symmetric. However, we have that $\tilde{\beta} \geq \beta$.

6. Go back to step 2 until convergence $\tilde{\beta} = \beta$ is achieved.

Let us briefly comment on the differences between the proposed algorithm and the one in [PV10]. Steps 2 and 4 are added for the following reasons: Step 2 enforces that the same set of measurements is used at each site, whereas step 4 guarantees that the state giving the current quantum violation β is translationally invariant. Applying step 2 does not guarantee that β is nondecreasing at every step. However, the numerics we have performed suggest that this is not the case, which enables us to conjecture that this is the general case.

The algorithm has been implemented and tested on inequalities 64 to 103 in Table C.6 (*i.e.*, those for which a translationally invariant 4-qubit states were insufficient), and we observe that, for all cases, $d_{\min} \leq 6$ holds; *i.e.*, a six-dimensional local Hilbert space at each site can accomodate a translationally invariant state and the same set of measurements that will lead to β_Q. Observe that the constructive bound we have proved analytically would be $2 \times 4 = 8$. More precisely, in the majority of cases we can say that $d_{\min} \leq 3$, with the only exceptions being listed below:

- $d_{\min} \leq 4$ for inequalities 64, 65, 73, 78, 81, 86, 91, 99 and 100,
- $d_{\min} \leq 5$ for inequalities 70 and 82, and
- $d_{\min} \leq 6$ for inequalities 67, 68, 69, 74 and 75.

In all cases, real-valued observables can be taken that satisfy these bounds and we conjecture that all of them are tight.

4.7. Experimental Considerations

In this section we introduce a preliminary analysis of the effect of imperfections and experimental errors in the detection of nonlocality in many-body systems with $\mathfrak{S}_n$-symmetric 2-body Bell inequalities of the form (4.22).

In the case in which all parties measure the same set of observables, the expectation value of the Bell Operator $\mathcal{B}(\hat{\mathbf{n}}_0, \hat{\mathbf{n}}_1)$ can be found through

collective measurements of the total spin components

$$J_\alpha := \frac{1}{2}\sum_{i=0}^{n-1}\sigma_\alpha^{(i)}, \qquad \alpha \in \{x,y,z\}, \tag{4.141}$$

where σ_x, σ_y and σ_z are the qubit Pauli matrices, and their combinations $\hat{\mathbf{n}}\cdot\vec{\mathbf{J}}$, where $\hat{\mathbf{n}}$ is a unit vector in the Bloch Sphere and $\vec{\mathbf{J}} := [J_x, J_y, J_z]$. Considering a pair of qubit measurements $\mathcal{M}_k = \hat{\mathbf{n}}_k\cdot\vec{\boldsymbol{\sigma}}$, with $\vec{\boldsymbol{\sigma}} := [\sigma_x,\sigma_y,\sigma_z]$. It is direct to find the expression of the Symmetric correlators $\mathcal{S}_0$, $\mathcal{S}_1$, $\mathcal{S}_{00}$, $\mathcal{S}_{01}$ and $\mathcal{S}_{11}$, defined as in Eqs. (4.14) and (4.15), in terms of $\hat{\mathbf{n}}_0$, $\hat{\mathbf{n}}_1$ and $\vec{\mathbf{J}}$.

$$\begin{aligned}
\mathcal{S}_k &= 2\cdot\hat{\mathbf{n}}_k\cdot\vec{\mathbf{J}}, \qquad k\in\{0,1\} && (4.142)\\
\mathcal{S}_{kk} &= 4\cdot(\hat{\mathbf{n}}_k\cdot\vec{\mathbf{J}})^2 - n \qquad k\in\{0,1\} && (4.143)\\
\mathcal{S}_{01} &= ((\hat{\mathbf{n}}_0+\hat{\mathbf{n}}_1)\cdot\vec{\mathbf{J}})^2 - ((\hat{\mathbf{n}}_0-\hat{\mathbf{n}}_1)\cdot\vec{\mathbf{J}})^2 - n\cdot\hat{\mathbf{n}}_0\cdot\hat{\mathbf{n}}_1. && (4.144)
\end{aligned}$$

The analysis we present was motivated by recent experiments on entanglement detection in Dicke states [Lüc+14]. We study how the errors in the measured quantities J_θ^2 (the second order moment of the collective spin component (4.141) in the direction determined by the angle θ between x and z: $J_\theta := \cos\theta J_z + \sin\theta J_x$) in the ability to detect nonlocality.

Let us take the quantities $\mathcal{S}_u$ and $\mathcal{S}_{uv}$, where $u,v\in\{x,z\}$, which are defined in Eq. (B.1) and let us express the symmetric correlators $\mathcal{S}_0$, $\mathcal{S}_1$, $\mathcal{S}_{00}$, $\mathcal{S}_{01}$ and $\mathcal{S}_{11}$ in terms of them. An inequality of the form (4.22) can be expressed as

$$\beta_c + A\mathcal{S}_z + A'\mathcal{S}_x + \frac{B}{2}\mathcal{S}_{zz} + \frac{C}{2}\mathcal{S}_{xx} + D\mathcal{S}_{xz} \geq 0, \tag{4.145}$$

where the constants A, A', B, C and D are defined as in Theorem 4.6.

Using the following equivalences[28] between $\mathcal{S}_u$, $\mathcal{S}_{uv}$ and J_u, J_u^2, $J_{\pi/4}^2$ ($u,v\in\{x,z\}$)

$$\begin{cases}
\mathcal{S}_x &= 2J_x\\
\mathcal{S}_z &= 2J_z\\
\mathcal{S}_{xx} &= 4J_x^2 - n\\
\mathcal{S}_{zz} &= 4J_z^2 - n\\
\mathcal{S}_{xz} &= 2(2J_{\pi/4}^2 - J_x^2 - J_z^2)
\end{cases} \tag{4.146}$$

[28] We have used that $\mathcal{S}_{xz} = 2\{J_x, J_z\}$.

we can arrive at the expression for (4.22) in terms of the total spin operators J:

$$\beta_c + 2AJ_z + 2A'J_x + \frac{B}{2}(4J_z^2 - n) + \frac{C}{2}(4J_x^2 - n) + 2D(2J_{\pi/4}^2 - J_x^2 - J_z^2) \geq 0, \tag{4.147}$$

which is convenient to rewrite in the form

$$\beta_c + 2AJ_z + 2A'J_x + 2(B-D)J_z^2 + 2(C-D)J_x^2 + 4DJ_{\pi/4}^2 - n\frac{B+C}{2} \geq 0. \tag{4.148}$$

Stimulated by discussions with the Hannover group [LK14], we introduce the following model for experimental errors:

$$\langle J_\theta^2 \rangle_{\text{measured}} = \eta(\kappa + \langle J_\theta^2 \rangle_{\text{ideal}}), \tag{4.149}$$

where $\eta \in (0,1)$ is a visibility parameter and $\kappa > 0$ is an offset parameter that depends on n. The values of θ actually measured in the experiment would be $0, \pi/4$ and $\pi/2$. Eq. (4.149) captures the behavior of the experimental data of [Lüc+14], for which $\eta \approx 0.8$, $\kappa \approx 100$ and $n \approx 8000$. Note that, for a symmetric state, $\langle J_z^2 \rangle_{\text{ideal}} = 0$, so that the error in z is dominated by the κ parameter. On the other hand, $\langle J_x \rangle_{\text{ideal}} \in O(n^2)$ which means that the error is in this case dominated by the visibility parameter η. The data for $\langle J_{\pi/4}^2 \rangle$ is not available, as this measurement had not been performed, but both effects should be taken into account by (4.149).

Example 4.19. *Let us take $n = 8000$ and the Half-filled Dicke state $|D_n^{n/2}\rangle$. The ideal values of the total spin components and its second order moments are $\langle J_x \rangle = \langle J_z \rangle = \langle J_z^2 \rangle = 0$, $\langle J_x^2 \rangle = (n^2+2n)/8$, and $\langle J_{\pi/4}^2 \rangle = (n^2+2n)/16$. We use a Bell inequality of the class (4.87) to detect the nonlocality of this state:*

$$\left\lceil \frac{n+2}{2} \right\rceil \binom{n}{2} + \frac{1}{2}\binom{n}{2}\mathcal{S}_{00} + \frac{n}{2}\mathcal{S}_{01} - \frac{1}{2}\mathcal{S}_{11} \geq 0. \tag{4.150}$$

In Fig. 4.19 we present the effect of the errors (4.149) in the nonlocality detection.

As we can see from Example 4.19, the offset κ severely reduces the applicability of Inequality (4.150). The reason is that the condition $\langle J_z^2\rangle_{\text{ideal}} = 0$ is in fact $\langle J_z^2\rangle_{\text{measured}} \approx 80$, an effect that gets multiplied by the very nonlinear form of the coefficients γ, δ and ε in (4.150), which are $O(n^2)$, $O(n)$, and $O(1)$ respectively. In order to improve the performance of Example 4.19, one could try to look for Bell inequalities with more balanced coefficients, at the price of having a smaller effective quantum violation.

However, if we do not restrict ourselves to the state $|D_n^{n/2}\rangle$, by using a Bell inequality with a more *balanced* set of coefficients, we can vastly improve the results of Fig. 4.19:

Example 4.20. *We take the Bell inequality of Example 4.10, namely*

$$2n - 2\mathcal{S}_0 + \frac{1}{2}\mathcal{S}_{00} - \mathcal{S}_{01} + \frac{1}{2}\mathcal{S}_{11} \geq 0, \tag{4.151}$$

and the corresponding Gaussian superposition of Dicke states, namely $|\psi_n\rangle = \sum_{k=0}^{n} \psi_k^{(n)} |D_n^k\rangle$*, with the coefficients* $\psi_k^{(n)}$ *defined as in (4.71). The ideal values of the total spin components and its second order moments are given by* $\langle J_z\rangle = 1/(2\sqrt{3})$*,* $\langle J_x\rangle = n/2$*,* $\langle J_z^2\rangle = 0$*,* $\langle J_x^2\rangle = n^2/4$ *and* $\langle J_{\pi/4}^2\rangle = (n^2/2 + n/\sqrt{3})/4$*. In Fig. 4.20 we report the effect of the errors (4.149) in the detection of nonlocality of* $|\psi_{8000}\rangle$*.*

We observe that, contrary to Example 4.19, Example 4.20 shows an improvement of almost five orders of magnitude in the error that one can tolerate in κ (provided that one can prepare the state (4.71) in the laboratory) thanks to the balance that now have the coefficients γ, δ and ε in (4.73). In comparison to the values obtained in [Lüc+14], Example 4.20 shows that the class of inequalities described in Theorem 4.4 can tolerate an error in J_z^2 almost one order of magnitude higher.

4.7.1. Experimental realizations

We conclude this chapter by discussing a collection of setups in which nonlocality in many-body systems may be tested implementing our inequalities.

Ultracold trapped atoms

One can create a spinor Bose-Einstein Condensate (BEC) of Rubidium $F = 1$ atoms. The process to achieve this goal is to use spin changing collisions, in which $m_F = 0$ atoms collide to produce a $m_F = \pm 1$ pair. In this way, many thousands of neutral atoms can be entangled in their spin degree of freedom. In [Lüc+14], a Dicke-like state was created using this procedure, with a genuine multipartite entanglement of at least 28 particles and a generalized squeezing parameter of $11.4(5)\mathrm{dB}$.

In a similar fashion, one can employ Rubidium pseudo-spin $1/2$ atoms in a BEC to generate scalable squeezed states. A theoretical proposal can be found in [Sor+01], and for experiments see [Mue+14]. Using this procedure, non-squeezed, non-Gaussian, entangled states of many atoms were generated [Str+14] very recently.

In all these experiments, the number of atoms involved is in the order of 10^3 or even greater. However, as Example 4.19 points out, the experimental imperfections and errors are too large, and the fidelities are too small to allow for many-body nonlocality. It could be possible to achieve a compromise; *i.e.*, to perform such experiments with a mesoscopic number of atoms (*e.g.* $\lesssim 100$), where there would be the possibility of controlling the atom number to a single atom level (in [Hum+13], resonant fluorescence detection of Rb^{87} atoms in a MOT is performed; in [Wen+13; Zür+13], optically trapped spin-$1/2$ fermions are used).

Ultracold trapped ions

Ultracold trapped ions with internal pseudo-spin can, via phonon excitations, *talk* to each other; in some conditions it is even possible to make them behave as spin chains with long range interactions. There are basically two ways to do this: the original proposal was using inhomogeneous magnetic fields [MW01], but it is also possible to appropriately tailor laser-ion interactions [PC04]. The first experiments ever performed were those of [Fri+08; Kim+10]. The first theoretical studies considered spin interactions whose strength decayed with the third power of the distance [PC04; DPC05; Hau+10; Mai+12]; however, it was shown that it was possible experimentally to achieve decaying powers between 0.1 and 3 in 2-dimensional arrays of traps, via mediating phonon interactions [Bri+12].

Recently, there has been progress on the experimental realization of a quantum integer-spin chain in whic the interactions can be controlled [Sen+14]. Additionally, trapped ions systems in relation to long range $SU(3)$ spin chains and quantum chaos have been considered [Gra+13], as well as trapped-ion quantum simulation of tunable-range Heisenberg chains [GL14]. In [GL14] it was shown that significant violation of the Bell inequalities discussed in this chapter (Example 4.19) is possible for the ground states of models with large -although finite- interaction range.

Ultracold atoms in nanostructures

The very rapid experimental progress in coupling ultracold atomic gases to nanophotonic waveguides, started by [Nay+07; Vet+10; Gob+12] (see also [Gob+14]) suggests the possibility to consider systems of ultracold atom traps in the vicinity of tapered optical fibers and optical crystals, which are band gap materials. The remarkable properties of such kind of systems was already highlighted in early theoretical studies [KH08; ZR10; CGS11; Cha+12]. More recently, the attention has been focused on the development of long range spin models [CCK13; GT+15; Dou+15].

Cold and ultracold atomic ensembles

Cold and untracold atomic ensembles [HSP10] allow for unprecedented degrees of squeezing of the total atomic spin by means of the quantum Faraday effect [Nap+11; Sew+14], as well as extraordinary degrees of precision of quantum magnetometry [Luc+14]. As the Bell inequalities derived in this chapter require very precise measurements of the total spin components and its second order moments (*i.e.*, quantum fluctuations), it seems that Quantum Faraday effect (also referred to as spin polarization spectroscopy) is a very well suited method to fulfill this objective; in principle, it also allows to reach spatial resolution and/or the measurement of spatial Fourier components of the total spin [Eck+08].

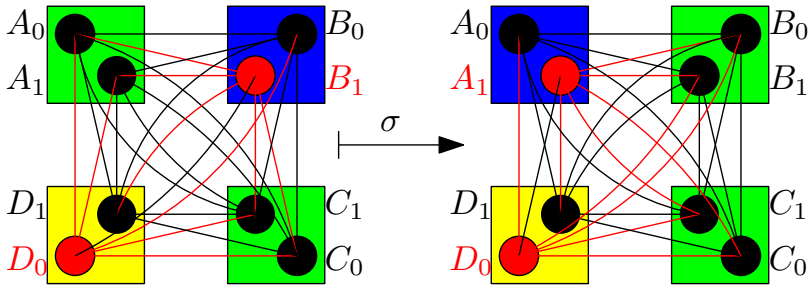

Figure 4.1.: *The action of a permutation* $\sigma = (A \mapsto C \mapsto B \mapsto A)(D \mapsto D)$ *on a DLS*. We take as an example the $(4, 2, 2)$ scenario with 4 parties, labelled A, B, C, D, each having a choice between the 0-th and the 1-st observables, and each observable can give ± 1 as a result. Each square represents a party and each circle corresponds to a measurement. We take the convention that if the circle is filled in black, its predetermined outcome is $+1$ $(+)$, whereas if it is filled in red, then its predetermined outcome is -1 $(-)$. All parties having the same DLS have squares with the same color. We consider the DLS f given by $f(A) = (+, +)$, $f(B) = (+, -)$, $f(C) = (+, +)$ and $f(D) = (-, +)$. Each line corresponds to a two-body correlator; if it is a black line, the results are correlated and if it is a red line, they are anti-correlated. Although the value of the single two-body correlators can be changed by σ (*e.g.*, A_0B_1 is anticorrelated on the left, but it is correlated on the right), observe that the symmetrized correlators do not change their respective value. Both before and after the action of σ, one has $S_{[A_0]} = A_0 + B_0 + C_0 + D_0 = 2$, $S_{[A_1]} = 2$, $S_{[A_0B_0]} = 0$, $S_{[A_0B_1]} = 4$, $S_{[A_1B_1]} = 0$. In terms of $\mathbf{P}_L$, the two graphs above correspond to two different vertices, but they are projected to the same point in $\mathbb{P}_2^{\mathfrak{S}_n}$.

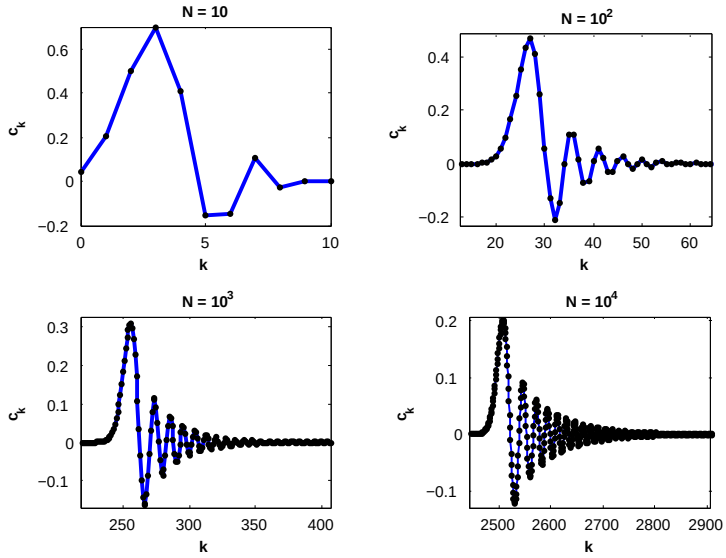

Figure 4.2.: Distributions of $c_k^{(n)}$ versus k for $n \in \{10, 10^2, 10^3, 10^4\}$. $c_k^{(n)}$ are the coefficients of the eigenstate corresponding to the minimal eigenvalue of $\mathcal{B}(0, \theta^* - \varphi^*)$, which is found in the invariant subspace where $\mathcal{B}_{n/2}(0, \theta^* - \varphi^*)$ acts, for the optimal $\theta - \varphi$. The black dots correspond to the values of $c_k^{(n)}$ and the blue line connecting them is added just to better show the behavior with k.

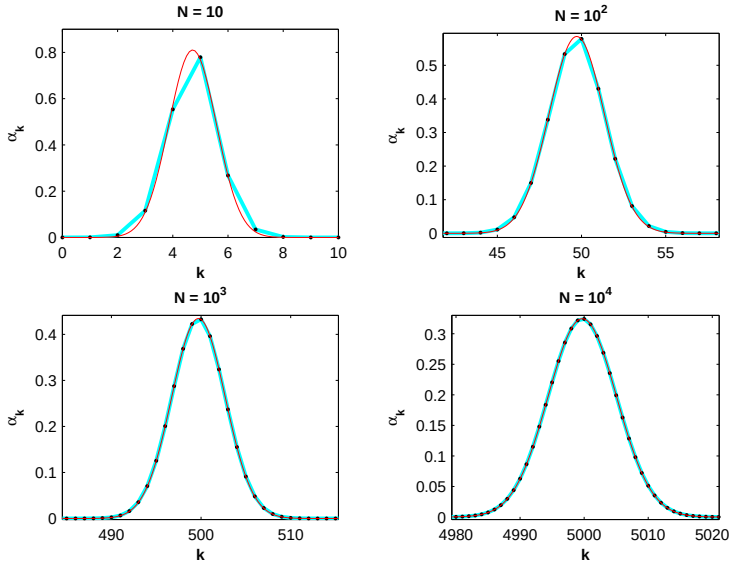

Figure 4.3.: The black points represent values of $\alpha_k^{(n)}$ for $n \in \{10, 10^2, 10^3, 10^4\}$. As in Fig. 4.2, the cyan line is added to mark better their behavior with k. The red lines are the square roots of the Gaussian distributions, as introduced in Theorem 4.9, with means μ_n and variances σ_n chosen so that the distributions best fit the points. Their explicit values are $\mu_n = n/2 + (1/4\cos\theta_n)$, where $\theta_{10} = 2.6672$, $\theta_{10^2} = 2.6334$, $\theta_{10^3} = 2.6231$, $\theta_{10^4} = 2.6180$, and $\sigma_{10} = 0.4049$, $\sigma_{10^2} = 1.3935$, $\sigma_{10^3} = 4.5109$, and $\sigma_{10^4} = 14.379$, respectively. Noticeably, already for $n = 10$, the red line matches the points very well. We quantify this agreement in Fig. 4.4.

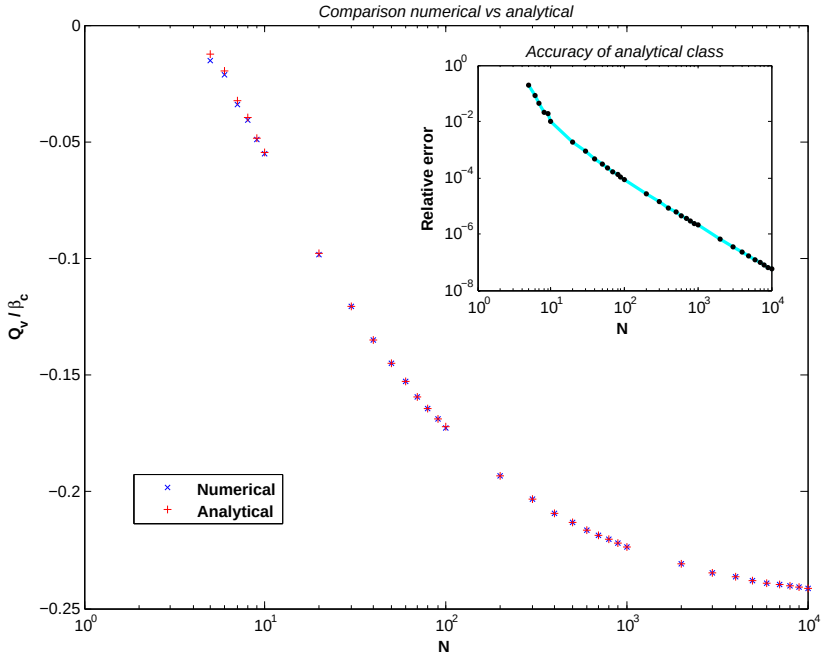

Figure 4.4.: Maximal quantum violations of inequality (4.73) (blue crosses) compared to the maximal violations achievable by the states defined in Theorem 4.9 (red crosses). All means and variances in the Gaussian distributions were chosen so that $|\psi_n^{\min}\rangle$ would maximally violate (4.73). The inset contains the relative difference between numerical and analytical violations. The points in the inset are the actual values of n for which we performed the calculations and the cyan line is just added to help in visualizing the tendency. Note that, already for $n = 10$, the two violations are almost the same.

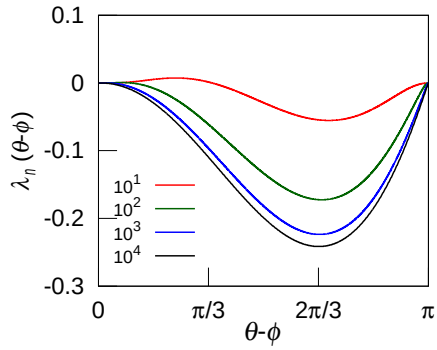

Figure 4.5.: The minimal negative eigenvalue −normalized to the classical bound− of the Bell operator $\mathcal{B}(\theta-\varphi)$ that corresponds to Inequality (4.73), denoted $\lambda_n(\theta-\varphi)$, for $n=10^k$, with $k\in\{1,2,3,4\}$.

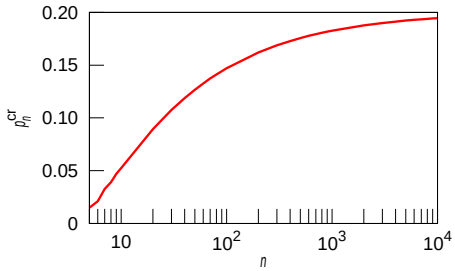

Figure 4.6.: The tolerance to white noise p_n^{cr} for the inequality (4.73) as a function of n. This is a monotonously increasing function (*cf.* Eq. 4.83). For $n=10^4$ the tolerance is almost 20%.

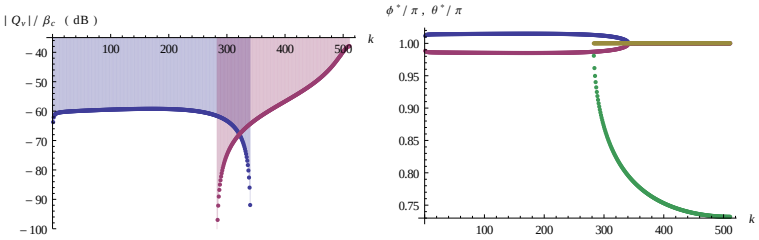

Figure 4.7.: On the left, the values $|Q_v|$ of the maximal quantum violation of (4.86 - 4.87) for the Dicke state $|D_n^k\rangle$ with $n = 2^{10} = 1024$ qubits. The violation is relative to the classical bound β_c. The blue curve corresponds to (4.86) and the red curve corresponds to (4.87). The maximal quantum violation has been plotted in logarithmic scale (in dB; *i.e.* $10\log_{10}(-\min_{\varphi,\theta} d_k/\beta_c)$ is what appears on the plot) in order to better compare the two bounds. The horizontal axis is cut at $k = n/2$ because of the symmetry with respect to $k = n/2$. The reason for that is that the same violation can be achieved by an inequality that results from renaming the outcomes of the measurements or, equivalently, by switching $|0\rangle \leftrightarrow |1\rangle$ for every qubit. The figure clearly shows that the two classes overlap, so these two classes cover all possible entangled Dicke states $|D_n^k\rangle$. On the right, we represent, for every k, the optimal measurement angles $\varphi^*/\pi, \theta^*/\pi$ that lead to the violation shown on the left. For the class of inequalities (4.86) ϕ^* and θ^* are plotted in blue and red, respectively, where the condition for optimality $\varphi = -\theta$ can be appreciated. For the class of inequalities (4.87), the optimal measurement angles ϕ^* and θ^* are plotted in yellow and green, respectively. Interestingly, although the plot suggests that $\varphi^* = \pi$ for the inequality (4.87), it is not the case: If the yellow line were exactly π, one could not achieve the optimal quantum violation. For this $n = 2^{10}$, $\phi^*|_{k=280} \approx \pi$ and $\phi^*|_{k=511} \approx 1.00023\pi$. Loosely speaking, the reason for this slight discrepancy is that d_k can be expressed as $d_k = 2n^4\cos(\varphi/2)^4 - 2n^3\cos(\varphi/2)^2(k - \cos\theta + (1+3k)\cos\varphi) + 2n^2k^2\cos^2(\varphi/2)(1+3\cos\varphi) + o(n^2k^2)$, an expression which can be made $o(n^2k^2)$ just by picking $\varphi = \pi$. However, one can do better by exploiting the fact that a value of $\cos(\varphi/2)$ small enough makes the whole expression effectively $o(n^2k^2)$ (this value of φ^* will actually depend on n and k), and the leading terms contribute to the minimization.

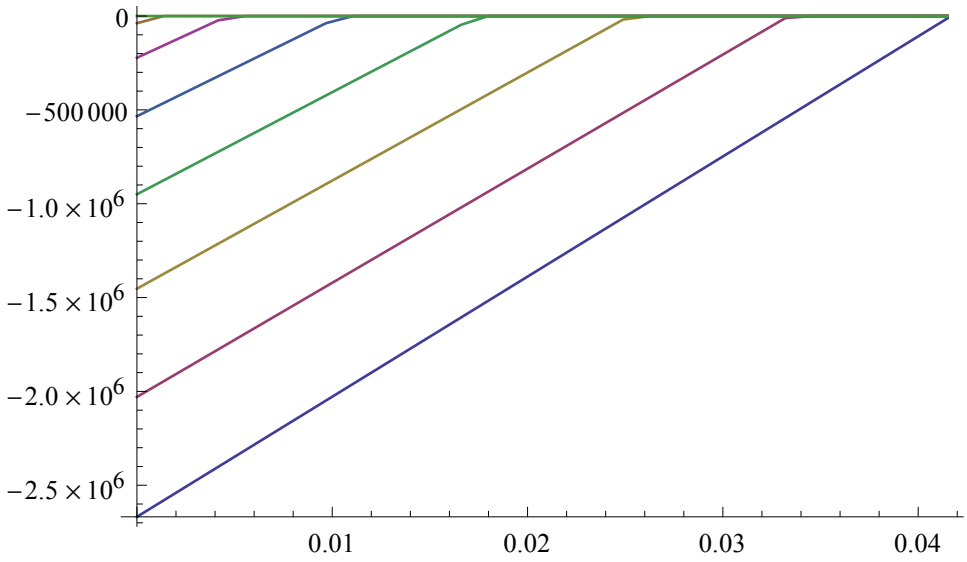

Figure 4.8.: The expecation value $\langle \mathcal{B}(\hat{\mathbf{n}}_0^*, \hat{\mathbf{n}}_1^*) \rangle$ for the optimal measurement directions $\hat{\mathbf{n}}_0^*$ and $\hat{\mathbf{n}}_1^*$, as a function of κ. The different curves correspond to $\eta \in \{1, 0.95, 0.9, \ldots\}$ starting at $\eta = 1$ (blue line).

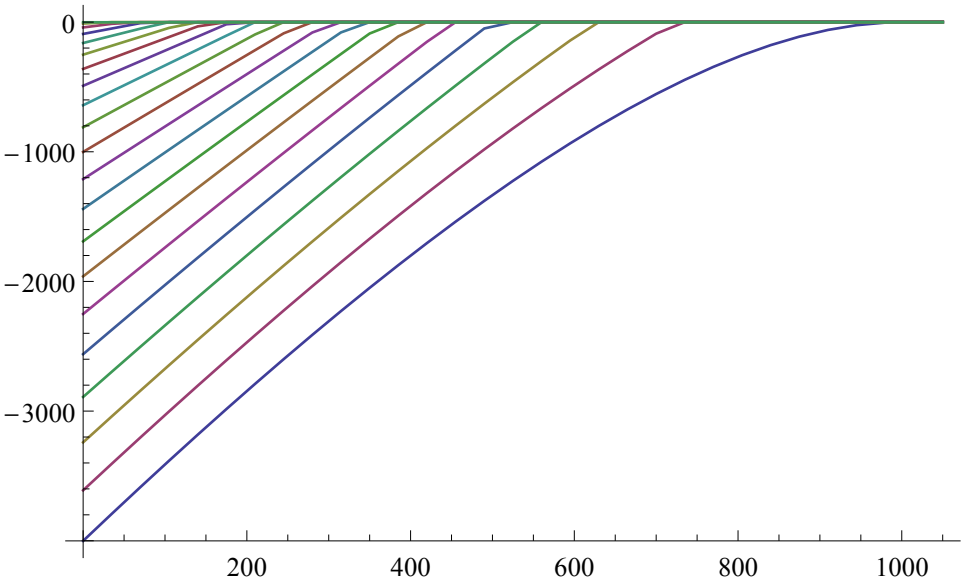

Figure 4.9.: We have taken Ineq. (4.73) for $n = 8000$ qubits and represented the expecation value $\langle \mathcal{B}(\hat{\mathbf{n}}_0^*, \hat{\mathbf{n}}_1^*) \rangle$ for the optimal measurement directions $\hat{\mathbf{n}}_0^*$ and $\hat{\mathbf{n}}_1^*$ and the optimal state (4.71), as a function of κ. The different curves correspond to $\eta \in \{1, 0.95, 0.9, \ldots\}$ starting at $\eta = 1$ (blue line).

5. Relating entanglement and nonlocality

Both entanglement and nonlocality are central concepts in modern physics. Their relation, however, is not fully understood yet. In 1964, Bell showed that some entangled states are nonlocal, in the sense that the statistics obtained when certain measurements are performed on them would violate a Bell inequality [Bel64]. In 1991, Gisin showed that every pure bipartite entangled state is nonlocal [Gis91], a result that was later generalized to any multipartite pure entangled quantum state a bit later by Popescu and Rohrlich [PR92]. Thus, one could naively identify nonlocality and entanglement, however, this intuition is—like in many situations in quantum physics—misleading, as the relation between those two quantum information resources is more involved.

In [Wer89], Werner started a program to explore the relation between these two concepts, showing that they are inequivalent in the bipartite case. In order to do so, he introduced a Local Hidden Variable Model (LHVM) that reproduces the statistics of any set of measurements that is performed on an entangled state, thus showing that entanglement does not imply nonlocality[1]. Observe that, if a bipartite state has a LHVM, then, for any Bell scenario $(2, m, d)$ and for any possible choice of measurements performed on the state, the obtained statistics correspond to a point belonging to the local polytope $\mathbf{P}_L$. Observe that the approach of Chapter 4 was taken from a quite opposite perspective: we wanted to show that nonlocality was present in some quantum states; hence, it was sufficient to choose a particular Bell scenario, to provide a Bell inequality and to show that it was violated when some measurements were performed on the state. Here we need to show that, whatever measurements are performed on the state, the statistics obtained satisfy *all* Bell inequalities for *all* scenarios. As the problem of finding all Bell inequalities is intractable, in practice one can only construct explicitly a LHVM for the state under consideration. This

[1] Observe that LHVMs always exist for separable states (*cf.* Eqs. (2.2) and (2.14)). Equivalently, nonlocality implies entanglement.

caveat is the main reason why the literature on the subject is so scarce [ADA14].

In the multipartite scenario, however, the relation between these two concepts is quite unexplored. The main reason lies in the subtelties that appear, both in the definition of multipartite entanglement (*cf.* Eq. (2.3)) and, especially, in the definition of multipartite nonlocality (*cf.* Eq. (2.17)). As a trivial example of an entangled state that admits a local model, one can always construct a multipartite entangled state that is local by taking a bipartite entangled, local state (*e.g.* a Werner state) that is fully product with respect of the rest of the parties. Clearly, this is just a manifestation of the already known inequivalence for the bipartite case.

Hence, the most natural question to ask is the following: do there exist, for any n, Genuinely Multipartite Entangled (GME) states which are not Genuinely Multipartite Nonlocal (GMN)? This is the main goal of the present chapter, in which we will show that this is indeed the case, hence proving that entanglement and nonlocality are inequivalent for any number of parties.

The results presented in this chapter are joint work with R. Augusiak, M. Demianowicz and A. Acín [Aug+14c].

5.1. Local Models

Before moving to the main result, let us summarize what has been known so far for the bipartite case. In 1989, Werner introduced a family of highly symmetric states, which are $U \otimes U$-invariant [Wer89], nowadays known as Werner states:

$$\rho_W(p) := p\binom{d}{2}^{-1} P_d^{(-)} + (1-p)d^{-2}\mathbb{1}_{d^2}, \tag{5.1}$$

where $P_d^{(-)}$ is the projector onto the antisymmetric space of $(\mathbb{C}^d)^{\otimes 2}$ (*cf.* Theorem A.9). Note that, for $d = 2$, $P_d^{(-)} = |\psi_-\rangle\langle\psi_-|$, where $|\psi_-\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$ is the singlet state.

Werner provided a LHVM that, for $p \geq (d-1)/d$, reproduces the statistics of any projective measurements performed on $\rho_W(p)$. As $\rho_W(p)$ is entangled if, and only if, $p > 1/(d+1)$, any Werner state in the range of

parameters $1/(d+1) < p \leq (d-1)/d$ proves that, in the bipartite case, entanglement and nonlocality are inequivalent for projective (von Neumann) measurements.

Example 5.1. *In order to construct Werner's model [Wer89], the shared randomness $\lambda \in \Lambda$ present in Eq. (2.14) is taken to be a normalized tuple of d complex numbers; it can be interpreted as a qudit quantum state $|\lambda\rangle \in \mathbb{C}^d$. Hence, the space of hidden variables is taken to be $\Lambda = \{|\lambda\rangle \in \mathbb{C}^d : \langle\lambda|\lambda\rangle = 1\}$. One can think of this as a referee that sends two qudits $|\lambda\rangle$ to the parties prior to the experiment. Now we consider two von Neumann measurements $\mathcal{A}$, $\mathcal{B}$ that are performed on Alice's and Bob's laboratories, respectively. Let $\{A_a\}_a$ and $\{B_b\}_b$ be the corresponding projections. We now have to give response functions $p(a|\mathcal{A}, \lambda)$ and $p(b|\mathcal{B}, \lambda)$ such that $P(ab|\mathcal{AB})$ takes the following form:*

$$P(ab|\mathcal{AB}) = \mathrm{Tr}(\rho_W(p) A_a \otimes B_b) = \int_\Lambda q(\lambda) p(a|\mathcal{A}, \lambda) p(b|\mathcal{B}, \lambda) \mathrm{d}\lambda. \tag{5.2}$$

Alice has to give an outcome a, based solely on the shared randomness $|\lambda\rangle$ available to her and the measurement that she performs $\mathcal{A}$. She always outputs the outcome corresponding to the projection with minimal overlap with λ:

$$p(a|\mathcal{A}\lambda) := \begin{cases} 1 & \text{if} \quad a = \arg\min_a \langle\lambda|A_a|\lambda\rangle \\ 0 & \text{otherwise} \end{cases}. \tag{5.3}$$

Similarly, Bob is given $|\lambda\rangle$ and $\mathcal{B}$ and he has to produce an outcome b. He does so according to the following rule:

$$p(b|\mathcal{B}, \lambda) := \langle\lambda|B_b|\lambda\rangle. \tag{5.4}$$

Finally, if the shared randomness $|\lambda\rangle$ is generated according to the unique probability density which is invariant under any unitary operation (which we denote $q(\lambda)$), then the LHVM of Eq. (5.2) is satisfied; i.e., the r. h. s. of Eq. (5.2) reproduces the probabilities that are given by Quantum Theory.

In [Bar02], Barrett generalized the model in Example 5.1 to general POVMs, obtaining a range of the parameter p in Eq. (5.1) for which Werner states were entangled, but nonlocality could never be revealed, regardless of the measurements performed. The construction given by Barrett was

adapted to states of a similar form to $\rho_W(p)$; *i.e.*, mixtures of white noise and a given quantum state ρ [Alm+07]. In particular, when ρ is the projector onto the maximally entangled state $\sum_{i=0}^{d-1} |ii\rangle/\sqrt{d}$, one obtains a local model for the isotropic states [HH99].

Grothendieck's constant

The violation of Bell inequalities for noisy states of the form $p\rho + (1-p)\mathbb{1}_{d^2}/d^2$ has been related to an important notion in functional analysis, which is the Grothendieck's constant[2]. This is particularly useful when one deals with states whose reduced density matrices are maximally mixed (*e.g.* Werner or isotropic states). In such case, any bipartite Bell inequality can be expressed purely in terms of two-body expectation values (as any one-body expectation value will vanish). If the observables are binary and their outcomes are ± 1, then we will have

$$\sum_{x,y=0}^{m-1} c_{xy} \langle A_x \otimes B_y \rangle \leq \beta_c, \tag{5.5}$$

where c_{xy} are real coefficients, m is the number of measurements and β_c is the classical bound of the Bell inequality (5.5). If the observables

[2] If A is a $n \times n$ square matrix with entries $(A)^i_j = a_{ij} \in \mathbb{R}$, such that

$$\max_{|s_i|,|t_j|\leq 1} \left| \sum_{i,j} a_{ij} s_i t_j \right| = 1,$$

where $s_i, t_j \in \mathbb{R}$, then, there exists a constant $K_{\mathbb{R}}(n)$ such that, for any vectors $\vec{s_i}, \vec{t_j}$ such that their norm is $|\vec{s_i}|, |\vec{t_j}| \leq 1$, the following holds:

$$\max_{|\vec{s_i}|,|\vec{t_j}|\leq 1} \left| \sum_{i,j} a_{ij} \vec{s_i} \cdot \vec{t_j} \right| = K_{\mathbb{R}}(n).$$

The number $K_{\mathbb{R}}(n)$ is known as Grothendieck's constant. Although its existence is proven, only bounds on its numerical value are known [Fin03]: $K_{\mathbb{R}}(2) = \sqrt{2}$, $K_{\mathbb{R}}(3) \leq 1.517$, $K_{\mathbb{R}}(4) \leq \pi/2$. In the limit, $K_{\mathbb{R}} := \lim_{n\to\infty} K_{\mathbb{R}}(n)$, it is known that $1.67696... \leq K_{\mathbb{R}} < \pi/\ln(1+\sqrt{2})^2 = 1.7822...$
In a similar fashion, a complex Grothendieck constant exists when $s_i, t_j, \vec{s_i}, \vec{t_j}$ are taken to be complex, with norm bounded by one. In such case, $1.1526 \leq K_{\mathbb{C}}(2) \leq 1.2157$, $1.2108 \leq K_{\mathbb{C}}(3) \leq 1.2744$, $1.2413 \leq K_{\mathbb{C}}(4) \leq 1.3048$ and, in the limit, $1.33807 \leq K_{\mathbb{C}} \leq 1.40491$.

have d outcomes, one can, in the spirit of the complex correlators introduced in Section 4.5.1, also express any Bell inequality purely in terms of two-body correlators, as one-body ones vanish on the state: We take $A_x^{(k)} := \sum_{i=0}^{d-1} \omega^{i\cdot k} |i_x\rangle\langle i_x|$, where $\{|i_x\rangle\langle i_x|\}$ forms a resolution of the identity corresponding to the x-th observable of Alice and ω is a primitive d-th root of the unity. Bob's measurements $B_y^{(l)}$ are defined in a similar way. Then, for any bipartite state with maximally mixed subsystems, any Bell inequality for the $(2, m, d)$ scenario takes the following form:

$$\sum_{k,l=1}^{d-1} \sum_{x,y=0}^{m-1} c_{xy}^{(kl)} \langle A_x^{(k)} \otimes B_y^{(l)} \rangle \leq \beta_c. \tag{5.6}$$

Example 5.2. *Let $\rho_{\text{iso}}(p) := p|\psi_+\rangle\langle\psi_+| + (1-p)\mathbb{1}_{d^2}/d^2$ be the isotropic states, where $|\psi_+\rangle := \sum_{i=0}^{d-1} |ii\rangle/\sqrt{d}$ is the maximally entangled state. Then,*

$$\langle A_x^{(k)} \otimes B_y^{(l)} \rangle_{\rho_{\text{iso}}} = p\langle\psi_+|A_x^{(k)} \otimes B_y^{(l)}|\psi_+\rangle. \tag{5.7}$$

As shown in [AGT06], the expectation values on the maximally entangled state can be written as scalar products of some vectors in $\mathbb{C}^{d^2}$: $\langle\psi_+|A_x^{(k)} \otimes B_y^{(l)}|\psi_+\rangle = \langle a_x^{(k)}|b_y^{(l)}\rangle$. Such vectors are normalized, because $(A_x^{(k)})^\dagger A_x^{(k)} = \mathbb{1}_d$ (and the same for $B_y^{(l)}$).

Hence, any bipartite Bell inequality of the form (5.6), when the corresponding expectation values are taken on the state ρ_{iso}, can be rewritten as:

$$p \sum_{k,l=1}^{d-1} \sum_{x,y=0}^{m-1} c_{xy}^{(kl)} \langle a_x^{(k)}|b_y^{(l)}\rangle \leq \beta_c. \tag{5.8}$$

Let us denote by Q_d the maximal quantum violation (for projective measurements) that one can attain on the maximally entangled state. Then,

$$Q_d = \lim_{m\to\infty} \sup_M \max_{|a_x^{(k)}\rangle, |b_y^{(l)}\rangle \in \mathbb{C}^{d^2}} \sum_{k,l=1}^{d-1} \sum_{x,y=0}^{m-1} c_{xy}^{(kl)} \langle a_x^{(k)}|b_y^{(l)}\rangle, \tag{5.9}$$

where we identify the coefficients of M with $c_{xy}^{(kl)}$.

Observe that Q_d is lower bounded by $K_{\mathbb{C}} \cdot C$, where the constant C is the result of the following optimization over complex numbers:

$$C := \max_{|a_x^{(k)}|,|b_y^{(l)}|\leq 1} \left| \sum_{k,l=1}^{d-1} \sum_{x,y=0}^{m-1} c_{xy}^{(kl)} a_x^{(k)} \cdot b_y^{(l)} \right|. \tag{5.10}$$

Hence, the l. h. s. of (5.6) can be upper bounded by $p \cdot K_{\mathbb{C}} \cdot C$. By imposing that $p \cdot K_{\mathbb{C}} \cdot C \leq \beta_c$, we obtain the condition $p \leq \beta_c / K_{\mathbb{C}} C$, for which the states $\rho_{\text{iso}}(p)$ never violate Bell inequality (5.6) for projective measurements.

5.2. Bilocal models in the multipartite scenario

To our knowledge, the only published result about local models in the multipartite scenario is [TA06]. There, Tóth and Acín constructed a fully local model for projective measurements on a three-qubit GME state. It remains unknown, however, whether this model can be extended to more parties.

In [Aug+14c], we show that entanglement and nonlocality are in general inequivalent concepts; *i.e.*, for any number of parties n. We do so by constructing GME states that admit a bilocal model for any $n \geq 2$. There are two main steps in this construction: first, in Section 5.2.1 we prove that every bilocal bipartite state can be mapped to a multipartite state admitting a bilocal model. Second, in Section 5.2.2 we argue that the construction provided in Section 5.2.1 can lead to GME states for any n.

5.2.1. The extension

Let us consider the set of parties $\mathbf{A} = \{A_1, \ldots, A_n\}$ and a bipartition $S|\overline{S}$ of $\mathbf{A}$. Let us consider an arbitrary bipartite state $\rho_{AB} \in \mathcal{D}(\mathbb{C}^d)^{\otimes 2}$. As a generalization of a fact stated in [Bar02], let us consider a pair of quantum channels (CPTP maps)

$$\Lambda_{A\to S} : \mathcal{B}(\mathbb{C}^d) \longrightarrow \mathcal{B}((\mathbb{C}^{d'})^{\otimes |S|}) \tag{5.11}$$

as well as

$$\Lambda_{B\to \overline{S}} : \mathcal{B}(\mathbb{C}^d) \longrightarrow \mathcal{B}((\mathbb{C}^{d'})^{\otimes |\overline{S}|}). \tag{5.12}$$

The maps $\Lambda_{A\to S}$ and $\Lambda_{B\to\overline{S}}$ send operators that act on a single-party d-dimensional Hilbert Space to operators that act on a $|S|-$partite (or $|\overline{S}|$-partite) Hilbert space with local dimension d'. We then have the following theorem:

Theorem 5.3. *Let $\rho_{AB}\in\mathcal{D}(\mathbb{C}^d)^{\otimes 2}$ and let $\Lambda_{A\to S}$ and $\Lambda_{B\to\overline{S}}$ be defined as in Eqs. (5.11) and (5.12), respectively. Let us define the n-partite state $\sigma_{\mathbf{A}}\in\mathcal{D}(\mathbb{C}^{d'})^{\otimes n}$ as*

$$\sigma_{\mathbf{A}} := (\Lambda_{A\to S}\otimes\Lambda_{B\to\overline{S}})[\rho_{AB}]. \tag{5.13}$$

If ρ_{AB} admits a local model for POVMs, $\sigma_{\mathbf{A}}$ admits a bilocal model for POVMs.

Proof. Our reasoning goes along the lines of [Bar02]. Let $\mathcal{M}_X$ be the measurement performed by party X ($X\in\{A,B\}$) and let $\{M_x^X\}$ be the POVM elements representing its outcomes. Because ρ_{AB} is local, the probability of obtaining outcomes (a,b) when the pair of measurements $(\mathcal{M}_A,\mathcal{M}_B)$ is performed takes the form of Eq. (2.17) for $K=2$:

$$P(a,b|\mathcal{M}_A,\mathcal{M}_B)=\int_\Lambda p(\lambda)p_\rho(a|\mathcal{M}_A,\lambda)p_\rho(b|\mathcal{M}_B,\lambda)\mathrm{d}\lambda. \tag{5.14}$$

Let us make a couple of brief remarks concerning the notation employed in Eq. (5.14). Both the space of hidden variables λ and quantum channels are typically denoted by Λ. It is clear from the context which one we refer to, as they are concepts with nothing in common. Moreover, for the response functions p we have added the subscript ρ to indicate that these probabilities correspond to the state ρ_{AB}.

Let $\mathcal{M}_i$ be the measurement performed by the i-th party in $\mathbf{A}$, with POVM elements $\{M_{a_i}^{(i)}\}$. We shall now construct a bilocal model for $\sigma_{\mathbf{A}}$ with respect to the $S|\overline{S}$ bipartition. To this end, consider the dual[3] maps of

[3] Let $\mathcal{H}$ and $\mathcal{K}$ be two finite-dimensional Hilbert spaces. Given a linear map $\Lambda:\mathcal{B}(\mathcal{H})\longrightarrow\mathcal{B}(\mathcal{K})$, its dual map, denoted $\Lambda^\dagger$, is defined as the linear map $\Lambda^\dagger:\mathcal{B}(\mathcal{K})\longrightarrow\mathcal{B}(\mathcal{H})$ that satisfies $\mathrm{Tr}(X\circ\Lambda[Y])=\mathrm{Tr}(\Lambda^\dagger[X]\circ Y)$, for any $X\in\mathcal{B}(\mathcal{K})$ and for any $Y\in\mathcal{B}(\mathcal{H})$. If Λ is a positive map (in particular, when it is a quantum channel, it is Completely Positive), its dual $\Lambda^\dagger$ is also positive. If, in addition, Λ is Trace Preserving (for all X, $\mathrm{Tr}\Lambda[X])=\mathrm{Tr}X$), its dual map $\Lambda^\dagger$ is unital; *i.e.*, it maps the identity to the identity: $\Lambda^\dagger[\mathbb{1}_{\mathcal{K}}]=\mathbb{1}_{\mathcal{H}}$.

$\Lambda_{A\to S}$ and $\Lambda_{B\to\overline{S}}$, denoted $\Lambda^\dagger_{S\to A}$ and $\Lambda^\dagger_{\overline{S}\to B}$, respectively, and define the operators

$$\overline{M^A_{\mathbf{a}_S}} := \Lambda^\dagger_{S\to A}\left(\bigotimes_{i=1}^{|S|} M^{(i)}_{a_i}\right), \qquad \overline{M^B_{\mathbf{a}_{\overline{S}}}} := \Lambda^\dagger_{\overline{S}\to B}\left(\bigotimes_{i=|S|+1}^{|\overline{S}|} M^{(i)}_{a_i}\right), \quad (5.15)$$

where the indices $\mathbf{a}_S := a_1 \dots a_{|S|}$ and $\mathbf{a}_{\overline{S}} := a_{|S|+1} \dots a_n$ denote the possible tuples of outcomes corresponding to the parties in S and $\overline{S}$, respectively. As a consequence that the dual map of a quantum channel is positive and unital, the operators defined in Eq. (5.15) form a set of POVM elements. Let us denote the associated POVMs by $\overline{\mathcal{M}_A}$ and $\overline{\mathcal{M}_B}$.

We can now define the response functions that correspond to the extended state $\sigma_{\mathbf{A}}$ for the partition $S|\overline{S}$. Let us take $\boldsymbol{\mathcal{M}} := \mathcal{M}_1 \dots \mathcal{M}_n$ as the set of measurements that are performed on $\sigma_{\mathbf{A}}$ and $\boldsymbol{\mathcal{M}}_S$ ($\boldsymbol{\mathcal{M}}_{\overline{S}}$) its restriction to S ($\overline{S}$). Then, the response functions which are defined as follows:

$$p_\sigma(\mathbf{a}_S|\boldsymbol{\mathcal{M}}_S,\lambda) := p_\rho(\mathbf{a}_S|\overline{\mathcal{M}_A},\lambda) \quad (5.16)$$

and

$$p_\sigma(\mathbf{a}_{\overline{S}}|\boldsymbol{\mathcal{M}}_{\overline{S}},\lambda) := p_\rho(\mathbf{a}_{\overline{S}}|\overline{\mathcal{M}_B},\lambda) \quad (5.17)$$

indeed constitute a bilocal model for $\sigma_{\mathbf{A}}$ for POVMs:

$$\begin{aligned} P(\mathbf{a}|\boldsymbol{\mathcal{M}}) &= \mathrm{Tr}\left[M^{(1)}_{a_1}\otimes\cdots\otimes M^{(n)}_{a_n}\sigma_{\mathbf{A}}\right] \\ &= \mathrm{Tr}\left[M^{(1)}_{a_1}\otimes\cdots\otimes M^{(n)}_{a_n}(\Lambda_{A\to S}\otimes\Lambda_{B\to\overline{S}})[\rho_{AB}]\right] \\ &= \mathrm{Tr}\left[\overline{M^A_{a_1\dots a_{|S|}}}\otimes\overline{M^B_{a_{|S|+1}\dots a_n}}\rho_{AB}\right] \\ &= \int_\Lambda p(\lambda)p_\rho(\mathbf{a}_S|\overline{\mathcal{M}_A})p_\rho(\mathbf{a}_{\overline{S}}|\overline{\mathcal{M}_B})\mathrm{d}\lambda \\ &= \int_\Lambda p(\lambda)p_\sigma(\mathbf{a}_S|\boldsymbol{\mathcal{M}}_S)p_\sigma(\mathbf{a}_{\overline{S}}|\boldsymbol{\mathcal{M}}_{\overline{S}})\mathrm{d}\lambda. \end{aligned} \quad (5.18)$$

□

5.2.2. Certifying genuinely multipartite entanglement

Let us now see how the construction introduced in Section 5.2.1 can lead to GME states. To this end, we first prove that, if a state $\sigma_{\mathbf{A}}$, whose subsystems

(with respect to a bipartition $S|\overline{S}$) act on the symmetric space, is entangled across $S|\overline{S}$, then it has to be GME. With this in mind, consider a bipartite entangled state $\rho_{AB} \in \mathcal{D}(\mathbb{C}^d \otimes \mathbb{C}^d)$ and two quantum channels $\Lambda_{A\to S} : \mathcal{B}(\mathbb{C}^d) \longrightarrow \mathcal{B}(\mathcal{S}(\mathbb{C}^{d'})^{\otimes|S|})$ and $\Lambda_{B\to\overline{S}} : \mathcal{B}(\mathbb{C}^d) \longrightarrow \mathcal{B}(\mathcal{S}(\mathbb{C}^{d'})^{\otimes|\overline{S}|})$ such that there exists, for each of them, a retraction[45]. Because these channels produce states acting on the corresponding $|S|$- and $|\overline{S}|$-partite symmetric spaces, the resulting global state $\sigma_{\mathbf{A}}$ is symmetric on the subspaces S and $\overline{S}$. Furthermore, because ρ_{AB} is entangled, it must be GME; if it were not the case, because $\Lambda_{A\to S}$ and $\Lambda_{B\to\overline{S}}$ can be retracted, ρ_{AB} must be separable, which is a contradiction. By supposing, in addition, that ρ_{AB} is local, Theorem 5.3 constructs a bilocal model for $\sigma_{\mathbf{A}}$, proving the main result of this section.

To complete the proof we now show that, if $\sigma_{\mathbf{A}}$ is symmetric on its subsystems $S|\overline{S}$, then it is either biseparable or GME. Before proving formally this result in Theorem 5.4, let us briefly comment on the steps we are going to take: Let P_S be the projector onto the symmetric space constituted by the parties in S, as defined in Eq. (3.7). We are considering a state $\sigma_{\mathbf{A}}$ for which $\sigma_{\mathbf{A}} = P_S \otimes P_{\overline{S}} \sigma_{\mathbf{A}} P_S \otimes P_{\overline{S}}$ holds. We suppose that $\sigma_{\mathbf{A}}$ is not GME and our aim is to prove that it is then biseparable across the $S|\overline{S}$ bipartition; *i.e.*,

$$\sigma_{\mathbf{A}} = \sum_i p_i \sigma_S^i \otimes \sigma_{\overline{S}}^i, \tag{5.19}$$

where $\sigma_S^i \in \mathcal{D}(\mathcal{S}(\mathbb{C}^{d'})^{\otimes|S|})$ and $\sigma_{\overline{S}}^i \in \mathcal{D}(\mathcal{S}(\mathbb{C}^{d'})^{\otimes|\overline{S}|})$. As $\sigma_{\mathbf{A}}$ is not GME, then it admits the decomposition of Eq. (2.3) with $K = 2$. Hence,

$$\sigma_{\mathbf{A}} = \sum_{T|\overline{T}\in\mathcal{S}_2} p_{T|\overline{T}} \rho_{T|\overline{T}}, \tag{5.20}$$

where $\rho_{T|\overline{T}}$ is a biseparable state across the partition $T|\overline{T}$ (recall that $\mathcal{S}_K$ is the set of all K-partitions of $\mathbf{A}$). By the very definition of biseparability (*cf.*

[4] By analogy with category theory, we adopt the same terminology here for quantum channels: Given two morphisms $g : Y \to X$ and $f : X \to Y$ such that $f \circ g = \mathbb{1}_Y$, g is called a *section* of f, whereas f is a *retraction* of g. In the context of quantum channels, the term *isometry* is typically used.

[5] We demand that, for the construction to lead to GME states, given Λ, there exists a quantum channel $\tilde{\Lambda}$ such that $\tilde{\Lambda} \circ \Lambda$ is the identity on $\mathcal{B}(\mathbb{C}^d)$.

Eq. (2.2)), we can write

$$\rho_{T|\overline{T}} = \sum_i q^i_{T|\overline{T}} |e^i_T\rangle\langle e^i_T| \otimes |f^i_{\overline{T}}\rangle\langle f^i_{\overline{T}}|. \tag{5.21}$$

We want to prove that every $\rho_{T|\overline{T}}$ present in the decomposition of $\sigma_{\mathbf{A}}$ is already of the form (5.19) and for this purpose we can work with pure states. But then, every pure state $|e^i_T\rangle|f^i_{\overline{T}}\rangle$ has to obey $P_S \otimes P_{\overline{S}}|e^i_T\rangle|f^i_{\overline{T}}\rangle = |e^i_T\rangle|f^i_{\overline{T}}\rangle$, which implies (after some algebra) that $|e^i_T\rangle|f^i_{\overline{T}}\rangle$ must be also product with respect to the $S|\overline{S}$ bipartition.

We are going to prove here a slightly more general result, which holds for K-partitions, instead of bipartitions.

Theorem 5.4. *Consider an n-partite state of qudits $\rho_{\mathbf{A}} \in \mathcal{D}(\mathbb{C}^d)^{\otimes n}$ such that, for any K-partition $\mathcal{S} \in \mathcal{S}_K$ with groups being labelled $\mathcal{S} = \{S_k\}_{k=1\ldots K}$, the subsystems of $\rho_{\mathbf{A}}$ that correspond to S_k act on the symmetric space; i.e.,*

$$P_{S_k}\rho_{\mathbf{A}}P_{S_k} = \rho_{\mathbf{A}}, \qquad k = 1\ldots K. \tag{5.22}$$

Then, $\rho_{\mathbf{A}}$ is either GME or it has the biseparable decomposition

$$\rho_{\mathbf{A}} = \sum_{\mathcal{T}|\overline{\mathcal{T}}} p_{\mathcal{T}|\overline{\mathcal{T}}}\rho_{\mathcal{T}|\overline{\mathcal{T}}}, \tag{5.23}$$

where $\mathcal{T}$ ($\overline{\mathcal{T}}$) is the union of at least one of the S_k's (its complementary).

Proof. We assume that $\rho_{\mathbf{A}}$ is not GME. Then, it must be biseparable; in principle, across any bipartition of $\mathbf{A}$, so that it has the form

$$\rho_{\mathbf{A}} = \sum_{T|\overline{T}\in\mathcal{S}_2} p'_{T|\overline{T}}\rho_{T|\overline{T}}, \tag{5.24}$$

where $p'_{T|\overline{T}}$ is a probability distribution and $\rho_{T|\overline{T}}$ is a separable state across the bipartition $T|\overline{T}$, meaning that it can be expressed as

$$\rho_{T|\overline{T}} = \sum_i q^i_{T|\overline{T}} |e^i_T\rangle\langle e^i_T| \otimes |f^i_{\overline{T}}\rangle\langle f^i_{\overline{T}}|, \tag{5.25}$$

where $q^i_{T|\overline{T}}$ is a probability distribution and $|e^i_T\rangle$ and $|f^i_{\overline{T}}\rangle$ are pure states defined on the Hilbert space of the parties that belong to T and $\overline{T}$, respectively.

Our next step is to prove that, due to the symmetry present in each set of parties S_k, each of the T's has to be a union of some of the S_k's. Let $|e_T^i\rangle|f_{\overline{T}}^i\rangle$ be one of the product vectors appearing in the decomposition (5.25). We shall now prove that it is product across some $\mathcal{T}|\overline{\mathcal{T}}$ as well.

Because the subsystems S_k of $\rho_{\mathbf{A}}$ are symmetric by assumption, the product vectors $|e_T^i\rangle|f_{\overline{T}}^i\rangle$ appearing in the range of $\rho_{\mathbf{A}}$ enjoy the same symmetries as $\rho_{\mathbf{A}}$; thus, they obey the following:

$$P_{S_k}|e_T^i\rangle|f_{\overline{T}}^i\rangle = |e_T^i\rangle|f_{\overline{T}}^i\rangle, \tag{5.26}$$

and this holds for all $k = 1 \dots K$. In particular, for any two parties belonging to the same subset, $A_m, A_n \in S_k$, we have

$$\Pi_{(m,n)}|e_T^i\rangle|f_{\overline{T}}^i\rangle = |e_T^i\rangle|f_{\overline{T}}^i\rangle, \tag{5.27}$$

where $\Pi_{(m,n)}$ is the swap operator permuting parties A_m and A_n (*cf.* Eq. (A.5)).

Let us consider any bipartition $T|\overline{T}$ that appears in the biseparable decomposition of Eq. (5.24). We can assume that T is not a union of some of the S_k, otherwise we are done. Then, there must exist a pair of particles A_m, A_n, such that $A_m, A_n \in S_k$, but $A_m \in T$ and $A_n \in \overline{T}$.

We now consider the bipartitions $T \setminus A_m|A_m$ and $\overline{T} \setminus A_n|A_n$ and we take the Schmidt decomposition (*cf.* Eq. (2.4)) of $|e_T^i\rangle$ and $|f_{\overline{T}}^i\rangle$, respectively (we omit the indices i and $T \setminus A_m$ ($\overline{T} \setminus A_n$) in the interest of notation):

$$|e_T\rangle = \sum_j \sqrt{\mu_j}|e_{A_m}^j\rangle|e_{T\setminus A_m}^j\rangle \tag{5.28}$$

and

$$|f_{\overline{T}}\rangle = \sum_j \sqrt{\nu_j}|f_{A_n}^j\rangle|f_{\overline{T}\setminus A_n}^j\rangle. \tag{5.29}$$

Applying the swap condition (5.27) we obtain

$$\sum_{j,j'} \sqrt{\mu_j\nu_{j'}}|f_{A_n}^{j'}\rangle|e_{T\setminus A_m}^j\rangle|e_{A_m}^j\rangle|f_{\overline{T}\setminus A_n}^{j'}\rangle = \sum_{j,j'} \sqrt{\mu_j\nu_{j'}}|e_{A_m}^j\rangle|e_{T\setminus A_m}^j\rangle|f_{A_n}^{j'}\rangle|f_{\overline{T}\setminus A_n}^{j'}\rangle. \tag{5.30}$$

Because of the orthogonality of the vectors appearing in the Schmidt decompositions (5.28) and (5.29), for any pair of indices (j, j'), we have

that (up to a global phase) $|e^j_{A_m}\rangle = |f^{j'}_{A_n}\rangle$. It is then well defined to put $|g\rangle := |e^j_{A_m}\rangle = |f^{j'}_{A_n}\rangle$, which implies that every product vector in Eq. (5.25) is also product with respect to parties A_n and A_m:

$$|e^i_T\rangle|f^i_{\overline{T}}\rangle = |g_{A_m}\rangle|\tilde{e}_{T\setminus A_m}\rangle|g_{A_n}\rangle|\tilde{f}_{\overline{T}\setminus A_n}\rangle, \tag{5.31}$$

where $\tilde{e}$ and $\tilde{f}$ are some vectors which we are not interested in.

The same argument works for any pair (m,n) such that $A_m \in T$, $A_n \notin T$ and $A_m, A_n \in S_k$. Hence, every $|e^i_T\rangle|f^i_{\overline{T}}\rangle$ in (5.25) is necessarily product with respect to some bipartition $\mathcal{T}|\overline{\mathcal{T}}$, with $\mathcal{T}$, $\overline{\mathcal{T}}$ being a union of (at least one) of the S_k's.

Now we can repeat the same argument for the rest of the bipartitions $T|\overline{T} \in \mathcal{S}_2$ and conclude that $\rho_{T|\overline{T}}$ is separable with respect to bipartitions of the form $\mathcal{T}|\overline{\mathcal{T}}$, thus having the form given in Eq. (5.23) □

Let us remark that, as a corollary, we have the case for a bipartition $S|\overline{S}$ of symmetric subspaces; *i.e.*, when $\rho_{\mathbf{A}}$ obeys

$$P_S \rho_{\mathbf{A}} P_S = \rho_{\mathbf{A}} \tag{5.32}$$

and

$$P_{\overline{S}} \rho_{\mathbf{A}} P_{\overline{S}} = \rho_{\mathbf{A}}, \tag{5.33}$$

then it follows that, if $\rho_{\mathbf{A}}$ is not GME, it has to be separable across the bipartition $S|\overline{S}$; *i.e.*,

$$\rho_{\mathbf{A}} = \sum_i p_i \rho^i_S \otimes \overline{\rho}^i_{\overline{S}}, \tag{5.34}$$

where ρ^i_S and $\overline{\rho}^i_{\overline{S}}$ act on subsystems S and $\overline{S}$, respectively. Equivalently, if $\rho_{\mathbf{A}}$ is not of the form (5.23), then it is GME.

5.3. K-local models in the multipartite scenario

The extension of a local model to a bilocal model can be generalized to an extension in which a fully local model of K parties is mapped to a K-local model. The following result is a generalization of Theorem 5.3.

Theorem 5.5. *Consider a quantum state $\rho_{A_1\ldots A_K} \in \mathcal{D}(\mathbb{C}^d)^{\otimes K}$ and a collection of retractable quantum channels $\left\{\Lambda_{A_k\to S_k} : \mathcal{B}(\mathbb{C}^d) \longrightarrow \mathcal{B}(\mathbb{C}^{d'})^{\otimes|S_k|}\right\}$, where $\{S_k\}$ forms a K-partition of $\mathbf{A}$. If $\rho_{A_1\ldots A_K}$ has a fully local model for POVMs, the quantum state $\sigma_{\mathbf{A}}$ defined as*

$$\sigma_{\mathbf{A}} := (\Lambda_{A_1\to S_1} \otimes \cdots \otimes \Lambda_{A_K\to S_K})[\rho_{A_1\ldots A_K}] \tag{5.35}$$

has a K-local model for POVMs with respect to the K-partition of $\mathbf{A}$ given by the S_k's ($S_1 \sqcup \cdots \sqcup S_K = \mathbf{A}$).

Proof. As, by hypothesis, $\rho_{A_1\ldots A_K}$ has a fully local model, the probabilities of obtaining outcomes $a_1, \ldots, a_k$ upon measuring $\mathcal{M}_i$ $(i = 1 \ldots K)$ take the following form

$$\begin{aligned} P(a_1 \ldots a_K|\mathcal{M}_1 \ldots \mathcal{M}_K) = &\quad \mathrm{Tr}\left[\left(M^{(1)}_{a_1} \otimes \cdots \otimes M^{(K)}_{a_K}\right)\rho_{A_1\ldots A_K}\right] \\ = &\quad \int_\Lambda p(\lambda)p_\rho(a_1|M^{(1)}_{a_1},\lambda)\cdots p_\rho(a_K|M^{(K)}_{a_K},\lambda)\mathrm{d}\lambda, \end{aligned}$$

where $\{M^{(i)}_{a_i}\}$ are the POVM elements of the measurement $\mathcal{M}_i$ that the i-th party performs, Λ is the space of hidden variables over which λ is distributed, according to a probability distribution $p(\lambda)$, and the subscript ρ in the response functions is used to emphasize that the response functions are calculated for $\rho_{A_1\ldots A_K}$.

We are now going to construct a K-local model for $\sigma_{\mathbf{A}}$ with respect to the K-partition of $\mathbf{A}$ given by $\mathbf{A} = S_1 \sqcup \cdots \sqcup S_K$. Let us assume that, on their share of the state $\sigma\mathbf{A}$, each of the parties $A_1 \ldots A_n$ performs measurements denoted $\widetilde{\mathcal{M}_i}$, with $\{\widetilde{M^{(i)}_{a_i}}\}$ being their corresponding POVM elements. Let us define the following operators:

$$\begin{aligned} \overline{M^{(1)}_{\mathbf{a}_{S_1}}} &:= \Lambda^\dagger_{S_1\to A_1}\left[\widetilde{M^{(1)}_{a_1}} \otimes \cdots \otimes \widetilde{M^{h_1}_{a_{h_1}}}\right] \\ \overline{M^{(2)}_{\mathbf{a}_{S_2}}} &:= \Lambda^\dagger_{S_2\to A_2}\left[\widetilde{M^{(h_1+1)}_{h_1+1}} \otimes \cdots \otimes \widetilde{M^{h_2}_{a_{h_2}}}\right] \\ &\vdots \\ \overline{M^{(K)}_{\mathbf{a}_{S_K}}} &:= \Lambda^\dagger_{S_K\to A_K}\left[\widetilde{M^{(h_{K-1}+1)}_{h_{K-1}+1}} \otimes \cdots \otimes \widetilde{M^{n}_{a_n}}\right], \end{aligned}$$

where $h_k := \sum_{l=1}^{k} |S_l|$ and $\mathbf{a}_{S_k}$ groups the outcomes of all parties in S_k into a $|S_k|$-tuple.

As the maps $\Lambda^{\dagger}_{S_k \to A_k} : \mathcal{B}((\mathbb{C}^{d'})^{\otimes |S_k|}) \longrightarrow \mathcal{B}(\mathbb{C}^d)$ are the dual maps of the $\Lambda_{A_k \to S_k}$, and the dual map of a quantum channel is unital and positive, the set of operators $\overline{\mathcal{M}_k} := \{\overline{M}^{(k)}_{\mathbf{a}_{S_k}}\}_{\mathbf{a}_{S_k}}$ forms a POVM; *i.e.*, $\overline{M^{(k)}_{\mathbf{a}_{S_k}}} \succeq 0$ for every tuple $\mathbf{a}_{S_k}$ and they form a resolution of the identity: $\sum_{\mathbf{a}_{S_k}} \overline{M^{(k)}_{\mathbf{a}_{S_k}}} = \mathbb{1}_d$.

With the aid of the measurements $\mathcal{M}_k$ we can now define the response functions for every set of parties S_k in $\mathbf{A}$: for every $k = 1 \dots K$, let

$$p_\sigma(\mathbf{a}_{S_k} | \boldsymbol{\mathcal{M}}_{S_k}, \lambda) := p_\rho(\mathbf{a}_{S_k} | \overline{\mathcal{M}}_k, \lambda). \tag{5.36}$$

Then, the probability of obtaining outcome $\mathbf{a}$ upon measuring a set of n measurements $\widetilde{\boldsymbol{\mathcal{M}}}$ on the state $\sigma_{\mathbf{A}}$ is given by

$$\begin{aligned} P(\mathbf{a}|\widetilde{\boldsymbol{\mathcal{M}}}) &= \mathrm{Tr}\left[\left(\widetilde{M^{(1)}_{a_1}} \otimes \cdots \otimes \widetilde{M^{(n)}_{a_n}}\right) \sigma_{\mathbf{A}}\right] \\ &= \mathrm{Tr}\left[\left(\widetilde{M^{(1)}_{a_1}} \otimes \cdots \otimes \widetilde{M^{(n)}_{a_n}}\right) \left(\bigotimes_{k=1}^{K} \Lambda_{A_k \to S_k}\right) [\rho_{A_1 \dots A_K}]\right]. \end{aligned}$$

Due to the definition of $\overline{M^{(k)}_{\mathbf{a}_{S_k}}}$, we can express this probability as

$$P(\mathbf{a}|\widetilde{\boldsymbol{\mathcal{M}}}) = \mathrm{Tr}\left[\left(\overline{M^{(1)}_{\mathbf{a}_{S_1}}} \otimes \cdots \otimes \overline{M^{(K)}_{\mathbf{a}_{S_K}}}\right) \rho_{A_1 \dots A_K}\right].$$

The K-local model for $\sigma_{\mathbf{A}}$ is then given, because, since the state $\rho_{A_1 \dots A_K}$ is fully local,

$$P(\mathbf{a}|\widetilde{\boldsymbol{\mathcal{M}}}) = \int_\Lambda p(\lambda) \prod_{k=1}^{K} p_\rho(\mathbf{a}_{S_k}|\overline{\mathcal{M}_k}, \lambda) \mathrm{d}\lambda = \int_\Lambda p(\lambda) \prod_{k=1}^{K} p_\sigma(\mathbf{a}_{S_k}|\boldsymbol{\mathcal{M}}_{S_k}, \lambda) \mathrm{d}\lambda. \tag{5.37}$$

This is a K-local model for POVMs with respect to the K-partition that is defined by the set of S_k's. Let us finally remark that both $p(\lambda)$ and the space of hidden variables Λ are the same in both models. □

As a result of Theorem 5.4, let us observe the following corollary: given a state $\rho_{\mathbf{A}} \in \mathcal{D}(\mathbb{C}^d)^{\otimes n}$ such that, for a K-partition $\mathcal{S} \in \mathcal{S}_K$, the reduced

states on the subsystems corresponding to $S_k \in \mathcal{S}$ are symmetric; then, if it does not admit a decomposition of the form (5.23), it is GME. We can now write in full generality the main result of this chapter:

Theorem 5.6. *Let $\rho_{A_1,\dots A_K}$ be GME acting on $(\mathbb{C}^d)^{\otimes K}$. If $\rho_{A_1,\dots A_K}$ has a local model for POVMs then, for every collection consisting of K retractable quantum channels*

$$\Lambda_{A_k \to S_k} : \mathcal{B}(\mathbb{C}^d) \longrightarrow \mathcal{B}(\mathcal{S}(\mathbb{C}^{d'})^{\otimes |S_k|}), \tag{5.38}$$

where $\mathcal{S}$ indicates the symmetric subspace, the state

$$\sigma_{\mathbf{A}} := (\Lambda_{A_1 \to S_1} \otimes \cdots \otimes \Lambda_{A_K \to S_K})[\rho_{A_1 \dots A_K}] \tag{5.39}$$

admits a K-local model for POVMs with respect to the K-partition $\mathbf{A} = S_1 \sqcup \cdots \sqcup S_K$, and it is GME.

Proof. From Theorem 5.5 it follows that $\sigma_{\mathbf{A}}$ admits a K-local model for generalized measurements (POVMs), with respect to the K-partition defined by the S_k's. Because $\rho_{A_1 \dots A_K}$ is Genuinely Multipartite Entangled, Theorem 5.4 implies that $\sigma_{\mathbf{A}}$ is also GME:

If this were not the case, there would exist a decomposition of the form (5.23) for which every $\mathcal{T}|\overline{\mathcal{T}}$ would be unions of the S_k's. Note that Theorem 5.4 applies because of the choice of the $\Lambda_{A_k \to S_k}$, that make all subsystems S_k of $\mathbf{A}$ symmetric. In addition, all channels $\Lambda_{A_k \to S_k}$ are retractable, and this would imply that $\rho_{A_1 \dots A_K}$ is not GME, which is a contradiction, because $\rho_{A_1 \dots A_K}$ is taken to be GME. Hence, $\sigma_{\mathbf{A}}$ is GME and it admits a K-local model. □

5.4. Applications

In this section we provide a couple of examples to see how our method works in practice. We shall start from a bipartite quantum state with a local model and extend it to an n-partite GME state with a bilocal model. Two textbook examples in quantum information are the Werner [Wer89] and the isotropic [HH99] states.

We are going to consider the quantum channels $\Lambda_{A \to S} : X \mapsto V_m X V_m^\dagger$ and $\Lambda_{B \to \overline{S}} : X \mapsto V_{n-m} X V_{n-m}$, where $V_m : \mathbb{C}^d \longrightarrow \mathcal{S}((\mathbb{C}^d)^{\otimes m})$ is defined

on the computational basis elements as $V_m|i\rangle = |i\rangle^{\otimes m}$ and extended by linearity. Observe that $\Lambda_{A\to S}$ and $\Lambda_{B\to\overline{S}}$ can be retracted, as V_m is an isometry: $V_m^\dagger V_m = \mathbb{1}_d$. Note that $m = |S|$. In other words, due to the fact that the V's are isometries, the Λ's are invertible in the subspace of interest.

5.4.1. Isotropic states

The two-qudit isotropic states are a uniparametric family of quantum states which was introduced in [HH99]. They can be defined as

$$\rho_{\text{iso}}(p) := p|\psi^+\rangle\langle\psi^+| + (1-p)\frac{\mathbb{1}_{d^2}}{d^2}, \tag{5.40}$$

where $|\psi^+\rangle$ is the maximally entangled state $|\psi^+\rangle := \sum_{i=0}^{d-1}|ii\rangle/\sqrt{d}$. The isometries V_m that are applied to $\rho_{\text{iso}}(p)$ lead us to the mixture of a GHZ state of n qudits and some coloured noise:

$$\sigma_{\mathbf{A}}(p) = p|\text{GHZ}_{n,d}\rangle\langle\text{GHZ}_{n,d}| + (1-p)\frac{\mathcal{N}_{|S|,d}\otimes\mathcal{N}_{|\overline{S}|,d}}{d^2}, \tag{5.41}$$

where $|\text{GHZ}_{n,d}\rangle$ is defined as $\sum_{i=0}^{d-1}|i\rangle^{\otimes n}/\sqrt{d}$ and $\mathcal{N}_{m,d} := \sum_{i=0}^{d-1}|i\rangle\langle i|^{\otimes m}$. Because the isotropic states are local for POVMs for

$$p \leq \frac{(3d-1)(d-1)^{d-1}}{d^d(d+1)}, \tag{5.42}$$

as it was shown in [Alm+07], Theorem 5.3 proves that $\sigma_{\mathbf{A}}(p)$ has a bilocal model with respect to the $S|\overline{S}$ partition of $\mathbf{A}$ for the same range of parameters. Then, since isometric channels are invertible, they preserve entanglement ($V_m^\dagger V_m = \mathbb{1}_d$). As a consequence, $\sigma_{\mathbf{A}}(p)$ is GME whenever $\rho_{\text{iso}}(p)$ is entangled, namely $p > \frac{1}{d+1}$. Hence, $\sigma_{\mathbf{A}}(p)$ are our first examples of states which are GME and admit a bilocal model, for any number n of parties.

5.4.2. Werner states

Werner states have already been introduced in Eq. (5.1). Applying the isometries V_m and V_{n-m} we obtain the family of n-qudit states $\tilde{\sigma}_{\mathbf{A}}(p)$ such

that

$$\tilde{\sigma}_{\mathbf{A}}(p) = p\binom{d}{2}^{-1}\mathcal{A}_{m,d} + (1-p)d^{-2}\mathcal{N}_{m,d}\otimes\mathcal{N}_{n-m,d}, \tag{5.43}$$

where

$$\mathcal{A}_{m,d} := \sum_{0\leq i<j<d} |\psi_{ij}\rangle\langle\psi_{ij}| \tag{5.44}$$

and

$$|\psi_{ij}\rangle := \frac{|i\rangle^{\otimes m}|j\rangle^{\otimes n-m} + |j\rangle^{\otimes m}|i\rangle^{\otimes n-m}}{\sqrt{2}}. \tag{5.45}$$

Werner states $\rho_W(p)$ have a local model for POVMs for the same range of parameters as in (5.42) [Bar02]. They are entangled also for $p > 1/(d+1)$, so that the states $\tilde{\sigma}_{\mathbf{A}}(p)$ also constitute an example of states being GME and admitting a bilocal model at the same time, for any n.

5.5. Conclusions and outlook

After the definition of GMN introduced by Svetlichny [Sve87], it has been shown that it is inconsistent with operational definitions of nonlocality, and consistent definitions have been put forward. These are Time-Ordered Bi-Local (TOBL) [Gal+12] and No-Signalling Bi-Local (NSBL) [Ban+13]. The most stringent condition that one can require in the definition of Genuinely Multipartite Nonlocal (2.17), from the operational point of view, is that the response functions are No-Signalling, as the set of correlations that fulfills it is the smallest. This condition can be easily met in our construction, showing that we are consistent with these operational definitions of GMN:

The local models we employed in Section 5.4 have one response function being quantum (*cf.* Example 5.1). It is then enough to extend the part of the state in which the response function is given by Born's rule, and the resulting response function on such part will automatically fulfill the NS condition. Both isotropic and Werner states have local models for POVMs in which the response function on Bob's side is quantum. Hence, it is sufficient to consider a bipartition $S|\overline{S}$ of $\mathbf{A}$ for which $S = \{A\}$ and $\overline{S} = \{B, C, D\ldots\}$. This shows that a nonempty gap between GME and nonlocality exists even when one considers operational definitions of K-locality.

In this chapter we have shown how, from any n-partite GME quantum state with a K-local model for generalized measurements one can construct an m-partite GME state with the same degree of nonlocality. Even if operational definitions of multipartite nonlocality are considered, we have shown that there is a gap between GME and GMN. An interesting open question is to which degree does ithis inequivalence hold. So far, we know that there are GME n-partite quantum states that admit a 2- or even a 3-local[6] model for generalized measurements. Is there a maximum K for which a K-local model can be constructed? Does this K depend on n? It would be especially interesting to investigate the largest gap that one can imagine: are there GME n-partite states with a fully local model, for any n? Or is the GME condition too strong at some point to allow for a fully local model?

5.5.1. Other nonlocality frameworks

Besides TOBL and NSBL, other nonlocality scenarios which are operationally meaningful have been explored in the literature. During this Thesis, we have always worked with the single-copy definition. However, one can consider the network approach [Cav+11], Bell scenarios defined on copies of a state [Pal12] or sequential measurements [Pop95; Gis96; Hir+13]. A quantum state that is local according to one definition may not be local in another. It remains an interesting open question whether the inequivalence between entanglement and nonlocality also holds in these more general setups.

An intermediate level between entanglement and nonlocality that has attracted attention recently is quantum steering. In the bipartite case, a steering scenario consists of one trusted[7] party and an untrusted[8] party

[6] By applying our construction to the 3-qubit state introduced in [TA06], which is GME and fully local.

[7] This trusted party performs known quantum measurements on its share of the system. This is the procedure that one follows in quantum tomography; *i.e.*, when estimating the density matrix of the system. In order to do so, the measurements done in the laboratory have to match the ones in the paper. Once the density matrix is known, one can check for entanglement in the state.

[8] This party is treated as a black box. It does not known the measurements that it is performing, not even the dimension of its share of the system. One has access only to the choice of measurements and its outcomes. This is the approach that we take in the

[Sch35; WJD07]. The construction that we have presented in this chapter implies that GME is also inequivalent to steering: Applying it to a bipartite local state with one of the response functions being quantum, we obtain a GME state which is unsteerable -at least in one direction- across the same bipartition with respect to which the extended state is bilocal.

study of nonlocality.

6. Atomic monogamies of correlations

Entanglement and nonlocal correlations are fundamental resources in quantum information. We have already seen in Chapter 5 that these two resources are inequivalent, although they share many features, and one of them is that both entanglement and nonlocality are monogamous.

When one tries to distribute entanglement among many parties, there is a limit in the amount of entanglement that can be distributed among groups of particles: the more entangled a pair of particles in a system is, the more separable this pair of particles becomes from the rest of the system. This is the reason why entanglement is said to be monogamous. In some secure key distribution protocols based on entanglement, its security relies on the monogamy property. For example, consider the protocol of [Eke91]: If Alice and Bob share a pair of qubits which are maximally entangled (a singlet state), then monogamy forces any external party (say, an eavesdropper Eve) to have a state which is separable with respect to the singlet state that Alice and Bob are sharing; as Eve is separable with respect to Alice-Bob, the outcomes of any measurement that Eve performs are uncorrelated with the outcomes that Alice or Bob obtain: Eve is prevented to gain information in this way. To gain information, Eve has to become somewhat entangled with Alice and Bob, but then monogamy forces the amount of entanglement between Alice and Bob to decrease, so that the correlations between Alice and Bob gradually get away from being maximal; hence, Alice and Bob can detect the presence of Eve.

Physical principles (such as Local Hidden Variable Model (LHVM), Quantum Theory (QT), No-Signalling (NS)) constrain the way that resources (such as entanglement, nonlocal correlations) can be distributed among separated parties, and these constraints are known as monogamy relations. For instance, if one takes an entanglement measure such as concurrence[1], in

[1] Concurrence is defined as follows: Given the density matrix describing a pair of qubits, denoted ρ_{AB}, one takes the so-called *spin-flipped* density matrix $\tilde{\rho}_{AB} := (\sigma_y \otimes \sigma_y)\rho^*_{AB}(\sigma_y \otimes \sigma_y)$, where * denotes complex conjugation and σ_y is the Pauli

any pure three-qubit state, no party (*e.g.* Alice) can share a large amount of entanglement with all the remaing parties (*e.g.* Bob and Charlie) [CKW00]. Similar relations exist for nonlocal correlations, where the measure of nonlocality is taken to be the amount of violation of a Bell inequality. For instance, any Bell inequality whose NS maximal violation is achievable by a unique probability distribution will have monogamy constraints [Bar+05]. It was shown that, given the statistics obtained through a Bell experiment, there is a trade-off between the observed violation of a Bell inequality (with a unique NS distribution achieving its maximal NS violation) between Alice-Bob and the observed violation of the same Bell inequality for Alice-Charlie [MAG06].

In a quantitative sense, Toner and Verstraete [TV06] showed that if three parties A, B and C share any QT resource, only two of them can violate the CHSH inequality [Cla+69], as $I_{AB}^2 + I_{AC}^2 \leq 8$ holds (*cf.* Eq. (2.18)). Later on, Toner derived a similar relation holding for any NS resource, which is $|I_{AB}|+|I_{AC}| \leq 4$ [Ton09]. These monogamy relations for nonlocal correlations have been generalized to scenarios with more parties, measurements or outcomes, and some proposals have been made to obtain a general method to construct monogamy relations for NS correlations from any bipartite Bell inequality [PB09; RH14].

In this chapter, we show that nonlocal correlations are monogamous in a much stronger sense. Normally, one relates the nonlocality (as measured by the amount of violation of a Bell inequality) between a set of parties with the nonlocality between another set of parties (with nonempty intersection with the first set); for instance I_{AB} vs. I_{AC}. We see that the nonlocality observed by a set of parties may imply severe limitations on *any* form of correlations with a third party. In other words, we relate the Bell violation that a set of parties observe with the knowledge that an external observer may have on the outcomes of any of the measurements that any of the parties perform (see Fig. 6.1).

This means that any correlations (either classical or nonlocal) that an external observer may have with the results produced by one of the parties in the group is bounded by a function of the Bell violation that those parties

matrix. Both ρ_{AB} and its spin-flipped counterpart are positive operators and its product $\rho_{AB}\rho_{\tilde{A}B}$ has real and non-negative eigenvalues (although it is non-Hermitian). By denoting the square root of them $\lambda_1, \ldots, \lambda_4$, sorted in decreasing order, the concurrence of ρ_{AB} is defined as $C_{AB} := \max\{\lambda_1 - \lambda_2 - \lambda_3 - \lambda_4, 0\}$.

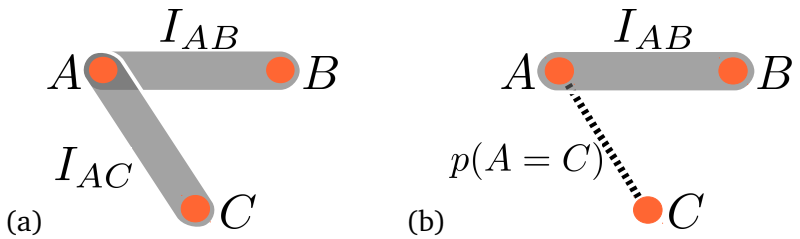

Figure 6.1.: (a) Typical monogamies of correlations compare the amount of violation of a bipartite Bell inequality between different groups of parties; *e.g.* I_{AB} vs I_{AC}. (b) The monogamy relations that we introduce in this chapter compare the nonlocality that a group of parties observes (the amount of violation of I_{AB}) with the knowledge (represented by the guessing probability $P(A=C)$) that an external party C may have about outcomes observed by any of the parties in the group. The monogamy relations in (b) are stronger and qualitatively different than those of (a).

observe.

We are going to generalize this idea to an arbitrary Bell scenario (n, m, d) of n parties performing m $d-$valued observables. These monogamy relations are stronger (and logically independent) from the existing relations: a bound on nonlocal correlations does not necessarily imply any nontrivial constraint on classical correlations, as depicted in Fig. 6.1.

In Section 6.1 we will show that our monogamies are useful in some Device-Independent (DI) protocols. The commonly used measure of randomness in DI protocols is the guessing probability and we will show in Section 6.2 that our monogamy relations introduced in Section 6.1 bound the guessing probability in a tighter way than the ones present in the literature [BKP06; Aol+12]. In Section 6.3 we discuss some applications in DI protocols. In particular, in Section 6.3.1 we see that this implies a superior performance for some Device-Independent Quantum Key Distribution (DIQKD) protocols such as [Pir+13] when one employs measurements with more than two outcomes. Furthermore, in Section 6.3.2 we conclude by showing that they are also useful to generalize the results on random-

ness amplification of [CR12] to any number of parties and outcomes; in particular, we prove that in the bipartite setup, certified randomness of an arbitrary quantity of arbitrarily good quality can be obtained through the DI protocol of randomness amplification.

The results presented in this chapter are based on [Aug+14b] and they were obtained in collaboration with R. Augusiak, M. Demianowicz, M. Pawłowski and A. Acín.

6.1. Monogamy relations

In this section we derive monogamy relations for NS and in a particular case QT. No-signalling monogamy relations are simpler to derive, as the set of NS correlations, $\mathbf{P}_{NS}$, is a polytope. On the other hand, the boundary of the set of correlations fulfilling QT, $\mathbf{Q}$, is unknown and can only be approximated with methods such as the NPA hierarchy [NPA08]. For this reason, it becomes more illustrative to begin with the larger, but simpler, set of NS correlations.

6.1.1. Monogamy relations for No-Signalling Theories

Let us begin with considering the simplest case: the tripartite scenario. We shall be working with the Barrett-Kent-Pironio (BKP) inequality [BKP06], which is a generalization of the CHSH inequality [Cla+69] to an arbitrary number of measurements and outcomes. We shall work with measurements that have d possible outcomes, which we label $\{0, 1, \ldots, d-1\}$. The expectation value of a random variable Ω which takes values in the $\{0, \ldots, d-1\}$ set is denoted by $\langle\Omega\rangle$ and it is given by

$$\langle\Omega\rangle = \sum_{i=1}^{d-1} iP(\Omega = i). \tag{6.1}$$

It will be necessary to introduce the notation $[\Omega] := \Omega \mod d$.

Definition 6.1. *Let us denote the Barrett-Kent-Pironio (BKP) inequality for the $(2, m, d)$ scenario as $I_{AB}^{2,m,d}$. It is given by*

$$I_{AB}^{2,m,d} := \sum_{\alpha=0}^{m-1} \left(\langle[A_\alpha - B_\alpha]\rangle + \langle[B_\alpha - A_{\alpha+1}]\rangle\right) \geq d - 1, \tag{6.2}$$

where $\Omega_m := \Omega_0 + 1$.

Remark 6.2. The BKP inequality, when particularized for the case of binary observables ($d = 2$), reproduces the chained Bell inequalities introduced in Ref. [BC90], whereas for the case of two observables, it reproduces the Collins-Gisin-Linden-Massar-Popescu (CGLMP) Bell inequalities [Col+02]. When there are two binary observables, inequality (6.2) is equivalent to the CHSH Bell inequality [Cla+69]. Let us also notice that the maximal violation of (6.2) for NS theories is $I_{AB}^{2,m,d} = 0$.

In [PB09], as a quantitative extension of the concept of m-shareability [MAG06], monogamy relations for inequality (6.2) were introduced in terms of its violations between an Alice and m Bobs. In this chapter, we go a step further and show how the BKP inequalities allow one to introduce *elemental* monogamy constraints satisfied by any NS theory.

Theorem 6.3. *Let* $\vec{P}$ *be a tripartite probability distribution* $\{P(abc|xyz)\}$ *corresponding to the* $(3, m, d)$ *scenario which satisfies the NS principle. The inequality*

$$I_{AB}^{2,m,d} + \langle [X_i - C_j] \rangle + \langle [C_j - X_i] \rangle \geq d - 1 \tag{6.3}$$

holds for any pair of indices $i, j = 0 \ldots m-1$ *and* X *being either* A *or* B.

Before proving Theorem 6.3, it is convenient to first observe a couple of properties that the operator $\langle [\cdot] \rangle$ fulfills:

Lemma 6.4. *Let* Ω *be a random variable taking values in the set* $\{0, \ldots, d-1\}$. *The following properties are satisfied:*

1. $\langle [\Omega] \rangle + \langle [-\Omega - 1] \rangle = d - 1$.
2. $\langle [\Omega] \rangle + \langle [-\Omega] \rangle = d(1 - P([\Omega] = 0))$.

Proof. For the first property, one simply has to apply the definitions of $\langle \cdot \rangle$ and $[\cdot]$. Let us begin by noting that $[\Omega] + [-\Omega - 1] = d - 1$. Hence, we have that, for expectation values, $\langle [-\Omega - 1] \rangle = \sum_{i=1}^{d-1} iP([\Omega] = d - i - 1)$. Changing the summation index, we have

$$\begin{aligned} \langle [-\Omega - 1] \rangle &= \sum_{i=0}^{d-2} (d - i - 1) P([\Omega] = i) \\ &= (d-1) \sum_{i=0}^{d-2} P([\Omega] = i) - \sum_{i=0}^{d-2} iP([\Omega] = i), \end{aligned}$$

and by definition of $\langle\cdot\rangle$,

$$\langle[-\Omega-1]\rangle = (d-1)\sum_{i=0}^{d-1} P([\Omega]=i) - \langle[\Omega]\rangle = (d-1) - \langle[\Omega]\rangle. \tag{6.4}$$

For the second property, we can write

$$\begin{aligned}
\langle[\Omega]\rangle + \langle[-\Omega]\rangle &= \sum_{i=1}^{d-1} i\,(P([\Omega]=i) + P([-\Omega]=i)) \\
&= \sum_{i=1}^{d-1} i\,(P([\Omega]=i) + P([\Omega]=d-i)) \\
&= \sum_{i=1}^{d-1} iP([\Omega]=i) + \sum_{i=1}^{d-1}(d-i)P([\Omega]=i) \\
&= d\sum_{i=1}^{d-1} P([\Omega]=i) \\
&= d(1-P([\Omega]=0)),
\end{aligned}$$

where we have used that $[\Omega]+[-\Omega]=d$ in the second equality and we have changed the summation index in the second sum for the third equality. □

Proof (of Theorem 6.3). We shall begin with the case $X=A$. The $X=B$ case is similar, and we shall just point out its differences. Because of Lemma 6.4, the identity $\langle[\Omega]\rangle + \langle[\Omega-1]\rangle = d-1$ holds for any observable; in particular, if we apply it to $\Omega = A_\beta - C_j$. By summing over all β's that are different from j we arrive at

$$\sum_{\substack{\beta=0\\ \beta\neq i}}^{m-1} (\langle[C_j - A_\beta - 1]\rangle + \langle[A_\beta - C_j]\rangle) = (m-1)(d-1). \tag{6.5}$$

Also, in virtue of Lemma 6.4, the property that, for any β and j, it holds that $\langle[C_j - A_\beta - 1]\rangle + \langle[A_\beta - C_j]\rangle = \langle[A_\beta - C_j - 1]\rangle + \langle[C_j - A_\beta]\rangle$ (because

both of them are $d-1$) allows us to express Eq. (6.5)) as

$$\sum_{\beta=0}^{i-1}\left(\langle[C_j - A_\beta - 1]\rangle + \langle[A_\beta - C_j]\rangle\right)$$
$$+\sum_{\beta=i+1}^{m-1}\left(\langle[A_\beta - C_j - 1]\rangle + \langle[C_j - A_\beta]\rangle\right) = (m-1)(d-1). \tag{6.6}$$

By addition of $\langle[A_i - C_j]\rangle + \langle[C_j - A_i]\rangle$ to both sides, we can rearrange some terms in Eq. (6.6) and write

$$\begin{aligned}\langle[A_i - C_j]\rangle + \langle[C_j - A_i]\rangle &= \sum_{\beta=0}^{i-1}\left(\langle[C_j - A_\beta - 1]\rangle + \langle[A_{\beta+1} - C_j]\rangle\right)\\ &+ \sum_{\beta=i}^{m-2}\left(\langle[A_{\beta+1} - C_j - 1]\rangle + \langle[C_j - A_\beta]\rangle\right)\\ &+ \langle[A_0 - C_j]\rangle + \langle[C_j - A_{m-1}]\rangle\\ &- (m-1)(d-1).\end{aligned} \tag{6.7}$$

On the other hand, the BKP inequality (6.2) can be decomposed in a similar fashion:

$$\begin{aligned}I_{AB}^{2,m,d} &= \sum_{\alpha=0}^{i-1}\left(\langle[A_\alpha - B_\alpha]\rangle + \langle[B_\alpha - A_{\alpha+1}]\rangle\right)\\ &+ \sum_{\alpha=i}^{m-2}\left(\langle[A_\alpha - B_\alpha]\rangle + \langle[B_\alpha - A_{\alpha+1}]\rangle\right)\\ &+ \langle[A_{m-1} - B_{m-1}]\rangle + \langle[B_{m-1} - A_0 - 1]\rangle.\end{aligned} \tag{6.8}$$

By adding line by line Eqs. (6.7) and (6.8) we get an expression which is basically the sum of m Bell expressions $I_{AB}^{2,2,d}$; however, *distributed* among three parties in a special way in which Bob and Charlie measure only a

single observable (B_α and C_j):

$$\begin{aligned} & I_{AB}^{2,m,d} + \langle [A_i - C_j] \rangle + \langle [C_j - A_i] \rangle \\ = & \sum_{\alpha=0}^{i-1} \left(\langle [C_j - A_\alpha - 1] \rangle + \langle [A_\alpha - B_\alpha] \rangle + \langle [B_\alpha - A_{\alpha+1}] \rangle + \langle [A_{\alpha+1} - C_j] \rangle \right) \\ + & \sum_{\alpha=i}^{m-2} \left(\langle [C_j - A_\alpha] \rangle + \langle [A_\alpha - B_\alpha] \rangle + \langle [B_\alpha - A_{\alpha+1}] \rangle + \langle [A_{\alpha+1} - C_j - 1] \rangle \right) \\ + & \langle [C_j - A_{m-1}] \rangle + \langle [A_{m-1} - B_{m-1}] \rangle + \langle [B_{m-1} - A_0 - 1] \rangle + \langle [A_0 - C_j] \rangle \\ - & (m-1)(d-1). \end{aligned} \tag{6.9}$$

As it was already shown in [PB09], the maximal value, for a particular choice of α, over $\mathbf{P}_{NS}$ of one of the summands appearing in Eq. (6.9) is the same as its classical bound, which is $d-1$. Hence, we have an inequality which is valid for NS correlations:

$$I_{AB}^{2,m,d} + \langle [A_i - C_j] \rangle + \langle [C_j - A_i] \rangle \geq m(d-1) - (m-1)(d-1) = d-1. \tag{6.10}$$

This completes the proof for the case that $X = A$. On the other hand, if $X = B$, one follows the same line of argument. The simplest way is to rewrite the BKP Bell inequality as

$$I_{AB}^{2,m,d} = \sum_{\alpha=0}^{m-1} \left(\langle [B_\alpha - A_{\alpha+1}] \rangle + \langle [A_{\alpha+1} - B_{\alpha+1}] \rangle \right) \tag{6.11}$$

and add it to the expression (6.5) with the A's replaced by B's and viceversa. To complete the proof, one performs the same manipulations as for the $X = A$ case.

□

Remark 6.5. Let us comment on the optimality of the monogamy relations introduced in Theorem 6.3. Inequalities of the form (6.3) are tight; *i.e.*, for any pair of values

$$\left(I_{AB}^{2,m,d}, \langle [X_i - C_j] \rangle + \langle [C_j - X_i] \rangle \right)$$

that saturate (6.3), one can find a $\vec{P} \in \mathbf{P}_{NS}$ realizing such values. In order to find such $\vec{P}$, one just has to take a probability distribution of

the form $P(abc|xyz) = P(ab|xy)P(c|z)$, where $P(ab|xy)$ is a mixture of a nonlocal model that maximally violates the BKP Bell inequality (6.2) and a local deterministic strategy saturating it, and $P(c|z)$ follows the same distribution of the local model used by A or B that saturates (6.2).

Remark 6.6. By rewriting the monogamy relations of Theorem 6.3, we can obtain a clear physical interpretation; we just need to express them in a slightly different form. Using the second result of Lemma 6.4, inequalities of the type (6.3) can be transformed to

$$I_{AB}^{2,m,d} + 1 \geq dP(X_i = C_j), \tag{6.12}$$

for any $X \in \{A, B\}$ and $i, j \in \{0, \ldots, m-1\}$. This result also holds if AB is replaced by any pair of parties from $\{A, B, C\}$ and if we replace the probability $P(X_i = C_j)$ by $P(X_i \equiv C_j + k \mod d)$, where k is an integer number.

Thus, the probability $P(X_i = C_j)$ that parties X and C obtain the same results (possibly shifted by a fixed offset k) is a measure of how the outcomes of the i-th and the j-th observables are classically correlated. As such, Theorem 6.3 establishes a tradeoff between the nonlocality that two parties A and B can generate, as measured by the quantum violation of (6.2), and he classical correlation that a third party C can share with the results of any measurement A_i or B_i that they can perform. In addition, they are tight, as there exist NS probability distributions saturating them.

Remark 6.7. At the point of maximal violation of (6.2) within NS theories, which is $I_{AB}^{2,m,d} = 0$, the relation (6.12) implies that $P(X_i = C_j) \leq 1/d$. We have that this bound is tight[2]; *i.e.*, $P(X_i = C_j) = 1/d$ for any $i, j = 0 \ldots m-1$. Hence, at a point of maximal violation within No-Signalling theories, observer C cannot share any correlations with any other party's measurement outcomes [BKP06].

However, if AB do not violate the BKP Bell inequality, then C can be arbitrarily correlated with A or B. For partial nonlocal violations, we shall see that there is a linear relation between the maximal guessing probability $P(X_i = C_j)$ in terms of the nonlocal violation of $I_{AB}^{2,m,d}$ (*cf.* Fig. 6.3).

[2] This is by normalization in the case $d = 2$. In the general case, one further needs to take into consideration that there may be a fixed offset k between the outcomes of X and C.

The general case

Let us now consider the scenario of n parties performing m $d-$valued observables each. The Bell inequality that we shall be working with is a generalization of the BKP inequality to n parties which it was introduced by Aolita-Gallego-Cabello-Acín (AGCA) in [Aol+12]. It can be defined in a recursive manner as follows:

Definition 6.8. *Let* $\mathbf{A}=\{A^{(1)},\dots,A^{(n)}\}$. *The AGCA inequality, for the* (n,m,d) *scenario is defined as*

$$I_{\mathbf{A}}^{n,m,d} := \frac{1}{m}\sum_{\alpha_{n-1}=0}^{m-1} I_{\mathbf{A}\setminus A^{(n)}}^{n-1,m,d}(\alpha_{n-1})\circ A_{\alpha_{n-1}}^{(n)} \geq d-1, \tag{6.13}$$

where

- $\circ A_\gamma^{(i)}$ *is the operator that acts as follows: To every correlator appearing in* $I_{\mathbf{A}\setminus A^{(n)}}^{n-1,m,d}(\alpha_{n-1})$ *(ending with, say,* $A_\delta^{(i-1)}$*), it attaches* $A_\gamma^{(i)}$ *with a sign opposite to that of* $A_\delta^{(i-1)}$.

- $I_{\mathbf{A}\setminus A^{(n)}}^{n-1,m,d}(\alpha_{n-1})$ *is defined as in Eq. (6.13), but for* $n-1$ *parties and with the following relabelling of the observables for the* $(n-2)$*-th party:* $\alpha_{n-2}\mapsto\alpha_{n-2}+\alpha_{n-1}-1$*; recall that* α_{n-1} *takes values from the set* $\{0,\dots,m-1\}$.

- *If* $n=2$*, then* $I_{\mathbf{A}}^{n,m,d}$ *corresponds to the BKP Bell inequality (6.2).*

The AGCA inequality is maximally violated within NS theories when $I_{\mathbf{A}}^{n,m,d}=0$ [Aol+12]. Its recursive formulation allows for a generalization of Theorem 6.3 to any number of parties:

Theorem 6.9. *For any* $\vec{P}\in\mathbf{P}_{NS}$ *corresponding to the* $(n+1,m,d)$ *Bell scenario, and for any* $x_k,x_{n+1}\in\{0,\dots,m-1\}$ *with* $1\leq k\leq n$*, the following inequality holds:*

$$I_{\mathbf{A}}^{n,m,d} + \langle[A_{x_k}^{(k)} - A_{x_{n+1}}^{(n+1)}]\rangle + \langle[A_{x_{n+1}}^{(n+1)} - A_{x_k}^{(k)}]\rangle \geq d-1. \tag{6.14}$$

Proof. It will be useful to exploit the recursive formulation in the definition of the AGCA inequality (6.13), so that we can prove (6.14) by induction. The particular case $n = 2$ holds true, as it is proven in Theorem 6.3. Let us start with the first case, $n = 3$. $I^{3,m,d}_{A^{(1)}A^{(2)}A^{(3)}}$ takes the following form:

$$I^{3,m,d}_{A^{(1)}A^{(2)}A^{(3)}} = \frac{1}{m}\sum_{\alpha_2=0}^{m-1} I^{2,m,d}_{A^{(1)}A^{(2)}}(\alpha_2)\circ A^{(3)}_{\alpha_2}. \tag{6.15}$$

Observe that, for any $\alpha_2 \in \{0,\dots,m-1\}$, the inequality

$$I^{2,m,d}_{A^{(1)}A^{(2)}}(\alpha_2) = \sum_{\alpha_1=0}^{m-1}\Big(\langle[A^{(1)}_{\alpha_1} - A^{(2)}_{\alpha_1+\alpha_2-1}]\rangle + \langle[A^{(2)}_{\alpha_1+\alpha_2-1} - A^{(1)}_{\alpha_1+1}]\rangle\Big) \geq d-1 \tag{6.16}$$

is actually a Bell inequality[3] that is equivalent to BKP (*cf.* Eq. (6.2)). Hence, it fulfills[4] the monogamy relation of Theorem 6.3 for $n = 2$ and for any α_2.

Let us now attach the term $\circ A^{(3)}_{\alpha_2}$ and see that every summand in Eq. (6.15) satisfies (6.14). As we are discussing the case $n = 3$, we need to show that, for any $\alpha_2 \in \{0,\dots,m-1\}$ and, for any pair $x_1, x_4 \in \{0,\dots,m-1\}$ with $k \in \{1,2,3\}$, the inequalities

$$I^{2,m,d}_{A^{(1)}A^{(2)}}(\alpha_2)\circ A^{(3)}_{\alpha_2} + \Big(\langle[A^{(k)}_{x_k} - A^{(4)}_{x_4}]\rangle + \langle[A^{(4)}_{x_4} - A^{(k)}_{x_k}]\rangle\Big) \geq d-1 \tag{6.17}$$

hold true.

- If $k = 1$, we write explicitly the expression for $I^{2,m,d}_{A^{(1)}A^{(2)}}(\alpha_2)\circ A^{(3)}_{\alpha_2}$,

[3] Note that the observables of $A^{(2)}$ have already been relabelled according to the rule $\alpha_1 \mapsto \alpha_1 + \alpha_2 - 1$.

[4] In order to see that explicitly, it is convenient to rename some of the indices. We can assume, without loss of generality, that $k = 1$ and that we rename $A \leftrightarrow A^{(1)}$, $B \leftrightarrow A^{(2)}$ and $C \leftrightarrow A^{(3)}$ in Eq. (6.9). In addition, we set $\alpha = \alpha_1$ for Alice and $\alpha = \alpha_1 + \alpha_2 - 1$ for Bob. One has to take into account that those observables $A^{(2)}_{\alpha_1+\alpha_2-1}$ for which $\alpha_1 + \alpha_2 - 1 \geq m$ have to be handled with especial care: Actually, one needs to apply the rule that, for all γ and i, $X_{i\cdot m+\gamma} = [X_\gamma + i]$ so that the terms $[A^{(2)}_\gamma + i]$ that appear (for some γ and i) can be replaced by another variable, which we call $\tilde{A}^{(2)}_\gamma$. Observe that the latter variable is the former with the outcomes shifted by a constant amount. The case $k = 2$ follows from Eq. (6.11). This proves the equivalence between Eq. (6.16) and Eq. (6.2).

which is

$$\sum_{\alpha_1=0}^{m-1}\left(\langle[A^{(1)}_{\alpha_1}-A^{(2)}_{\alpha_1+\alpha_2-1}+A^{(3)}_{\alpha_2}]\rangle+\langle[A^{(2)}_{\alpha_1+\alpha_2-1}-A^{(1)}_{\alpha_1+1}-A^{(3)}_{\alpha_2}]\rangle\right). \tag{6.18}$$

Observe that, for a fixed value of α_2, the third party $A^{(3)}$ measures only one observable. Hence, we can consider $A^{(2)}_{\alpha_1+\alpha_2-1}-A^{(3)}_{\alpha_2}$ as a single variable with d possible outcomes (because all the terms inside a $[\cdot]$ are treated *modulo* d). As Eq. (6.17) is, effectively, a three-partite inequality of the form of Eq. (6.9) for $n=2$, which has already been proven, this finishes the case $k=1$.

- If $k=2$, the same reasoning as above can be applied, but for the third party $A^{(3)}$ insterted into the expression (6.11).
- If $k=3$, a useful property of the AGCA inequality is that it is invariant under the exchange of the last and the $(n-2)$-th parties [Aol+12]. For the case $n=3$ that we are currently considering, this implies that we can write

$$I^{(3,m,d)}_{A^{(1)}A^{(2)}A^{(3)}}=\frac{1}{m}\sum_{\alpha_2=0}^{m-1}I^{(2,m,d)}_{A^{(3)}A^{(2)}}(\alpha_2)\circ A^{(1)}_{\alpha_2}. \tag{6.19}$$

Now the same reasoning can be applied, concluding the proof for $n=3$.

Let us now move to the induction step. If (6.14) holds for n parties for any NS distribution. The recursive formulation (6.13) allows us to group together the last two parties, leaving each term in (6.13) as an effective $(n-1)$-partite Bell expression that holds -by induction hypothesis- for any x_k and x_{n+1} for $k=1\dots n$. Summing each of these terms, indexed by the variable α_{n-1}, over α_{n-1}, and renormalizing by m^{n-2} leads us to (6.14), which holds for any pair x_k, x_{n+1} for $k=1\dots n-1$. The last case, $k=n$ is reached by exploiting the property that the AGCA inequality is invariant under the exchange of the last and the $(n-2)$-th parties [Aol+12], completing the proof. □

Theorem 6.9 guarantees that the monogamy properties that we have derived for the BKP inequality persist when one increases the number of

parties in the Bell experiment. Furthermore, tightness is also preserved and they can be re-expressed as follows:

$$I_{\mathbf{A}}^{n,m,d} + 1 \geq dP(A_{x_k}^{(k)} = [A_{x_{n+1}}^{(n+1)} + j]), \tag{6.20}$$

for every $x_k, x_{n+1} \in \{0, \ldots, m-1\}$ with $k \in \{1, \ldots, n\}$ and $j \in \{0, \ldots, d-1\}$. In addition, they remain valid if one tests nonlocality in any subset of $\mathbf{A} \cup \{A^{(n+1)}\}$ of n elements; *i.e.*, any party can play the role of the *third party*.

Remark 6.10. As a generalization of the $n = 2$ case, inequalities of the form (6.20) establish a trade-off between the nonlocality observed by a set $\mathbf{A}$ of parties, as measured by $I_{\mathbf{A}}^{2,m,d}$ with the correlations that an external observer, the $n+1$-th party, can share between the outcomes of any measurement performed by any of the parties in $\mathbf{A}$.

Remark 6.11. For the particular case of dichotomic observables ($d = 2$), it is relevant to highlight that $\langle [X - Y] \rangle = \langle [Y - X] \rangle$, which allows for a simpler expression of (6.14), which reads $I_{\mathbf{A}}^{n,m,2} + 2\langle [A_{x_k}^{(k)} - A_{x_{n+1}}^{(n+1)}] \rangle \geq 1$. After noting that $\langle [\cdot] \rangle$ is a function of $\langle \cdot \rangle$ for $d = 2$, a more traditional way to present this relation is

$$\left| \left\langle A_{x_k}^{(k)} A_{x_{n+1}}^{(n+1)} \right\rangle \right| \leq I_{\mathbf{A}}^{n,m,2}, \tag{6.21}$$

where the correlators $A_{x_k}^{(k)}$ are now dichotomic observables with outcomes ± 1, and $\langle XY \rangle = P(X = Y) - P(X \neq Y)$.

Observe that (6.21) implies the following: The strength of the Bell violation of (6.13) imposes tight bounds on every single expectation value of the form $\langle A_{x_k}^{(k)} A_{x_{n+1}}^{(n+1)} \rangle$ for every pair x_k, x_{n+1} with $k \in \{1, \ldots, n\}$. As $\langle A_{x_k}^{(k)} A_{x_{n+1}}^{(n+1)} \rangle$ is a measure of correlation between the outcomes of any measurement that an external observer $A^{(n+1)}$ can perform with those outcomes of a measurement performed by $A^{(k)}$ for any k, note that at the point of maximal NS violation, $I_{\mathbf{A}}^{n,m,2} = 0$, all these mean values are zero, whereas if a single pair of measurements, say $A_{x_k}^{(k)}$ and $A_{x_{n+1}}^{(n+1)}$, fulfill $|\langle A_{x_k}^{(k)} A_{x_{n+1}}^{(n+1)} \rangle| = 1$, the n parties cannot violate $I_{\mathbf{A}}^{n,m,2}$, as (6.21) enforces $I_{\mathbf{A}}^{n,m,2} \geq 1$, and 1 is the classical bound of the AGCA inequality (6.13) for $d = 2$.

6.1.2. Monogamy relations for Quantum Theory

It is a natural question to consider if similar monogamy relations hold for QT. This case is much more difficult to handle, and the main reason for that is that the shape of $\mathbf{Q}$ is mostly unknown or, at least, does not have an efficient description [NPA08]. On the other hand, $\mathbf{P}_{NS}$ is known to be a polytope, which can be described by a finite set of affine inequalities; in this sense, we would expect the quantum monogamy relations that we want to find to be non-linear. This difficulty is somehow expressed in the fact that the only progress made towards this direction has been rather scarce, concerning Bell inequalities for the $(n, 2, 2)$ scenario [TV06; Kur+11].

In this section we show how one can derive quantum analogs of the monogamy relations (6.3) for the $(3, 2, 2)$ Bell scenario. In order to do so, we introduce a uniparametric family of Bell inequalities which generalizes CHSH Bell inequality [Cla+69] (and (6.13) for $n = m = d = 2$).

Definition 6.12. *Let $\alpha \geq 1$ and let A_i and B_j be dichotomic observables with outcomes ± 1, where $i, j \in \{0, 1\}$. The modified CHSH inequality with parameter α, denoted $I^{\tilde{\alpha}}_{AB}$, is given by*

$$\tilde{I}^{\alpha}_{AB} = \alpha\left(\langle A_0 B_0\rangle + \langle A_0 B_1\rangle\right) + \langle A_1 B_0\rangle - \langle A_1 B_1\rangle \leq 2\alpha. \tag{6.22}$$

Note that the classical bound of the modified CHSH inequality follows from maximizing the term in the parenthesis with a local deterministic strategy such that $B_0 = A_0$ and $B_1 = A_0$; hence $B_0 = B_1$, so that, whatever value is assigned to A_1, the term outside the parenthesis is always cancelled out.

Remark 6.13. The case $\alpha < 1$ does not need to be considered, because it is enough to divide the whole Bell inequality by α and rename $\alpha \leftrightarrow \alpha^{-1}$, $A_0 \leftrightarrow A_1$.

We can now prove the following theorem, which generalizes the result of [TV06] for inequality (6.22).

Theorem 6.14. *Let $\vec{P} \in \mathbf{Q}$ for the Bell scenario $(3, 2, 2)$. Let also $\alpha \geq 1$ and*

$i, j \in \{0, 1\}$. *The following monogamy relations for QT hold:*

$$\alpha^2 \max\left\{\left(\tilde{I}^{\alpha}_{AB}\right)^2, \left(\tilde{I}^{\alpha}_{AC}\right)^2\right\} + \min\left\{\left(\tilde{I}^{\alpha}_{AB}\right)^2, \left(\tilde{I}^{\alpha}_{AC}\right)^2\right\} \leq 4\alpha^2(1+\alpha^2), \tag{6.23}$$

$$\left(\tilde{I}^{\alpha}_{AB}\right)^2 + 4\langle A_i C_j\rangle^2 \leq 4(1+\alpha^2). \tag{6.24}$$

Proof. Theorem 6.14 is proved using the tools introduced in [TV06; HHH95] with some slight modifications.

The first observation that we make is that the sets $\{\tilde{I}^{\alpha}_{AB}, \tilde{I}^{\alpha}_{AC}\}$ and $\{\tilde{I}^{\alpha}_{AB}, \langle A_i C_j\rangle\}$ define two two-dimensional cuts of $\mathbf{Q}$; hence the feasible region of pairs of values $\{\tilde{I}^{\alpha}_{AB}, \tilde{I}^{\alpha}_{AC}\}$ within QT is a convex set, and the same for $\{\tilde{I}^{\alpha}_{AB}, \langle A_i C_j\rangle\}$. Therefore, as shown in [TV06], every feasible point in their boundaries can be realized with a real three-qubit pure state and real, traceless, qubit observables. Such observables, which we denote X, take the form

$$X = \hat{\mathbf{n}}' \cdot \vec{\boldsymbol{\sigma}}', \tag{6.25}$$

where $\vec{\boldsymbol{\sigma}}' := [\sigma_x, \sigma_z]$ is a vector of the Pauli matrices, and $\hat{\mathbf{n}}' = [x, z]$; *i.e.*, X lies in the x-z plane of the Bloch sphere.

One can actually find, given any $\rho_{AB} \in \mathcal{D}(\mathcal{H})$ where $\mathcal{H} = \mathbb{C}^2 \otimes \mathbb{C}^2$, the maximal quantum violation of $\tilde{I}^{\alpha}_{AB}$ over observables of the form (6.25) [TV06; HHH95]. Such quantity yields

$$\max_{A_i, B_j} \tilde{I}^{\alpha}_{AB} = 2\sqrt{\alpha^2 \lambda_1 + \lambda_2}, \tag{6.26}$$

where λ_1 and λ_2 are the eigenvalues of $T_{AB} T_{AB}^T$ sorted in decreasing order $\lambda_1 \geq \lambda_2$, with T_{AB} being the so-called correlation matrix, defined as

$$T_{AB} := \begin{pmatrix} \langle \sigma_x \otimes \sigma_x\rangle_{\rho_{AB}} & \langle \sigma_x \otimes \sigma_z\rangle_{\rho_{AB}} \\ \langle \sigma_z \otimes \sigma_x\rangle_{\rho_{AB}} & \langle \sigma_z \otimes \sigma_z\rangle_{\rho_{AB}} \end{pmatrix}. \tag{6.27}$$

Recall that the expecation values appearing in (6.27) are computed via Born's rule (2.13): $\langle X \otimes Y\rangle_\rho = \mathrm{Tr}[X \otimes Y \rho]$.

In a similar fashion, one can obtain a tight upper bound on a single correlator level:

$$\max_{A,B} \langle A \otimes B\rangle = \lambda_1. \tag{6.28}$$

We now have the necessary tools to prove (6.23) and (6.24). We can assume, without loss of generality[5], that $\tilde{I}^{\alpha}_{AB} \geq \tilde{I}^{\alpha}_{AC}$. Then, inequality (6.23) can be written as

$$\alpha^2(\tilde{I}^{\alpha}_{AB})^2 + (\tilde{I}^{\alpha}_{AC})^2 \leq 4\alpha^2. \tag{6.29}$$

To prove it, let us consider $|\psi\rangle_{ABC}$ a pure state of three qubits and let us denote its reduced subsystems $\rho_{AB} := \mathrm{Tr}_C|\psi\rangle\langle\psi|$ and $\rho_{AC} := \mathrm{Tr}_B|\psi\rangle\langle\psi|$ and by T_{AB} and T_{AC} the associated correlation matrices (*cf.* Eq. (6.27)). Let us denote by $\lambda_1 \geq \lambda_2$ the eigenvalues of $T_{AB}T^T_{AB}$ and by $\tilde{\lambda}_1 \geq \tilde{\lambda}_2$ the eigenvalues of $T_{AC}T^T_{AC}$. The matrices $T_{AB}T^T_{AB}$ and $T_{AC}T^T_{AC}$ can be diagonalized in the same basis [TV06], which allows to maximize both $\tilde{I}^{\alpha}_{AB}$ and $\tilde{I}^{\alpha}_{AC}$ at the same time with the same observables at Alice's site. Hence, we can write

$$\begin{aligned}\max_{A_i,B_j,C_k}\left[\alpha^2\left(\tilde{I}^{\alpha}_{AB}\right)^2 + \left(\tilde{I}^{\alpha}_{AC}\right)^2\right] &= 4\left[\alpha^2(\alpha^2\lambda_1+\lambda_2)+\alpha^2\tilde{\lambda}_1+\tilde{\lambda}_2\right] \\ &= 4\left[\alpha^4\lambda_1+\alpha^2(\lambda_2+\tilde{\lambda}_1)+\tilde{\lambda}_2\right]\end{aligned} \tag{6.30}$$

where we have used Eq. (6.26). We can now use the monogamy relation given in [TV06] for the CHSH inequality, which, in terms of λ_i and $\tilde{\lambda}_j$ is

$$\lambda_2 + \tilde{\lambda}_1 \leq 2 - \lambda_1 - \tilde{\lambda}_2. \tag{6.31}$$

Hence, using the facts that $\lambda_1 \leq 1$, $\tilde{\lambda}_2 \geq 0$ and $\alpha \geq 1$ we obtain:

$$\begin{aligned}\max_{A_i,B_j,C_k}\left[\alpha^2\left(\tilde{I}^{\alpha}_{AB}\right)^2 + \left(\tilde{I}^{\alpha}_{AC}\right)^2\right] &\leq 4\left[(\alpha^2-1)(\alpha^2\lambda_1-\tilde{\lambda}_2)+2\alpha^2\right] \\ &\leq 4\left[\alpha^2(\alpha^2-1)+2\alpha^2\right] \\ &= 4\alpha^2(1+\alpha^2),\end{aligned} \tag{6.32}$$

which gives (6.23).

To prove inequality (6.24) the same reasoning leads to

$$\begin{aligned}\max_{A_i,B_j,C_k}\left[\left(\tilde{I}^{\alpha}_{AB}\right)^2 + 4\langle A_aC_c\rangle^2\right] &= 4(\alpha^2\lambda_1+\lambda_2)+4\tilde{\lambda}_1 \\ &= 4\alpha^2\lambda_1+4(\lambda_2+\tilde{\lambda}_1),\end{aligned} \tag{6.33}$$

[5] The other case follows from exchanging B and C.

with $a, c \in \{0, 1\}$. Applying the monogamy relation (6.31) to the term $\lambda_2 + \tilde{\lambda}_1$ directly yields (6.24), which completes the proof. □

Let us discuss a bit the tightness of the inequalities (6.24). If $i = 0$, they are tight for any $j \in \{0, 1\}$: it suffices to take the state $(\beta_+|01\rangle + \beta_-|10\rangle)|0\rangle$, with $\beta_\pm = \sqrt{1 \pm \sqrt{2}\sin\theta}/2$, where $\theta \in [0, \pi/4]$. Nevertheless, if $i = 1$, this property no longer holds true. For this case, we have numerically investigated monogamy relations for particular values of α with SDP techniques, which are an adaptation of the NPA hierarchy [NPA08] to this particular scenario and we have found the corresponding tight relations. We know that these relations are tight by using two methods: First, by fixing the value of $\tilde{I}^{\alpha}_{AB}$ we maximize the guessing probability over states of a certain dimension (here it was sufficient to pick states in $\mathcal{D}(\mathbb{C}^4)^{\otimes 2}$) and local dichotomic measurements (of dimension 4 in this case) with outcomes ± 1. From this we obtain a subset of correlations that are allowed by QT. Second, we obtain a superset of correlations with the aid of the NPA hierarchy, as it is a method that gives certificates of correlations being supra-quantum; *i.e.*, not in **Q**. If these two regions coincide, the monogamy relation describing its boundary is tight (see Fig. 6.2).

6.2. Bounds on randomness

We now show how the monogamy relations introduced in Theorems 6.3, 6.9 and 6.14 can be turned into tight bounds on the guessing probability that an external observer Eve[6] has of guessing any of the outcomes of the n parties performing the Bell experiment. This property makes them interestingly useful for DI applications, as we shall see in Section 5.4. Here we compare such bounds on the guessing probability with previous works.

The guessing probability of the outcome of the x_k-th measurement performed by the k-th party is defined as the most probable outcome:

$$P_g(x_k) := \max_{a_k} P(A^{(k)}_{x_k} = a_k) = \max_{a_k} P(A_k|x_k). \tag{6.34}$$

In order to derive a bound on $P_g(x_k)$ we have to go to the worst-case scenario, in which Eve has full knowledge about all parties' devices, and

[6] In this section it is convenient to distrust that external observer, so we call it Eve, which is a shortening of a placeholder name like Alice or Bob, which here stands for *Eavesdropper*.

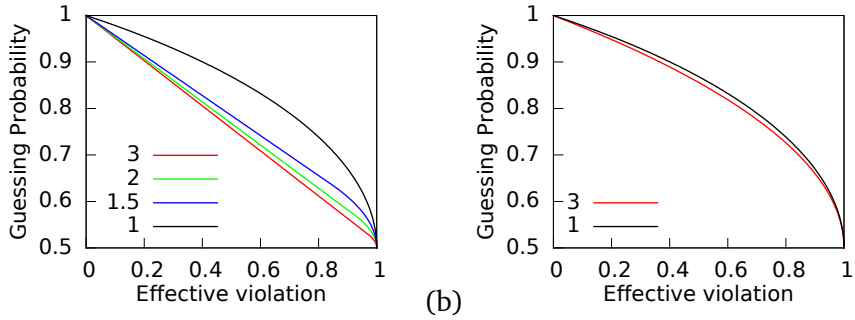

Figure 6.2.: (a) The guessing probability for $i = 1$ in Theorem 6.14 as a function of $(\tilde{I}^{\alpha}_{AB} - 2\alpha)/2(\sqrt{1+\alpha^2} - \alpha)$ (the curves have been renormalized so that for different $\alpha \in \{1, 3/2, 2, 3\}$ they start and end at the same point). The feasible region corresponds to the area below the curves. At the third level of the NPA hierarchy, the *sub-quantum* region (obtained by constructing states and measurements of a fixed dimension) and the *supra-quantum* region (given by the description of $\mathbf{Q}_3$ in the NPA hierarchy) coincide, with a relative error of 10^{-7}. This error may seem very large, but it lies in the order of the best precision that one can achieve with 64-bit arithmetic with SDP toolboxes like Self-Dual Minimization (SeDuMi) [Stu99] -the one we used- and when optimizing over matrices of considerable size, like the ones corresponding to $\mathbf{Q}_3$ in the NPA hierarchy. (b) We present a comparison between the non-tight monogamy relation (6.24) for $i = 1$ and the tight one found numerically and displayed in (a) for $\alpha = \{1, 3\}$ (the other values $\alpha \in \{3/2, 2\}$ fall in between and we have hidden them in the interest of clarity). The black curves ($\alpha = 1$, the usual CHSH) are the same on both plots.

their measurement choices $\{x_k\}$. Eve tries to guess the outcome of $A^{(k)}_{x_k}$. The best strategy for Eve is to measure one of the observables at her disposal, say the z-th one, and, independently of her result, return the most probable outcome of $A^{(k)}_{x_k}$. Then, we have that $P(E_z = A^{(k)}_{x_k}) = \max_{a_k} P(a_k|x_k)$ and the guessing probability is then bounded, for any x_k and k (*cf.* Eq. (6.20))

by

$$\max_{a_k} P(a_k|x_k) = \max_{a_k} P(A_{x_k}^{(k)} = a_k) \leq \frac{1}{d}(1 + I_{\mathbf{A}}^{n,m,d}). \tag{6.35}$$

The bound given in (6.35) is tight and, as shown in Fig. 6.3, significantly improves over the previously existing one [BKP06; Aol+12], which reads

$$\max_{a_k} P(a_k|x_k) \leq \frac{1}{d}\left[1 + \frac{d^n}{4}(n-1)I_{\mathbf{A}}^{n,m,d}\right]. \tag{6.36}$$

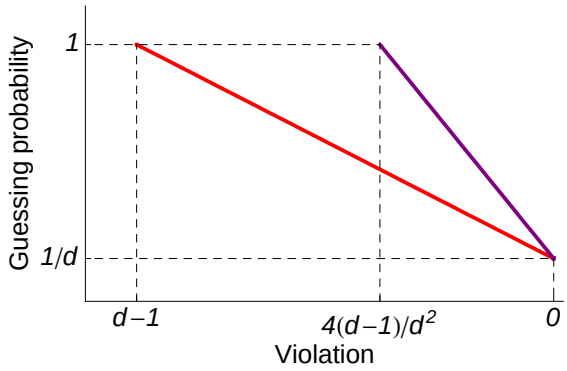

Figure 6.3.: The red line corresponds to the upper bound on the guessing probability of Eve (6.35) that we have derived from Theorem 6.9. The purple line corresponds to the existing one (6.36) provided in [BKP06; Aol+12]. The feasible region within NS theories lies below the red line, as (6.35) is tight for any value $I_{\mathbf{A}}^{n,m,d} \in [0, d-1]$. Observe that the existing bound (6.36) is nontrivial only if $I_{\mathbf{A}}^{n,m,d} < 4(d-1)d^{-2}$, a region that vanishes in the limit $d \longrightarrow \infty$.

If we treat Eve as a less powerful eavesdropper, and she is restricted by the rules of QT, we recover the bound for the $(3, 2, 2)$ scenario

$$\max_j P(X_i = j) \leq \frac{1 + \sqrt{1 + \alpha^2 - \left(\tilde{I}_{AB}^{\alpha}/2\right)^2}}{2}, \tag{6.37}$$

which was introduced in [AMP12], where $X = A$ or B, $i = 0, 1$ and $\alpha \geq 1$. Let us remark that (6.37) is tight only in the case $i = 0$. If $i = 1$ one should

employ the tight bounds that we have numerically found, for the desired α (*cf.* Fig. 6.2).

6.3. Applications

In this section we discuss how the bounds on the guessing probability (6.35) can be useful for some DI protocols, such as Device-Independent Quantum Key Distribution (DIQKD) (Section 6.3.1) and Randomness Amplification (RA) (Section 6.3.2).

6.3.1. Quantum Key Distribution

General security proofs in DIQKD protocols have not been found yet; *i.e.*, one usually requires more assumptions than the minimal set that we would like to have in the DI framework. The strongest proof in this direction requires that Eve is limitied, not only by the NS principle[7], but also does not have a long-term quantum memory, a scenario known as the Bounded-Storage (BS) model [Pir+13]. The BS assumption is not Device-Independent; however it is reasonable within the current state-of-the-art technology, as the degree of control required for Eve to perform the operations in [Pir+13] is too high.

In what follows, we will compare the performance on the existing bound (6.36) with respect to the one we obtained (6.35) for DIQKD in the BS model. In order to do so, we assume that Alice and Bob share a two-qudit maximally entangled state $|\psi\rangle = \sum_{i=0}^{d-1} |ii\rangle/\sqrt{d}$, which is used to maximally violate the BKP inequality (6.2), when the optimal measurements are used for this setup [BKP06]. With such measurements, Alice and Bob check that they are at the point of maximal violation of BKP. From time to time, however, Bob performs an extra measurement, B_2, which is equal to one of Alice's measurements, *e.g.* $B_2 = A_0$ and, because they are measuring a maximally entangled qudit state $|\psi\rangle$, their outcomes are perfectly correlated.

[7] The fact that we consider Eve to be a supra-quantum eavesdropper makes the proof even stronger, as $\mathbf{Q} \subsetneq \mathbf{P}_{NS}$. Hence, even in the extreme scenario that QT were incomplete, the proof would hold as long as one could not transmit information instantaneously. Note that, although we make the eavesdropper stronger, this allows us to have simpler the proofs, as $\mathbf{P}_{NS}$ is easier to characterize than $\mathbf{Q}$, a fact that is reflected in the monogamy relations (compare (6.35) with (6.37)).

Whenever Bob chooses B_2 and Alice chooses A_0, their outcome is used to generate the secret key.

The key rate, denoted R, of this protocol is lower bounded as follows [Pir+13]:

$$R \geq -\log_2 \tau \left(I_{AB}^{2,m,d} \right) - H(A|B), \tag{6.38}$$

where τ is any upper bound on the guessing probability for a NS eavesdropper and $H(A|B)$ is the conditional Shannon entropy between the measurements that Alice and Bob use for the generation of the secret key. Note that the term $H(A|B)$ acts as a correction to the fact that the outcomes of the measurements of Alice and Bob could not be perfectly correlated, thus lowering the key rate, as extra operations would need to be done. However, as they are measuring the maximally entangled state $|\psi\rangle$, their correlation is perfect, so that $H(A|B) = 0$.

In Fig. 6.4 we have compared the resources needed to achieve different key rates (6.38) when τ corresponds to (6.36) and when τ follows from the monogamy relations that we have derived (6.35). We see that, for a fixed key rate R, the minimal number of measurements required, denoted M, as a function on the number of outputs has a different behavior as d grows: for the bound (6.36), the minimal m to achieve a given R grows with d; whereas for our bound (6.35), the minimal m to achieve a given R decreases with d.

6.3.2. Randomness Amplification

If we assume the NS principle, a Bell inequality violation proves the existence of intrinsic randomness[8]. However, there is a subtlety in this claim. The observation of nonlocal correlations is actually insufficient to certify the existence of the intrinsic randomness that QT is so often said to have: in order to perform a Bell test, the choice of the measurements has to be random or, at least, uncorrelated[9] from the hidden variable λ. However,

[8] This claim depends on the interpretation that we take of QT. It is possible to have a deterministic QT, at the expense of dropping the NS principle (often referred to as Bohmian mechanics [Boh52]), but this theory is in direct contradiction with Einstein's Relativity theory, as it allows for instantaneous signalling.

[9] Measurement independence (the fact that $p(\mathbf{x}|\lambda) = p(\mathbf{x})$, where $\mathbf{x}$ are the settings that are chosen in the Bell experiment when the state of the system (the hidden variable) is λ) is needed in a Bell test. Absence of it is often referred to as denial of *free will*, as

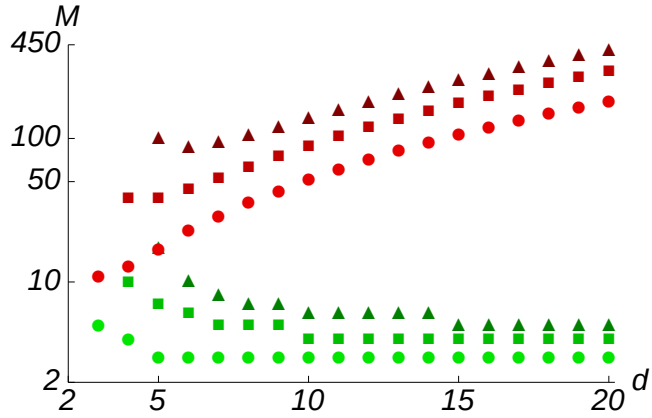

Figure 6.4.: The minimal number of measurements M on a two-qudit maximally entangled state $|\psi\rangle = \sum_{i=0}^{d-1} |ii\rangle/\sqrt{d}$ needed to achieve a given key-rate R in which the protocol is secure against NS eavesdroppers. The values of M to obtain, at least, bits ($R \geq 1$) per round correspond to circles; trits ($R \geq \log_2 3$) correspond to squares; and pairs of bits -or quarts- ($R \geq 2$) correspond to triangles. In red we have used the upper bound τ on the guessing probability given in (6.36) and in green we have used the upper bound τ that we have derived in (6.35). Observe that, with our bound, the parties need to perform a much simpler experiment, as many fewer measurements are needed in order to have the same key rate. In addition, the minimal number of measurements decreases with the dimension, contrary to what was predicted with the previously existing results (6.36) [BKP06; Aol+12].

how can one certify that the randomness used to choose the measurements is intrinsic in the first place? The extreme case is when all the measurement settings are pre-determined in advance. Then, any nonlocal correlation can be explained in terms of a deterministic local model. Is there, at least, some way to measure the quality of the randomness that is used?

The Santha-Vazirani (SV) ε-source is the answer to that question. It constitutes a way of quantifying the quality of the randomness that is used to feed the choices of measurements in a Bell test. The closest ε is to 0, the more independent are going to be the choices of measurements from λ:

Definition 6.15. *A Santha-Vazirani ε-source is a random variable that produces a sequence of bits $\{y_1, \ldots, y_n\}$ that satisfy the following rule:*

$$\frac{1}{2} - \varepsilon \leq P(y_k|w) \leq \frac{1}{2} + \varepsilon, \tag{6.39}$$

where w denotes any space-time variable that could have been the cause of y_k (in particular, this includes $\{y_1, \ldots, y_{k-1}\}$).

Observe that the bits produced by the SV source are correlated with each other to some extent; however, they keep some amount of intrinsic randomness, as quantified by ε (often referred to as being ε-free). The DI protocol that we are going to discuss in this section is the so-called Randomness Amplification (RA). The goal is to improve the quality of the randomness produced by a SV source. We have at our disposal a sequence of ε-free bits (or, more generally, $d$its) and we want to obtain a perfectly random bit (or $d$it) using correlations that violate a Bell inequality.

It had been proven that RA was impossible with classical resources [SV86]. This is not surprising, as the only randomness in Classical Physics comes from ignorance about the state of the system, so that it is not intrinsic. In the quantum regime, this question has been addressed recently [CR12], and it is useful to present it in the adversarial picture. A set of parties **A** wants to perform RA by using the AGCA inequality (6.13). An adversary Eve provides the parties that want to perform the Bell experiment with ε-sources, which they use to choose their measurements. Eve wants to

the measurement settings could, in principle, be chosen by human beings (although in practice one uses a computer to choose randomly a large number of measurement choices) whose free will would be maimed.

simulate a quantum violation of (6.13) and, as Eve is restricted only by the NS principle, she can give the parties any *resource* that produces any kind of NS correlations[10]. In other words, she controls the boxes that are shared by the parties. The random variable W that produces w in (6.39) is under the control of Eve, who uses it to tweak the SV -up to ε- and the physical devices that the parties possess. Hence, Eve controls the measurement apparatus, the resurce that is measured and—up to ε—the choice of the measurement that is to be performed. This means that, for any value of W, namely w, a vector of settings $\mathbf{x}$ is generated according to (6.39) and the n-partite probability distribution $\{P(\mathbf{a}|\mathbf{x},w)\}_{\mathbf{a},\mathbf{x}}$ is generated by the devices.

Let now $\{P(a_k,w|\mathbf{x})\}_{a_k,w}$ be the probability distributions that describe the correlations between the outcome of the k-th party and w, when a particular choice of measurements $\mathbf{x}$ is made. Let $\{\tilde{P}(a)\}$ be the one-party uniform distribution (simply, $\tilde{P}(a) := d^{-1}$). Let us also introduce the variational distance between two probability distributions p and q, which is given by

$$D(\{p(\mathbf{x})\},\{q(\mathbf{x})\}) := \frac{1}{2}\sum_{\mathbf{x}} |p(\mathbf{x}) - q(\mathbf{x})|. \tag{6.40}$$

The following theorem quantifies the variational distance between these probability distributions: $\{P(a_k,w|\mathbf{x})\}$ and the uniform distribution in which outcomes and W are uncorrelated $\{\tilde{P}(a_k)P(w|\mathbf{x})\}$:

Theorem 6.16. *For any w which is an outcome of W, consider an n-partite NS probability distribution conditioned on w given by $\vec{P} \in \mathbf{P}_{NS}$ with elements $\{P(\mathbf{a}|\mathbf{x}w)\}_{\mathbf{a},\mathbf{x}}$. Then,*

$$D(\{P(a_k,w|\mathbf{x})\}_{a_k,w},\{\tilde{P}(a_k)P(w|\mathbf{x})\}_{a_k,w}) \leq \frac{(d-1)^2+1}{2d} Q_m(\mathbf{x}) I_{\mathbf{A}}^{n,m,d}, \tag{6.41}$$

where $I_{\mathbf{A}}^{n,m,d}$ corresponds to the AGCA inequality (6.13) and is computed with the probabilities that the parties in $\mathbf{A}$ estimate; namely, $\{P(\mathbf{a}|\mathbf{x})\}_{\mathbf{a},\mathbf{x}}$, and $Q_m(\mathbf{x})$ is the following quantity:

$$Q_m(\mathbf{x}) := \sup_w \left[\frac{P(w|\mathbf{x})}{P_{\min}(w)}\right], \tag{6.42}$$

[10] In particular, Eve can give them local correlations from time to time, as generally the NS bound is higher than the QT bound; otherwise, an observation of a supra-quantum violation would look very suspicious to the parties in $\mathbf{A}$.

where $P_{\min}(w) := \min_{\mathbf{x}}\{P(w|\mathbf{x})\}_{\mathbf{x}}$ *and this minimum is taken over all the measurement settings that appear in (6.13).*

Proof. For simplicity, we prove Theorem 6.16 for the bipartite case. This does not constitute any loss of generality, as the multipartite case will follow directly from the bipartite one. Let us denote the parties performing the Bell test by $\mathbf{A} = \{A, B\}$ and Eve by E. Their respective choices of measurements are denoted x, y, z and their measurement results a, b, e, respectively.

We start by observing that, for any probability distribution of the form $\{P(ab|xyw)\}_{a,b,x,y}$, the maximal probability of getting (locally) an outcome by any of the parties must obey the monogamy relation for the guessing probability (6.12, 6.35). In the case of Alice, this would be

$$\max_a P(a|xw) \leq \frac{1}{d}\left(1 + I_w^{2,m,d}\right), \tag{6.43}$$

for every $x \in \{0, \ldots, m-1\}$. Observe that we have explicitly marked the dependence of I on w, as the BKP inequality is computed, in this case, for a particular value of w; *i.e.*, using $\{P(ab|xyw)\}_{a,b,x,y}$.

The normalization condition

$$P(a|xw) = 1 - \sum_{\alpha \neq a} P(\alpha|xw), \tag{6.44}$$

together with the bound (6.43), implies $P(a|xw) \geq \left[1 - (d-1)I_w^{2,m,d}\right]/d$. Consequently, the inequality

$$\left|P(a|xw) - d^{-1}\right| \leq \frac{d-1}{d} I_w^{2,m,d} \tag{6.45}$$

holds for every a and every x.

Joining inequality (6.43) for the most probable outcome $\max_a P(a|xw)$ and inequality (6.45) for the rest of the $P(a|xw)$ we can upper bound the variational distance between $\{P(a|xw)\}_a$ and the uniform distribution $\{\tilde{P}(a)\}$ for any strategy w that Eve can employ and for any measurement setting x:

$$D(\{P(a|xw)\}_a, \{\tilde{P}(a)\}) = \frac{1}{2}\sum_a \left|P(a|xw) - \tilde{P}(a)\right| \leq \frac{(d-1)^2 + 1}{2d} I_w^{2,m,d}. \tag{6.46}$$

At this stage, one can follow exactly the same steps that are used in [CR12], which we recall for completeness.

The observers A and B do not have access to the variable W which is held by Eve. Hence, inequality (6.46) needs to be averaged over w -for every particular choice of measurements x and y- with the weights given by the probability distribution $\{P(w|xy)\}_w$. The NS principle $P(a|xw) = P(a|xyw)$ and Bayes theorem $P(w|xy)P(a|xyw) = P(aw|xy)$ enable us to re-express (6.46) as

$$\begin{aligned} D(\{P(aw|xy)\}_{a,w}, \{\tilde{P}(a)P(w|xy)\}_{a,w}) &= \frac{1}{2}\sum_{a,w}\left|P(aw|xy) - \tilde{P}(a)P(w|xy)\right| \\ &\leq \frac{(d-1)^2+1}{2d}\sum_w P(w|xy)I_w^{2,m,d}. \end{aligned} \tag{6.47}$$

The r. h. s. of (6.47) can be expressed as follows:

$$\begin{aligned} \sum_w P(w|xy)I_w^{2,m,d} &= \sum_{w,\alpha} P(w|xy)\left(\langle[A_\alpha - B_\alpha]\rangle_w + \langle[B_\alpha - A_{\alpha+1}]\rangle_w\right) \\ &= \sum_{w,\alpha}\Bigg(P(w|\alpha\alpha)\frac{P(w|xy)}{P(w|\alpha\alpha)}\langle[A_\alpha - B_\alpha]\rangle_w \\ &\quad + P(w|\alpha+1,\alpha)\frac{P(w|xy)}{P(w|\alpha+1,\alpha)}\langle[B_\alpha - A_{\alpha+1}]\rangle_w\Bigg), \end{aligned}$$

where, again, the subscript w indicates that the expectation values $\langle[A_\alpha - B_\alpha]\rangle_w$ and $\langle[B_\alpha - A_{\alpha+1}]\rangle_w$ are to be computed using the probability distributions that are conditioned on w: $\{P(ab|xyw)\}_w$. Now, by definition of Q_m, we can write

$$\begin{aligned} \sum_w P(w|xy)I_w^{2,m,d} &\leq Q_m(x,y)\sum_{w,\alpha}[P(w|\alpha\alpha)\langle[A_\alpha - B_\alpha]\rangle_w \\ &+ P(w|\alpha+1,\alpha)\langle[B_\alpha - A_{\alpha+1}]\rangle_w] \\ &= Q_m(x,y)\sum_\alpha\left(\langle[A_\alpha - B_\alpha]\rangle + \langle[B_\alpha - A_{\alpha+1}]\rangle\right) \\ &= Q_m(x,y)I_{AB}^{2,m,d}. \end{aligned} \tag{6.48}$$

Observe that $I_{AB}^{2,m,d}$ is computed using the observed statistics $\{P(ab|xy)\}_{a,b,x,y}$. The proof is completed by substituting the bound (6.48) into (6.47), which leads to (6.41). □

Remark 6.17. One can also derive an inequality in the spirit of (6.41) with a slightly different approach, assuming that we know $P(\mathbf{x}|w)$ instead of $P(w|\mathbf{x})$.

Theorem 6.18. *For any outcome w of W, let us consider an n-partite NS probability distribution conditioned on w given by $\vec{P} \in \mathbf{P}_{NS}$ with elements $\{P(\mathbf{a}|\mathbf{x}w)\}_{\mathbf{a},\mathbf{x}}$. Furthermore, assume that $P(\mathbf{x}) = \sum_w p(w)p(\mathbf{x}|w)$ is the same for all $\mathbf{x}$[11]. Then,*

$$D(\{P(a_k, w|\mathbf{x})\}_{a_k,w}, \{\widetilde{P}(a_k)P(w|\mathbf{x})\}_{a_k,w}) \leq \frac{(d-1)^2+1}{2d}\widetilde{Q}_m(\mathbf{x})I_{\mathbf{A}}^{n,m,d}, \tag{6.49}$$

where $I_{\mathbf{A}}^{n,m,d}$ corresponds to the AGCA inequality (6.13) and is computed with the probabilities $\{P(\mathbf{a}|\mathbf{x})\}_{\mathbf{a},\mathbf{x}}$, and $\widetilde{Q}_m(\mathbf{x})$ is the following quantity:

$$\widetilde{Q}_m(\mathbf{x}) := \sup_w \left[\frac{P(w|\mathbf{x})}{\widetilde{P}_{\min}(w)}\right], \tag{6.50}$$

where $\widetilde{P}_{\min}(w) := \min_{\mathbf{x}}\{P(w|\mathbf{x})\}_{\mathbf{x}}$ and this minimum is taken over all the measurement settings that appear in (6.13).

Proof. As in the proof of Theorem 6.16, we also focus on the bipartite case and adopt the same notation. By analogy to (6.12), for any w, the probability distribution conditioned on w $\{P(a,b|x,y,w)\}_{a,b,x,y}$ satisfies the monogamy relations

$$\frac{I_w^{2,m,d}}{\widetilde{P}_{\min}(w)} + 1 \geq dP(X_i = E_j|w), \tag{6.51}$$

where X can be either A or B and $i, j \in \{0, \ldots, m-1\}$.

Let us then write $I_w^{2,m,d}$ as

$$I_w^{2,m,d} = \sum_{\alpha=0}^{m-1} \left[P(\alpha\alpha|w)\langle[A_\alpha - B_\alpha]\rangle_w + P(\alpha+1,\alpha|w)\langle[B_\alpha - A_{\alpha+1}]\rangle_w\right], \tag{6.52}$$

[11] The reason for this assumption is that Eve does not want Alice to notice her action from $p(\mathbf{x})$

where, again, we have written the subindex w to explicitly state that the correlators $\langle[A_\alpha - B_\alpha]\rangle_w$ and $\langle[B_\alpha - A_{\alpha+1}]\rangle_w$ are computed using the probability distribution that is conditioned on w, $\{P(a,b|x,y,w)\}_{a,b,x,y}$.

Observe that, since not all measurement settings appear in the BKP (or, in general, the AGCA) inequality, $\widetilde{P}_{\min}(w)$ takes the following form:

$$\widetilde{P}_{\min}(w) = \min_{\alpha=0\ldots m-1}\{P(\alpha,\alpha|w), P(\alpha+1,\alpha|w)\}, \tag{6.53}$$

with the convention that the α's are taken to be *modulo* m.

Now, the monogamy relations (6.51) imply that the guessing probability of Eve, when she is employing the w-th strategy to guess the outcomes of one of the measurements performed by one of the parties (*e.g.*, Alice), is bounded by

$$\max_a P(a|xw) \leq \frac{1}{d}\left(1 + \frac{I_w^{2,m,d}}{\widetilde{P}_{\min}(w)}\right), \tag{6.54}$$

for $x \in \{0,\ldots,m-1\}$.

As this bound holds for the maximum, so it does for every $P(a|xw)$. This implies, together with the normalization condition (6.44), that

$$P(a|xw) \geq \frac{1}{d} - \frac{d-1}{d}\left[\frac{I_w^{2,m,d}}{\widetilde{P}_{\min}(w)}\right]. \tag{6.55}$$

Hence, the following inequality holds for every a and x:

$$\left|P(a|xw) - d^{-1}\right| \leq \frac{d-1}{d}\frac{I_w^{2,m,d}}{\widetilde{P}_{\min}(w)}. \tag{6.56}$$

We combine inequality (6.54) for $\max_a P(a|xw)$ with (6.56) for the rest (the $P(a|xw)$ that do not correspond to the maximum) and we get, for every of Eve's strategies w,

$$\begin{aligned} D(\{P(a|xw)\}_a, \{\widetilde{P}(a)\}) &= \frac{1}{2}\sum_a \left|P(a|xw) - \widetilde{P}(a)\right| \\ &\leq \frac{(d-1)^2+1}{2d}\frac{I_w^{2,m,d}}{\widetilde{P}_{\min}(w)}. \end{aligned} \tag{6.57}$$

As neither Alice nor Bob has access to the random variable W, becase it is kept by Eve, it becomes necessary to average inequality (6.57) over all the

values of w, weighted with the probability distribution $\{P(w|xy)\}_w$. Like in Theorem 6.16, the NS principle $P(a|xw) = P(a|xyw)$ and Bayes theorem, $P(w|xy) = P(xy|w)P(w)/P(xy)$ which implies $P(w|xy)P(a|xyw) = P(aw|xy)$, we can now write

$$\begin{aligned} & D(\{P(a,w|x,y)\}_{a,w}, \{\widetilde{P}(a)P(w|xy)\}_{a,w}) \\ = \; & \frac{1}{2}\sum_{a,w}\Big|P(aw|xy) - \widetilde{P}(a)P(w|xy)\Big| \\ \leq \; & \frac{(d-1)^2+1}{2d}\sum_{w}\frac{P(xy|w)}{\widetilde{P}_{\min}(w)}\frac{P(w)}{P(xy)}I_w^{2,m,d} \\ \leq \; & \frac{(d-1)^2+1}{2d}\widetilde{Q}_m(x,y)\sum_{w}\frac{P(w)}{P(xy)}I_w^{2,m,d}, \end{aligned} \tag{6.58}$$

where we have used that $\widetilde{Q}_m(x,y) = \max_w\{P(xy|w)/\widetilde{P}_{\min}(w)\}$.

To finally obtain inequality (6.49) and complete the proof, we observe that

$$P(ab|xy) = \sum_w P(w|xy)P(ab|xyw). \tag{6.59}$$

By hypothesis, all the probabilities $P(xy)$ are equal, which lets us write

$$I_{AB}^{2,m,d} = \sum_w \frac{P(w)}{P(xy)}I_w^{2,m,d}, \tag{6.60}$$

where now $I_{AB}^{2,m,d}$ is calculated by using the the probability distribution $\{P(ab|xy)\}$ that the parties A and B have estimated and the probabilities $P(xy) = \sum_w P(w)P(xy|w)$ are, by assumption, equal for every $x, y \in \{0,\ldots,m_1\}$. Hence, we obtain (6.49), completing the proof. □

Remark 6.19. Let us observe that, under the assumption that $P(\mathbf{x})$ is equal for all $\mathbf{x}$ that we have made in Theorem 6.18, it holds that $\widetilde{Q}_m(\mathbf{x}) = Q_m(\mathbf{x})$.

Remark 6.20. Theorem 6.16 implies that, if the correlations $\{P(\mathbf{a},\mathbf{x})\}_{\mathbf{a},\mathbf{x}}$ that the parties observe violate maximally the AGCA inequality (6.13) for NS correlations, then each of the $d$its that each individual party obtains is perfectly random and uncorrelated from W [CR12].

Let us now discuss Randomness Amplification. Our task is as follows: Given partially random ε-free bits, we want to obtain perfectly random $d$its by using QT correlations that can produce an arbitrarily high amount of violation of the AGCA inequality $I_{\mathbf{A}}^{n,m,d}$. To generate the measurement settings, each of the parties in $\mathbf{A}$ uses its own SV source $r := \lceil \log_2 m \rceil$ times. Consequently, for any $\mathbf{x}$ the quantity $Q_r(\mathbf{x})$ is bounded as

$$Q_r(\mathbf{x}) \leq \left(\frac{1+2\varepsilon}{1-2\varepsilon} \right)^{nr}, \tag{6.61}$$

as it was shown in [CR12]. On the other hand, in the limit of large m, there exist a quantum state and a set of measurements such that the QT limit of $I_{\mathbf{A}}^{n,m,d}$ can be well approximated by [BKP06; Aol+12]

$$I_{\mathbf{A}}^{n,m,d} \approx \lambda(d)/m \leq \lambda(d) 2^{1-r}, \tag{6.62}$$

with $\lambda(d)$ being a function that only depends on d.

After substituting these bounds in (6.41), we obtain the following condition for the variational distance to go to zero as $m \longrightarrow \infty$: There exists a critical ε, denoted ε_n, such that the following must hold:

$$\varepsilon < \varepsilon_n := \frac{\sqrt[n]{2}-1}{2(\sqrt[n]{2}+1)}. \tag{6.63}$$

Note that, in the limit of large m, both the QT and the NS coincide, as $I_{\mathbf{A}}^{n,m,d}$ goes to 0 in (6.62), which is the NS bound.

Hence, any quantum correlations that approach the point of maximal[12] NS violation can be used for Randomness Amplification, provided that $\varepsilon < \varepsilon_n$ holds.

Remark 6.21. If $n = 2$ we recover the bound of [CR12] $\varepsilon_2 = (\sqrt{2}-1)^2/2 \simeq 0,0859$. Note that, as ϵ_n is a strictly decreasing function of n; that is, the critical epsilon value gets lower as n grows. Hence, $n = 2$ is the best choice in this particular scenario. Nevertheless, it should be observed that ε_n does

[12] We need this NS violation to be maximal; otherwise Eve could mix such correlations with local ones, for which she has full knowledge.

not depend on d, implying that almost perfect $d$its are obtained from ε-free bits. Hence, if $\varepsilon < \varepsilon_2$, not only we achieve RA, but also Randomness Expansion[13].

Remark 6.22. In [Gru+14], the authors recently managed to push this critical epsilon a bit further, from 0.0859 to 0.0961 in the $(2, m, 2)$ scenario. We finish this chapter by showing how, with a slight modification of the setup in [CR12] we can almost double the critical ε, by considering a common SV source. The key observation is that, out of the m^n measurement settings that are possible, only $2m^{n-1}$ are actually used in the AGCA inequality $I_{\mathbf{A}}^{n,m,d}$. Then, the number of bits that is necessary to generate all the settings is $r' := \lceil \log_2(2m^{n-1}) \rceil \leq 1 + (n-1)r$, a bit less than nr, which was the case in (6.61).

Hence, we have that

$$Q_r(\mathbf{x}) \leq \left(\frac{1+2\varepsilon}{1-2\varepsilon} \right)^{1+(n-1)r}, \tag{6.64}$$

which implies (using (6.62)) that randomness can be amplified as $m \to \infty$ if, and only if,

$$\varepsilon < \varepsilon'_n := \frac{1}{2} \frac{\sqrt[n-1]{2} - 1}{\sqrt[n-1]{2} + 1}. \tag{6.65}$$

In particular, this implies that the best scenario is the bipartite, for which $\varepsilon'_2 = 1/6$.

[13] The problem of Randomness Expansion is typically stated as follows: Given a finite sequence of perfectly random bits, one has to generate longer sequence of perfectly random bits. In our case, the parameter that we increase is the dimension of the $d$its that we are using: from 2 to d. We start, however, with imperfect bits, as they are given by a SV source. As we do not use an infinite amount of ε-free bits, we can achieve at the same time Randomness Amplification and Randomness Expansion.

7. Conclusions and outlook

Understanding entanglement and nonlocal correlations is one of the most relevant challenges in quantum information. Still, there is plenty of open questions in this field and, in this Thesis, we have answered some of them. In particular, we have focused on the characterization and the relation between those quantum information resources under symmetries. In this chapter, we review the obtained results and point towards future research directions that naturally follow.

7.1. PPT Entangled Symmetric States

We have solved the open question concerning the existence of 4-qubit PPT entangled symmetric states (PPTESS) by constructing families of quantum states with such properties and we have characterized these states with respect to separability, edgeness and extremality properties. We have seen that states of ranks other than $(5, 7, 7)$ or $(5, 7, 8)$ are generically not edge. By exploiting the geometric properties of the convex set of PPTESS we have generalized an algorithm [LMO07] to numerically generate extremal PPTESS. Interestingly, none of the extremal PPTESS found by this method have configurations of ranks $(5, 7, 7)$, suggesting that this case can also be ruled out.

Exploring scenarios involving more qubits, we have given several simple criteria under which extremal PPTESS can exist, classifying them with respect to their configurations of ranks, complementing the criterion in [Eck+02]. These criteria imply that, out of all the -in principle- possible configurations of ranks, most of them correspond to PPT symmetric states which are generically separable. Hence, PPT entanglement vanishes as the number of parties increases. Analysing edgness, even more of these configurations of ranks can be disregarded, and we have shown it for 4 and 5 qubits, for which there remain 2 and 3 configurations, respectively.

We have generated extremal PPTESS up to 23 qubits and, interestingly, numerics suggests that most of the allowed configurations of ranks are atypical, while the typical ones show some regularity (*cf.* Table 3.2), as well as that the most balanced bipartitions impose the most stringent PPT conditions. Can the characterization of PPTESS be ultimately reduced to few cases?

As extremal PPTESS are, geometrically, the most entangled within the PPTESS set, they are natural candidates to prove/disprove the Peres conjecture for symmetric states. If this conjecture were true, the characterization of extremal PPTESS could give some insight in its proof. If it were false, extremal PPTESS would constitute promising potential counterexamples.

7.2. Detection of nonlocality in many-body systems

We have shown that Bell inequalities with at most two-body correlators are sufficient to detect nonlocality in many-body systems. We have provided a detailed characterization of the polytope of local correlations when a general symmetry is considered. Of special interest are the Translationally Invariant (TI) and the Permutationally Invariant (PI) cases. In the TI case, we have shown the rich mathematical structure that already appears for a number of parties as low as 4 and we have classified all the Bell inequalities of this kind. In the PI case, we have found multiparametric, analytical classes of inequalities that are violated for any number of parties. We have studied its maximal quantum violation as well as the analytical form of the states and measurements achieving such maximally nonlocal correlations. Furthermore, these inequalities are shown to be robust with respect to imperfections such as misalignments, particle losses or white noise.

In the PI case, we have shown that the quantities needed to check nonlocality with the Bell inequalities we propose can be easily accessed from an experiment, with great precision and with currently available technology, simply by measuring global observables such as the total spin operator and its fluctuations (*cf.* Eqs. (4.142 - 4.144)) up to the second order moment.

Furthermore, we have shown that two-body Bell inequalities can reveal the nonlocality of every entangled Dicke state [Dic54]. Dicke states are important for at least two reasons: on the one hand, they can be prepared

in experiments; on the other hand, they arise as ground states of physically relevant models, such as Lipkin-Meshkov-Glick (LMG) Hamiltonians. Several experimental setups have been proposed in which such test could be carried out: Ultracold trapped atoms [Lüc+14; Mue+14], ultracold trapped ions [PC04; Bri+12; GL14], ultracold atoms in nanostructures [CCK13] or cold and ultracold atomic ensembles [Nap+11; Eck+08].

The next research lines point towards many directions: Are two-body Bell inequalities sufficient to reveal if correlations possess stronger forms of nonlocality, such as being Genuinely Multipartite Nonlocal (GMN)? To answer this question, one should find low-order Bell inequalities that detect Time-Ordered Bi-Local (TOBL) or No-Signalling Bi-Local (NSBL) correlations, possibly with some symmetries.

This procedure can be generalized to correlators up to full order, in which one would recover the inequalities in [BGP10] for a low number of parties. It can also be generalized to an arbitrary (n, m, d) Bell scenario. The parametrizations of the local polytope given in Chapter 4 indicate that one can also find classes of inequalities for these more general scenarios which work for any number of parties. An efficient method to do that would be to use Semi-Definite Program (SDP) techniques to approximate convex hulls of semialgebraic sets [BPT; GT].

The two-body form of the Bell inequalities we propose makes them specially interesting to be studied from a tensor network perspective. Specially, in the $1D$ case, one can apply a variety of techniques: dynamic programming turns out to be very useful procedure to efficiently compute the classical bound of Bell inequalities for many-body $1D$ systems [SC10], and one can employ Matrix Product States (MPS) or Density Matrix Renormalization Group (DMRG) numerical techniques to explore quantum properties of systems with a large number of parties. Even analytically, in the TI case, one can obtain results by mapping a two-body Bell operator to a quadratic fermionic Hamiltonian, which can be efficiently solved for some sets of observables. This is an ongoing project we are currently investigating.

7.3. Entanglement and nonlocality are inequivalent in general

We have provided a method which, starting from a n-partite GME quantum state admitting a Positive-Operator Valued Measure (POVM) K-local model, generates states which the same degree of locality, but involving a higher number of parties while still being Genuinely Multipartite Entangled (GME). This implies that entanglement and nonlocality are inequivalent concepts in any scenario, and we have shown this to be the case even if operational (TOBL, NSBL) definitions of GMN are taken into consideration.

The next question to ask is to which extent does this incompatibility hold. Up to day, only 2- and 3-local models are known. Which is the maximum value of K for which, for any n, there exist states n-partite states admitting a K-local model? A similar question is whether one can find GME states with a fully local model; *i.e.*, does GME become, at some point, too restrictive to allow for models which are fully local?

Other nonlocality scenarios have been considered: the network approach [Cav+11], many copies of a state [Pal12] or sequential measurements [Pop95; Gis96; Hir+13]. States that are local in one scenario may be nonlocal in others. It remains an interesting open question whether this inequivalence can be translated beyond the typical Bell scenario.

7.4. Atomic monogamies of correlations

We have presented a class of monogamy constraints of correlations compatible with any No-Signalling (NS) theory. They are qualitatively different than the existing ones, as they tightly relate the amount of nonlocality, measured as the amount of a Bell inequality violation, that a set of parties $\mathbf{A}$ observe, to the classical correlations that any external observer shares with the outcomes that are obtained by any of the parties.

These trade-off relations can be applied to Device-Independent Quantum Information Processing (DIQIP) protocols and they improve their performance. In particular, we have shown their usefulness for Device-Independent Quantum Key Distribution (DIQKD) and Randomness Amplification (RA), where we could prove that bipartite quantum correlations allow for RA for ε-free $d$its up to $\varepsilon < 1/6$.

We also derived monogamy relations for the $(3, 2, 2)$ scenario that Quantum Theory (QT) should fulfill. Can one derive elemental monogamy relations for a general (n, m, d) Bell scenario?

From a more fundamental point of view, it is interesting to consider the characterization of a minimal set of monogamy relations that enables one to recover QT or the NS principle.

A. Schur-Weyl duality

In this appendix we describe the construction of Schur duality as a tool in quantum information to efficiently work with permutationally invariant states. Good references from a quantum information perspective are [Har01; Chr06; Aud06] and for a mathematical and more general overview I would recommend [FH91; GW09].

The idea behind Schur-Weyl duality is to choose a *nice* basis of $(\mathbb{C}^d)^{\otimes n}$ such that a permutationally invariant state $\rho_{\mathbf{A}}$ has a simple form. It is clear that Condition (2.20) imposes a lot of redundancy in $\rho_{\mathbf{A}}$ and we want to pick a basis of $(\mathbb{C}^d)^{\otimes n}$ such that this redundancy becomes evident.

The tools used to this aim come from representation theory, which is a branch of mathematics that studies, loosely speaking, how to perform calculations in sets endowed with an algebraic structure, such as groups[1] (intuitively, if one can assign a matrix to every group element such that the product of matrices behaves exactly as the group operation, one has a representation of this group).

The groups that we are interested in are the Symmetric group $\mathfrak{S}_n$, which is the group of all permutations of n elements, and the Unitary group $\mathcal{U}_d$ consisting of all the $d \times d$ unitary matrices.

A.1. A crash course on representation theory

In this section we review the concepts of representation theory needed to introduce Schur-Weyl duality.

[1] Recall that a pair $(G, \circ)$ that consists of a set G endowed with a binary operation $\circ : G \times G \longrightarrow G$ defined as $(g_1, g_2) \mapsto \circ(g_1, g_2) \equiv g_1 \circ g_2$ is a group if the following requirements are met: The operation $\circ$ is associative: $\forall\, g_1, g_2, g_3 \in G$, $(g_1 \circ (g_2 \circ g_3)) = ((g_1 \circ g_2) \circ g_3)$, G has a neutral element, denoted e, that fulfills $g \circ e = e \circ g = g$ for every $g \in G$, and every element g in G has an inverse, denoted g^{-1}, that fulfills $g \circ g^{-1} = g^{-1} \circ g = e$. If $\circ$ is commutative, the group is called Abelian. When the operation is clear from the context, we denote the group simply by G.

Recall that a *morphism* (or *homomorphism*) between two groups $(G, \circ)$ and $(G', \times)$ is a function $f : G \longrightarrow G'$ such that for all $g_1, g_2 \in G$, $f(g_1 \circ g_2) = f(g_1) \times f(g_2)$. An invertible homomorphism is called an *isomorphism*.

Also, given a vector space V, the set of linear maps from V to itself is denoted $\mathrm{End}(V)$; such maps are called *endomorphisms*. Those endomorphisms which are invertible are called *automorphisms*; the set of automorphisms of from V to itself is denoted $\mathrm{Aut}(V)$ and it has the structure of a group. When V is finite-dimensional, $\mathrm{Aut}(V)$ is isomorphic to the *general linear group* $\mathrm{GL}(V)$ of invertible matrices acting on V.

Definition A.1. *A representation of a group G consists of a vector space V and a homomorphism $R : G \longrightarrow Aut(V)$ (i.e., for all $g_i, g_2 \in G$, $R(g_1)R(g_2) = R(g_1 g_2)$). It is denoted (R, V).*

If V is a $\mathbb{C}$-vector space, the representation R is called complex. If $R(g)$ is a unitary operator for all $g \in G$, then the representation is called unitary. In addition, if V is finite-dimensional, then (R, V) is finite-dimensional as well.

The connection between quantum information theory and representation theory lies in the fact that a complex vector space can be seen both as the state-space of a system and as a representation of a group. In addition, we want to study unitary representations, as the transformations allowed by quantum mechanics are unitary operators (thus we can assign to every group element a quantum operation). Finally, in practice, we are interested in finite-dimensional Hilbert spaces, so in this Thesis we will consider finite-dimensional representations. We shall, unless stated otherwise, refer to complex, unitary, finite-dimensional representations just as *representations*.

A linear subspace $W \subseteq V$ is *G-invariant* if, for all $g \in G$, $R(g)(W) \subseteq W$. Then, (R, W) is called a *subrepresentation* of G.

Definition A.2. *A representation (R, V) is irreducible, called irrep, if the only subrepresentations of G are (R, V) and $(R, \{0\})$.*

Hence, a representation being reducible indicates that there exist some bases which are more intrinsic to the action of that group. Let us illustrate this with an example.

Example A.3. *Consider $G = \mathfrak{S}_3$ acting on $V = \mathbb{C}^3$ and the representation that permutes the elements of the canonical basis of V: $R(\sigma)|e_i\rangle = |e_{\sigma^{-1}(i)}\rangle$. This representation is called standard and it is reducible: It suffices to express*

$R(\sigma)$ in the basis $|u_1\rangle = (|e_1\rangle + |e_2\rangle + |e_3\rangle)/\sqrt{3}$, $|u_2\rangle, |u_3\rangle \in |u_1\rangle^\perp$. We choose u_2, u_3 so that u forms an orthonormal basis: for example, $|u_2\rangle = (|e_1\rangle - |e_3\rangle)/\sqrt{2}$ and $|u_3\rangle = (|e_1\rangle - 2|e_2\rangle + |e_3\rangle)/\sqrt{6}$. Then, in the u basis, the elements of $\mathfrak{S}_3$ are represented as follows[2]:

$(1)(2)(3)$	(123)	(132)
$\begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & & \\ & -1/2 & \sqrt{3}/2 \\ & -\sqrt{3}/2 & -1/2 \end{pmatrix}$	$\begin{pmatrix} 1 & & \\ & -1/2 & -\sqrt{3}/2 \\ & \sqrt{3}/2 & -1/2 \end{pmatrix}$
$(12)(3)$	$(13)(2)$	$(1)(23)$
$\begin{pmatrix} 1 & & \\ & 1/2 & -\sqrt{3}/2 \\ & -\sqrt{3}/2 & -1/2 \end{pmatrix}$	$\begin{pmatrix} 1 & & \\ & -1 & \\ & & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & & \\ & 1/2 & \sqrt{3}/2 \\ & \sqrt{3}/2 & -1/2 \end{pmatrix}$

(A.1)

There are three irreducible representations for $\mathfrak{S}_3$: two are one-dimensional (the trivial one, $R(\sigma) = 1$ and the alternating one $R(\sigma) = \operatorname{sgn}(\sigma)$) and one is two-dimensional (given by the lower-right 2×2 boxes in (A.1)). In fact, (A.1) shows that $\mathbb{C}^3 \cong W \oplus W^\perp$, where W is spanned by $|u_1\rangle$ and both W and $W^\perp$ are irreducible subrepresentations.

Schur's lemma

An important concept in representation theory are the automorphisms of a representation, which measure to which extent the decomposition of a representation into irreps is unique; *i.e.*, given $R(g)$, one can change the basis in which $R(g)$ is expressed and obtain a different representation. However, loosely speaking, this is nothing but staring at the same representation from another perspective.

[2] Recall that a permutation σ can be uniquely expressed as a product of disjoint cycles (up to permutations of the cycles). This is the notation we used in (A.1). A cycle (abc) stands for a permutation $a \mapsto b \mapsto c \mapsto a$. Two permutations $\pi, \rho \in \mathfrak{S}_n$ have the same *cycle type* if they decompose in products of cycles of the same number of elements. A cycle of 2 elements is called a *transposition*. Because of the identity $(a, a_k) \circ (a_1, \ldots, a_k, \ldots, a_m) \circ (a_k, a) = (a_1, \ldots, a, \ldots, a_m)$ and the fact that every permutation decomposes as a product of transpositions (non-uniquely), ρ and σ have the same cycle type if, and only if, they are *conjugate*; *i.e.*, $\rho = \sigma^{-1}\pi\sigma$ for some $\sigma \in \mathfrak{S}_n$. Although the decomposition of a permutation σ as a product of transpositions is non-unique, it always has the same parity, so one can define the *sign* of σ, denoted $\operatorname{sgn}(\sigma)$, as $(-1)^{t(\sigma)}$, where $t(\sigma)$ counts the number of transpositions in a decomposition of σ.

One can readily check that the matrices in (A.1) behave as the permutations they represent when we multiply them.

Given a representation (R, V), one defines the subspace V^G to be the set of $G-$invariant vectors of V; *i.e.*, $V^G = \{|v\rangle \in V : \forall g \in G,\ R(g)|v\rangle = |v\rangle\}$. In particular, given representations V_1 and V_2, the set $\mathrm{Hom}(V_1, V_2)^G$ of $G-$invariant homomorphisms contains the homomorphisms from V_1 to V_2 which commute with the action of G: $\mathrm{Hom}(\mathrm{V_1}, \mathrm{V_2})^G = \{U \in \mathrm{Hom}(V_1, V_2) : \forall g \in G,\ UR_1(g) = R_2(g)U\}$.

When $\mathrm{Hom}(V_1, V_2)^G$ contains invertible elements, this motivates the concept of equivalence in representations:

Definition A.4. *Two representations (R_1, V_1) and (R_2, V_2) are equivalent if there is a change of basis $U : V_1 \longrightarrow V_2$ such that, for all $g \in G$, $UR_1(g)U^{-1} = R_2(g)$. We write then $(R_1, V_1) \cong_G (R_2, V_2)$.*

Proposition A.5. *For a finite group G, one can always decompose a representation V as $V \cong \bigoplus_i W_i$, where W_i are irreps.*

Proof. For any $G-$invariant subspace $W \subseteq V$, then $W^\perp$, its orthogonal complement, is also $G-$invariant: Indeed, any scalar product (w_1, w_2) in V can be *averaged over* G to obtain a new $G-$invariant scalar product in V, which is

$$\langle w_1, w_2\rangle = |G|^{-1} \sum_{g\in G} (R(g)w_1, R(g)w_2). \tag{A.2}$$

Now, take $w_1 \in W$, $w_2 \in W^\perp$. We want to see that $W^\perp$ is $G-$invariant (*i.e.*, $\langle w_1, R(g)w_2\rangle = 0$ for all $g \in G$). Because W is a subrepresentation of V (it is $G-$invariant), $0 = \langle w_1, w_2\rangle = \langle R(g^{-1})w_1, w_2\rangle$. Because (A.2) is a $G-$invariant scalar product, $\langle w_1, R(g)w_2\rangle = 0$ by multiplying both entries by $R(g)$.
Hence, $V = W \oplus W^\perp$. One can repeat this procedure until all the W_i are irreps, which will eventually happen, as $\dim V$ is finite. □

Schur's lemma, which is probably the most used result in representation theory, and it states the following:

Lemma A.6 (Schur's lemma)**.** *Consider two irreps V and W of a group G. Consider also $\varphi \in \mathrm{Hom}(V, W)^G$. Then,*

- *φ is either 0 or an isomorphism.*
- *If $V = W$, then $\varphi = \lambda\mathbb{1}$ for some $\lambda \in \mathbb{C}$.*

Proof. Because V is irreducible and $\ker\varphi$ is a $G-$invariant subspace, it can only be $\{0\}$ or V. The same applies to W and $\mathrm{Im}\varphi$. This proves the first part. Now pick an eigenvalue $\lambda \in \mathbb{C}$, which exists because $\mathbb{C}$ is an algebraically closed field. Then $\ker\varphi - \lambda\mathbb{1}$ has dimension at least 1, so $\varphi - \lambda\mathbb{1}$ cannot be an isomorphism. However, it is clearly $G-$invariant, so we apply the first part of the lemma to it and obtain $\varphi - \lambda\mathbb{1} = 0$. □

By virtue of Schur's lemma, grouping the subspaces in the decomposition $V \cong \bigoplus_i W_i$ from Proposition A.5 into isomorphic components, one obtains the so-called *isotypical decomposition*:

$$V \cong \bigoplus_k W_k^{\oplus n_k} \cong \bigoplus_k W_k \otimes \mathbb{C}^{n_k}, \tag{A.3}$$

where W_k are the so-called *isotypical components* and n_k is the multiplicity of the corresponding isotypical component. The index k runs over a set of inequivalent irreps of V. The vector space $\mathbb{C}^{n_k}$ is called the *multiplicity space*, and it is isomorphic to $\mathrm{Hom}(W_k, V)^G$ [GW09].

The character of a representation

When one considers $R(g)$ for some $g \in G$, one obtains a matrix whose elements are basis-dependent. However, we would like to work with some elements which better grasp the intrinsic features of G; *i.e.*, they are basis-independent, or *invariants*. The best known invariants of an endomorphism are the symmetric functions of its eigenvalues, *i.e.*, the coefficients of the characteristic polynomial $\det_V(\lambda\mathbb{1} - R(g))$. For example, the map $g \mapsto \det R(g)$ gives a $1-$dimensional representation of G; however it turns out to be too weak to distinguish isomorphism classes of representations. The invariant which is convenient to work with is the trace.

Definition A.7. *The character of a representation (R, V) is the function $\chi : G \longrightarrow \mathbb{C}$ defined as $\chi_V(g) = \mathrm{Tr}R(g)|_V$.*

A strong result in representation theory is that χ completely determines R up to isomorphism. Furthermore, χ_V is a *class function*, meaning that it is constant on the conjugacy classes of G: $\chi_V(R(h)R(g)R(h^{-1})) = \chi_V(R(g))$ for all $h \in G$, so one needs just to specify χ on the conjugacy classes of G, which we denote as $[g]$.

One can then construct the so-called character table χ, which is a matrix whose elements are $(\chi)^{\lambda}_{[g]} = \chi_\lambda(g)\ \forall g \in [g]$; λ runs over the irreps and $[g]$ over the conjugacy classes of G. An auxiliary row is added to the character table, containing the number of elements in each conjugacy class, typically denoted $h_{[g]}$.

Let us illustrate its use with an example, following the previous one of $G = \mathfrak{S}_3$.

Example A.8. *For the Symmetric group $\mathfrak{S}_n$ it is easy to identify its conjugacy classes. Recall that two permutations are conjugated if, and only if, they have the same cycle type, implying that there are as many conjugacy classes as partitions of n. We will denote a partition of n in k elements $\lambda \vdash (k, n)$. Its elements will be specified as $\lambda = (1^{m_1} 2^{m_2} \dots r^{m_r} \dots)$ and we define $\lambda^i = m_i(\lambda)$ (the number of times that i appears in the partition λ). Clearly one has the relations $\sum_{i=1}^n \lambda^i = k$ and $\sum_{i=1}^n i\lambda^i = n$.*

The number of elements in the conjugacy class $[\sigma]$ (note that we can use $[\sigma]$ and λ indistinctly) is given by the function $h_{[\sigma]} = n! z_\lambda^{-1}$, where $z_\lambda = \lambda^1! 1^{\lambda^1} \lambda^2! 2^{\lambda^2} \cdots \lambda^n! n^{\lambda^n}$, as one has $\lambda^k!$ ways to rearrange the λ^k cycles of k elements and each cycle of k elements admits k independent cyclic permutations, providing the factor k^{λ^k}.

We now go a bit ahead of ourselves and use the fact that the irreps of $\mathfrak{S}_n$ are given by the partitions of n, hence the character table χ is a square matrix.

$\lambda \setminus [g]$	(3^1)	$(1^1 2^1)$	(1^3)
$h_{[g]}$	2	3	1
(3^1)	1	1	1
$(1^1 2^1)$	-1	0	2
(1^3)	1	-1	1

(A.4)

It is worth to compare (A.4) with Example A.3. The irrep (3) corresponds to the trivial representation W, whereas (1^3) corresponds to the sign representation. Finally, the irrep $(1^1 2^1)$ corresponds to $W^\perp$.

A.2. The Symmetric and the Unitary groups

The groups that are relevant for permutationally invariant quantum states are the Symmetric group $\mathfrak{S}_n$ of permutations of n elements, and the Unitary

group $\mathcal{U}_d$ of $d \times d$ unitary matrices. The representation we are interested in is the Hilbert space of n qudits, namely $\mathcal{H} = (\mathbb{C}^d)^{\otimes n}$. Both groups act naturally on $\mathcal{H}$: for all $\sigma \in \mathfrak{S}_n$ and for all $U \in \mathcal{U}_d$ one defines

$$\Pi_\sigma |i_1 \dots i_n\rangle = |i_{\sigma^{-1}(1)} \dots i_{\sigma^{-1}(n)}\rangle \tag{A.5}$$

and

$$\Xi_U |i_1 \dots i_n\rangle = U|i_1\rangle \cdots U|i_n\rangle. \tag{A.6}$$

Hence, we are considering $(\Pi, \mathcal{H})$ and $(\Xi, \mathcal{H})$ as representations of $\mathfrak{S}_n$ and $\mathcal{U}_d$, respectively. The fact that $\Pi_\sigma \Xi_U = \Xi_U \Pi_\sigma$ for all permutations σ and unitaries U immediately follows from the definitions (A.5, A.6). Schur's lemma then implies that the isotypical decompositions of Π and Ξ, namely

$$(\Pi_\sigma, \mathcal{H}) \cong_{\mathfrak{S}_n} \bigoplus_a \mathbb{1}_{n_a} \otimes \pi_{\sigma,a} \tag{A.7}$$

and

$$(\Xi_U, \mathcal{H}) \cong_{\mathcal{U}_d} \bigoplus_b \mathbb{1}_{m_b} \otimes \xi_{U,b}, \tag{A.8}$$

where $\pi_{\sigma,a}$ and $\xi_{U,b}$ are irreps of multiplicities n_a and m_b of $(\Pi, \mathcal{H})$ and $(\Xi, \mathcal{H})$, respectively, are related: The same basis that produces the decomposition of Π_σ also produces the decomposition of Ξ_U. Indeed, one considers the simultaneous action[3] of Π and Ξ on $\mathcal{H}$

$$\Pi_\sigma \Xi_U \cong_{\mathfrak{S}_n \times \mathcal{U}_d} \bigoplus_{a,b} \mathbb{1}_{\nu_{a,b}} \otimes \pi_{\sigma,a} \otimes \xi_{U,b}, \tag{A.9}$$

where $\nu_{a,b}$ is the multiplicity of irrep[4] $\pi_{\sigma,a} \otimes \xi_{U,b}$.

When one considers the $\mathbb{C}$-vector space whose basis elements are the elements of the group, one obtains an algebra (the so-called *group algebra*) in which the multiplication is the (left) multiplication of the group

[3] Technically, one has to consider the *direct product group* $\mathfrak{S}_n \times \mathcal{U}_d$ as we choose both a permutation and a unitary. It is simply the set of pairs (σ, U) with the corresponding group operation applied to each component independently.

[4] Note that the tensor product $(R_1 \otimes R_2, V_1 \otimes V_2)$ of two irreps (R_1, V_1), (R_2, V_2) of G, as another representation of G is, in general, not an irrep (the typical example being the Clebsch-Gordan decomposition). However, for the direct product group $G \times H$ of two compact groups G and H, the whole list of irreps consists of the tensor products of the irreps of G and H.

elements. The group algebra is usually denoted $\mathbb{C}[G]$ and it turns out that the algebra generated by $\{\Pi_\sigma\}_{\sigma\in\mathfrak{S}_n}$, denoted $\mathcal{A}$ and the algebra generated by $\{\Xi_U\}_{U\in\mathcal{U}_d}$, denoted $\mathcal{B}$, are each other centralizer[5] (a result known as the *double commutant theorem*, [GW09]).

This fact radically simplifies (A.9), for it implies that, not only Π and Ξ commute, but $\nu_{a,b}$ can be only 0 or 1 and each a and b appear no more than once. Thus, one finally obtains [GW09]

Theorem A.9 (Schur-Weyl duality)**.** *Consider $\mathcal{H} = (\mathbb{C}^d)^{\otimes n}$ and the natural representations Π and Ξ of $\mathfrak{S}_n$ and $\mathcal{U}_d$, respectively. Then, one has the decomposition*

$$\mathcal{H} \cong \bigoplus_{\lambda\vdash(d,n)} \mathcal{K}_\lambda \otimes \mathcal{H}_\lambda \tag{A.10}$$

$$\Pi_\sigma = \bigoplus_{\lambda\vdash(d,n)} \mathbb{1}_{\mathcal{K}_\lambda} \otimes \pi_{\sigma,\lambda} \tag{A.11}$$

$$\Xi_U = \bigoplus_{\lambda\vdash(d,n)} \xi_{U,\lambda} \otimes \mathbb{1}_{\mathcal{H}_\lambda} \tag{A.12}$$

in which $(\xi_{\cdot,\lambda}, \mathcal{K}_\lambda)$ and $(\pi_{\cdot,\lambda}, \mathcal{H}_\lambda)$ are irreps of $\mathcal{U}_d$ and $\mathfrak{S}_n$ respectively and $\lambda\vdash(d,n)$ runs over all partitions of n with at most d elements.

By varying d in the labelling $\lambda \vdash (d,n)$ one enumerates the different irreps $(\pi_\lambda, \mathcal{H}_\lambda)$ of $\mathfrak{S}_n$, whereas a variation of n enumerates the polynomial[6] irreps $(\xi_\lambda^{(d)}, \mathcal{K}_\lambda^{(d)})$ of $\mathcal{U}_d$.

Let us finish by illustrating this construction with an example.

Example A.10. *Let us consider the case of three qubits; i.e., $n = 3$, $d = 2$; equivalently, $\mathcal{H} = (\mathbb{C}^2)^{\otimes 3}$. Following the notation introduced in Example A.8, there are two partitions of 3 into 2 elements, which we denote (3^1) and $(1^1 2^1)$. Then, Theorem A.9 tells that $(\mathbb{C}^2)^{\otimes 3} \cong \mathcal{K}^{(2)}_{(3^1)} \otimes \mathcal{H}_{(3^1)} \oplus \mathcal{K}^{(2)}_{(1^1 2^1)} \otimes \mathcal{H}_{(1^1 2^1)}$.*

We have that $\Pi_{(3^1)}$ is the trivial representation of $\mathfrak{S}_3$, so it is one-dimensional. On the other hand, $\mathcal{K}^{(2)}_{(3^1)}$ is a four-dimensional irrep of $\mathcal{U}_2$, which is spanned

[5] The *centralizer* of G, denoted G', is the set of elements that commute with each element of G: $G' = \{g \in G : \forall h \in G,\ g \circ h = h \circ g\}$.

[6] A superindex (d) is in fact needed, as the same partition $\lambda \vdash (d,n)$ may label different irreps for different $\mathcal{U}_d$, whereas for $\mathfrak{S}_n$ one always has $\sum_i \lambda_i = n$.

by the 3-qubit Dicke states $\{|D_3^k\rangle\}_{k=0\ldots3}$ *defined in Eq. (2.27), which are*

$$|0\rangle^{\otimes 3}, \quad |W\rangle, \quad |\overline{W}\rangle, \quad |1\rangle^{\otimes 3}, \tag{A.13}$$

where $|W\rangle = (|001\rangle + |010\rangle + |100\rangle)/\sqrt{3}$ *and* $|\overline{W}\rangle$ *is the same as* $|W\rangle$ *but changing* 0 *to* 1 *and vice-versa.*

It is convenient, for any partition λ*, to fix an index over the basis of the irrep of the Unitary group, say* m_λ*, and an index over the basis of the Symmetric group, say* α_λ*, in order to easily enumerate the elements of the basis corresponding to* λ*, so that the Schur basis vectors are denoted as* $|\lambda, m_\lambda, \alpha_\lambda\rangle$*. Usually,* m_λ *is taken to be* $m_\lambda \in \{-(\dim \mathcal{K}_\lambda^{(2)} - 1)/2, \ldots, (\dim \mathcal{K}_\lambda^{(2)} - 1)/2\}$*;* α *is taken to be* $\alpha_\lambda \in \{0, \ldots, \dim \mathcal{H}_\lambda - 1\}$*. So, for the block* $\lambda = (3^1)$ *one simply has* $|D_3^k\rangle = |(3^1), 3/2 - k, 0\rangle$*.*

For the $(1^1 2^1)$ *partition, the* $\mathcal{K}^{(2)}_{(1^1 2^1)}$ *component corresponds to a two-dimensional irrep of* $\mathcal{U}_2$ *and* $\mathcal{H}_{(1^1 2^1)}$ *to a two-dimensional irrep of* $\mathfrak{S}_3$*. Its basis elements are given by*

$$\begin{array}{rcl} |(1^1 2^1), 1/2, 0\rangle & = & \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle) \otimes |0\rangle \\ |(1^1 2^1), -1/2, 0\rangle & = & \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle) \otimes |1\rangle \end{array} \tag{A.14}$$

and

$$\begin{array}{rcl} |(1^1 2^1), 1/2, 1\rangle & = & \sqrt{\frac{2}{3}}|001\rangle - \frac{(|10\rangle + |01\rangle) \otimes |0\rangle}{\sqrt{6}} \\ |(1^1 2^1), -1/2, 1\rangle & = & \sqrt{\frac{2}{3}}|110\rangle - \frac{(|10\rangle + |01\rangle) \otimes |1\rangle}{\sqrt{6}}. \end{array} \tag{A.15}$$

In the particular case of qubits, the partitions of n into 2 elements are easy to enumerate, so that any permutationally invariant qubit operator ρ, when expressed in the Schur basis, can be written as

$$\rho = \bigoplus_{J=J_0}^{n/2} \frac{p_J}{\dim \mathcal{H}_J} \mathbb{1}_{\dim \mathcal{H}_J} \otimes \rho_J, \tag{A.16}$$

where ρ_J is a density operator, p_J forms a probability distribution and $\dim \mathcal{H}_J$ is 1 if $J = n/2$ and

$$\dim \mathcal{H}_J = \binom{n}{n/2 - J} - \binom{n}{n/2 - J - 1} \tag{A.17}$$

otherwise. Hence, in order to describe ρ, one just needs to know ρ_J, which have a size $(2J+1) \times (2J+1)$, which is $O(n)$, instead of the $2^n \times 2^n$ size of ρ. The blocks ρ_J are obtained from the projection of ρ onto the elements of the Schur basis indexed by $|J, m, 0\rangle$, (so one does not even need to construct the whole Schur basis for that) which are given by

$$\{|D_{2J}^k\rangle \otimes |\psi^-\rangle^{\otimes \frac{n-2J}{2}}\}_{k=0\ldots 2J}, \tag{A.18}$$

where $|\psi^-\rangle$ is the singlet state $|\psi^-\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$.

B. Additional Proofs

In this appendix we give the proofs of theorems which were either too long or technical to be included in the main text.

We begin by discussing what is the form, in the block-decomposition given by the Schur-Weyl basis (A.18), of S_u and S_{uv} for $u, v \in \{x, y, z\}$, which are defined as

$$S_u := \sum_{i=0}^{n-1} \sigma_k^{(i)}, \qquad S_{uv} = \sum_{\substack{i,j=0 \\ i \neq j}}^{n-1} \sigma_k^{(i)} \otimes \sigma_l^{(j)}, \tag{B.1}$$

where σ_x, σ_y and σ_z are the Pauli matrices.

Theorem B.1. *Let us define $m = n - 2J$ and let us denote $|\xi_{k,J}\rangle := |D_{2J}^k\rangle \otimes |\psi^-\rangle^{\otimes m/2}$, as in (A.18). Then, the J-th block ρ_J of S_u or S_{uv}, where $u, v \in \{x, y, z\}$, in the form (A.16) is given by*

$$\begin{aligned}
&\langle \xi_{k,J}|S_x|\xi_{l,J}\rangle \\
&\quad = \sqrt{(l+1)(2J-l)}\delta(k-l-1) + \sqrt{(k+1)(2J-k)}\delta(l-k-1) \\
&\langle \xi_{k,J}|S_y|\xi_{l,J}\rangle = \mathbb{i} \cdot \operatorname{sgn}(k-l)\langle \xi_{k,J}|S_x|\xi_{l,J}\rangle \\
&\langle \xi_{k,J}|S_z|\xi_{l,J}\rangle = (2J-2k)\delta(k-l) \\
&\langle \xi_{k,J}|S_{xx}|\xi_{l,J}\rangle = (2k(2J-k)-m)\delta(k-l) \\
&\quad + \sqrt{(l+1)(l+2)(2J-l)(2J-l-1)}\delta(k-l-2) \\
&\quad + \sqrt{(k+1)(k+2)(2J-k)(2J-k-1)}\delta(l-k-2) \\
&\langle \xi_{k,j}|S_{xy}|\xi_{l,J}\rangle \\
&\quad = \mathbb{i} \cdot \operatorname{sgn}(k-l)\sqrt{(l+1)(l+2)(2J-l)(2J-l-1)}\delta(k-l-2) \\
&\quad + \mathbb{i} \cdot \operatorname{sgn}(k-l)\sqrt{(k+1)(k+2)(2J-k)(2J-k-1)}\delta(l-k-2) \\
&\langle \xi_{k,J}|S_{xz}|\xi_{l,J}\rangle \\
&\quad = (2J-1-2l)\sqrt{(2J-l)(l+1)}\delta(k-l-1) \\
&\quad + (2J-1-2k)\sqrt{(2J-k)(k+1)}\delta(l-k-1)
\end{aligned}$$

$$\begin{aligned}
&\langle \xi_{k,J}|S_{yy}|\xi_{l,J}\rangle = (2k(2J-k)-m)\delta(k-l) \\
&\quad -\sqrt{(l+1)(l+2)(2J-l)(2J-l-1)}\delta(k-l-2) \\
&\quad -\sqrt{(k+1)(k+2)(2J-k)(2J-k-1)}\delta(l-k-2) \\
&\langle \xi_{k,J}|S_{yz}|\xi_{l,J}\rangle \\
&\quad = \mathbb{i}\cdot \mathrm{sgn}(k-l)(2J-1-2l)\sqrt{(2J-l)(l+1)}\delta(k-l-1) \\
&\quad +\mathbb{i}\cdot \mathrm{sgn}(k-l)(2J-1-2k)\sqrt{(2J-k)(k+1)}\delta(l-k-1) \\
&\langle \xi_{k,J}|S_{zz}|\xi_{l,J}\rangle = ((2J-2k)^2-2J-m)\delta(k-l),
\end{aligned} \tag{B.2}$$

where $0 \leq k,l \leq m$*,* δ *is the Kronecker delta function, defined as*

$$\delta(a) = \begin{cases} 1 & \textit{if} \quad a=0 \\ 0 & \textit{else} \end{cases}, \tag{B.3}$$

and sgn *is the sign function.*

Proof. Let us begin by introducing a bit of notation which shall help in keeping calculations simpler. Let us denote $(A)^{\mathbf{i}}_{\mathbf{j}} := \langle \mathbf{i}|A|\mathbf{j}\rangle$; *i.e.*, the $\mathbf{i}$-th row, $\mathbf{j}$-th column of a $2^n \times 2^n$ size matrix A, $0 \leq \mathbf{i},\mathbf{j} < 2^n$.

We shall represent $\mathbf{i}$ in binary $\mathbf{i} = i_0 i_1 \dots i_{n-1}$, with its digits being $i_k \in \{0,1\}$, and the same for $\mathbf{j}$. We refer to i_k as *bits* and to $\mathbf{i}$ as *words*. The *weight* of $\mathbf{i}$ is the number of ones in its binary representation, and it is denoted $|\mathbf{i}| := |\{i_k : i_k = 1\}|$. A natural operation to perform in binary words is the bit-wise XOR function, which is the bit-wise addition *modulo* 2, $\mathbf{i}\oplus\mathbf{j} := (i_0 \oplus j_0)(i_1 \oplus j_1)\cdots(i_{n-1}\oplus j_{n-1})$. The *Hamming distance* between two words is the number of bits in which they differ: two words $\mathbf{i}$ and $\mathbf{j}$ are at Hamming distance k if $|\mathbf{i}\oplus\mathbf{j}| = k$.

As a first step, let us derive the expression of (B.1) in the computational basis.

- $(S_x)^{\mathbf{i}}_{\mathbf{j}} = \delta(|\mathbf{i}\oplus\mathbf{j}|-1)$.
  As $(\sigma_x^{(v)})^{\mathbf{i}}_{\mathbf{j}}$ has nonzero entries (actually, their value is either 0 or 1) on those elements whose indices satisfy $i_a \oplus j_a = \delta(a-v)$ for all $0 \leq a < n$. This implies that $\mathbf{i}$ and $\mathbf{j}$ only differ in the bit that corresponds to the party in which σ_x is applied. Recall that $\sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|$, and this bit difference is a consequence of this form. The result follows by summing over all parties v.

- $(S_y)^{\mathbf{i}}_{\mathbf{j}} = \mathbb{i}\cdot\mathrm{sgn}(\mathbf{i}-\mathbf{j})\delta(|\mathbf{i}\oplus\mathbf{j}|-1)$.
  The same reasoning as in S_x applies here, with a minor difference:

as we have the form of $\sigma_y = -\mathbb{i}|0\rangle\langle 1| + \mathbb{i}|1\rangle\langle 0|$, the elements above the diagonal are multiplied by $-\mathbb{i}$ whereas the elements below the diagonal are multiplied by $\mathbb{i}$.

- $(S_z)^{\mathbf{i}}_{\mathbf{j}} = (n - 2|\mathbf{i}|)\delta(\mathbf{i} - \mathbf{j})$.
  Exploiting the fact that σ_z is diagonal and, when we sum $\sigma_z^{(v)}$ over all the parties (indiced by v), those indices $\mathbf{i}$ with a 0 in the v-th bit (*i.e.,* $i_v = 0$) get a contribution of $+1$, whereas the bits with $i_v = 1$ get a contribution of -1, the result follows.

- $(S_{xx})^{\mathbf{i}}_{\mathbf{j}} = 2\delta(|\mathbf{i} \oplus \mathbf{j}| - 2)$.
  Let us first make this observation: $(\sigma_x^{(v)}\sigma_x^{(w)})^{\mathbf{i}}_{\mathbf{j}} = \delta((\mathbf{i} \oplus \mathbf{j}) - (2^v + 2^w))$. This condition is telling us that the bits in the positions v and w of $\mathbf{i}$ and $\mathbf{j}$ must be different. We obtain the result by summing over all (ordered) pairs of parties v and w.

- $(S_{xy})^{\mathbf{i}}_{\mathbf{j}} = \mathbb{i} \cdot \mathrm{sgn}(\mathbf{i} - \mathbf{j})(1 - (-1)^{\frac{|\mathbf{i}|-|\mathbf{j}|}{2}})\delta(|\mathbf{i} \oplus \mathbf{j}| - 2)$.
  It is convenient to start with computing the value of $(\sigma_x^{(v)}\sigma_y^{(w)})^{\mathbf{i}}_{\mathbf{j}}$. Observe that the identities $(\sigma_x^{(v)})^{\mathbf{i}}_{\mathbf{j}} = \delta((\mathbf{i} \oplus \mathbf{j}) - 2^v)$ and $(\sigma_y^{(w)})^{\mathbf{i}}_{\mathbf{j}} = -\mathbb{i}\mathrm{sgn}(\mathbf{i} - \mathbf{j})\delta((\mathbf{i} \oplus \mathbf{j}) - 2^w)$ hold. Then,

$$\begin{aligned}(\sigma_x^{(v)}\sigma_y^{(w)})^{\mathbf{i}}_{\mathbf{j}} &= \sum_{\mathbf{k}} (\sigma_x^{(v)})^{\mathbf{i}}_{\mathbf{k}} (\sigma_y^{(w)})^{\mathbf{k}}_{\mathbf{j}} \\ &= -\mathbb{i} \sum_{\mathbf{k}} \delta((\mathbf{i} \oplus \mathbf{k}) - 2^v)\delta((\mathbf{k} \oplus \mathbf{j}) - 2^w)\mathrm{sgn}(\mathbf{k} - \mathbf{j}). \qquad \text{(B.4)}\end{aligned}$$

  Now consider the factor $\delta((\mathbf{k} \oplus \mathbf{j}) - 2^w)\mathrm{sgn}(\mathbf{k} - \mathbf{j})$. Since $\mathbf{k}$ and $\mathbf{j}$ only differ in the w-th bit, the sign of $\mathbf{k} - \mathbf{j}$ must be positive whenever $j_w = 0$ ($k_w = 1$) and negative whenever $j_w = 1$ ($k_w = 0$). Consequently, one can express $\delta((\mathbf{k} \oplus \mathbf{j}) - 2^w)\mathrm{sgn}(\mathbf{k} - \mathbf{j})$ as $\delta((\mathbf{k} \oplus \mathbf{j}) - 2^w)(\delta(j_w) - \delta(j_w - 1))$, which is $\delta((\mathbf{k} \oplus \mathbf{j}) - 2^w)(-1)^{j_w}$.

$$\begin{aligned}(\sigma_x^{(v)}\sigma_y^{(w)})^{\mathbf{i}}_{\mathbf{j}} &= -\mathbb{i}(-1)^{j_w} \sum_{\mathbf{k}} \delta((\mathbf{i} \oplus \mathbf{k}) - 2^v)\delta((\mathbf{k} \oplus \mathbf{j}) - 2^w) \\ &= -\mathbb{i}(-1)^{j_w} (\sigma_x^{(v)}\sigma_x^{(w)})^{\mathbf{i}}_{\mathbf{j}}. \qquad \text{(B.5)}\end{aligned}$$

  Hence,

$$(\sigma_x^{(v)}\sigma_y^{(w)})^{\mathbf{i}}_{\mathbf{j}} = -\mathbb{i}(-1)^{j_w}\delta((\mathbf{i} \oplus \mathbf{j}) - (2^v + 2^w)). \qquad \text{(B.6)}$$

Our aim now is to sum, over all ordered pairs of particles (v, w), the expression (B.6). A useful way to perform this sum is to group the terms (v, w) with (w, v):

$$\begin{aligned}(S_{xy})^{\mathbf{i}}_{\mathbf{j}} &= \sum_{v\neq w} (\sigma_x^{(v)}\sigma_y^{(w)})^{\mathbf{i}}_{\mathbf{j}} \\ &= -\mathbb{i}\sum_{0\leq v<w<n} \left((-1)^{j_w} + (-1)^{j_v}\right)\delta((\mathbf{i}\oplus\mathbf{j}) - (2^v + 2^w)).\end{aligned} \tag{B.7}$$

The term $(-1)^{j_w} + (-1)^{j_v}$ can take only 3 different values, depending on j_w and j_v: It will be 0 whenever $j_v \neq j_w$, it will be 2 whenever $j_v = j_w = 0$ and it will be -2 whenever $j_v = j_w = 1$. However, only the terms for which $i_v \neq j_v$ and $i_w \neq j_w$ really count in the sum (B.7). This enables us to substitute (B.7) by the following expression:

$$\begin{aligned}(S_{xy})^{\mathbf{i}}_{\mathbf{j}} &= -\mathbb{i}\sum_{0\leq v<w<n} \left(1 - (-1)^{\frac{|\mathbf{i}|-|\mathbf{j}|}{2}}\right)\operatorname{sgn}(\mathbf{i}-\mathbf{j})\delta((\mathbf{i}\oplus\mathbf{j}) - (2^v + 2^w)) \\ &= -\mathbb{i}\left(1 - (-1)^{\frac{|\mathbf{i}|-|\mathbf{j}|}{2}}\right)\operatorname{sgn}(\mathbf{i}-\mathbf{j})(S_{xx})^{\mathbf{i}}_{\mathbf{j}}/2.\end{aligned} \tag{B.8}$$

Now we can apply the same argument that we did for $(S_{xx})^{\mathbf{i}}_{\mathbf{j}}$ and the result follows.

- $(S_{xz})^{\mathbf{i}}_{\mathbf{j}} = (n - |\mathbf{i}| - |\mathbf{j}|)\delta(|\mathbf{i}\oplus\mathbf{j}| - 1)$.
  In this case, we exploit the identity $S_{xz} = S_xS_z - \sum_{v=0}^{n-1}(\sigma_x\sigma_z)^{(v)}$. Because the multiplication of σ_x and σ_z has the following form:

$$\sigma_x\sigma_z = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \tag{B.9}$$

  $\sum_{v=0}^{n-1}(\sigma_x\sigma_z)^{(v)}$ behaves almost like S_x, with the only difference being that there is a -1 instead of a 1 above the diagonal. Now, we can write

$$\left(\sum_{v=0}^{n-1}(\sigma_x\sigma_z)^v\right)^{\mathbf{i}}_{\mathbf{j}} = \operatorname{sgn}(\mathbf{i}-\mathbf{j})\delta(|\mathbf{i}\oplus\mathbf{j}| - 1) = (|\mathbf{i}| - |\mathbf{j}|)\delta(|\mathbf{i}\oplus\mathbf{j}| - 1), \tag{B.10}$$

where, to derive the last equality, we have used the following fact: Given a number $\mathbf{j}$, a number $\mathbf{i}$ which is both greater than $\mathbf{j}$ and at Hamming distance 1 from this $\mathbf{j}$, can be constructed only in one way; namely, by changing one of the 0 bits of $\mathbf{j}$ to 1, so that $|\mathbf{i}| = |\mathbf{j}| + 1$ and its value increases. The opposite happens when we want to get a lower number: we turn one of the 1 bits of $\mathbf{j}$ to 0, hence lowering its weight by 1 and its value. Now we can derive the result by performing a simple calculation:

$$\begin{aligned}(S_{xz})^{\mathbf{i}}_{\mathbf{j}} &= \sum_{\mathbf{k}} \left((S_x)^{\mathbf{i}}_{\mathbf{k}} (S_z)^{\mathbf{k}}_{\mathbf{j}} \right) - (|\mathbf{i}| - |\mathbf{j}|)\delta(|\mathbf{i} \oplus \mathbf{j}| - 1) \\ &= \sum_{\mathbf{k}} (\delta(|\mathbf{i} \oplus \mathbf{k}| - 1)(n - 2|\mathbf{k}|)\delta(\mathbf{k} - \mathbf{j})) \\ &\quad -(|\mathbf{i}| - |\mathbf{j}|)\delta(|\mathbf{i} \oplus \mathbf{j}| - 1) \\ &= (n - 2|\mathbf{j}|)\delta(|\mathbf{i} \oplus \mathbf{j}| - 1) - (|\mathbf{i}| - |\mathbf{j}|)\delta(|\mathbf{i} \oplus \mathbf{j}| - 1) \\ &= (n - |\mathbf{i}| - |\mathbf{j}|)\delta(|\mathbf{i} \oplus \mathbf{j}| - 1).\end{aligned}$$

- $(S_{yy})^{\mathbf{i}}_{\mathbf{j}} = 2 \cdot (-1)^{\frac{|\mathbf{i}|-|\mathbf{j}|}{2}} \delta(|\mathbf{i} \oplus \mathbf{j}| - 2)$.
  This case is close to $(S_{xy})^{\mathbf{i}}_{\mathbf{j}}$, so we follow a similar path:

$$\begin{aligned}(\sigma_y^{(v)} \sigma_y^{(w)})^{\mathbf{i}}_{\mathbf{j}} &= \sum_{\mathbf{k}} (S_y)^{\mathbf{i}}_{\mathbf{k}} (S_y)^{\mathbf{k}}_{\mathbf{j}} \\ &= -\sum_{\mathbf{k}} \delta(\mathbf{i} \oplus \mathbf{k} - 2^v)\delta(\mathbf{k} \oplus \mathbf{j} - 2^w) \\ &\quad \times \mathrm{sgn}(\mathbf{i} - \mathbf{k})\mathrm{sgn}(\mathbf{k} - \mathbf{j}) \\ &= \sum_{\mathbf{k}} \delta(\mathbf{i} \oplus \mathbf{k} - 2^v)\delta(\mathbf{k} \oplus \mathbf{j} - 2^w)(-1)^{i_v + j_w} \\ &= (-1)^{i_v + j_w} (\sigma_x^{(v)} \sigma_x^{(w)})^{\mathbf{i}}_{\mathbf{j}}.\end{aligned} \tag{B.11}$$

  The result is obtained by summing (B.11) over all parties, using the fact that $(-1)^{i_v + j_w}$ is equal to 1 whenever $i_v = j_w$ and to -1 whenever $i_v \neq j_w$. Observe that, in this particular case, the Kronecker deltas in (B.11) allow us to substitute $(-1)^{i_v + j_w}$ by $(-1)^{\frac{|\mathbf{i}|-|\mathbf{j}|}{2}}$.

- $(S_{yz})^{\mathbf{i}}_{\mathbf{j}} = \mathbb{i} \cdot \mathrm{sgn}(\mathbf{i} - \mathbf{j})(S_{xz})^{\mathbf{i}}_{\mathbf{j}}$.
  In a similar fashion as we proceeded to go to $(S_y)^{\mathbf{i}}_{\mathbf{j}}$ from $(S_x)^{\mathbf{i}}_{\mathbf{j}}$, it suffices to change the signs the upper half of the matrix and multiply by $\mathbb{i}$, in this case.

- $(S_{zz})^{\mathbf{i}}_{\mathbf{j}} = (n(n-1) - 4|\mathbf{i}|(n-|\mathbf{i}|))\delta(\mathbf{i}-\mathbf{j})$.
  This is the last case, for which we make use of the identity $S_{zz} = S_z S_z - \sum_{v=0}^{n-1}(\sigma_z\sigma_z)^{(v)}$. Now we calculate $(S_{zz})^{\mathbf{i}}_{\mathbf{j}}$:

$$\begin{aligned}(S_{zz})^{\mathbf{i}}_{\mathbf{j}} &= \sum_{\mathbf{k}}(S_z)^{\mathbf{i}}_{\mathbf{k}}(S_z)^{\mathbf{k}}_{\mathbf{j}} - \left(\sum_v(\sigma_z\sigma_z)^{(v)}\right)^{\mathbf{i}}_{\mathbf{j}} \\ &= \sum_{\mathbf{k}}\left((n-2|\mathbf{k}|)^2\delta(\mathbf{i}-\mathbf{k})\delta(\mathbf{k}-\mathbf{j})\right) - n\delta(\mathbf{i}-\mathbf{j}) \qquad \text{(B.12)}\end{aligned}$$

  Using the fact that $\delta(\mathbf{i}-\mathbf{k})\delta(\mathbf{k}-\mathbf{j}) = \delta(\mathbf{i}-\mathbf{j})\delta(\mathbf{k}-\mathbf{j})$, we obtain the result, which can also be expressed as:

$$(S_{zz})^{\mathbf{i}}_{\mathbf{j}} = \delta(\mathbf{i}-\mathbf{j})\left((n-2|\mathbf{i}|)^2 - n\right). \qquad \text{(B.13)}$$

Let us move now to the second part of the proof.

We start by expressing $|D^k_{2J}\rangle|\psi^-\rangle^{\otimes m/2}$ in the computational basis. Let us define the following $\Delta(\mathbf{i}') := \prod_{a=0}^{m/2-1}\delta(i'_{2a} - i'_{2a+1} - 1)$ and $\aleph := 10101010...10$. Let $\mathbf{i}'\cdot\aleph$ be the scalar product $\sum_{a=0}^{m/2-1} i'_{2a+1}$. Then, the following expressions hold:

$$|D^k_{2J}\rangle = \sum_{\mathbf{i}=0}^{2^{2J}-1}\binom{2J}{k}^{-1/2}\delta(|\mathbf{i}|-k)|\mathbf{i}\rangle, \qquad \text{(B.14)}$$

$$|\psi^-\rangle^{\otimes m/2} = \sum_{\mathbf{i}'=0}^{2^m-1} 2^{-m/4}(-1)^{\mathbf{i}'\cdot\aleph}\Delta(\mathbf{i}')|\mathbf{i}'\rangle. \qquad \text{(B.15)}$$

The matrix for the change of basis is denoted p; note that it depends on the J-th block that we are considering, but we omit to explicitly write this dependence in the interest of notation:

$$p = \sum_{\mathbf{i}=0}^{2^{2J}-1}\sum_{\mathbf{i}'=0}^{2^m-1}\sum_{j=0}^{2J}\frac{(-1)^{\mathbf{i}'\cdot\aleph}}{\sqrt{\binom{2J}{j}2^{m/2}}}\delta(|\mathbf{i}|-j)\Delta(\mathbf{i}')|\mathbf{i}\rangle|\mathbf{i}'\rangle\langle D^k_{2J}|\langle\psi^-|^{\otimes m/2}. \qquad \text{(B.16)}$$

Observe that $p^T p = \mathbb{1}_{2J+1}$, whereas pp^T is the projector onto the space $\mathcal{H}_J$ in (2.21). We shall define $|\underline{\mathbf{i}}\rangle := |\mathbf{i}\rangle|\mathbf{i}'\rangle$, but sometimes we shall use $\underline{\mathbf{i}} = 2^m\mathbf{i} + \mathbf{i}'$ in order to compactify the expressions.

Now we have the tools to calculate the projections onto the symmetric blocks.

- $(p^T S_x p)_l^k$.

$$
\begin{aligned}
(p^T S_x p)_l^k &= \sum_{\underline{\mathbf{i}},\underline{\mathbf{j}}} p_k^{\underline{\mathbf{i}}} (S_x)_{\underline{\mathbf{i}}}^{\underline{\mathbf{j}}} p_l^{\underline{\mathbf{j}}} \\
&= \sum_{\underline{\mathbf{i}},\underline{\mathbf{j}}} \frac{(-1)^{\mathbf{i}'\cdot\aleph}(-1)^{\mathbf{j}'\cdot\aleph}}{\sqrt{2^m \binom{2J}{k}\binom{2J}{l}}} \Delta(\mathbf{i}')\Delta(\mathbf{j}')\delta(|\underline{\mathbf{i}}\oplus\underline{\mathbf{j}}|-1)\delta(|\mathbf{i}|-k)\delta(|\mathbf{j}|-l).
\end{aligned}
$$

Observe that the identity $|\underline{\mathbf{i}}\oplus\underline{\mathbf{j}}| = |\mathbf{i}\oplus\mathbf{j}| + |\mathbf{i}'\oplus\mathbf{j}'|$ holds, which suggests to distinguish the two possible cases for which $\delta(|\underline{\mathbf{i}}\oplus\underline{\mathbf{j}}|-1)$ is nonzero: Either $|\mathbf{i}\oplus\mathbf{j}| = 0$ (so that $|\mathbf{i}'\oplus\mathbf{j}'| = 1$) or $|\mathbf{i}\oplus\mathbf{j}| = 1$ (so that $|\mathbf{i}'\oplus\mathbf{j}'| = 0$). Equivalently, either $\mathbf{i} = \mathbf{j}$ or $\mathbf{i}' = \mathbf{j}'$ must hold.

We can now split the expression $\delta(|\underline{\mathbf{i}}\oplus\underline{\mathbf{j}}|-1)$ into two parts: $\delta(\mathbf{i}-\mathbf{j})\delta(|\mathbf{i}'\oplus\mathbf{j}'|-1) + \delta(|\mathbf{i}\oplus\mathbf{j}|-1)\delta(\mathbf{i}'-\mathbf{j}')$. Observe that the first term has a zero contribution to the sum, and the reason is that $\mathbf{i}'$ and $\mathbf{j}'$ differ exactly in one bit, which implies that either $|\mathbf{i}'|$ or $|\mathbf{j}'|$ cannot be $m/2$; however, the term $\Delta(\mathbf{i}')\Delta(\mathbf{j}')$ neutralizes any index with weight other than $m/2$. Hence, we need to consider only the last summand, which means that $(p^T S_x p)_l^k$ now takes the form

$$
\begin{aligned}
&\sum_{\underline{\mathbf{i}},\underline{\mathbf{j}}} \frac{(-1)^{\mathbf{i}'\cdot\aleph}(-1)^{\mathbf{j}'\cdot\aleph}}{\sqrt{2^m \binom{2J}{k}\binom{2J}{l}}} \Delta(\mathbf{i}')\Delta(\mathbf{j}')\delta(|\mathbf{i}\oplus\mathbf{j}|-1)\delta(\mathbf{i}'-\mathbf{j}')\delta(|\mathbf{i}|-k)\delta(|\mathbf{j}|-l) \\
&\quad= \sum_{\mathbf{i},\mathbf{j},\mathbf{i}'} \frac{(-1)^{2\mathbf{i}'\cdot\aleph}}{\sqrt{2^m \binom{2J}{k}\binom{2J}{l}}} \Delta(\mathbf{i}')\delta(|\mathbf{i}\oplus\mathbf{j}|-1)\delta(|\mathbf{i}|-k)\delta(|\mathbf{j}|-l) \\
&\quad= \sum_{\mathbf{i},\mathbf{j}} \frac{1}{\sqrt{2^m \binom{2J}{k}\binom{2J}{l}}} \delta(|\mathbf{i}\oplus\mathbf{j}|-1)\delta(|\mathbf{i}|-k)\delta(|\mathbf{j}|-l) \sum_{\mathbf{i}'} \Delta(\mathbf{i}') \\
&\quad= \sum_{\mathbf{i},\mathbf{j}} \frac{1}{\sqrt{\binom{2J}{k}\binom{2J}{l}}} \delta(|\mathbf{i}\oplus\mathbf{j}|-1)\delta(|\mathbf{i}|-k)\delta(|\mathbf{j}|-l).
\end{aligned}
$$

In order to proceed, we need to observe the following:

$$
\sum_{\mathbf{j}=0}^{2^{2J}-1} \delta(|\mathbf{j}|-l)\delta(|\mathbf{i}\oplus\mathbf{j}|-1) = |\mathbf{i}|\delta(|\mathbf{i}|-l-1) + (2J-|\mathbf{i}|)\delta(|\mathbf{i}|-l+1), \tag{B.17}
$$

an identity that is justified as follows: The left hand side of Eq. (B.17) counts how many words $\mathbf{j}$ have weight l while being at Hamming distance 1 from a given word $\mathbf{i}$ (*i.e.*, they differ exactly in one bit). We split them into two sets: $|\mathbf{i}|$ of them have weight $l = |\mathbf{i}| - 1$ (*i.e.*, when we turn a 1 of $\mathbf{i}$ into a 0) and there are $2J - |\mathbf{i}|$ of them which have weight $l = |\mathbf{i}| + 1$ (*i.e.*, we turn a 0 of $\mathbf{i}$ into a 1).

Now, the result follows from a simple calculation:

$$\begin{aligned}
(p^T S_x p)_l^k &= \sum_{\mathbf{i}} \frac{\delta(|\mathbf{i}| - k)}{\sqrt{\binom{2J}{k}\binom{2J}{l}}} (k\delta(k-l-1) + (2J-k)\delta(k-l+1)) \\
&= \frac{k\binom{2J}{k}\delta(k-l-1) + (2J-k)\binom{2J}{k}\delta(k-l+1)}{\sqrt{\binom{2J}{k}\binom{2J}{l}}} \\
&= (l+1)\sqrt{\binom{2J}{l+1}\binom{2J}{l}}\delta(k-l-1) \\
&\quad + (2J-k)\sqrt{\binom{2J}{k}/\binom{2J}{k+1}}\delta(l-k-1) \\
&= \sqrt{(l+1)(2J-l)}\delta(k-l-1) \\
&\quad + \sqrt{(k+1)(2J-k)}\delta(l-k-1).
\end{aligned}$$

- For $(p^T S_y p)_l^k$, we follow the same line of reasoning as in $(p^T S_x p)_l^k$, using the additional fact that the term $\mathrm{sgn}(\mathbf{i}-\mathbf{j})$ is turned into $\mathrm{sgn}(k-l)$, because $\mathrm{sgn}(\underline{\mathbf{i}}-\underline{\mathbf{j}})\delta(\mathbf{i}'-\mathbf{j}')\delta(|\mathbf{i}\oplus\mathbf{j}|-1)\delta(|\mathbf{i}|-k)\delta(|\mathbf{j}|-l)$ is equal to $\mathrm{sgn}(\mathbf{i}-\mathbf{j})\delta(|\mathbf{i}\oplus\mathbf{j}|-1)\delta(|\mathbf{i}|-k)\delta(|\mathbf{j}|-l)$, which is simply $k-l$. Hence, $(k-l)(\delta(k-l-1)+\delta(l-k-1)) = \mathrm{sgn}(k-l)$.

- To calculate $(p^T S_z p)_l^k$, we shall use the following property: any function f of $|\mathbf{i}'|$, when multiplied by $\Delta(\mathbf{i}')$, is a function of $m/2$, because the only words which survive $\Delta(\mathbf{i}')$ are those with weight $m/2$. The following calculation leads to the result $(p^T S_z p)_l^k = 2(J-k)\delta(k-l)$:

$$\begin{aligned}
(p^T S_z p)_l^k &= \sum_{\underline{\mathbf{i}},\underline{\mathbf{j}}} p_k^{\underline{\mathbf{i}}} (S_z)_{\underline{\mathbf{j}}}^{\underline{\mathbf{i}}} p_l^{\underline{\mathbf{j}}} \\
&= \sum_{\underline{\mathbf{i}},\underline{\mathbf{j}}} \frac{(n-2|\underline{\mathbf{i}}|)(-1)^{\mathbf{i}'\aleph}(-1)^{\mathbf{j}'\aleph}}{\sqrt{2^m\binom{2J}{k}\binom{2J}{l}}} \Delta(\mathbf{i}')\Delta(\mathbf{j}') \\
&\quad \times \delta(\underline{\mathbf{i}}-\underline{\mathbf{j}})\delta(|\mathbf{i}|-k)\delta(|\mathbf{j}|-l) \\
&= \sum_{\underline{\mathbf{i}}} \frac{(n-2|\underline{\mathbf{i}}|)(-1)^{(\mathbf{i}'+\mathbf{i}')\cdot\aleph}}{\sqrt{2^m\binom{2J}{k}\binom{2J}{l}}} \Delta(\mathbf{i}')\delta(|\mathbf{i}|-k)\delta(|\mathbf{i}|-l)
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{\mathbf{i}} \frac{\delta(|\mathbf{i}|-k)\delta(k-l)}{\sqrt{\binom{2J}{k}\binom{2J}{l}}} \sum_{\mathbf{i}'} \frac{(n-2|\mathbf{i}|-2|\mathbf{i}'|)}{\sqrt{2^m}}\Delta(\mathbf{i}') \\
&= \frac{\binom{2J}{k}\delta(k-l)}{\sqrt{\binom{2J}{k}\binom{2J}{k}}} \sum_{\mathbf{i}'} \frac{(n-2k-2m/2)}{\sqrt{2^m}}\Delta(\mathbf{i}') \\
&= \delta(k-l)\sum_{\mathbf{i}'} \frac{2J-2k}{2^{m/2}}\Delta(\mathbf{i}') = (2J-2k)\delta(k-l).
\end{aligned}
$$

- Let us focus on $(p^T S_{xx} p)^k_l$.

$$
\begin{aligned}
(p^T S_{xx} p)^k_l &= \sum_{\underline{\mathbf{i}},\underline{\mathbf{j}}} p^{\underline{\mathbf{i}}}_k (S_{xx})^{\underline{\mathbf{i}}}_{\underline{\mathbf{j}}} p^{\underline{\mathbf{j}}}_l \\
&= 2\sum_{\underline{\mathbf{i}},\underline{\mathbf{j}}} \frac{(-1)^{\mathbf{i}'\cdot\aleph}(-1)^{\mathbf{j}'\cdot\aleph}}{\sqrt{2^m\binom{2J}{k}\binom{2J}{l}}}\Delta(\mathbf{i}')\Delta(\mathbf{j}') \\
&\quad \times\delta(|\underline{\mathbf{i}}\oplus\underline{\mathbf{j}}|-2)\delta(|\mathbf{i}|-k)\delta(|\mathbf{j}|-l).
\end{aligned}
$$

  Similarly to the case of S_x, now we use the fact that $\delta(|\underline{\mathbf{i}}\oplus\underline{\mathbf{j}}|-2) = \delta(\mathbf{i}-\mathbf{j})\delta(|\mathbf{i}'\oplus\mathbf{j}'|-2)+\delta(|\mathbf{i}\oplus\mathbf{j}|-1)\delta(|\mathbf{i}'\oplus\mathbf{j}'|-1)+\delta(|\mathbf{i}\oplus\mathbf{j}|-2)\delta(\mathbf{i}'-\mathbf{j}')$. Because of $\delta(|\mathbf{i}'\oplus\mathbf{j}'|-1)$, the term in the middle is irrelevant, as the delta factors $\Delta(\mathbf{i}')\Delta(\mathbf{j}')$ cancel it out ($\mathbf{i}'$ and $\mathbf{j}'$ can not have weight $m/2$ at the same time). Let us consider the remaining terms:

  - To obtain the contribution for the case that $\mathbf{i}=\mathbf{j}$, we use the following:

    Let us encode $|0_L\rangle := |01\rangle$ and $|1_L\rangle := |10\rangle$ as logical qubits. Then, we have the following identity: $\Delta(\mathbf{i}')\Delta(\mathbf{j}')\delta(|\mathbf{i}'\oplus\mathbf{j}'|-2) = \delta(|\mathbf{i}'_{\mathbf{L}}\oplus\mathbf{j}'_{\mathbf{L}}|-1)$, because only the pairs 01 that go to 10 and vice-versa are considered. We shall also use the following fact: $\sum_{\mathbf{j}'_{\mathbf{L}}}\delta(|\mathbf{i}'_{\mathbf{L}}\oplus\mathbf{j}'_{\mathbf{L}}|-1) = m/2$, as there are $m/2$ logical bits to flip for any $\mathbf{i}'_{\mathbf{L}}$. These properties lead to

$$
\begin{aligned}
&2\sum_{\mathbf{i},\mathbf{i}',\mathbf{j}'} \frac{(-1)^{\mathbf{i}'\cdot\aleph}(-1)^{\mathbf{j}'\cdot\aleph}}{\sqrt{2^m\binom{2J}{k}\binom{2J}{l}}}\Delta(\mathbf{i}')\Delta(\mathbf{j}') \\
&\times\delta(|\mathbf{i}'\oplus\mathbf{j}'|-2)\delta(|\mathbf{i}|-k)\delta(|\mathbf{i}|-l) \\
= \;& 2\delta(k-l)\sum_{\mathbf{i}',\mathbf{j}'} \frac{(-1)^{\mathbf{i}'\cdot\aleph}(-1)^{\mathbf{j}'\cdot\aleph}}{\sqrt{2^m}}\Delta(\mathbf{i}')\Delta(\mathbf{j}')\delta(|\mathbf{i}'\oplus\mathbf{j}'|-2)
\end{aligned}
$$

$$
\begin{aligned}
&= (-1)2\delta(k-l)\sum_{\mathbf{i}'_{\mathbf{L}},\mathbf{j}'_{\mathbf{L}}=0}^{2^{m/2}-1}\frac{(-1)}{\sqrt{2^m}}\delta(|\mathbf{i}'_{\mathbf{L}}\oplus\mathbf{j}'_{\mathbf{L}}|-1)\\
&= -2\delta(k-l)\sum_{\mathbf{i}'_{\mathbf{L}}=0}^{2^{m/2}-1}\frac{m/2}{\sqrt{2^m}} = -m\delta(k-l),
\end{aligned}
$$

– And for the case $\mathbf{i}' = \mathbf{j}'$, we need the following facts, in order to compute its contribution: Given a word $\mathbf{i}$, the words $\mathbf{j}$ at Hamming distance 2 from $\mathbf{i}$ can be classified into 3 sets:

  * A set of $\binom{|\mathbf{i}|}{2}$ elements, each of them having weight $|\mathbf{j}| = |\mathbf{i}| - 2$.
  * A set of $\binom{|\mathbf{i}|}{1}\binom{2J-|\mathbf{i}|}{1}$ elements, each of them having weight $|\mathbf{j}| = |\mathbf{i}|$.
  * A set of $\binom{2J-|\mathbf{i}|}{2}$ elements, each of them having weight $|\mathbf{j}| = |\mathbf{i}| + 2$.

  The relation $\binom{2J}{2} = \binom{|\mathbf{i}|}{2} + \binom{|\mathbf{i}|}{1}\binom{2J-|\mathbf{i}|}{1} + \binom{2J-|\mathbf{i}|}{2}$ holds, because it counts all the ways to pick the 2 different bits between $\mathbf{i}$ and $\mathbf{j}$.

  Finally, we have

$$
\begin{aligned}
&2\sum_{\mathbf{i},\mathbf{j},\mathbf{i}'}\frac{(-1)^{\mathbf{i}'\cdot\aleph}(-1)^{\mathbf{i}'\cdot\aleph}}{\sqrt{2^m\binom{2J}{k}\binom{2J}{l}}}\Delta(\mathbf{i}')\delta(|\mathbf{i}\oplus\mathbf{j}|-2)\delta(|\mathbf{i}|-k)\delta(|\mathbf{j}|-l)\\
=\;& 2\sum_{\mathbf{i},\mathbf{j}}\frac{1}{\sqrt{\binom{2J}{k}\binom{2J}{l}}}\delta(|\mathbf{i}\oplus\mathbf{j}|-2)\delta(|\mathbf{i}|-k)\delta(|\mathbf{j}|-l)\\
=\;& \frac{2}{\sqrt{\binom{2J}{k}\binom{2J}{l}}}\sum_{\mathbf{i}}\delta(|\mathbf{i}|-k)\\
&\times\Big(\tbinom{|\mathbf{i}|}{2}\delta(|\mathbf{i}|-2-l)+|\mathbf{i}|(2J-|\mathbf{i}|)\delta(|\mathbf{i}|-l)+\tbinom{2J-|\mathbf{i}|}{2}\delta(|\mathbf{i}|+2-l)\Big)\\
=\;& \frac{2\binom{2J}{k}}{\sqrt{\binom{2J}{k}\binom{2J}{l}}}\Big(\tbinom{k}{2}\delta(k-2-l)+k(2J-k)\delta(k-l)+\tbinom{2J-k}{2}\delta(k+2-l)\Big)\\
=\;& 2k(2J-k)\delta(k-l)+2\tbinom{k}{2}\sqrt{\tbinom{2J}{k}/\tbinom{2J}{l}}\delta(k-2-l)\\
&+2\tbinom{2J-k}{2}\sqrt{\tbinom{2J}{k}/\tbinom{2J}{l}}\delta(k+2-l)\\
=\;& 2k(2J-k)\delta(k-l)+\sqrt{(l+2)(l+1)(2J-l)(2J-l-1)}\delta(k-2-l)\\
&+\sqrt{(2J-k)(2J-k-1)(k+1)(k+2)}\delta(l-k-2).
\end{aligned}
$$

- As the case $(p^T S_{xy} p)_l^k$ is very similar to $(p^T S_{xx} p)_l^k$, we point out their only differences.

We have the expression:

$$
\begin{aligned}
(p^T S_{xy} p)_l^k &= \sum_{\underline{\mathbf{i}},\underline{\mathbf{j}}} p_k^{\underline{\mathbf{i}}} (S_{xy})_{\underline{\mathbf{i}}}^{\underline{\mathbf{j}}} p_l^{\underline{\mathbf{j}}} \\
&= \mathbb{i} \sum_{\underline{\mathbf{i}},\underline{\mathbf{j}}} \frac{(-1)^{\mathbf{i}'\cdot\aleph}(-1)^{\mathbf{j}'\cdot\aleph}}{\sqrt{2^m \binom{2J}{k}\binom{2J}{l}}} \Delta(\mathbf{i}')\Delta(\mathbf{j}') \\
&\times \mathrm{sgn}(\underline{\mathbf{i}} - \underline{\mathbf{j}}) \left(1 - (-1)^{\frac{|\underline{\mathbf{i}}|-|\underline{\mathbf{j}}|}{2}}\right) \delta(|\underline{\mathbf{i}} \oplus \underline{\mathbf{j}}| - 2)\delta(|\mathbf{i}| - k)\delta(|\mathbf{j}| - l).
\end{aligned}
$$

Again, we divide into the cases where either $\mathbf{i} = \mathbf{j}$ or $\mathbf{i}' = \mathbf{j}'$ holds.

- Case $\mathbf{i} = \mathbf{j}$ and $|\mathbf{i}' \oplus \mathbf{j}'| = 2$:
  In this case, the sign function is determined by the part that corresponds to the singlet; *i.e.*, $\mathrm{sgn}(\mathbf{i}' - \mathbf{j}')$, and we have

  $$
  \begin{aligned}
  &\mathbb{i} \sum_{\mathbf{i},\mathbf{i}',\mathbf{j}'} \frac{(-1)^{\mathbf{i}'\cdot\aleph}(-1)^{\mathbf{j}'\cdot\aleph}}{\sqrt{2^m \binom{2J}{k}\binom{2J}{l}}} \Delta(\mathbf{i}')\Delta(\mathbf{j}')\mathrm{sgn}(\mathbf{i}' - \mathbf{j}') \\
  &\times \left(1 - (-1)^{\frac{|\mathbf{i}'|-|\mathbf{j}'|}{2}}\right) \delta(|\mathbf{i}' \oplus \mathbf{j}'| - 2)\delta(|\mathbf{i}| - k)\delta(|\mathbf{i}| - l).
  \end{aligned}
  $$

  But we are in the case where $\mathbf{i}'$ and $\mathbf{j}'$ differ exactly in two bits. Then, because of the factors $\Delta(\mathbf{i}')\Delta(\mathbf{j}')$, we only need to consider the case when a pair 01 turns into a pair 10 and viceversa. So, their weights must be equal ($|\mathbf{i}'| = |\mathbf{j}'|$) and the whole expression is zero.

- Case $\mathbf{i}' = \mathbf{j}'$ and $|\mathbf{i} \oplus \mathbf{j}| = 2$: Now the sign function is determined by the part corresponding to the Dicke states; *i.e.*, $\mathrm{sgn}(\mathbf{i} - \mathbf{j})$, so we are left with

  $$
  \begin{aligned}
  & \mathbb{i} \sum_{\mathbf{i},\mathbf{j},\mathbf{i}'} \frac{(-1)^{2\mathbf{i}'\cdot\aleph}}{\sqrt{2^m \binom{2J}{k}\binom{2J}{l}}} \Delta(\mathbf{i}')\Xi(\mathbf{i},\mathbf{j}) \\
  = \; & \mathbb{i} \sum_{\mathbf{i},\mathbf{j}} \frac{1}{\sqrt{\binom{2J}{k}\binom{2J}{l}}} \Xi(\mathbf{i},\mathbf{j}) \sum_{\mathbf{i}'} \frac{\Delta(\mathbf{i}')}{2^{m/2}} \\
  = \; & \mathbb{i} \sum_{\mathbf{i},\mathbf{j}} \frac{1}{\sqrt{\binom{2J}{k}\binom{2J}{l}}} \Xi(\mathbf{i},\mathbf{j}),
  \end{aligned}
  $$

where we have defined $\Xi(\mathbf{i},\mathbf{j}) := \mathrm{sgn}(\mathbf{i}-\mathbf{j})\left(1-(-1)^{\frac{|\mathbf{i}|-|\mathbf{j}|}{2}}\right)\delta(|\mathbf{i}\oplus\mathbf{j}|-2)\delta(|\mathbf{i}|-k)\delta(|\mathbf{j}|-l)$ in the interest of notation. As before, there are only 3 possibilities: $|\mathbf{i}| = |\mathbf{j}| \pm 2$ and $|\mathbf{i}| = |\mathbf{j}|$. Observe that the last possibility immediately leads to 0. If $|\mathbf{i}| = |\mathbf{j}| + 2$, then $\mathbf{i} > \mathbf{j}$, because we must change exactly two bits, which have to be two ones turning into two zeroes, because of the presence of the $\delta(|\mathbf{i}\oplus\mathbf{j}|-2)$ factor. Analogously, if $|\mathbf{i}| = |\mathbf{j}| - 2$, then $\mathbf{i} < \mathbf{j}$. Thus, there is no loss of generality in the simplification $\mathrm{sgn}(\mathbf{i}-\mathbf{j}) = (|\mathbf{i}|-|\mathbf{j}|)/2$. Hence, we arrive at the expression below:

$$2\mathbb{i}\sum_{\mathbf{i},\mathbf{j}}\frac{1}{\sqrt{\binom{2J}{k}\binom{2J}{l}}}\frac{k-l}{2}\delta(|\mathbf{i}\oplus\mathbf{j}|-2)\delta(|\mathbf{i}|-k)\delta(|\mathbf{j}|-l)$$

By following the same discussion as in $(p^T S_{xx} p)_l^k$, we derive the expression

$$\begin{aligned}&\tfrac{k-l}{2}\mathbb{i}2k(2J-k)\delta(k-l)\\&+\tfrac{k-l}{2}\mathbb{i}\sqrt{(l+2)(l+1)(2J-l)(2J-l-1)}\delta(k-l-2)\\&+\tfrac{k-l}{2}\mathbb{i}\sqrt{(2J-k)(2J-k-1)(k+2)(k+1)}\delta(l-k-2).\end{aligned}$$

Notice that the first term vanishes and the factor $(k-l)/2$ can be substituted by $\mathrm{sgn}(k-l)$ because of the Kronecker deltas, leading to the result.

- Let us now move to $(p^T S_{xz} p)_l^k$.

$$\begin{aligned}(p^T S_{xz} p)_l^k &= \sum_{\underline{\mathbf{i}},\underline{\mathbf{j}}} p_k^{\underline{\mathbf{i}}}(S_{xz})_{\underline{\mathbf{j}}}^{\underline{\mathbf{i}}} p_l^{\underline{\mathbf{j}}}\\&= \sum_{\underline{\mathbf{i}},\underline{\mathbf{j}}}\frac{(-1)^{\mathbf{i}'\cdot\aleph}(-1)^{\mathbf{j}'\cdot\aleph}}{\sqrt{2^m\binom{2J}{k}\binom{2J}{l}}}\Delta(\mathbf{i}')\Delta(\mathbf{j}')\\&\quad\times(n-|\underline{\mathbf{i}}|-|\underline{\mathbf{j}}|)\delta(|\underline{\mathbf{i}}\oplus\underline{\mathbf{j}}|-1)\delta(|\mathbf{i}|-k)\delta(|\mathbf{j}|-l).\end{aligned}$$

Similarly to $(p^T S_x p)_l^k$, it is convenient to split $\delta(|\underline{\mathbf{i}}\oplus\underline{\mathbf{j}}|-1)$ into the cases $|\mathbf{i}| = |\mathbf{j}| \pm 1, \mathbf{i}' = \mathbf{j}'$ or $\mathbf{i} = \mathbf{j}, |\mathbf{i}'| = |\mathbf{j}'| \pm 1$. We observe that the latter is neutralized by the functions $\Delta(\mathbf{i}')\Delta(\mathbf{j}')$, so we only need to

consider $\delta(|\mathbf{i}\oplus\mathbf{j}|-1)\delta(\mathbf{i}'-\mathbf{j}')$: We sum over $\mathbf{i}'$ in order to obtain

$$\begin{aligned}(p^T S_{xz} p)_l^k &= \sum_{\mathbf{i},\mathbf{j}} \frac{1}{\sqrt{\binom{2J}{k}\binom{2J}{l}}}(n-|\mathbf{i}|-|\mathbf{j}|-2(m/2)) \\ &\quad \times\delta(|\mathbf{i}\oplus\mathbf{j}|-1)\delta(|\mathbf{i}|-k)\delta(|\mathbf{j}|-l).\end{aligned}$$

Recall that, given $\mathbf{i}$, there are $|\mathbf{i}|$ words $\mathbf{j}$ at Hamming distance 1 from $\mathbf{i}$ having weight $|\mathbf{i}|-1$ and $2J-|\mathbf{i}|$ words $\mathbf{j}$ at Hamming distance 1 from $\mathbf{i}$ having weight $|\mathbf{i}|+1$. Thus, summing over $\mathbf{j}$ we get

$$\begin{aligned}(p^T S_{xz} p)_l^k &= \sum_{\mathbf{i}} \frac{1}{\sqrt{\binom{2J}{k}\binom{2J}{l}}}(2J-k-l)\delta(|\mathbf{i}|-k) \\ &\quad \times[|\mathbf{i}|\delta(|\mathbf{i}|-l-1)+(2J-|\mathbf{i}|)\delta(|\mathbf{i}|-l+1)] \\ &= \tbinom{2J}{k}\tfrac{2J-k-l}{\sqrt{\binom{2J}{k}\binom{2J}{l}}}[k\delta(k-l-1)+(2J-k)\delta(k-l+1)] \\ &= (2J-2l-1)\sqrt{(2J-l)(l+1)}\delta(k-l-1) \\ &\quad +(2J-2k-1)\sqrt{(2J-k)(k+1)}\delta(l-k-1).\end{aligned}$$

- Now we consider the case $(p^T S_{yy} p)_l^k$.

$$\begin{aligned}(p^T S_{yy} p)_l^k &= \sum_{\underline{\mathbf{i}},\underline{\mathbf{j}}} p_{\underline{k}}^{\underline{\mathbf{i}}}(S_{yy})_{\underline{\mathbf{j}}}^{\underline{\mathbf{i}}} p_l^{\underline{\mathbf{j}}} \\ &= 2\sum_{\underline{\mathbf{i}},\underline{\mathbf{j}}} \frac{(-1)^{\mathbf{i}'\cdot\aleph}(-1)^{\mathbf{j}'\cdot\aleph}}{\sqrt{2^m\binom{2J}{k}\binom{2J}{l}}}\Delta(\mathbf{i}')\Delta(\mathbf{j}') \\ &\quad \times(-1)^{\frac{|\underline{\mathbf{i}}|-|\underline{\mathbf{j}}|}{2}}\delta(|\underline{\mathbf{i}}\oplus\underline{\mathbf{j}}|-2)\delta(|\mathbf{i}|-k)\delta(|\mathbf{j}|-l).\end{aligned}$$

We proceed analogously to the $(p^T S_{xx} p)_l^k$ case. Recall that $\delta(|\underline{\mathbf{i}}\oplus\underline{\mathbf{j}}|-2)=\delta(\mathbf{i}-\mathbf{j})\delta(|\mathbf{i}'\oplus\mathbf{j}'|-2)+\delta(|\mathbf{i}\oplus\mathbf{j}|-1)\delta(|\mathbf{i}'\oplus\mathbf{j}'|-1)+\delta(|\mathbf{i}\oplus\mathbf{j}|-2)\delta(\mathbf{i}'-\mathbf{j}')$ and that the term in the middle becomes irrelevant because the delta factors $\Delta(\mathbf{i}')\Delta(\mathbf{j}')$ cancel it out. Hence, we need to distinguish the two remaining cases

– Case $\mathbf{i} = \mathbf{j}$: For this case, its contribution is

$$\begin{aligned}
&2\sum_{\mathbf{i},\mathbf{i}',\mathbf{j}'} \frac{(-1)^{\mathbf{i}'\cdot\aleph}(-1)^{\mathbf{j}'\cdot\aleph}}{\sqrt{2^m\binom{2J}{k}\binom{2J}{l}}}\Delta(\mathbf{i}')\Delta(\mathbf{j}') \\
&\quad\times(-1)^{\frac{|\mathbf{i}'|-|\mathbf{j}'|}{2}}\delta(|\mathbf{i}'\oplus\mathbf{j}'|-2)\delta(|\mathbf{i}|-k)\delta(|\mathbf{i}|-l) \\
&\quad= 2\delta(k-l)\sum_{\mathbf{i}',\mathbf{j}'}\frac{(-1)^{(\mathbf{i}'+\mathbf{j}')\cdot\aleph}}{\sqrt{2^m}}\Delta(\mathbf{i}')\Delta(\mathbf{j}') \\
&\quad\times(-1)^{\frac{|\mathbf{i}'|-|\mathbf{j}'|}{2}}\delta(|\mathbf{i}'\oplus\mathbf{j}'|-2).
\end{aligned}$$

Observe that $(-1)^{(\mathbf{i}'+\mathbf{j}')\cdot\aleph} = (-1)^{(\mathbf{i}'\oplus\mathbf{j}')\cdot\aleph}$ and the condition for the expression $(-1)^{(\mathbf{i}'\oplus\mathbf{j}')\cdot\aleph}\Delta(\mathbf{i}')\Delta(\mathbf{j}')\delta(|\mathbf{i}'\oplus\mathbf{j}'|-2)$ to be nonzero is precisely $(\mathbf{i}'\oplus\mathbf{j}')\cdot\aleph = 1$; *i.e.*, $(-1)^{(\mathbf{i}'\oplus\mathbf{j}')\cdot\aleph}\Delta(\mathbf{i}')\Delta(\mathbf{j}')\delta(|\mathbf{i}'\oplus\mathbf{j}'|-2)$ is nonzero only in those terms for which $\mathbf{i}'\oplus\mathbf{j}'$ is of the form $0000\cdots001100\cdots0000$. Additionally, the combination $\Delta(\mathbf{i}')\Delta(\mathbf{j}')\delta(|\mathbf{i}'\oplus\mathbf{j}'|-2)$ only allows for words with equal weight to be considered. Thus,

$$\begin{aligned}
& 2\delta(k-l)\sum_{\mathbf{i}',\mathbf{j}'}\frac{(-1)}{\sqrt{2^m}}\Delta(\mathbf{i}')\Delta(\mathbf{j}')(-1)^{\frac{|\mathbf{i}'|-|\mathbf{j}'|}{2}}\delta(|\mathbf{i}'\oplus\mathbf{j}'|-2) \\
= \;& -2\delta(k-l)\sum_{\mathbf{i}',\mathbf{j}'}\frac{1}{\sqrt{2^m}}\Delta(\mathbf{i}')\Delta(\mathbf{j}')\delta(|\mathbf{i}'\oplus\mathbf{j}'|-2) \\
= \;& -2\delta(k-l)\sum_{\mathbf{i}'_{\mathbf{L}},\mathbf{j}'_{\mathbf{L}}}\frac{1}{\sqrt{2^m}}\delta(|\mathbf{i}'_{\mathbf{L}}\oplus\mathbf{j}'_{\mathbf{L}}|-1) \\
= \;& -2\delta(k-l)\sum_{\mathbf{i}'_{\mathbf{L}}=0}^{2^{m/2}-1}\frac{m/2}{\sqrt{2^m}} = -m\delta(k-l).
\end{aligned}$$

– Case $\mathbf{i}' = \mathbf{j}'$: For this case, it is convenient to consider

$$\sum_{\mathbf{j}}(-1)^{\frac{|\mathbf{i}|-|\mathbf{j}|}{2}}\delta(|\mathbf{i}\oplus\mathbf{j}|-2)\delta(|\mathbf{j}|-l).$$

Consider a given word $\mathbf{i}$. We distinguish three cases:

∗ There are $\binom{|\mathbf{i}|}{2}$ words $\mathbf{j}$ at Hamming distance 2 with weight $|\mathbf{j}| = |\mathbf{i}|-2$. They are counted with the factor $(-1)^{(|\mathbf{i}|-|\mathbf{j}|)/2} = -1$.

* There are $|\mathbf{i}|(2J-|\mathbf{i}|)$ words $\mathbf{j}$ with weight $|\mathbf{j}|=|\mathbf{i}|$ which are counted with a factor $(-1)^{(|\mathbf{i}|-|\mathbf{j}|)/2}=1$.
* There are $\binom{2J-|\mathbf{i}|}{2}$ words $\mathbf{j}$ with weight $|\mathbf{j}|=|\mathbf{i}|+2$, counted with a factor $(-1)^{(|\mathbf{i}|-|\mathbf{j}|)/2}=-1$.

The same argument for $(p^T S_{xx} p)_l^k$ applies. The contribution from this term is then equal to

$$\begin{aligned}&2k(2J-k)\delta(k-l)\\&-\sqrt{(l+2)(l+1)(2J-l)(2J-l-1)}\delta(k-2-l)\\&-\sqrt{(2J-k)(2J-k-1)(k+1)(k+2)}\delta(l-k-2).\end{aligned}$$

Summing the two contributions, we arrive at the result.

- For the case $(p^T S_{yz} p)_l^k$, we use the same line of argumentation that we applied to $(p^T S_{xz} p)_l^k$ and, similarly to the $(p^T S_y p)_l^k$ case, we gain the extra factor $\mathbb{i}\mathrm{sgn}(k-l)$.
- Finally, for the case $(p^T S_{zz} p)_l^k$, we have to consider

$$\begin{aligned}(p^T S_{zz} p)_l^k &= \sum_{\underline{\mathbf{i}},\underline{\mathbf{j}}} p_k^{\underline{\mathbf{i}}} (S_{zz})_{\underline{\mathbf{i}}}^{\underline{\mathbf{j}}} p_l^{\underline{\mathbf{j}}}\\
&= \sum_{\underline{\mathbf{i}},\underline{\mathbf{j}}} \frac{(-1)^{\mathbf{i}'\cdot\aleph}(-1)^{\mathbf{j}'\cdot\aleph}}{\sqrt{2^m\binom{2J}{k}\binom{2J}{l}}}\Delta(\mathbf{i}')\Delta(\mathbf{j}')((n-2|\underline{\mathbf{i}}|)^2-n)\\
&\quad\times\delta(\underline{\mathbf{i}}-\underline{\mathbf{j}})\delta(|\mathbf{i}|-k)\delta(|\mathbf{j}|-l)\\
&= \sum_{\underline{\mathbf{i}}} \frac{(-1)^{\mathbf{i}'\cdot\aleph}(-1)^{\mathbf{i}'\cdot\aleph}}{\sqrt{2^m\binom{2J}{k}\binom{2J}{l}}}\Delta(\mathbf{i}')\Delta(\mathbf{i}')\\
&\quad\times((n-2|\underline{\mathbf{i}}|)^2-n)\delta(|\mathbf{i}|-k)\delta(|\mathbf{i}|-l)\\
&= \delta(k-l)\sum_{\mathbf{i}} \frac{1}{\sqrt{\binom{2J}{k}\binom{2J}{l}}}((n-2|\mathbf{i}|-2m/2)^2-n)\\
&\quad\times\delta(|\mathbf{i}|-k)\textstyle\sum_{\mathbf{i}'}\frac{\Delta(\mathbf{i}')}{\sqrt{2^m}}\\
&= \delta(k-l)\sum_{\mathbf{i}} \frac{1}{\sqrt{\binom{2J}{k}\binom{2J}{l}}}((2J-2|\mathbf{i}|)^2-n)\delta(|\mathbf{i}|-k)\\
&= \delta(k-l)((2J-2k)^2-n)\\
&= ((2J-2k)^2-2J-m)\delta(k-l).\end{aligned}$$

□

Proof of Theorem 4.6

Proof. The Bell operator $\mathcal{B}(\varphi,\theta)$ can be decomposed as

$$\begin{aligned}\mathcal{B}(\varphi,\theta) &= \alpha\mathcal{S}_0+\beta\mathcal{S}_1+\tfrac{\gamma}{2}\mathcal{S}_{00}+\delta\mathcal{S}_{01}+\tfrac{\varepsilon}{2}\mathcal{S}_{11}+\beta_c\mathbb{1}_{2^n}\\ &= AS_z+A'S_x+BS_{zz}+CS_{xx}+DS_{xz}+\beta_c\mathbb{1}_{2^n},\end{aligned} \tag{B.18}$$

where S_k and S_{kl}, with $k,l\in\{x,z\}$, are defined as $S_k:=\sum_v\sigma_k^{(v)}$ and $S_{kl}:=\sum_{v\neq w}\sigma_k^{(v)}\sigma_l^{(w)}$. As the projection of S_k and $S_{k,l}$ is given by Theorem B.1, by projecting $\mathcal{B}(\varphi,\theta)$ into the space $\mathcal{H}_J$ of (2.21), we obtain the analytic expression of every block $\mathcal{B}_J(\varphi,\theta)$. By grouping terms we arrive at the form (4.67). □

Proof of Theorem 4.7

Proof. Let $\{|e_\varphi\rangle,|f_\varphi\rangle\}$ be the eigenvectors of $\mathcal{M}_0$. They are of the following form

$$\begin{cases}|e_\varphi\rangle &= (\cos\varphi/2,\ \sin\varphi/2)\\ |f_\varphi\rangle &= (-\sin\varphi/2,\cos\varphi/2)\end{cases} \tag{B.19}$$

Observe that we can write $\mathcal{M}_0=|e_\varphi\rangle\langle e_\varphi|-|f_\varphi\rangle\langle f_\varphi|$. Similarly, $\mathcal{M}_1=|e_\theta\rangle\langle e_\theta|-|f_\theta\rangle\langle f_\theta|$. We are looking for a unitary transformation U such that $U|e_\varphi\rangle=|e_{\varphi+c}\rangle$ and $U|f_\varphi\rangle=|f_{\varphi+c}\rangle$ (and the same for θ instead of φ). Thus, such transformation is given by $U(\varphi,c)=|e_{\varphi+c}\rangle\langle e_\varphi|+|f_{\varphi+c}\rangle\langle f_\varphi|$. Because, for all φ, $\{|e_\varphi\rangle,|f_\varphi\rangle\}$ are orthonormal, unitarity follows. Actually, U is orthogonal because $\{|e_\varphi\rangle,|f_\varphi\rangle\}$ are real vectors.

A short calculation shows that $U(\varphi,c)$ does not depend on φ and that it can be expressed as (4.69). One has

$$\begin{cases}U\mathcal{M}_0U^\dagger &= |e_{\varphi+c}\rangle\langle e_{\varphi+c}|-|f_{\varphi+c}\rangle\langle f_{\varphi+c}|\\ U\mathcal{M}_1U^\dagger &= |e_{\theta+c}\rangle\langle e_{\theta+c}|-|f_{\theta+c}\rangle\langle f_{\theta+c}|\end{cases} \tag{B.20}$$

By taking n copies of U, $\mathcal{U}:=U^{\otimes n}$, this automatically gives the shift on the measurements used in the Bell operator that we were lookign for: $\mathcal{U}\mathcal{B}(\varphi,\theta)\mathcal{U}^\dagger=\mathcal{B}(\varphi+c,\theta+c)$. The result follows:

$$\begin{aligned}\langle\mathcal{B}(\varphi,\theta)\rangle_\rho &= \mathrm{Tr}[\mathcal{B}(\varphi,\theta)\rho]=\mathrm{Tr}[\mathcal{U}^\dagger\mathcal{U}\mathcal{B}(\varphi,\theta)\mathcal{U}^\dagger\mathcal{U}\rho]=\mathrm{Tr}[\mathcal{U}\mathcal{B}(\varphi,\theta)\mathcal{U}^\dagger\mathcal{U}\rho\mathcal{U}^\dagger]\\ &= \mathrm{Tr}\mathcal{B}(\varphi+c,\theta+c)\mathcal{U}\rho\mathcal{U}^\dagger=\langle\mathcal{B}(\varphi+c,\theta+c)\rangle_{\rho'}.\end{aligned}$$

□

Proof of Theorem 4.8

Proof. Our aim is to make $C = 0$, where C is defined in Eq. (4.68). Let us denote by $\theta_\pm$ the solution to such equation: $C = \gamma/2 \sin^2\varphi + \delta \sin\varphi \sin\theta + \varepsilon/2 \sin^2\theta = 0$. This implies

$$\begin{aligned} \sin\varphi &= \frac{-2\delta\sin\theta \pm \sqrt{4\delta^2\sin^2\theta - 4\gamma\varepsilon\sin^2\theta}}{2\gamma} = \frac{-\delta\sin\theta \pm \sqrt{\delta^2-\gamma\varepsilon}|\sin\theta|}{\gamma} \\ &= \frac{-\delta \pm \sqrt{\delta^2-\gamma\varepsilon}}{\gamma}\sin\theta. \end{aligned} \tag{B.21}$$

Let us denote

$$\xi := \frac{-\delta \pm \sqrt{\Delta}}{\gamma}, \quad \Delta := \delta^2 - \gamma\varepsilon.$$

To solve for θ the equation $\sin(\theta-\kappa) = \xi\sin(\theta)$, where $\xi, \kappa \in \mathbb{R}$, we can assume that $\kappa \neq m\pi,\ m \in \mathbb{Z}$ (otherwise the equation is trivially satisfied by setting $\theta = 0$, which leads to $\mathcal{M}_0 = \pm\mathcal{M}_1$, which is a degenerate case).

By expanding the term $\sin(\theta-\kappa)$, one obtains

$$\xi = \frac{\sin\theta\cos\kappa - \cos\theta\sin\kappa}{\sin\theta} = \cos\kappa - \frac{\sin\kappa}{\tan\theta},$$

which provides the result

$$\theta = \arctan\left(\frac{\sin\kappa}{\cos\kappa - \xi}\right) = \arctan\left(\frac{\gamma\sin\kappa}{\gamma\cos\kappa + \delta \pm \sqrt{\Delta}}\right).$$

□

Proof of Theorem 4.9

Proof. Before starting the proof of Theorem 4.9, it will be convenient to review some useful results from probability theory.

Recall that the non-central moments of the Gaussian distribution are given by

$$\mathbb{E}_{\mu,\sigma}(x^k) = \int_{-\infty}^{\infty} x^k \frac{e^{-(x-\mu)^2/2\sigma}}{\sqrt{2\pi\sigma}}\mathrm{d}x = \sigma^{k/2} H_k(\mu\sigma^{-1/2}),$$

where $H_k(x)$ are the Hermite polynomials, which can be defined as

$$H_k(x) = e^{-x^2/2}\frac{d^k}{dx^k}e^{x^2/2}.$$

So, we have that the set $\{\mathbb{E}_{\mu,\sigma}(x^k)\}_{k\geq 0}$ corresponds to

$$\{1, \mu, \mu^2+\sigma, \mu^3+3\mu\sigma, \mu^4+6\mu^2\sigma+3\sigma^2, \mu^5+10\mu^3\sigma+15\mu\sigma^2, \ldots\}. \quad \text{(B.22)}$$

In addition, for the proof of Theorem 4.9, we shall make use of the two following facts:

- Let $c_1, c_2 \in \mathbb{R}$. Then

$$\int_{-\infty}^{\infty} x^k \frac{e^{-(x-\mu+c_1)^2/4\sigma-(x-\mu+c_2)^2/4\sigma}}{\sqrt{2\pi\sigma}}\mathrm{d}x = e^{-(c_1-c_2)^2/8\sigma}\mathbb{E}_{\mu',\sigma}(x^k), \quad \text{(B.23)}$$

  where $\mu' = \mu - (c_1+c_2)/2$.

  Note that Eq. (B.23) easily follows when the following expression is taken into consideration:

$$\frac{(x-a)^2+(x-b)^2}{2} = \left(x-\left(\frac{a+b}{2}\right)\right)^2 + \left(\frac{a-b}{2}\right)^2,$$

  with $a = \mu - c_1$ and $b = \mu - c_2$.

- Consider now the family of states[1]

$$|\varphi_n\rangle = \frac{1}{\mathcal{N}_n}\sum_{k=0}^{n}\gamma_k^{(n)}|D_n^k\rangle = \frac{1}{\mathcal{N}_n}\sum_{k=0}^{n}\frac{e^{-(k-\mu)^2/4\sigma}}{\sqrt[4]{2\pi\sigma}}|D_n^k\rangle,$$

  where $\mu = n/2 + A/(2B-C)$ and $e^{-1}/2\pi \ll \sigma \ll n$. Then, we have the convergence $\lim_{n\to\infty}\mathcal{N}_n = 1$. This is checked because the normalization factor $\mathcal{N}_n$ for large n is such that $\langle\varphi_n|\varphi_n\rangle = 1$:

$$1 = \langle\varphi_n|\varphi_n\rangle = \frac{1}{\mathcal{N}_n^2}\sum_{k=0}^{n}\frac{e^{-(k-\mu)^2/2\sigma}}{\sqrt{2\pi\sigma}} \simeq \frac{1}{\mathcal{N}_n^2}\int_0^n \frac{e^{-(k-\mu)^2/2\sigma}}{\sqrt{2\pi\sigma}}\mathrm{d}k \simeq \frac{1}{\mathcal{N}_n^2}.$$

[1] This is to see when it is justified to substitute the $|\varphi_n\rangle$ states, which are properly normalized, with the $|\psi_n\rangle$ that are defined in Theorem 4.9.

Observe that the choice of σ can not be arbitrary. If σ were too small, the first approximation (which substitutes the sum by an integral) would be invalid. If σ were too large, the second approximation (integration over $\mathbb{R}$ instead of just the interval $[0, n]$) would break down. Thus, these are the reasons why we impose the constraints $e^{-1}/2\pi \ll \sigma \ll n$.

Hence, from now on, we assume that n is large enough make the factor $\mathcal{N}_n$ negligible.

Let us now move to the calculation of the expectation value of the $J = n/2$-th block of the Bell operator with the state $|\psi_n\rangle$ defined in Theorem 4.9.

In order to find $\langle\psi_n|\mathcal{B}_{n/2}(\varphi(\theta), \theta)|\psi_n\rangle$, let us first express d_k and u_k conveniently as polynomials in terms of k (note that $C = 0$, so that the pentadiagonal term v_k is always zero):

- $d_k = 2Bk^2 - 2(A + nB)k + (\beta_c + n(A - B/2) + n^2 B/2)$, for $0 \leq k \leq n$.

- $u_k = u_{k'+m-1} \equiv \tilde{u}_{k'} = (A' - 2k'D)m\sqrt{1 - \frac{k'^2}{m^2}}$, for $-m + 1 \leq k' \leq m - 1$, where $m = (n + 1)/2$ and $k' = k - (n - 1)/2$. Considering the Taylor expansion of the function $\sqrt{1 - x^2}$ centered at $x = 0$,

$$\sqrt{1 - x^2} = \sum_{l=0}^{\infty} c_l x^{2l} = 1 - \frac{1}{2}x^2 - \frac{1}{8}x^4 - \frac{1}{16}x^6 - \frac{5}{128}x^8 + o(x^{10}),$$

  we can express $u_{k'}$ as a polynomial in k', which is a good approximation provided that $|k'| \ll m$:

$$u_{k'} = (A' - 2k'D)\left(m - \frac{k'^2}{2m} - \frac{k'^4}{8m^3} - \frac{k'^6}{16m^5} - \frac{5k'^8}{128m^7} - \dots\right).$$

- $v_k = 0$ for $0 \leq k \leq n - 2$.

As the elements of the diagonal and those of the off-diagonal have quite different forms, it is convenient to consider them separately.

On the one hand, the expectation value of the elements of the diagonal of $\mathcal{B}_{n/2}(\varphi(\theta),\theta)$ is given by

$$\begin{aligned}\sum_{k=0}^{n}(\psi_k^{(n)})^2 d_k &\simeq \int_0^n d_k \frac{e^{-(k-\mu)^2/2\sigma}}{\sqrt{2\pi\sigma}}\mathrm{d}k \simeq \int_{-\infty}^{\infty} d_k \frac{e^{-(k-\mu)^2/2\sigma}}{\sqrt{2\pi\sigma}}\mathrm{d}k \\ &= 2B\mathbb{E}_{\mu,\sigma}(x^2) - 2(A+nB)\mathbb{E}_{\mu,\sigma}(x) \\ &\quad +(\beta_c + n(A-B/2) + n^2 B/2)\mathbb{E}_{\mu,\sigma}(1) \\ &= 2B(\mu^2+\sigma) - 2(A+nB)\mu + (\beta_c + n(A-B/2) + n^2 B/2) \\ &= 0\cdot n^2 + \left(\frac{\beta_c}{n} - \frac{B}{2}\right) n + 2B\sigma - \frac{A^2}{2B}, \end{aligned} \tag{B.24}$$

where we have applied (B.22).

On the other hand, the contribution to the expectation value of the elements corresponding to the off-diagonal terms of $\mathcal{B}_{n/2}(\varphi(\theta),\theta)$ is given by (let us put $c := A/2B$ to shorten the expressions)

$$\begin{aligned}\sum_{k=0}^{n-1}\psi_k^{(n)}\psi_{k+1}^{(n)}u_k &= \sum_{k'=-(m-1)}^{m-1}\psi_{k'+m-1}^{(n)}\psi_{k'+m}^{(n)}\tilde{u}_{k'} \\ &\simeq \int_{-m+1}^{m-1}\tilde{u}_{k'}\frac{e^{-(k'+m-1-\mu)^2/4\sigma-(k'+m-\mu)^2/4\sigma}}{\sqrt{2\pi\sigma}}\mathrm{d}k' \\ &= \int_{-m+1}^{m-1}\tilde{u}_{k'}\frac{e^{-(k'-(c-1/2))^2/4\sigma-(k'-(c+1/2))^2/4\sigma}}{\sqrt{2\pi\sigma}}\mathrm{d}k' \\ &\simeq \int_{-\infty}^{\infty}\tilde{u}_{k'}\frac{e^{-(k'-(c-1/2))^2/4\sigma-(k'-(c+1/2))^2/4\sigma}}{\sqrt{2\pi\sigma}}\mathrm{d}k' \\ &= \int_{-\infty}^{\infty}(A'-2k'D)\left(m - \frac{k'^2}{2m} - \frac{k'^4}{8m^3} - \frac{k'^6}{16m^5} - \frac{5k'^8}{128m^7} - \dots\right) \\ &\qquad\qquad \times\frac{e^{-(k'-(c-1/2))^2/4\sigma-(k'-(c+1/2))^2/4\sigma}}{\sqrt{2\pi\sigma}}\mathrm{d}k'\end{aligned}$$

$$
\begin{aligned}
&= e^{-1/8\sigma} \int_{-\infty}^{\infty} (A' - 2k'D) \left(m - \frac{k'^2}{2m} - \frac{k'^4}{8m^3} - \frac{k'^6}{16m^5} - \frac{5k'^8}{128m^7} - \dots \right) \\
&\times \qquad\qquad \frac{e^{-(k'-c)^2/2\sigma}}{\sqrt{2\pi\sigma}} \mathrm{d}k' \\
&= e^{-1/8\sigma} \left(A'm\mathbb{E}_{c,\sigma}(1) - 2Dm\mathbb{E}_{c,\sigma}(x) - \frac{A'}{2m}\mathbb{E}_{c,\sigma}(x^2) + \frac{D}{m}\mathbb{E}_{c,\sigma}(x^3) \right. \\
&\qquad\qquad \left. - \frac{A'}{8m^3}\mathbb{E}_{c,\sigma}(x^4) + \frac{D}{4m^3}\mathbb{E}_{c,\sigma}(x^5) - \cdots \right) \\
&= e^{-1/8\sigma} \left(\frac{A' - 2Dc}{2} n + \frac{A' - 2Dc}{2} - \frac{(c^2+\sigma)A' - 2Dc(c^2+3\sigma)}{n+1} \right. \\
&\qquad\qquad \left. + o(\sigma^2 n^{-3}) \right),
\end{aligned}
$$

where we have applied Eqs. (B.22 and B.23).

Therefore, the expectation value $\langle\psi_n|\mathcal{B}_{n/2}(\varphi(\theta),\theta)|\psi_n\rangle$ is given by

$$
\begin{aligned}
\langle\psi_n|B_n^S(\varphi(\theta),\theta)|\psi_n\rangle &= \sum_{k=0}^{n} \left(\psi_k^{(n)}\right)^2 d_k + 2\sum_{k=0}^{n-1} \psi_k^{(n)}\psi_{k+1}^{(n)} u_k \\
&\simeq \left(\frac{\beta_c}{n} - \frac{B}{2} + e^{-1/8\sigma}\left(A' - \frac{AD}{B} \right) \right) n \\
&\quad + \left(2B\sigma - \frac{A^2}{2B} + e^{-1/8\sigma}\left(A' - \frac{AD}{B} \right) \right) + o(\sigma n^{-1}).
\end{aligned}
$$

□

Proof of Theorem 4.11

Proof. Since ρ is acting on the symmetric space, all reduced states are equal, regardless of which parties are traced out. Hence, without loss of generality, we shall compute its partial trace by forgetting about the last $n-d$ subsystems.

Recall that, in general, when ρ acts on the Hilbert Space of n qubits $(\mathbb{C}^2)^{\otimes n}$, its partial trace after discarding the last $n-d$ subsystems is given by

$$
(\mathrm{Tr}_{n-d}(\rho))_{j_0\dots j_{d-1}}^{i_0\dots i_{d-1}} = \sum_{0\le i_d,\dots,i_{n-1}\le 1} \rho_{j_0,\dots,j_{d-1},i_d,\dots,i_{n-1}}^{i_0,\dots,i_{d-1},i_d,\dots,i_{n-1}}.
$$

Now, let us expand $\rho_{\mathcal{S}}$ to the full Hilbert Space $(\mathbb{C}^2)^{\otimes n}$:

$$(\rho)^{\mathbf{i}}_{\mathbf{j}} = (p\rho_{\mathcal{S}}p^T)^{\mathbf{i}}_{\mathbf{j}} = \sum_{0\leq k,l\leq n} p^{\mathbf{i}}_k (\rho_{\mathcal{S}})^k_l p^{\mathbf{j}}_l = \sum_{0\leq k,l\leq n} \frac{(\rho_{\mathcal{S}})^k_l}{\sqrt{\binom{n}{k}\binom{n}{l}}}\delta(k-|\mathbf{i}|)\delta(l-|\mathbf{j}|),$$

where p is the same matrix for the change of basis as the one defined in the proof of Theorem B.1, but in this case we are interested just in the $J = n/2$-th block.

By joining the last two expressions and introducing the notation $\overline{\mathbf{i}'} := i_d \dots i_{n-1}$ and $\overline{\mathbf{j}'} := j_d \dots j_{n-1}$, we have

$$\begin{aligned}
&(\mathrm{Tr}_{n-d}(\rho))^{\mathbf{i}'}_{\mathbf{j}'} = \left(\mathrm{Tr}_{n-d}(p\rho_{\mathcal{S}}p^T)\right)^{\mathbf{i}'}_{\mathbf{j}'} \\
&\quad = \textstyle\sum_{\overline{\mathbf{i}'}} \sum_{0\leq k,l\leq n} \frac{(\rho_{\mathcal{S}})^k_l}{\sqrt{\binom{n}{k}\binom{n}{l}}}\delta(k-|\mathbf{i}'|-|\overline{\mathbf{i}'}|)\delta(l-|\mathbf{j}'|-|\overline{\mathbf{i}'}|) \\
&\quad = \textstyle\sum_{\overline{\mathbf{i}'}} \sum_{0\leq k,l\leq n} \frac{(\rho_{\mathcal{S}})^k_l}{\sqrt{\binom{n}{k}\binom{n}{l}}}\delta(k-|\mathbf{i}'|-|\overline{\mathbf{i}'}|)\delta(k-|\mathbf{i}'|-l+|\mathbf{j}'|) \\
&\quad = \textstyle\sum_{0\leq k,l\leq n} \frac{(\rho_{\mathcal{S}})^k_l}{\sqrt{\binom{n}{k}\binom{n}{l}}}\delta(k-|\mathbf{i}'|-l+|\mathbf{j}'|) \sum_{\overline{\mathbf{i}'}} \delta(k-|\mathbf{i}'|-|\overline{\mathbf{i}'}|),
\end{aligned}$$

where in the third equality we have used the following property of the Kronecker delta functions: $\delta(a-b)\delta(a-c) = \delta(a-b)\delta(b-c)$.

Let us now define the indicator function $I_{[a,b]}(k)$:

$$I_{[a,b]}(k) = \begin{cases} 1 & \text{if} \quad a \leq k \leq b \\ 0 & \text{otherwise} \end{cases} \tag{B.25}$$

Observe that the expression $\sum_{\overline{\mathbf{i}'}} \delta(k-|\mathbf{i}'|-|\overline{\mathbf{i}'}|)$ is equal to the expression $\binom{n-d}{k-|\mathbf{i}'|} I_{[|\mathbf{i}'|,|\mathbf{i}'|+n-d]}(k)$. The reason for that is the following: we are just counting how many indices $\mathbf{i}$ with the first d bits already set and with weight $|\mathbf{i}'|$ have a total weight k. Hence, we have to choose from the remaining $n-d$ bits, indexed by $\overline{\mathbf{i}'}$, those that have weight $k-|\mathbf{i}'|$. This is possible only if $|\mathbf{i}'|$ is not already greater than k and it is not smaller than $n-d-k$; that is the reason why the indicator function appears, so that

$|\mathbf{i}'| \leq k \leq |\mathbf{i}'| + n - d$. We can then write

$$
\begin{aligned}
(\mathrm{Tr}_{n-d}(\rho))^{\mathbf{i}'}_{\mathbf{j}'} &= \sum_{0\leq k,l\leq n} \frac{(\rho_{\mathcal{S}})^k_l}{\sqrt{\binom{n}{k}\binom{n}{l}}} \delta(k - |\mathbf{i}'| - l + |\mathbf{j}'|) \binom{n-d}{k-|\mathbf{i}'|} I_{[|\mathbf{i}'|,|\mathbf{i}'|+n-d]}(k) \\
&= \sum_{0\leq k\leq n} \frac{(\rho_{\mathcal{S}})^k_{k-|\mathbf{i}'|+|\mathbf{j}'|}}{\sqrt{\binom{n}{k}\binom{n}{k-|\mathbf{i}'|+|\mathbf{j}'|}}} \binom{n-d}{k-|\mathbf{i}'|} I_{[|\mathbf{i}'|,|\mathbf{i}'|+n-d]}(k) \\
&= \sum_{|\mathbf{i}'|\leq k\leq |\mathbf{i}'|+n-d} \frac{(\rho_{\mathcal{S}})^k_{k-|\mathbf{i}'|+|\mathbf{j}'|}}{\sqrt{\binom{n}{k}\binom{n}{k-|\mathbf{i}'|+|\mathbf{j}'|}}} \binom{n-d}{k-|\mathbf{i}'|}.
\end{aligned}
$$

The following change of variables $m = k - |\mathbf{i}'|$ lets us obtain the expression

$$
(\mathrm{Tr}_{n-d}(\rho))^{\mathbf{i}'}_{\mathbf{j}'} = \sum_{0\leq m\leq n-d} \frac{\binom{n-d}{m}(\rho_{\mathcal{S}})^{m+|\mathbf{i}'|}_{m+|\mathbf{j}'|}}{\sqrt{\binom{n}{m+|\mathbf{i}'|}\binom{n}{m+|\mathbf{j}'|}}},
$$

which completes the proof. Note that we arrived at a permutationally invariant expression, as it only depends on the weights of the indices. □

Proof of Theorem 4.12

Proof. In order to prove Theorem 4.12, we shall use some of the tools already developed in Appendix B. In particular, we shall make use of the formula provided in Theorem 4.11 and use the same kind of approximations as in the proof of Theorem 4.9. We shall also use the definition for the function f given in Eq. (4.81) and its relation (4.79) and we shall adopt the notation in Eq. (B.22).

The simplest elements of ρ_2 to begin with are its diagonal elements:

$$
\begin{aligned}
(\rho_2)^{00}_{00} &\simeq \int_0^{n-2} f(n,x,2,0,0)\psi^2_x \mathrm{d}x = \tfrac{1}{n(n-1)} \int_0^{n-2} (n-x)(n-x-1) \tfrac{e^{-(x-\mu)^2/2\sigma}}{\sqrt{2\pi\sigma}} \mathrm{d}x \\
&\simeq \tfrac{1}{n(n-1)} \left(n(n-1)\mathbb{E}_{\mu,\sigma}(1) - (2n-1)\mathbb{E}_{\mu,\sigma}(x) + \mathbb{E}_{\mu,\sigma}(x^2) \right), \\
(\rho_2)^{01}_{01} &\simeq \int_0^{n-2} f(n,x,2,1,1)\psi^2_{x+1} \mathrm{d}x = \tfrac{1}{n(n-1)} \int_0^{n-2} (n-x-1)(x+1) \tfrac{e^{-(x-(\mu-1))^2/2\sigma}}{\sqrt{2\pi\sigma}} \mathrm{d}x \\
&\simeq \tfrac{1}{n(n-1)} \left((n-1)\mathbb{E}_{\mu-1,\sigma}(1) + (n-2)\mathbb{E}_{\mu-1,\sigma}(x) - \mathbb{E}_{\mu-1,\sigma}(x^2) \right), \\
(\rho_2)^{11}_{11} &\simeq \int_0^{n-2} f(n,x,2,2,2)\psi^2_{x+2} \mathrm{d}x = \tfrac{1}{n(n-1)} \int_0^{n-2} (x+1)(x+2) \tfrac{e^{-(x-(\mu-2))^2/2\sigma}}{\sqrt{2\pi\sigma}} \mathrm{d}x \\
&\simeq \tfrac{1}{n(n-1)} \left(2\mathbb{E}_{\mu-2,\sigma}(1) + 3\mathbb{E}_{\mu-2,\sigma}(x) + \mathbb{E}_{\mu-2,\sigma}(x^2) \right).
\end{aligned}
$$

Note that $(\rho_2)^{01}_{01} = (\rho_2)^{10}_{10} = (\rho_2)^{10}_{01} = (\rho_2)^{01}_{10}$. It is worth noticing that $\mathrm{Tr}\,\rho_2$ depends on neither μ nor σ and it is exactly 1.

Now we consider the off-diagonal elements, starting with $(\rho_2)^{00}_{11}$ (which is equal to $(\rho_2)^{11}_{00}$). Using the approximations $\sqrt{(n-x)(n-x-1)} \simeq (n-x-1/2)$ and $\sqrt{(x+1)(x+2)} \simeq x+3/2$ and the change of variables $y = x+1$, we arrive at the following:

$$\begin{aligned}
(\rho_2)^{00}_{11} &\simeq \int_0^{n-2} f(n,x,2,0,2)\psi_x\psi_{x+2}\mathrm{d}x \\
&= \tfrac{1}{n(n-1)}\int_0^{n-2}\sqrt{(n-x)(n-x-1)(x+1)(x+2)}\,\tfrac{e^{-\frac{(x-\mu)^2}{4\sigma}-\frac{-(x-\mu+2)^2}{4\sigma}}}{\sqrt{2\pi\sigma}}\mathrm{d}x \\
&\simeq \tfrac{e^{-1/2\sigma}}{n(n-1)}\int_{-\infty}^{\infty}(n-x-1/2)(x+3/2)\,\tfrac{e^{-\frac{(x-(\mu-1))^2}{2\sigma}}}{\sqrt{2\pi\sigma}}\mathrm{d}x \\
&= \tfrac{e^{-1/2\sigma}}{n(n-1)}\int_{-\infty}^{\infty}(n+1/2-y)(y+1/2)\,\tfrac{e^{-(y-\mu)^2/2\sigma}}{\sqrt{2\pi\sigma}}\mathrm{d}y \\
&= \tfrac{e^{-1/2\sigma}}{n(n-1)}\left(\tfrac{(2n+1)}{4}\mathbb{E}_{\mu,\sigma}(1)+n\mathbb{E}_{\mu,\sigma}(x)-\mathbb{E}_{\mu,\sigma}(x^2)\right).
\end{aligned}$$

Finally, we consider the cases $(\rho_2)^{00}_{01} = (\rho_2)^{00}_{10} = (\rho_2)^{01}_{00} = (\rho_2)^{10}_{00}$ and $(\rho_2)^{01}_{11} = (\rho_2)^{10}_{11} = (\rho_2)^{11}_{01} = (\rho_2)^{11}_{10}$. To this end, let us recall that $\mu = n/2 + A/2B$. We denote $c := A/2B$ and we also define $m := (n+1)/2$ and $\mu' := \mu - 1/2$.

$$\begin{aligned}
(\rho_2)^{00}_{01} &\simeq \int_0^{n-2} f(n,x,2,0,1)\psi_x\psi_{x+1}\mathrm{d}x \\
&= \tfrac{1}{n(n-1)}\int_0^{n-2}(n-x-1)\sqrt{(n-x)(x+1)}\,\tfrac{e^{-\frac{(x-\mu)^2}{4\sigma}-\frac{-(x-\mu+1)^2}{4\sigma}}}{\sqrt{2\pi\sigma}}\mathrm{d}x \\
&\simeq \tfrac{e^{-1/8\sigma}}{n(n-1)}\int_{-\infty}^{\infty}(n-x-1)\sqrt{(n-x)(x+1)}\,\tfrac{e^{-\frac{(x-\mu')^2}{2\sigma}}}{\sqrt{2\pi\sigma}}\mathrm{d}x \\
&= \tfrac{e^{-1/8\sigma}}{n(n-1)}\int_{-\infty}^{\infty}(m-1-y)m\sqrt{1-(y/m)^2}\,\tfrac{e^{-(y-c)^2/2\sigma}}{\sqrt{2\pi\sigma}}\mathrm{d}y \\
&= \tfrac{e^{-1/8\sigma}}{n(n-1)}\int_{-\infty}^{\infty}(m-1-y)m\textstyle\sum_{l=0}^{\infty}c_l(y/m)^{2l}\,\tfrac{e^{-(y-c)^2/2\sigma}}{\sqrt{2\pi\sigma}}\mathrm{d}y \\
&= \tfrac{e^{-1/8\sigma}}{n(n-1)}\int_{-\infty}^{\infty}(m-1-y)m\left(1-\tfrac{y^2}{2m^2}-\tfrac{y^4}{8m^4}-O((y/m)^6)\right)\tfrac{e^{-(y-c)^2/2\sigma}}{\sqrt{2\pi\sigma}}\mathrm{d}y \\
&\simeq \tfrac{e^{-1/8\sigma}}{n(n-1)}\big(m(m-1)\mathbb{E}_{c,\sigma}(1)-m\mathbb{E}_{c,\sigma}(x)-\tfrac{m-1}{2m}\mathbb{E}_{c,\sigma}(x^2) \\
&\qquad +\tfrac{1}{2m}\mathbb{E}_{c,\sigma}(x^3)-\tfrac{m-1}{8m^3}\mathbb{E}_{c,\sigma}(x^4)+\tfrac{1}{8m^3}\mathbb{E}_{c,\sigma}(x^5)\big) \\
&\simeq \tfrac{e^{-1/8\sigma}}{n(n-1)}\left(\tfrac{(n+1)(n-1)}{4}-\tfrac{(n+1)}{2}c-\tfrac{n-1}{2(n+1)}(c^2+\sigma)+\tfrac{1}{n+1}(c^3+3c\sigma)+\cdots\right) \\
&= \tfrac{e^{-1/8\sigma}}{n(n-1)}\left(\tfrac{1}{4}n^2-\tfrac{c}{2}n-\tfrac{2c^2+2c+1+2\sigma}{4}+\tfrac{c^2+\sigma+c^3+3c\sigma}{n}+\cdots\right),
\end{aligned}$$

where c_l are the coefficients of the Taylor expansion of the function $\sqrt{1-x^2}$ centered at $x = 0$. Note that we have also used the change of variables $y = x - (n-1)/2$ and the fact that

$$\frac{1}{n-a} = \frac{1}{n}\sum_{k=0}^{\infty}(a/n)^k \tag{B.26}$$

in order to obtain an expression purely in powers of n.

Finally, using the change of variables $y = x - (n-3)/2$ and a similar argumentation, we arrive at

$$\begin{aligned}
(\rho_2)^{01}_{11} &\simeq \int_0^{n-2} f(n,x,2,1,2)\psi_{x+1}\psi_{x+2}\mathrm{d}x \\
&= \tfrac{1}{n(n-1)}\int_0^{n-2}(x+1)\sqrt{(n-x-1)(x+2)}\,\frac{e^{-\frac{(x-\mu+1)^2}{4\sigma}-\frac{-(x-\mu+2)^2}{4\sigma}}}{\sqrt{2\pi\sigma}}\mathrm{d}x \\
&\simeq \tfrac{e^{-1/8\sigma}}{n(n-1)}\int_{-\infty}^{\infty}(x+1)\sqrt{(n-x-1)(x+2)}\,\frac{e^{-\frac{(x-(\mu'-1))^2}{2\sigma}}}{\sqrt{2\pi\sigma}}\mathrm{d}x \\
&= \tfrac{e^{-1/8\sigma}}{n(n-1)}\int_{-\infty}^{\infty}(m-1+y)m\sqrt{1-(y/m)^2}\,\frac{e^{-(y-c)^2/2\sigma}}{\sqrt{2\pi\sigma}}\mathrm{d}y \\
&= \tfrac{e^{-1/8\sigma}}{n(n-1)}\int_{-\infty}^{\infty}(m-1+y)m\left(1-\tfrac{y^2}{2m^2}-\tfrac{y^4}{8m^4}-O((y/m)^6)\right)\frac{e^{-(y-c)^2/2\sigma}}{\sqrt{2\pi\sigma}}\mathrm{d}y \\
&\simeq \tfrac{e^{-1/8\sigma}}{n(n-1)}\left(m(m-1)\mathbb{E}_{c,\sigma}(1)+m\mathbb{E}_{c,\sigma}(x)-\tfrac{m-1}{2m}\mathbb{E}_{c,\sigma}(x^2)\right. \\
&\qquad \left.-\tfrac{1}{2m}\mathbb{E}_{c,\sigma}(x^3)-\tfrac{m-1}{8m^3}\mathbb{E}_{c,\sigma}(x^4)-\tfrac{1}{8m^3}\mathbb{E}_{c,\sigma}(x^5)\right) \\
&\simeq \tfrac{e^{-1/8\sigma}}{n(n-1)}\left(\tfrac{(n+1)(n-1)}{4}+\tfrac{n+1}{2}c-\tfrac{n-1}{2(n+1)}(c^2+\sigma)-\tfrac{1}{n+1}(c^3+3c\sigma)+\cdots\right) \\
&= \tfrac{e^{-1/8\sigma}}{n(n-1)}\left(\tfrac{1}{4}n^2+\tfrac{c}{2}n-\tfrac{2c^2+2c+1+2\sigma}{4}+\tfrac{c^2+\sigma-(c^3+3c\sigma)}{n}+\cdots\right).
\end{aligned}$$

Joining all terms, we see that ρ_2 can be expressed as

$$\begin{aligned}
\rho_2 = \frac{1}{n(n-1)}\Bigg(&\frac{n^2}{4}\begin{pmatrix} 1 & e^{-1/8\sigma} & e^{-1/8\sigma} & e^{-1/2\sigma} \\ e^{-1/8\sigma} & 1 & 1 & e^{-1/8\sigma} \\ e^{-1/8\sigma} & 1 & 1 & e^{-1/8\sigma} \\ e^{-1/2\sigma} & e^{-1/8\sigma} & e^{-1/8\sigma} & 1 \end{pmatrix} \\
&+\frac{n}{2}\begin{pmatrix} -(2c+1) & -ce^{-1/8\sigma} & -ce^{-1/8\sigma} & e^{-1/2\sigma} \\ -ce^{-1/8\sigma} & 0 & 0 & ce^{-1/8\sigma} \\ -ce^{-1/8\sigma} & 0 & 0 & ce^{-1/8\sigma} \\ e^{-1/2\sigma} & ce^{-1/8\sigma} & ce^{-1/8\sigma} & -1+2c \end{pmatrix}+o(n)\Bigg).
\end{aligned}$$

Since $\sigma \in O(n^{1/2})$, we can neglect the exponential terms and we obtain the form given in Eq. (4.82), which completes the proof.

□

Proof of Theorem 4.13

Proof. We have to prove that the choice of coefficients (4.86) defines a valid Bell inequality; *i.e.*, (4.22) is non-negative on all points $\mathbb{P}_2^{\mathfrak{S}_n}$. As $\mathbb{P}_2^{\mathfrak{S}_n}$ is convex, it is enough to prove it on its extreme points.

To this aim, we shall express the inequality (4.22) in terms of the variables a, b, c, d and finding the minimum to its left hand side, subject to the conditions $a, b, c, d \geq 0$. If we denote by $F(a, b, c, d)$ the left hand side of

(4.22), interestingly we find that it does not depend on the variable d, and, as a quadratic function of a, b and c, it can be written in the following form:

$$(1,a,b,c,d)\begin{pmatrix} 4k(1+k)(1+2k) & 2(1+2k)^2 & -k(3+4k) & -k(3+4k) & 0 \\ 2(1+2k)^2 & 4(1+2k) & 2(1+2k) & 2(1+2k) & 0 \\ -k(3+4k) & 2(1+2k) & 2k & 2(1+k) & 0 \\ -k(3+4k) & 2(1+2k) & 2(1+k) & 2k & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ a \\ b \\ c \\ d \end{pmatrix}. \tag{B.27}$$

We aim to prove that $F(a,b,c,d) \geq 0$ on all vertices $\mathrm{Ext}(\mathbb{P}_2^{\mathfrak{S}_n})$. The condition for extrema is $\partial_a F = \partial_b F = \partial_c F = 0$, which reads

$$\partial_a F = 4(1+2k)(2a+b+c-(1+2k)) = 0, \tag{B.28}$$
$$\partial_b F = 2(2b-(4k+3))k + 4c(1+k) + 4a(1+2k) = 0, \tag{B.29}$$
$$\partial_c F = 2(2c-(4k+3))k + 4b(1+k) + 4a(1+2k) = 0, \tag{B.30}$$

and we have to take into account the boundary of the space of parameters, which leads to 8 cases to be considered, depending on whether the inequalities $a, b, c \geq 0$ are saturated, which are summarized in the following table:

$(a=0, b=0, c=0)$	(a^*, b^*, c^*)	$F(a^*, b^*, c^*)$
(Y,Y,Y)	$(0,0,0)$	$4k(1+k)(1+2k)$
(Y,Y,N)	$(0,0,3/2+2k)$	$-k/2$
(Y,N,Y)	$(0,3/2+2k,0)$	$-k/2$
(Y,N,N)	$(0,\frac{k(3+4k)}{2(1+2k)},\frac{k(3+4k)}{2(1+2k)})$	$\frac{k(8k^2+11k+4)}{1+2k}$
(N,Y,Y)	$(1/2+k,0,0)$	$-(1+2k)$
(N,Y,N)	$(k/2,0,1+k)$	k^2
(N,N,Y)	$(k/2,1+k,0)$	k^2
(N,N,N)	The system is incompatible	N/A

(B.31)

Thus, in order to prove $F(a,b,c) \geq 0$ on $Ext(\mathbb{P}_2^{\mathfrak{S}_n})$, we need to inspect the cases where $F(a^*,b^*,c^*)$ is negative. Since $k > 0$, it is immediate to see from (B.31) that this occurs when two, and only two, of the variables a, b, c are set equal to zero.

Observe that, in such cases, F is a quadratic function of the remaining nonzero variable. Thus, it is needed to check just two cases; namely, the neighboring integer values to the optimal value given in (B.31) for this

nonzero variable (which is a real number in general, but we have to ensure $a, b, c \in \mathbb{Z}$ in order to be at $Ext(\mathbb{P}_2^{\mathfrak{S}_n})$)[2].

In the following table we have collected the local deterministic strategies for which $F = 0$ (the rest are $F > 0$ so they are not listed) thus proving inequality (4.86). The first two rows of (B.32) come from the condition $c > 0$; the third and the fourth come from the condition $b > 0$; the remaining rows of (B.32) are obtained from $a > 0$.

a	b	c	d	$\mathcal{S}_0$	$\mathcal{S}_1$	$\mathcal{Z}$	n
0	0	$1+2k$	$n-(2k+1)$	$-n$	$2(2k+1)-n$	$n-2(2k+1)$	n
0	0	$2+2k$	$n-(2k+2)$	$-n$	$4(k+1)-n$	$n-4(k+1)$	n
0	$1+2k$	0	$n-(2k+1)$	$2(2k+1)-n$	$-n$	$n-2(2k+1)$	n
0	$2+2k$	0	$n-(2k+2)$	$4(k+1)-n$	$-n$	$n-4(k+1)$	n
k	0	0	$n-(k+1)+1$	$2k-n$	$2k-n$	n	n
k	0	1	$n-(k+1)$	$2k-n$	$2(k+1)-n$	$n-2$	n
k	1	0	$n-(k+1)$	$2(k+1)-n$	$2k-n$	$n-2$	n
$k+1$	0	0	$n-(k+1)$	$2(k+1)-n$	$2(k+1)-n$	n	n

(B.32)

Recall that the Bell inequalities belonging to the class (4.86) are symmetric under the exchange of measurements. This fact is reflected into the following: if a vertex exists for which $F = 0$, then by swapping b and c (note that these variables corresponded to $(\mathcal{M}_0, \mathcal{M}_1) = (+,-)$ and $(\mathcal{M}_0, \mathcal{M}_1) = (-,+)$, respectively) we always obtain another vertex for which $F = 0$. Equivalently, one can swap the values of $\mathcal{S}_0$ and $\mathcal{S}_1$, and the same happens. □

Proof of Theorem 4.14

Proof. Let us start by making a general observation. For any vertex in $\mathbb{P}_2^{\mathfrak{S}_n}$, the following bounds hold:

$$-n \leq \mathcal{S}_{00}, \mathcal{S}_{11} \leq n(n-1), \qquad |\mathcal{S}_{01}| \leq n(n-1), \qquad |\mathcal{S}_0|, |\mathcal{S}_1| \leq n. \quad \text{(B.33)}$$

Observe that the dominating term in the Bell inequalities of the class (4.87 – 4.88) is the one corresponding to $\gamma\mathcal{S}_{00}/2$, as it amounts to $O(n^4)$, while the rest are $O(n^3)$.

[2] When this nonzero variable is ronded below (cf. the case $a > 0$ in table (B.32)), note that we have to take into account also the possibility that one of the variables that were set to zero increases its value by 1; otherwise solutions could be lost.

Hence, in order to minimize the value of the Bell inequality, a necessary condition is that the term containing $\mathcal{S}_{00}$ should be small, at least, it should not be greater than $O(n^3)$. As $\mathcal{S}_{00} = (\mathcal{S}_0)^2 - n$ in the vertices of $\mathbb{P}_2^{\mathfrak{S}_n}$, this suggests to treat $\mathcal{S}_0$ as a parameter and minimize, while $\mathcal{S}_0$ being fixed, the left hand side of (4.22) with the coefficients given in (4.87 – 4.88). This leaves us with just two variables to consider in the optimization, because n and $\mathcal{S}_0$ are fixed. We pick, for example, b and d, so that we have

$$a \equiv a(b) = \frac{n + \mathcal{S}_0}{2} - b, \qquad c \equiv c(d) = \frac{n - \mathcal{S}_0}{2} - d. \tag{B.34}$$

Equation (B.34) allows us to rewrite $\mathcal{S}_1$ and $\mathcal{Z}$ as

$$\mathcal{S}_1 = n - 2(b + d), \qquad \mathcal{Z} = \mathcal{S}_0 - 2(b - d). \tag{B.35}$$

Now the inequalities $a \geq 0, c \geq 0$ impose bounds on the acceptable values of b and d, which together with their non-negativity conditions become

$$0 \leq b \leq \frac{n + \mathcal{S}_0}{2}, \qquad 0 \leq d \leq \frac{n - \mathcal{S}_0}{2}. \tag{B.36}$$

We distinguish the cases of even n and odd n, which have a similar proof:

- Even n.
  By treating the Bell inequality (4.87) as a function of (b, d), with n and $\mathcal{S}_0$ being parameters, and by denoting it $I_{n,\mathcal{S}_0}(b, d)$ we write:
  - Case $a = 0$ (equivalently, $b = (n + \mathcal{S}_0)/2$). We have

    $$I_{n,\mathcal{S}_0}\left(\frac{n + \mathcal{S}_0}{2}, d\right) = -4d^2 + f_1(\nu, \mathcal{S}_0, n)d + f_0(\nu, \mathcal{S}_0, n), \tag{B.37}$$

    where f_i are expressions that are independent of d. Eq. (B.37) is a quadratic function of d, with the property that its second derivative is negative for all d, so Eq. (B.37) has only one maximum. Thus, its minimal value is attained at the boundary of the domain of d; *i.e.*, either at $d = 0$ or at $d = (n - \mathcal{S}_0)/2$. The first case does not lead to the optimal solution (See the supplementary material of [Tur+14a] for the case $\nu = 0$, where the same argument follows). The second case gives

    $$I_{n,\mathcal{S}_0}\left(\frac{n + \mathcal{S}_0}{2}, \frac{n - \mathcal{S}_0}{2}\right) = \binom{n}{2}(\mathcal{S}_0 + 2\nu)(\mathcal{S}_0 + 2\nu - 2), \tag{B.38}$$

which is minimal for $\mathcal{S}_0 = 1 - 2\nu$. However, since by hypothesis, n is even, $\mathcal{S}_0$ must be even as well, which is not the case. So we look for the closest even integers, which are $2 - 2\nu$ and -2ν. One readily sees from Eq. (B.38) that $I = 0$ on such points. Hence, we obtain the following tuples (a, b, c, d) that saturate I:

$$\left(0, \frac{n}{2} - \nu, 0, \frac{n}{2} + \nu\right), \qquad \left(0, \frac{n}{2} + 1 - \nu, 0, \frac{n}{2} - 1 + \nu\right). \tag{B.39}$$

– Case $b = 0$. In this case we consider

$$I_{n,\mathcal{S}_0}(0, d) = -4d^2 + g_1(\nu, \mathcal{S}_0, n)d + g_0(\nu, \mathcal{S}_0, n), \tag{B.40}$$

where g_i are some expressions which do not depend on d. Similarly as above, Eq. (B.40) implies that I has only one maximum, so its minimum must lie either at the boundary of the domain of the variable d, which is either $d = 0$ or $d = (n - \mathcal{S}_0)/2$.

If $d = 0$, we have that

$$I_{n,\mathcal{S}_0}(0, 0) = \binom{n}{2}(\mathcal{S}_0 + 2\nu)(\mathcal{S}_0 + 2\nu + 2), \tag{B.41}$$

which is minimal for $\mathcal{S}_0 = -1 - 2\nu$. Again, as $\mathcal{S}_0$ must be even (now it is odd), we consider two cases, $\mathcal{S}_0 = -2 - 2\nu$ and $\mathcal{S}_0 = -2\nu$, for which Eq. (B.41) becomes $I = 0$ on these points. We then obtain two additional tuples of (a, b, c, d):

$$\left(\frac{n}{2} - 1 - \nu, 0, \frac{n}{2} + 1 + \nu, 0\right), \qquad \left(\frac{n}{2} - \nu, 0, \frac{n}{2} + \nu, 0\right). \tag{B.42}$$

If $d = (n - \mathcal{S}_0)/2$ then

$$I_{n,\mathcal{S}_0}\left(0, \frac{n - \mathcal{S}_0}{2}\right) = (n - 1)(\mathcal{S}_0 + 2\nu)((n + 2)\mathcal{S}_0 + 2n\nu)/2, \tag{B.43}$$

which achieves its minimum for $\mathcal{S}_0 = -2\nu\frac{n+1}{n+2}$, which is not an integer. The closest even integers to $\mathcal{S}_0$ are -2ν and $-2\nu + 2$ and in this case, only -2ν leads to $I = 0$, which corresponds to the following tuple (a, b, c, d):

$$\left(\frac{n}{2} - \nu, 0, 0, \frac{n}{2} + \nu\right). \tag{B.44}$$

The points (B.39, B.42 and B.44) comprise all the vertices of $\mathbb{P}_2^{\mathfrak{S}_n}$ in which I is minimum, with corresponding value 0, showing that (4.87) is a valid Bell inequality, as there are no more cases to be taken into consideration.

- Odd n.
  The line of argument is similar to that of even n and we shall also discriminate the cases $a = 0$ and $b = 0$. We denote by $\tilde{I}$ the inequality corresponding to the class (4.88).
  - Case $a = 0$ (equivalently, $b = (n + \mathcal{S}_0)/2$). As in Eq. (B.37), we have

    $$\tilde{I}_{n,\mathcal{S}_0}\left(\frac{n+\mathcal{S}_0}{2}, d\right) = -4d^2 + \tilde{f}_1(\nu, \mathcal{S}_0, n)d + \tilde{f}_0(\nu, \mathcal{S}_0, n). \quad \text{(B.45)}$$

    Again, its second derivative is negative, so we shall find the minimum at the boundary; *i.e.,* either at $c = 0$ or $d = 0$. If we choose $d = 0$ (See the supplementary material of [Tur+14a] for the $\nu = 0$ studied in detail) then we obtain $\tilde{I} > 0$ for all n, so we are not interested in this case. Thus, we consider $d = (n - \mathcal{S}_0)/2$, and we have

    $$\tilde{I}_{n,\mathcal{S}_0}\left(\frac{n+\mathcal{S}_0}{2}, \frac{n-\mathcal{S}_0}{2}\right) = \binom{n}{2}(\mathcal{S}_0 + 2\nu + 1)(\mathcal{S}_0 + 2\nu - 1), \quad \text{(B.46)}$$

    an expression which is minimal for $\mathcal{S}_0 = -2\nu$. However, now n is odd by hypothesis, enforcing that $\mathcal{S}_0$ must be odd as well. Hence, the closest odd integer values to -2ν are $1 - 2\nu$ and $-1 - 2\nu$ which give the tuple (a, b, c, d) below that saturates the inequality $\tilde{I}$:

    $$\left(0, \frac{n \pm 1}{2} - \nu, 0, \frac{n \mp 1}{2} + \nu\right). \quad \text{(B.47)}$$

  - Case $b = 0$.
    Now we are considering

    $$\tilde{I}_{n,\mathcal{S}_0}(0, d) = -4d^2 + \tilde{g}_1(\nu, \mathcal{S}_0, n)d + \tilde{g}_0(\nu, \mathcal{S}_0, n), \quad \text{(B.48)}$$

    and we check the boundary of the domain of d.

In the case that $d = 0$, we work with the expression

$$\tilde{I}_{n,\mathcal{S}_0}(0,0) = \binom{n}{2}(\mathcal{S}_0 + 2\nu + 1)(\mathcal{S}_0 + 2\nu + 3), \tag{B.49}$$

which is minimal for $\mathcal{S}_0 = -2(1+\nu)$, which is an even number. As it has to be odd, the candidates to be considered are its neighbours; namely $-3-2\nu$ and $-1-2\nu$, both of which produce a value of $\tilde{I} = 0$. We obtain two tuples (a, b, c, d) which are

$$\left(\frac{n-1}{2} - \nu, 0, \frac{n+1}{2} + \nu, 0\right), \qquad \left(\frac{n-3}{2} - \nu, 0, \frac{n+3}{2} + \nu, 0\right). \tag{B.50}$$

Finally, if $d = (n - \mathcal{S}_0)/2$, we consider

$$\tilde{I}_{n,\mathcal{S}_0}\left(0, \frac{n-\mathcal{S}_0}{2}\right) = (n-1)(\mathcal{S}_0+2\nu+1)(2\mathcal{S}_0+n(\mathcal{S}_0+2\nu+1))/2, \tag{B.51}$$

an expression that is minimal for $\mathcal{S}_0 = -(1+2\nu)\frac{n+1}{n+2}$, a value which, again, is not integer. The closest odd integers in this case are $-(1+2\nu)$ and $1-2\nu$, and the smallest value of $\tilde{I}$ is given by the former, for which we obtain $\tilde{I} = 0$ and the last tuple (a, b, c, d):

$$\left(\frac{n-1}{2} - \nu, 0, 0, \frac{n+1}{2} + \nu\right). \tag{B.52}$$

Since the points (B.47, B.50 and B.52) are all five vertices of $\mathbb{P}_2^{\mathfrak{S}_n}$ in which $\tilde{I}$ is minimum and it is 0, we have proved that (4.87) is a valid Bell inequality, as there are no remaining cases.

□

C. Tables

#	β_c	α	β	γ	δ	ε
1	1	0	0	0	0	1
2	18	-2	6	-2	-3	6
3	3	0	0	1	1	0
4	6	2	2	0	1	0
5	3	2	0	1	0	0
6	3	0	0	0	0	-1

Table C.1.: Equivalence classes for the facets of $\mathbb{P}_2^{\mathfrak{S}_n}$ for $n = 3$.

#	β_c	α	β	γ	δ	ε
1	2	0	-1	0	0	1
2	42	-9	12	1	-6	6
3	30	-3	-12	-1	2	6
4	54	-6	12	-1	-8	12
5	20	-3	5	0	-3	4
6	18	0	0	-1	-2	6
7	12	-3	-3	1	2	1
8	6	0	3	0	0	1
9	8	1	3	0	1	2
10	6	0	0	0	1	1
11	8	-2	0	1	1	1
12	12	3	3	0	1	0
13	6	0	0	0	0	-1

Table C.2.: Equivalence classes for the facets of $\mathbb{P}_2^{\mathfrak{S}_n}$ for $n = 4$.

#	β_c	α	β	γ	δ	ε
1	4	0	-2	0	0	1
2	8	0	0	0	-1	2
3	24	-6	6	1	-2	1
4	14	-4	2	1	-1	1
5	400	-36	60	2	-45	60
6	160	-12	-60	-2	5	20
7	90	-20	22	3	-8	5
8	80	4	-20	-2	-5	20
9	20	-2	8	0	-1	3
10	130	-28	-36	3	10	8
11	110	-24	-30	3	9	7
12	10	0	2	1	1	1
13	20	0	0	3	3	1
14	20	4	4	0	1	0
15	70	-20	-14	5	5	1
16	20	-4	0	3	2	1
17	20	4	4	1	2	1
18	200	-60	-24	30	15	-2
19	40	8	12	1	3	3
20	30	4	10	1	2	3
21	40	6	12	0	3	5
22	10	4	0	1	0	0
23	2	0	0	1	0	0
24	10	0	0	0	0	-1

Table C.3.: Equivalence classes for the facets of $\mathbb{P}_2^{\mathfrak{S}_n}$ for $n = 5$.

#	β_c	α	β	γ	δ	ε
1	7	0	-3	0	0	1
2	16	-4	2	1	-1	1
3	15	1	-4	0	-1	3
4	240	15	-45	-1	-18	45
5	132	-25	27	4	-9	6
6	180	-10	-60	-1	3	15
7	70	-18	12	3	-3	1

8	52	-15	7	3	-2	1
9	156	-35	31	5	-8	3
10	375	-30	45	8	-36	45
11	90	5	-30	-1	-3	15
12	300	0	0	1	-27	45
13	34	-7	7	1	-2	1
14	24	-3	1	1	-2	3
15	114	-15	19	4	-11	12
16	129	-20	24	5	-12	12
17	225	-54	41	8	-10	3
18	192	-46	36	7	-9	3
19	39	3	-8	0	-3	7
20	112	12	-26	1	-9	17
21	156	17	-37	1	-12	23
22	42	-9	-9	1	2	1
23	3	0	1	0	0	1
24	120	-20	30	1	-5	5
25	240	-45	-55	4	13	10
26	165	-20	-40	1	12	20
27	24	-6	-4	1	1	1
28	195	-20	60	-1	-8	20
29	24	-3	7	0	-1	2
30	60	0	0	-1	3	15
31	87	-15	-22	1	4	4
32	12	-2	0	1	1	1
33	30	-5	-5	2	3	2
34	15	0	5	0	0	1
35	42	3	15	0	1	4
36	24	1	5	1	2	3
37	45	5	10	1	4	6
38	51	4	15	1	3	6
39	99	11	20	2	9	13
40	273	32	60	5	24	36
41	105	-30	-15	6	4	1
42	87	-27	-10	6	3	1
43	51	-16	-5	4	2	1
44	48	-13	-5	4	3	2

45	30	0	0	1	3	3
46	39	12	-3	4	-2	1
47	30	5	5	0	1	0
48	15	0	0	0	0	-1

Table C.4.: Equivalence classes for the facets of $\mathbb{P}_2^{\mathfrak{S}_n}$ for $n = 6$.

#	β_c	α	β	γ_1	δ_1	δ_2	ε_1
1	1	0	0	0	0	0	1
2	3	0	0	0	1	-1	-1
3	3	0	0	1	1	1	0
4	3	1	1	0	1	0	0
5	3	2	0	1	0	0	0
6	9	-1	-3	-1	1	2	3

Table C.5.: The list of classes of three-partite translationally invariant two-body Bell inequalities (4.123) completely defining $\mathbb{P}_2^{\mathbb{Z}_n}$ for $n = 3$.

#	β_N	β_Q	β_Q^{TI}	β_c	α	β	γ_1	δ_1	δ_3	ε_1	γ_2	δ_2	ε_2
1	4	4.00	4.00	4	0	2	0	0	0	0	0	0	1
2	4	4.00	4.00	4	1	1	0	0	1	0	0	0	0
3	4	4.00	4.00	4	1	1	0	0	0	0	0	1	0
4	4	4.00	4.00	4	0	-2	0	0	0	2	0	0	1
5	4	4.00	4.00	4	0	0	0	0	1	1	0	1	0
6	4	4.00	4.00	4	0	2	0	0	0	1	0	0	0
7	4	4.00	4.00	4	0	0	0	1	1	0	0	0	1
8	4	4.00	4.00	4	0	0	0	0	0	-2	0	0	1
9	8	8.00	8.00	8	-1	-1	-1	1	1	1	1	1	0
10	8	8.00	8.00	8	-1	1	1	1	1	1	0	1	1
11	8	8.00	8.00	8	0	2	-1	-1	1	1	0	0	0
12	8	8.00	8.00	8	1	1	0	1	1	-2	0	-1	1
13	8	8.00	8.00	8	-1	3	0	-1	-1	2	0	-1	1
14	8	8.00	8.00	8	-2	-2	1	1	1	1	0	2	0
15	8	8.00	8.00	8	-2	-2	0	2	2	0	1	0	1
16	16	16.00	16.00	16	0	4	0	2	2	4	1	2	1
17	16	16.00	16.00	16	-4	0	2	2	2	2	1	2	1
18	16	16.00	16.00	16	2	2	-2	3	1	-2	1	-2	1
19	20	20.00	20.00	20	-3	5	0	-3	-3	4	0	-3	2
20	20	20.00	20.00	20	-1	5	-1	-2	-2	5	1	-3	1
21	44/3	12.00	12.00	12	0	2	-2	0	2	2	1	0	0
22	116/5	20.00	20.00	20	0	4	-1	-3	3	3	-1	2	0

Continued on the next page...

Table C.6.: continued.

#	β_N	β_Q	β_Q^{TI}	β_c	α	β	γ_1	δ_1	δ_3	ε_1	γ_2	δ_2	ε_2
23	32	28.00	28.00	28	-2	-8	-2	-2	4	4	-1	2	2
24	32	28.00	28.00	28	-2	-8	-4	0	4	4	1	0	2
25	48/5	8.42	8.42	8	-2	-2	1	0	1	1	0	1	0
26	12	9.27	9.27	8	0	0	-2	-1	-1	2	1	0	1
27	16	11.31	11.31	8	0	0	0	0	0	0	-1	2	1
28	76/5	12.26	12.26	12	0	2	-2	0	0	2	1	2	0
29	76/5	12.97	12.97	12	0	2	-3	-1	-1	1	1	2	0
30	52/3	13.60	13.60	12	0	0	-1	-1	-2	4	0	-1	2
31	20	14.42	14.42	12	0	0	1	1	2	2	-1	3	1
32	20	14.77	14.77	12	0	0	0	-1	-1	4	-1	-2	2
33	96/5	16.60	16.60	16	-2	-2	1	2	2	-4	0	0	3
34	96/5	16.72	16.72	16	-4	-4	1	2	2	0	0	2	1
35	64/3	17.25	17.25	16	-1	-1	-5	2	2	1	3	-1	0
36	24	17.50	17.50	16	1	3	1	2	2	3	-1	3	2
37	24	18.02	18.02	16	0	0	-2	-3	-3	4	1	0	3
38	24	18.37	18.37	16	-2	-2	2	2	2	2	-1	4	1
39	116/5	20.36	20.36	20	-2	-4	0	2	2	4	1	4	0
40	24	20.77	20.77	20	-2	-8	-1	2	2	4	0	0	2
41	24	20.84	20.84	20	-2	-8	-1	1	1	4	0	2	2
42	28	21.18	21.18	20	-2	4	0	-2	-2	4	-1	-4	2
43	28	21.89	21.89	20	0	2	-6	2	2	2	3	-2	0
44	28	21.93	21.93	20	0	2	-4	-2	-2	0	2	4	-1
45	32	25.01	25.01	24	0	4	-2	2	4	0	-1	-4	3
46	32	25.30	25.30	24	-2	-2	-6	4	4	2	5	0	1
47	32	28.40	28.40	28	-2	-8	-4	0	0	4	1	4	2
48	156/5	28.41	28.41	28	-6	8	1	-4	-4	4	0	-4	2
49	156/5	28.48	28.48	28	-6	8	0	-4	-4	4	1	-4	2
50	36	29.20	29.20	28	-1	-7	-2	4	4	2	0	-3	4
51	36	29.25	29.25	28	-2	4	-2	-6	-4	6	1	-2	4
52	36	29.29	29.29	28	-4	-4	0	3	3	4	2	6	-1
53	44	31.73	31.73	28	-2	4	1	-3	-3	7	-2	-6	3
54	44	31.84	31.84	28	-2	4	0	-2	-2	6	-2	-6	3
55	40	33.64	33.64	32	-4	0	0	4	4	-4	-1	-6	3
56	124/3	36.57	36.57	36	-4	8	-1	-5	-6	8	0	-5	4
57	52	39.11	39.11	36	-2	4	-4	-8	-8	6	3	0	6
58	60	42.82	42.82	36	2	-4	2	-4	-4	8	-3	-8	4
59	48	40.92	40.92	40	-4	8	-2	-8	-6	8	1	-4	5
60	56	42.32	42.32	40	-4	8	1	-5	-5	9	-2	-8	4
61	64	50.49	50.49	48	-4	8	-4	-10	-10	8	3	-2	7
62	500/7	62.89	62.89	60	-14	16	-4	-8	-8	4	5	-4	2
63	104	74.50	74.50	64	-4	8	4	-8	-8	12	-5	-14	7
64	10	8.83	8.00	8	-2	0	1	1	-1	1	0	0	0
65	18	16.56	16.00	16	-3	-1	1	-2	3	1	0	2	-1
66	56/3	16.59	16.00	16	2	2	-2	1	-1	-2	1	2	1
67	68/3	20.46	20.00	20	-2	4	-1	-2	-4	4	0	-2	2
68	24	21.24	20.00	20	-2	4	-2	-2	-4	4	1	-2	2
69	100/3	29.15	28.00	28	-2	4	-2	-2	-6	6	0	-2	3
70	44/3	12.52	12.05	12	-1	3	-2	-1	-2	2	1	0	1

Continued on the next page...

Table C.6.: continued.

#	β_N	β_Q	β_Q^{TI}	β_c	α	β	γ_1	δ_1	δ_3	ε_1	γ_2	δ_2	ε_2
71	24	21.31	20.06	20	-2	6	1	-3	0	4	-1	-3	1
72	192/5	32.69	32.10	32	-1	-7	-1	-4	5	5	-2	4	1
73	96/5	16.45	16.18	16	-2	-2	1	-2	4	1	-1	2	-1
74	44/3	12.60	12.21	12	-1	-1	-3	1	2	1	2	0	0
75	96/5	16.60	16.28	16	-4	-2	2	-1	3	1	0	2	-1
76	20	17.66	16.36	16	0	4	0	-2	2	2	-1	2	1
77	20	17.66	16.43	16	-1	-5	0	-1	2	3	-1	2	1
78	28	24.47	24.44	24	-4	8	1	-2	-2	4	-1	-4	2
79	16	13.66	12.58	12	0	2	1	0	2	2	-1	2	1
80	24	21.43	20.63	20	-2	-8	0	0	2	4	-1	2	2
81	24	21.43	20.68	20	-4	2	2	-4	2	2	0	-2	-1
82	500/7	61.83	60.69	60	-10	12	-12	-8	-8	4	9	0	2
83	32	25.00	24.70	24	0	4	2	2	4	4	-1	4	3
84	16	13.66	12.75	12	0	2	-2	2	2	2	2	0	1
85	36	31.31	28.82	28	-2	8	1	-4	0	6	-2	-4	2
86	44	36.89	36.85	36	-4	8	0	-5	-5	8	-1	-6	4
87	44	39.31	36.90	36	-6	-12	1	0	4	4	-2	4	2
88	28	25.31	24.90	24	-8	-4	3	3	0	1	1	3	-1
89	24	21.43	20.93	20	-2	-8	-2	2	2	4	1	0	2
90	16	13.66	12.93	12	0	2	-1	0	2	0	-1	-2	1
91	16	13.66	13.14	12	-2	-2	1	1	1	0	-1	2	1
92	36	31.31	29.15	28	-2	-8	-1	-2	2	4	-2	4	2
93	32	27.31	25.19	24	-2	6	-4	-4	-4	4	3	0	3
94	20	17.66	17.21	16	0	4	-2	2	2	2	1	-2	1
95	40	30.62	29.27	28	-2	4	-4	-6	-6	4	3	0	4
96	44	39.31	37.82	36	-6	-12	-4	4	4	4	3	0	2
97	36	31.31	29.87	28	-2	-8	-4	4	4	4	2	-2	3
98	44	38.70	37.98	36	-2	-8	-8	4	4	4	3	-4	2
99	40	30.85	30.06	28	-2	4	-8	-4	-4	4	5	0	2
100	268/5	46.34	46.15	44	-10	12	3	-4	-4	4	-2	-8	2
101	32	23.31	22.77	20	-2	4	1	-2	-2	4	-2	-4	2
102	88	68.91	67.63	64	-4	8	-8	-14	-14	8	5	2	9
103	80	69.75	67.97	64	-4	-16	-8	10	10	8	3	-6	7

Table C.6.: The list of all classes of four-partite translationally invariant two-body Bell inequalities (4.125) that completely define $\mathbb{P}_2^{\mathbb{Z}_n}$ for $n = 4$. With β_{NS}, β_Q and β_c we denote, respectively, the maximal value that the Bell inequality can take under nonsignalling, quantum or classical correlations. By β_Q^{TI} we denote the maximal quantum violation with the same qubit observables per site; in this case, the Bell operator is translationally invariant.

Acronyms

AGCA	Aolita-Gallego-Cabello-Acín. 186–189, 200, 201, 203, 204, 206, 207
BEC	Bose-Einstein Condensate. 146
BKP	Barrett-Kent-Pironio. 180, 181, 183–188, 197, 201, 204
BS	Bounded-Storage. 196
CDD	C-library Double Description method. 107, 133–135, 137
CES	Completely Entangled Subspace. 21
CGLMP	Collins-Gisin-Linden-Massar-Popescu. 107, 181
CHSH	Clauser-Horne-Shimony-Holt. 10, 31, 79, 135, 136, 138, 178, 180, 181, 190, 192, 194
CP	Completely Positive. 18, 19, 22, 163
CPTP	Completely Positive and Trace Preserving. 18, 162
CQRNG	Certified Quantum Random Number Generation. 3, 79
DI	Device-Independent. 2, 3, 10, 23, 79, 179, 180, 193, 196, 199
DIQIP	Device-Independent Quantum Information Processing. 2, 3, 7, 212
DIQKD	Device-Independent Quantum Key Distribution. 3, 10, 79, 179, 180, 196, 212
DLS	Deterministic Local Strategy. 89, 91, 94, 96–98, 102, 122–124, 132, 133, 149

DMRG	Density Matrix Renormalization Group. 211
DW	Dimensionality Witnessing. 3, 79
EPR	Einstein-Podolsky-Rosen. 2, 22, 79, 81
EPR2	Elitzur-Popescu-Rohrlich. 31
EW	Entanglement Witness. 18, 20–22, 51, 268, 269
GHZ	Greenberger-Horne-Zeilinger. 110, 172
GME	Genuinely Multipartite Entangled. 4, 6, 9, 16, 17, 32, 35, 36, 39, 42, 43, 81, 110, 158, 162, 164–166, 168, 171–175, 212
GMN	Genuinely Multipartite Nonlocal. 6, 9, 30, 32, 81, 158, 173, 174, 211, 212, 267
GYNI	Guess-Your-Neighbor-Input. 136
IID	Independent and Identically Distributed. 23
l. h. s.	Left-hand side. 48, 51, 53, 100, 101, 103, 107, 108, 162
LHVM	Local Hidden Variable Model. 6, 9, 22, 23, 28, 29, 32, 79, 80, 94, 157–159, 177, 267, 269
LMG	Lipkin-Meshkov-Glick. 8, 118, 119, 211
LOCC	Local Operations and Classical Communication. 15, 18
MOT	Magneto-Optical Trap. 146
MPS	Matrix Product States. 5, 82, 211
NP	Nondeterministic Polynomial time. 17, 37, 59, 81, 99
NPA	Navascués-Pironio-Acín. 27, 99, 180, 193, 194
NS	No-Signalling. 9, 10, 25, 26, 31, 80, 173, 177, 178, 180, 181, 184–186, 188, 189, 195–198, 200, 202, 203, 205, 206, 212, 213, 269

NSBL No-Signalling Bi-Local. 30, 173, 174, 211, 212, 269
NV Nitrogen-Vacancy. 81

PI Permutationally Invariant. 5, 8, 11, 32, 33, 35, 210
PM Projective Measurement. 27
POVM Positive-Operator Valued Measure. 27, 81, 107, 159, 163, 164, 169–173, 212
PPT Positive under Partial Transposition. 3, 4, 7, 8, 10, 18, 19, 35–38, 40, 43, 44, 46, 47, 50–53, 55–61, 63–75, 78, 209, 210, 270
PPTESS PPT entangled symmetric states. 4, 7, 8, 37, 38, 53, 63, 64, 67, 68, 73, 209, 210
PR Popescu-Rohrlich. 26

QIP Quantum Information Processing. 2, 3, 6, 7, 79
QIT Quantum Information Theory. 9
QKD Quantum Key Distribution. 2
QPT Quantum Phase Transition. 5, 81, 82
QT Quantum Theory. 1, 2, 9, 26, 159, 177, 178, 180, 190, 191, 193, 196, 197, 199, 200, 206, 213, 269

r. h. s. Right-hand side. 159, 202
RA Randomness Amplification. 3, 10, 79, 196, 199, 200, 206, 207, 212, 213

SDP Semi-Definite Program. 27, 131, 193, 194, 211
SeDuMi Self-Dual Minimization. 194
SPA Structural Physical Approximation. 22
SV Santha-Vazirani. 199, 200, 206, 207

TI Translationally Invariant. 5, 8, 9, 210, 211

TOBL	Time-Ordered Bi-Local. 30, 173, 174, 211, 212, 269
TP	Trace Preserving. 18, 163

Notation

(n, m, d)	A Bell scenario of n parties with m d-valued observables each. 24, 81, 84, 86, 95, 99, 122, 127, 211, 213
$\lfloor \cdot \rceil$	The rounding function. 112
Λ	The space of hidden variables for a LHVM. 28
δ	The Kronecker Delta function. 28
$\lvert i \rangle$	The i-th element from the computational basis of $\mathcal{H}$. 14
$\lceil \cdot \rceil$	The ceiling function. 49
$\lfloor \cdot \rfloor$	The floor function. 25
$\mathbb{C}$	The field of Complex numbers. 14, 268, 269
$\mathbb{R}$	The field of Real numbers. 18, 268
$\mathbf{P}$	The polytope of mathematically sound correlations. 25, 30
$\mathbf{P}_{\text{Svetlichny}}$	The polytope of Svetlichny correlations of GMN. 30
Tr	The trace operator. 14
$\otimes$	Tensor product. 15
ρ	An element from $\mathcal{D}(\mathcal{H})$. 14
$\succeq$	Positive semi-definite ($A \succeq B \iff A - B \succeq 0$). 14
$\vec{P}$	A vector of correlations. 24, 25, 31, 181, 185, 186, 191, 200, 203
$\widehat{\cdot}$	A missing element. 26
p_i	A probability distribution. 15
$\mathcal{B}(\mathcal{H})$	The set of bounded linear operators acting on $\mathcal{H}$. 14, 270
$\mathcal{D}_{\text{sep}}$	The set of separable states. 18–20

$\mathcal{P}_K$	The set of K-body correlators. 88
$\mathcal{U}_d$	The group of $d \times d$ unitary matrices. 33, 215, 221, 222
(R, V)	A representation of the group G on the vector space V. 216, 268
E_G	Geometric measure of Entanglement. 135
G'	The centralizer of a group G. 222
G	A group. 88, 215, 268, 269
$K_{\mathbb{C}}$	Grothendieck's constant over $\mathbb{C}$. 160, 162
$K_{\mathbb{R}}$	Grothendieck's constant over $\mathbb{R}$. 160
M_d	The set of $d \times d$ matrices with complex entries. 14, 21
$P_{\mathbf{A}}$	The projector onto the symmetric subspace. 41
$S\|\overline{S}$	A bipartition of $\mathbf{A}$. 16, 19, 35, 270
V^G	The vector subspace of V fixed by a representation (R, V) of G. 218
V	A vector space. 216, 268, 269
$[g]$	A conjugacy class of a group G. 220
Δ_W	The set of states detected by W. 20
Im	Image or Range. 40
Π_W	The set of product states with zero expectation value on W. 20
Π_σ	The permutation matrix representing σ. 32, 41, 221, 222
Ξ_U	The simultaneous action of U on every subsystem. 221, 222
$\mathcal{H}$	A finite-dimensional complex Hilbert Space. 14, 222, 267, 270
$\mathcal{L}$	The set of linear maps. 21
$\mathcal{W}$	The set of EWs. 20
$\cap$	Intersection. 16
χ	The character of a representation (R, V). 219
$\cong$	Isomorphism. 33
$\cup$	Union. 21
$\emptyset$	The empty set. 16

$\equiv$	Congruence. 103
gcd	Greatest Common Divisor. 105
$\hat{\mathbf{n}}$	A real 3-dimensional unit vector. 108, 191
ker	Kernel. 40
$\|D_n^k\rangle$	The Dicke state of n qubits with k excitations. 34, 35
$\leq$	Subgroup. 87, 88
$\mathbb{1}_d$	The identity matrix acting on a d-dimensional Hilbert Space. 14
$\mathbb{C}[x, y]$	The ring of polynomials in the variables x and y with coefficients in $\mathbb{C}$. 47
$\mathbb{Z}_n$	The ideal of integer numbers *modulo* n. 131
$\mathbf{A}$	A set of parties $\{A_1, \ldots, A_n\}$. 16, 19, 31, 186, 189, 212, 268, 270
$\mathbf{P}_L$	The polytope of correlations compatible with a LHVM. 28, 30, 31
$\mathbf{P}_{NSBL}$	The polytope of NSBL correlations. 30
$\mathbf{P}_{NS}$	The polytope of NS correlations. 26, 31, 180, 184–186, 190, 196, 200, 203
$\mathbf{P}_{TOBL}$	The polytope of TOBL correlations. 30
$\mathbf{Q}$	The set of QT correlations. 26, 180, 190, 191, 193, 196
$\mathrm{Aut}(V)$	The set of automorphisms of V. 216
CH	Convex Hull. 95, 131
$\mathrm{End}(V)$	The set of endomorphisms of V. 216
Ext	The set of extremal points of the convex set S. 15, 21, 59, 87
$\mathrm{GL}(V)$	The general linear group acting on a finite-dimensional V. 216
$\mathrm{Hom}(V_1, V_2)^G$	The set of G-invariant homomorphisms between two vector spaces. 218
$\mathrm{Hom}(V_1, V_2)$	The set of homomorphisms between two vector spaces. 218
Opt	The set of Optimal EWs. 21
Span	The subspace spanned by a set. 35
mod	*Modulo*. 103

$\operatorname{sgn}(\sigma)$	The parity of the permutation $\sigma \in \mathfrak{S}_n$. 217
$\oplus$	Direct sum. 33
∂	The boundary of a set. 21
$\propto$	Proportional. 61
$\setminus$	Intersection with the complementary set. 16, 21
$\sqcup$	Disjoint union. 88, 169, 171
$\subseteq$	Subset of. 16
$\vdash$	Partition of. 33, 124–126, 220, 222
$\vec{\boldsymbol{\sigma}}$	A vector of pauli matrices $[\sigma_x, \sigma_y, \sigma_z]$. 108, 143, 191
$\vec{\mathbf{J}}$	A vector of spin component matrices $[J_x, J_y, J_z]$. 143
$\vec{r}_{\mathbf{A}}$	The ranks of a state and its partial transpositions. 46, 63
$\{p_i, \lvert\psi_i\rangle\}_i$	An ensemble generating a quantum state (*cf.* Eq. (2.1)). 15, 18
$r(\lvert\psi\rangle)$	The Schmidt Rank of $\lvert\psi\rangle$. 17
$\mathcal{D}(\mathcal{H})$	The set of elements of $\mathcal{B}(\mathcal{H})$ that correspond to quantum states. 14, 191, 267
$\mathcal{D}^{\mathrm{PPT},S}(\mathcal{H})$	The set of states that are PPT with respect to the $S\lvert\overline{S}$ bipartition. 59
$\mathcal{D}_{\mathcal{S}}^{\mathrm{PPT}}(\mathcal{H})$	The set of fully PPT symmetric states. 36, 40
$\mathcal{S}(\mathcal{H})$	The symmetric subspace of $\mathcal{H}$. 35
$\mathcal{S}_K$	The set of K-partitions of $\mathbf{A}$. 16
$\mathfrak{S}_n$	The symmetric group of permutations of n elements. 32, 33, 41, 87, 88, 215, 217, 221, 222, 270
$\lvert$	Divisor of. 132

Bibliography

[ADA14] R Augusiak, M Demianowicz, and A Acín Local hidden–variable models for entangled quantum states in: *Journal of Physics A: Mathematical and Theoretical*, **47**:42 (2014), 424002 DOI: 10.1088/1751-8113/47/42/424002 (see pp. 30, 156)

[AGR82] Alain Aspect, Philippe Grangier, and Gérard Roger Experimental Realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: A New Violation of Bell's Inequalities in: *Phys. Rev. Lett.*, **49**: (2 1982), 91–94 DOI: 10.1103/PhysRevLett.49.91 (see pp. 2, 21)

[AGT06] Antonio Acín, Nicolas Gisin, and Benjamin Toner Grothendieck's constant and local models for noisy entangled quantum states in: *Phys. Rev. A*, **73**: (6 2006), 062105 DOI: 10.1103/PhysRevA.73.062105 (see p. 159)

[Alm+07] Mafalda L. Almeida, Stefano Pironio, Jonathan Barrett, Géza Tóth, and Antonio Acín Noise Robustness of the Nonlocality of Entangled Quantum States in: *Phys. Rev. Lett.*, **99**: (4 2007), 040403 DOI: 10.1103/PhysRevLett.99.040403 (see pp. 158, 170)

[Alm+10a] Mafalda L. Almeida, Jean-Daniel Bancal, Nicolas Brunner, Antonio Acín, Nicolas Gisin, and Stefano Pironio Guess Your Neighbor's Input: A Multipartite Nonlocal Game with No Quantum Advantage in: *Phys. Rev. Lett.*, **104**: (23 2010), 230404 DOI: 10.1103/PhysRevLett.104.230404 (see p. 134)

[Alm+10b] Mafalda L. Almeida, Daniel Cavalcanti, Valerio Scarani, and Antonio Acín Multipartite fully nonlocal quantum states in: *Phys. Rev. A*, **81**: (5 2010), 052111 DOI: 10.1103/PhysRevA.81.052111 (see p. 28)

[AMP12] ANTONIO ACÍN, SERGE MASSAR, and STEFANO PIRONIO Randomness versus Nonlocality and Entanglement in: *Phys. Rev. Lett.*, **108**: (10 2012), 100402 DOI: 10.1103/PhysRevLett.108.100402 (see p. 193)

[Aol+12] LEANDRO AOLITA, RODRIGO GALLEGO, ADÁN CABELLO, and ANTONIO ACÍN Fully Nonlocal, Monogamous, and Random Genuinely Multipartite Quantum Correlations in: *Phys. Rev. Lett.*, **108**: (10 2012), 100401 DOI: 10.1103/PhysRevLett.108.100401 (see pp. 9, 80, 177, 184, 186, 193, 196, 204)

[Arn12] FRANÇOIS ARNAULT A complete set of multidimensional Bell inequalities in: *Journal of Physics A: Mathematical and Theoretical*, **45**:25 (2012), 255304 DOI: 10.1088/1751-8113/45/25/255304 (see p. 127)

[AS65] MILTON ABRAMOWITZ and IRENE STEGUN *Handbook of Mathematical Functions: with Formulas, Graphs, and Mathematical Tables (Dover Books on Mathematics)* Dover Publications, 1965 ISBN: 0486612724 (see pp. 88, 123)

[ATL11] R AUGUSIAK, J TURA, and M LEWENSTEIN A note on the optimality of decomposable entanglement witnesses and completely entangled subspaces in: *Journal of Physics A: Mathematical and Theoretical*, **44**:21 (2011), 212001 DOI: 10.1088/1751-8113/44/21/212001 Featured with insights. Editor's choice: Highlights of 2011. (See p. 19)

[Aud06] KOENRAAD M. R. AUDENAERT *A Digest on Representation Theory of the Symmetric Group* 2006 (see p. 213)

[Aug+10] REMIGIUSZ AUGUSIAK, JANUSZ GRABOWSKI, MAREK KUŚ, and MACIEJ LEWENSTEIN Searching for extremal {PPT} entangled states in: *Optics Communications*, **283**:5 (2010) Quo vadis Quantum Optics?, 805–813 ISSN: 0030-4018 DOI: 10.1016/j.optcom.2009.10.050 (see pp. 35, 57, 58, 60)

[Aug+12] R. Augusiak, J. Tura, J. Samsonowicz, and M. Lewenstein Entangled symmetric states of N qubits with all positive partial transpositions in: *Phys. Rev. A*, **86**: (4 2012), 042316 DOI: 10.1103/PhysRevA.86.042316 (see pp. 7, 10, 36, 60, 117, 133)

[Aug+14a] R Augusiak, J Bae, J Tura, and M Lewenstein Checking the optimality of entanglement witnesses: an application to structural physical approximations in: *Journal of Physics A: Mathematical and Theoretical*, **47**:6 (2014), 065301 DOI: 10.1088/1751-8113/47/6/065301 Editor's choice: Highlights of 2014. (See p. 20)

[Aug+14b] R. Augusiak, M. Demianowicz, M. Pawłowski, J. Tura, and A. Acín Elemental and tight monogamy relations in nonsignaling theories in: *Phys. Rev. A*, **90**: (5 2014), 052323 DOI: 10.1103/PhysRevA.90.052323 (see pp. 9, 10, 178)

[Aug+14c] R. Augusiak, M. Demianowicz, J. Tura, and A. Acín *Entanglement and nonlocality are inequivalent for any number of particles* 2014 arXiv:1407.3114. Under review in Physical Review Letters (see pp. 9, 10, 156, 160)

[Ban+13] Jean-Daniel Bancal, Jonathan Barrett, Nicolas Gisin, and Stefano Pironio Definitions of multipartite nonlocality in: *Phys. Rev. A*, **88**: (1 2013), 014102 DOI: 10.1103/PhysRevA.88.014102 (see pp. 28, 171)

[Bar+05] Jonathan Barrett, Noah Linden, Serge Massar, Stefano Pironio, Sandu Popescu, and David Roberts Nonlocal correlations as an information-theoretic resource in: *Phys. Rev. A*, **71**: (2 2005), 022101 DOI: 10.1103/PhysRevA.71.022101 (see pp. 12, 24, 27, 77, 176)

[Bar02] Jonathan Barrett Nonsequential positive - operator - valued measurements on entangled mixed states do not always violate a Bell inequality in: *Phys. Rev. A*, **65**: (4 2002), 042302 DOI: 10.1103/PhysRevA.65.042302 (see pp. 6, 79, 157, 160, 161, 171)

[BB84] CHARLES H BENNETT and GILLES BRASSARD "Quantum cryptography: Public key distribution and coin tossing" in: *Proceedings of International Conference on Computers, Systems and Signal Processing* vol. 175 150 1984, 175–179 (see p. 2)

[BC90] SAMUEL L BRAUNSTEIN and CARLTON M CAVES Wringing out better Bell inequalities in: *Annals of Physics*, **202**:1 (1990), 22–56 ISSN: 0003-4916 DOI: 10.1016/0003-4916(90)90339-P (see p. 179)

[Bel04] J.S. BELL *Speakable and Unspeakable in Quantum Mechanics: Collected Papers on Quantum Philosophy* Collected papers on quantum philosophy Cambridge University Press, 2004 ISBN: 9780521523387 (see p. 77)

[Bel64] JOHN S BELL On the einstein-podolsky-rosen paradox in: *Physics*, **1**:3 (1964), 195–200 (see pp. 2, 11, 20, 27, 77, 155)

[Ben+93] CHARLES H. BENNETT, GILLES BRASSARD, CLAUDE CRÉPEAU, RICHARD JOZSA, ASHER PERES, and WILLIAM K. WOOTTERS Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels in: *Phys. Rev. Lett.*, **70**: (13 1993), 1895–1899 DOI: 10.1103/PhysRevLett.70.1895 (see pp. 2, 12)

[BFL91] LÁSZLÓ BABAI, LANCE FORTNOW, and CARSTEN LUND Non-deterministic exponential time has two-prover interactive protocols English in: *computational complexity*, **1**:1 (1991), 3–40 ISSN: 1016-3328 DOI: 10.1007/BF01200056 (see p. 79)

[BGP10] JEAN-DANIEL BANCAL, NICOLAS GISIN, and STEFANO PIRONIO Looking for symmetric Bell inequalities in: *Journal of Physics A: Mathematical and Theoretical*, **43**:38 (2010), 385303 DOI: 10.1088/1751-8113/43/38/385303 (see pp. 80, 81, 84, 85, 88, 209)

[BKP06] JONATHAN BARRETT, ADRIAN KENT, and STEFANO PIRONIO Maximally Nonlocal and Monogamous Quantum Correlations in: *Phys. Rev. Lett.*, **97**: (17 2006), 170409 DOI:

10.1103/PhysRevLett.97.170409 (see pp. 9, 177, 178, 183, 193, 194, 196, 204)

[Boh52] DAVID BOHM A Suggested Interpretation of the Quantum Theory in Terms of "Hidden" Variables. I in: *Phys. Rev.*, **85**: (2 1952), 166–179 DOI: 10.1103/PhysRev.85.166 (see p. 195)

[Boo62] GEORGE BOOLE On the Theory of Probabilities in: *Philosophical Transactions of the Royal Society of London*, **152**: (1862), 225–252 DOI: 10.1098/rstl.1862.0015 (see p. 22)

[BPT] GRIGORIY BLEKHERMAN, PABLO A. PARRILO, and REKHA R. THOMAS *Semidefinite Optimization and Convex Algebraic Geometry* chap. 0, i–xix DOI: 10.1137/1.9781611972290 (see pp. 97, 129, 209)

[Bra+06] GILLES BRASSARD, HARRY BUHRMAN, NOAH LINDEN, ANDRÉ ALLAN MÉTHOT, ALAIN TAPP, and FALK UNGER Limit on Nonlocality in Any World in Which Communication Complexity Is Not Trivial in: *Phys. Rev. Lett.*, **96**: (25 2006), 250401 DOI: 10.1103/PhysRevLett.96.250401 (see p. 25)

[Bru+14] NICOLAS BRUNNER, DANIEL CAVALCANTI, STEFANO PIRONIO, VALERIO SCARANI, and STEPHANIE WEHNER Bell nonlocality in: *Rev. Mod. Phys.*, **86**: (2 2014), 419–478 DOI: 10.1103/RevModPhys.86.419 (see pp. 3, 20, 30, 79)

[BW92] CHARLES H. BENNETT and STEPHEN J. WIESNER Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states in: *Phys. Rev. Lett.*, **69**: (20 1992), 2881–2884 DOI: 10.1103/PhysRevLett.69.2881 (see p. 12)

[Car11] C. CARATHÉODORY Über den variabilitätsbereich der fourier'schen konstanten von positiven harmonischen funktionen Italian in: *Rendiconti del Circolo Matematico di Palermo*, **32**:1 (1911), 193–217 ISSN: 0009-725X DOI: 10.1007/BF03014795 (see p. 16)

[CB97] RICHARD CLEVE and HARRY BUHRMAN Substituting quantum entanglement for communication in: *Phys. Rev. A*, **56**: (2 1997), 1201–1204 DOI: 10.1103/PhysRevA.56.1201 (see p. 12)

[CCK13] D. E. CHANG, J. I. CIRAC, and H. J. KIMBLE Self-Organization of Atoms along a Nanophotonic Waveguide in: *Phys. Rev. Lett.*, **110**: (11 2013), 113606 DOI: 10.1103/PhysRevLett.110.113606 (see pp. 145, 209)

[CGS11] YUE CHANG, Z. R. GONG, and C. P. SUN Multiatomic mirror for perfect reflection of single photons in a wide band of frequency in: *Phys. Rev. A*, **83**: (1 2011), 013825 DOI: 10.1103/PhysRevA.83.013825 (see p. 145)

[Cha+12] D E CHANG, L JIANG, A V GORSHKOV, and H J KIMBLE Cavity QED with atomic mirrors in: *New Journal of Physics*, **14**:6 (2012), 063003 DOI: 10.1088/1367-2630/14/6/063003 (see p. 145)

[Cha93] BERNARD CHAZELLE An optimal convex hull algorithm in any fixed dimension English in: *Discrete & Computational Geometry*, **10**:1 (1993), 377–409 ISSN: 0179-5376 DOI: 10.1007/BF02573985 (see pp. 23, 79)

[Che+14] QING CHEN, SIXIA YU, CHENGJIE ZHANG, C.H. LAI, and C.H. OH Test of Genuine Multipartite Nonlocality without Inequalities in: *Phys. Rev. Lett.*, **112**: (14 2014), 140404 DOI: 10.1103/PhysRevLett.112.140404 (see p. 117)

[Cho75] MAN-DUEN CHOI Completely positive linear maps on complex matrices in: *Linear Algebra and its Applications*, **10**:3 (1975), 285–290 ISSN: 0024-3795 DOI: 10.1016/0024-3795(75)90075-0 (see pp. 17, 19)

[Chr06] MATTHIAS CHRISTANDL *The Structure of Bipartite Quantum States Insights from Group Theory and Cryptography*. PhD thesis University of Cambridge, 2006 (see p. 213)

[CK06a] DARIUSZ CHRUŚCIŃSKI and ANDRZEJ KOSSAKOWSKI Multipartite invariant states. I. Unitary symmetry in: *Phys. Rev. A*, **73**: (6 2006), 062314 DOI: 10.1103/PhysRevA.73.062314 (see p. 35)

[CK06b] DARIUSZ CHRUŚCIŃSKI and ANDRZEJ KOSSAKOWSKI Multipartite invariant states. II. Orthogonal symmetry in: *Phys. Rev. A*, **73**: (6 2006), 062315 DOI: 10.1103/PhysRevA.73.062315 (see p. 35)

[CKW00] VALERIE COFFMAN, JOYDIP KUNDU, and WILLIAM K. WOOTTERS Distributed entanglement in: *Phys. Rev. A*, **61**: (5 2000), 052306 DOI: 10.1103/PhysRevA.61.052306 (see pp. 7, 29, 176)

[Cla+69] JOHN F. CLAUSER, MICHAEL A. HORNE, ABNER SHIMONY, and RICHARD A. HOLT Proposed Experiment to Test Local Hidden-Variable Theories in: *Phys. Rev. Lett.*, **23**: (15 1969), 880–884 DOI: 10.1103/PhysRevLett.23.880 (see pp. 27, 29, 77, 133, 136, 176, 178, 179, 188)

[CMW08] TOBY CUBITT, ASHLEY MONTANARO, and ANDREAS WINTER On the dimension of subspaces with bounded Schmidt rank in: *Journal of Mathematical Physics*, **49**:2, 022107 (2008), – DOI: 10.1063/1.2862998 (see p. 50)

[Col+02] DANIEL COLLINS, NICOLAS GISIN, NOAH LINDEN, SERGE MASSAR, and SANDU POPESCU Bell Inequalities for Arbitrarily High-Dimensional Systems in: *Phys. Rev. Lett.*, **88**: (4 2002), 040404 DOI: 10.1103/PhysRevLett.88.040404 (see pp. 105, 179)

[CR12] COLBECK ROGER and RENNER RENATO Free randomness can be amplified in: *Nat Phys*, **8**:6 (2012) 10.1038/nphys2300, 450–453 ISSN: 1745-2473 DOI: 10.1038/nphys2300 (see pp. 3, 77, 178, 197, 200, 203–205)

[CS14] DARIUSZ CHRUŚCIŃSKI and GNIEWOMIR SARBICKI Entanglement witnesses: construction, analysis and classification in: *Journal of Physics A: Mathematical and Theoretical*, **47**:48 (2014), 483001 DOI: 10.1088/1751-8113/47/48/483001 (see p. 19)

[Dam99] WIM VAN DAM *Nonlocality and communication complexity*. PhD thesis University of Oxford, 1999 (see p. 25)

[Dic54] R. H. DICKE Coherence in Spontaneous Radiation Processes in: *Phys. Rev.*, **93**: (1 1954), 99–110 DOI: 10.1103/PhysRev.93.99 (see pp. 8, 32, 208)

[Dou+15] J. S. DOUGLAS, H. HABIBIAN, A. V. GORSHKOV, H. J. KIMBLE, and D. E. CHANG Quantum many-body models with cold atoms coupled to photonic crystals in: *Nature Photonics*, **9**:5 (2015), 331 DOI: 10.1038/nphoton.2015.57 (see p. 145)

[DPC05] X.-L. DENG, D. PORRAS, and J. I. CIRAC Effective spin quantum phases in systems of trapped ions in: *Phys. Rev. A*, **72**: (6 2005), 063407 DOI: 10.1103/PhysRevA.72.063407 (see p. 144)

[Dür+99] W. DÜR, H.-J. BRIEGEL, J. I. CIRAC, and P. ZOLLER Quantum repeaters based on entanglement purification in: *Phys. Rev. A*, **59**: (1 1999), 169–181 DOI: 10.1103/PhysRevA.59.169 (see p. 12)

[Eck+02] K. ECKERT, J. SCHLIEMANN, D. BRUSS, and M. LEWENSTEIN Quantum Correlations in Systems of Indistinguishable Particles in: *Annals of Physics*, **299**:1 (2002), 88–127 ISSN: 0003-4916 DOI: 10.1006/aphy.2002.6268 (see pp. 4, 7, 34, 37, 40, 49, 76, 117, 207)

[ECP10] J. EISERT, M. CRAMER, and M. B. PLENIO *Colloquium* : Area laws for the entanglement entropy in: *Rev. Mod. Phys.*, **82**: (1 2010), 277–306 DOI: 10.1103/RevModPhys.82.277 (see p. 79)

[Edw95] R.E. EDWARDS *Functional Analysis: Theory and Applications* Dover books on mathematics Dover Pub., 1995 ISBN: 9780486681436 (see p. 18)

[Eke91] ARTUR K. EKERT Quantum cryptography based on Bell's theorem in: *Phys. Rev. Lett.*, **67**: (6 1991), 661–663 DOI: 10.1103/PhysRevLett.67.661 (see pp. 2, 12, 175)

[EPR35] A. EINSTEIN, B. PODOLSKY, and N. ROSEN Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? in: *Phys. Rev.*, **47**: (10 1935), 777–780 DOI: 10.1103/PhysRev.47.777 (see pp. 2, 11, 20, 77)

[EPR92] AVSHALOM C. ELITZUR, SANDU POPESCU, and DANIEL ROHRLICH Quantum nonlocality for each pair in an ensemble in: *Physics Letters A*, **162**:1 (1992), 25–28 ISSN: 0375-9601 DOI: 10.1016/0375-9601(92)90952-I (see p. 29)

[EW01] T. EGGELING and R. F. WERNER Separability properties of tripartite states with $U \otimes U \otimes U$ symmetry in: *Phys. Rev. A*, **63**: (4 2001), 042111 DOI: 10.1103/PhysRevA.63.042111 (see p. 35)

[FH91] W. FULTON and J. HARRIS *Representation Theory: A First Course* Graduate Texts in Mathematics / Readings in Mathematics Springer New York, 1991 ISBN: 9780387974958 (see p. 213)

[Fin03] S.R. FINCH *Mathematical Constants* Encyclopedia of Mathematics and its Applications Cambridge University Press, 2003 ISBN: 9780521818056 (see p. 158)

[Fin82] ARTHUR FINE Hidden Variables, Joint Probability, and the Bell Inequalities in: *Phys. Rev. Lett.*, **48**: (5 1982), 291–295 DOI: 10.1103/PhysRevLett.48.291 (see p. 26)

[Fri+13] TOBIAS FRITZ, ANA BELÉN SAINZ, REMIGIUSZ AUGUSIAK, JONATHAN BOHR BRASK, RAFAEL CHAVES, ANTHONY LEVERRIER, and ANTONIO ACÍN Local orthogonality as a multipartite principle for quantum correlations in: *Nat Commun*, **4**: (2263 2013) DOI: 10.1038/ncomms3263 (see p. 25)

[Fri12] TOBIAS FRITZ Polyhedral duality in Bell scenarios with two binary observables in: *Journal of Mathematical Physics*, **53**:7, 072202 (2012), – DOI: 10.1063/1.4734586 (see pp. 24, 27)

[Fro81] M. FROISSART Constructive generalization of Bell's inequalities English in: *Il Nuovo Cimento B*, **64**:2 (1981), 241–251 ISSN: 0369-3554 DOI: 10.1007/BF02903286 (see p. 22)

[Fuk14] KOMEI FUKUDA *cddlib* http://www.inf.ethz.ch/personal/fukudak/cdd_home/ 2014 (see pp. 23, 105, 131–133, 135)

[Gal+10] RODRIGO GALLEGO, NICOLAS BRUNNER, CHRISTOPHER HADLEY, and ANTONIO ACÍN Device-Independent Tests of Classical and Quantum Dimensions in: *Phys. Rev. Lett.*, **105**: (23 2010), 230501 DOI: 10.1103/PhysRevLett.105.230501 (see pp. 3, 77)

[Gal+12] RODRIGO GALLEGO, LARS ERIK WÜRFLINGER, ANTONIO ACÍN, and MIGUEL NAVASCUÉS Operational Framework for Nonlocality in: *Phys. Rev. Lett.*, **109**: (7 2012), 070401 DOI: 10.1103/PhysRevLett.109.070401 (see pp. 28, 171)

[GHG10] OLEG GITTSOVICH, PHILIPP HYLLUS, and OTFRIED GÜHNE Multiparticle covariance matrices and the impossibility of detecting graph-state entanglement with two-particle correlations in: *Phys. Rev. A*, **82**: (3 2010), 032306 DOI: 10.1103/PhysRevA.82.032306 (see p. 81)

[Gis14] N. GISIN *Quantum Chance: Nonlocality, Teleportation and Other Quantum Marvels* Springer International Publishing, 2014 ISBN: 9783319054728 (see p. 77)

[Gis91] N. GISIN Bell's inequality holds for all non-product states in: *Physics Letters A*, **154**:5–6 (1991), 201–202 ISSN: 0375-9601 DOI: 10.1016/0375-9601(91)90805-I (see pp. 6, 29, 79, 155)

[Gis96] N. GISIN Hidden quantum nonlocality revealed by local filters in: *Physics Letters A*, **210**:3 (1996), 151–156 ISSN: 0375-9601 DOI: 10.1016/S0375-9601(96)80001-6 (see pp. 172, 210)

[GL14] TOBIAS GRASS and MACIEJ LEWENSTEIN Trapped-ion quantum simulation of tunable-range Heisenberg chains in: *EPJ Quantum Technology*, **1**:1 (2014), 8 ISSN: 2196-0763 DOI: 10.1140/epjqt8 (see pp. 145, 209)

[Gob+12] A. GOBAN, K. S. CHOI, D. J. ALTON, D. DING, C. LACROÛTE, M. POTOTSCHNIG, T. THIELE, N. P. STERN, and H. J. KIMBLE Demonstration of a State-Insensitive, Compensated Nanofiber Trap in: *Phys. Rev. Lett.*, **109**: (3 2012), 033603 DOI: 10.1103/PhysRevLett.109.033603 (see p. 145)

[Gra+13] TOBIAS GRASS, BRUNO JULIÁ-DÍAZ, MAREK KUŚ, and MACIEJ LEWENSTEIN Quantum Chaos in SU(3) Models with Trapped Ions in: *Phys. Rev. Lett.*, **111**: (9 2013), 090404 DOI: 10.1103/PhysRevLett.111.090404 (see p. 145)

[Gro97] LOV K. GROVER Quantum Mechanics Helps in Searching for a Needle in a Haystack in: *Phys. Rev. Lett.*, **79**: (2 1997), 325–328 DOI: 10.1103/PhysRevLett.79.325 (see p. 12)

[Gru+14] ANDRZEJ GRUDKA, KAROL HORODECKI, MICHAŁ HORODECKI, PAWEŁ HORODECKI, MARCIN PAWŁOWSKI, and RAVISHANKAR RAMANATHAN Free randomness amplification using bipartite chain correlations in: *Phys. Rev. A*, **90**: (3 2014), 032322 DOI: 10.1103/PhysRevA.90.032322 (see p. 205)

[GT] JOÃO GOUVEIA and REKHA R. THOMAS *Chapter 7: Spectrahedral Approximations of Convex Hulls of Algebraic Sets*. in: *Semidefinite Optimization and Convex Algebraic Geometry* chap. 7, 293–340 DOI: 10.1137/1.9781611972290.ch7 (see pp. 97, 129, 209)

[GT+15] A. GONZÁLEZ-TUDELA, C.-L. HUNG, D. E. CHANG, J. I. CIRAC, and H. J. KIMBLE Subwavelength vacuum lattices and atom-atom interactions in two-dimensional photonic crystals in: *Nature Photonics*, **9**:5 (2015), 325 DOI: 10.1038/nphoton.2015.54 (see p. 145)

[GTB05] OTFRIED GÜHNE, GÉZA TÓTH, and HANS J BRIEGEL Multipartite entanglement in spin chains in: *New Journal of Physics*, **7**:1 (2005), 229 DOI: 10.1088/1367-2630/7/1/229 (see p. 14)

[Gur03] LEONID GURVITS "Classical Deterministic Complexity of Edmonds' Problem and Quantum Entanglement" in: *Proceedings of the Thirty-fifth Annual ACM Symposium on Theory of Computing* STOC '03 San Diego, CA, USA: ACM, 2003, 10–19 ISBN: 1-58113-674-9 DOI: 10.1145/780542.780545 (see pp. 15, 35, 56)

[GW09] R. GOODMAN and N.R. WALLACH *Symmetry, Representations, and Invariants* Graduate Texts in Mathematics Springer, 2009 ISBN: 9780387798523 (see pp. 213, 217, 220)

[Har01] ARAM WETTROTH HARROW *Applications of coherent classical communication and the Schur transform to quantum information theory*. PhD thesis Massachusetts Institute of Technology, 2001 (see p. 213)

[Hau+10] PHILIPP HAUKE, FERNANDO M CUCCHIETTI, ALEXANDER MÜLLER-HERMES, MARI-CARMEN BAÑULS, J IGNACIO CIRAC, and MACIEJ LEWENSTEIN Complete devil's staircase and crystalsuperfluid transitions in a dipolar XXZ spin chain: a trapped ion quantum simulation in: *New Journal of Physics*, **12**:11 (2010), 113037 DOI: 10.1088/1367-2630/12/11/113037 (see p. 144)

[HE02] PAWEŁ HORODECKI and ARTUR EKERT Method for Direct Detection of Quantum Entanglement in: *Phys. Rev. Lett.*, **89**: (12 2002), 127902 DOI: 10.1103/PhysRevLett.89.127902 (see p. 20)

[HH99] MICHAŁ HORODECKI and PAWEŁ HORODECKI Reduction criterion of separability and limits for a class of distillation protocols in: *Phys. Rev. A*, **59**: (6 1999), 4206–4216 DOI: 10.1103/PhysRevA.59.4206 (see pp. 158, 169, 170)

[HHH95] R. Horodecki, P. Horodecki, and M. Horodecki Violating Bell inequality by mixed spin-1/2 states: necessary and sufficient condition in: *Physics Letters A*, **200**:5 (1995), 340–344 ISSN: 0375-9601 DOI: 10.1016/0375-9601(95)00214-N (see p. 189)

[HHH96] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki Separability of mixed states: necessary and sufficient conditions in: *Physics Letters A*, **223**:1–2 (1996), 1–8 ISSN: 0375-9601 DOI: 10.1016/S0375-9601(96)00706-2 (see pp. 4, 17, 18, 20, 49)

[HHH98] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki Mixed-State Entanglement and Distillation: Is there a "Bound" Entanglement in Nature? in: *Phys. Rev. Lett.*, **80**: (24 1998), 5239–5242 DOI: 10.1103/PhysRevLett.80.5239 (see pp. 4, 34)

[Hir+13] Flavien Hirsch, Marco Túlio Quintino, Joseph Bowles, and Nicolas Brunner Genuine Hidden Quantum Nonlocality in: *Phys. Rev. Lett.*, **111**: (16 2013), 160402 DOI: 10.1103/PhysRevLett.111.160402 (see pp. 172, 210)

[HK11] Kil-Chan Ha and Seung-Hyeok Kye Entanglement Witnesses Arising from Exposed Positive Linear Maps in: *Open Systems & Information Dynamics*, **18**:04 (2011), 323–337 DOI: 10.1142/S1230161211000224 (see p. 19)

[Hor+00] Paweł Horodecki, Maciej Lewenstein, Guifré Vidal, and Ignacio Cirac Operational criterion and constructive checks for the separability of low-rank density matrices in: *Phys. Rev. A*, **62**: (3 2000), 032310 DOI: 10.1103/PhysRevA.62.032310 (see pp. 41, 75)

[Hor+09] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki Quantum entanglement in: *Rev. Mod. Phys.*, **81**: (2 2009), 865–942 DOI: 10.1103/RevModPhys.81.865 (see pp. 2, 4)

[Hor97] PAWEL HORODECKI Separability criterion and inseparable mixed states with positive partial transposition in: *Physics Letters A*, **232**:5 (1997), 333–339 ISSN: 0375-9601 DOI: 10.1016/S0375-9601(97)00416-7 (see pp. 7, 17, 44, 66–69)

[HSP10] KLEMENS HAMMERER, ANDERS S. SØRENSEN, and EUGENE S. POLZIK Quantum interface between light and atomic ensembles in: *Rev. Mod. Phys.*, **82**: (2 2010), 1041–1093 DOI: 10.1103/RevModPhys.82.1041 (see p. 145)

[Hum+13] D. B. HUME, I. STROESCU, M. JOOS, W. MUESSEL, H. STROBEL, and M. K. OBERTHALER Accurate Atom Counting in Mesoscopic Ensembles in: *Phys. Rev. Lett.*, **111**: (25 2013), 253001 DOI: 10.1103/PhysRevLett.111.253001 (see p. 144)

[Hüb+09] ROBERT HÜBENER, MATTHIAS KLEINMANN, TZU-CHIEH WEI, CARLOS GONZÁLEZ-GUILLÉN, and OTFRIED GÜHNE Geometric measure of entanglement for symmetric states in: *Phys. Rev. A*, **80**: (3 2009), 032324 DOI: 10.1103/PhysRevA.80.032324 (see p. 133)

[Jam72] A. JAMIOŁKOWSKI Linear transformations which preserve trace and positive semidefiniteness of operators in: *Reports on Mathematical Physics*, **3**:4 (1972), 275–278 ISSN: 0034-4877 DOI: 10.1016/0034-4877(72)90011-0 (see pp. 17, 19)

[KH08] FAM LE KIEN and K. HAKUTA Cooperative enhancement of channeling of emission from atoms into a nanofiber in: *Phys. Rev. A*, **77**: (1 2008), 013801 DOI: 10.1103/PhysRevA.77.013801 (see p. 145)

[KL01] SINIŠA KARNAS and MACIEJ LEWENSTEIN Separability and entanglement in $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^n$ composite quantum systems in: *Phys. Rev. A*, **64**: (4 2001), 042313 DOI: 10.1103/PhysRevA.64.042313 (see p. 44)

[Kol33] A. N. KOLMOGÓROV *Grundbegriffe der Wahrscheinlichkeitsrechnung* Springer, Berlin, 1933 (see p. 22)

[Kra+00] B. KRAUS, J. I. CIRAC, S. KARNAS, and M. LEWENSTEIN Separability in $2 \times N$ composite quantum systems in: *Phys. Rev. A*, **61**: (6 2000), 062302 DOI: 10.1103/PhysRevA.61.062302 (see pp. 40–42, 45, 46, 54)

[Kur+11] P. KURZYŃSKI, T. PATEREK, R. RAMANATHAN, W. LASKOWSKI, and D. KASZLIKOWSKI Correlation Complementarity Yields Bell Monogamy Relations in: *Phys. Rev. Lett.*, **106**: (18 2011), 180402 DOI: 10.1103/PhysRevLett.106.180402 (see p. 188)

[Lew+00] M. LEWENSTEIN, B. KRAUS, J. I. CIRAC, and P. HORODECKI Optimization of entanglement witnesses in: *Phys. Rev. A*, **62**: (5 2000), 052310 DOI: 10.1103/PhysRevA.62.052310 (see pp. 18, 19, 44)

[Lin+07] NOAH LINDEN, SANDU POPESCU, ANTHONY J. SHORT, and ANDREAS WINTER Quantum Nonlocality and Beyond: Limits from Nonlocal Computation in: *Phys. Rev. Lett.*, **99**: (18 2007), 180502 DOI: 10.1103/PhysRevLett.99.180502 (see p. 25)

[LK14] BERND LÜCKE and CARSTEN KLEMPT Private communication 2014 (see pp. 8, 142)

[LMG65] H.J. LIPKIN, N. MESHKOV, and A.J. GLICK Validity of many-body approximation methods for a solvable model: (I). Exact solutions and perturbation theory in: *Nuclear Physics*, **62**:2 (1965), 188198 ISSN: 0029-5582 DOI: 10.1016/0029-5582(65)90862-X (see pp. 8, 117)

[LMO07] J. M. LEINAAS, J. MYRHEIM, and E. OVRUM Extreme points of the set of density matrices with positive partial transpose in: *Phys. Rev. A*, **76**: (3 2007), 034304 DOI: 10.1103/PhysRevA.76.034304 (see pp. 7, 35, 57, 60, 207)

[LMS10] JON MAGNE LEINAAS, JAN MYRHEIM, and PER ØYVIND SOLLID Numerical studies of entangled positive-partial-transpose states in composite quantum systems in: *Phys. Rev. A*, **81**: (6 2010), 062329 DOI: 10.1103/PhysRevA.81.062329 (see p. 63)

[LS98] MACIEJ LEWENSTEIN and ANNA SANPERA Separability and Entanglement of Composite Quantum Systems in: *Phys. Rev. Lett.*, **80**: (11 1998), 2261–2264 DOI: 10.1103/PhysRevLett.80.2261 (see p. 44)

[Luc+14] VITO GIOVANNI LUCIVERO, PAWEL ANIELSKI, WOJCIECH GAWLIK, and MORGAN W. MITCHELL Shot-noise-limited magnetometer with sub-picotesla sensitivity at room temperature in: *Review of Scientific Instruments*, **85**:11, 113108 (2014), DOI: 10.1063/1.4901588 (see p. 145)

[Lüc+14] BERND LÜCKE, JAN PEISE, GIUSEPPE VITAGLIANO, JAN ARLT, LUIS SANTOS, GÉZA TÓTH, and CARSTEN KLEMPT Detecting Multiparticle Entanglement of Dicke States in: *Phys. Rev. Lett.*, **112**: (15 2014), 155304 DOI: 10.1103/PhysRevLett.112.155304 (see pp. 141–144, 209)

[MAG06] LL. MASANES, A. ACÍN, and N. GISIN General properties of nonsignaling theories in: *Phys. Rev. A*, **73**: (1 2006), 012112 DOI: 10.1103/PhysRevA.73.012112 (see pp. 176, 179)

[Mai+12] MICHAŁ MAIK, PHILIPP HAUKE, OMJYOTI DUTTA, JAKUB ZAKRZEWSKI, and MACIEJ LEWENSTEIN Quantum spin models with long-range interactions and tunnelings: a quantum Monte Carlo study in: *New Journal of Physics*, **14**:11 (2012), 113006 DOI: 10.1088/1367-2630/14/11/113006 (see p. 144)

[Maj32] ETTORE MAJORANA Atomi orientati in campo magnetico variabile Italian in: *Il Nuovo Cimento*, **9**:2 (1932), 43–50 ISSN: 0029-6341 DOI: 10.1007/BF02960953 (see p. 33)

[Mar11] DAMIAN J. H. MARKHAM Entanglement and symmetry in permutation-symmetric states in: *Phys. Rev. A*, **83**: (4 2011), 042332 DOI: 10.1103/PhysRevA.83.042332 (see p. 33)

[Mue+14] W. MUESSEL, H. STROBEL, D. LINNEMANN, D. B. HUME, and M. K. OBERTHALER Scalable Spin Squeezing for Quantum-Enhanced Magnetometry with Bose-Einstein Condensates in: *Phys. Rev. Lett.*, **113**: (10 2014), 103004

DOI: 10.1103/PhysRevLett.113.103004 (see pp. 144, 209)

[MW01] FLORIAN MINTERT and CHRISTOF WUNDERLICH Ion-Trap Quantum Logic Using Long-Wavelength Radiation in: *Phys. Rev. Lett.*, **87**: (25 2001), 257904 DOI: 10.1103/PhysRevLett.87.257904 (see p. 144)

[Nav+15] MIGUEL NAVASCUÉS, YELENA GURYANOVA, MATTY J. HOBAN, and ANTONIO ACÍN Almost quantum correlations in: *Nature Communications*, **6**: (2015), 6288 DOI: doi:10.1038/ncomms7288 (see p. 25)

[Nay+07] K. P. NAYAK, P. N. MELENTIEV, M. MORINAGA, FAM LE KIEN, V. I. BALYKIN, and K. HAKUTA Optical nanofiber as an efficient tool for manipulating and probing atomicFluorescence in: *Opt. Express*, **15**:9 (2007), 5431–5438 DOI: 10.1364/OE.15.005431 (see p. 145)

[NC00] MICHAEL A NIELSEN and ISAAC L CHUANG *Quantum computation and quantum information* 2000 DOI: 10.1080/00107514.2011.587535 (see pp. 2, 15)

[Nie99] M. A. NIELSEN Conditions for a Class of Entanglement Transformations in: *Phys. Rev. Lett.*, **83**: (2 1999), 436–439 DOI: 10.1103/PhysRevLett.83.436 (see p. 16)

[NPA08] MIGUEL NAVASCUÉS, STEFANO PIRONIO, and ANTONIO ACÍN A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations in: *New Journal of Physics*, **10**:7 (2008), 073013 DOI: 10.1088/1367-2630/10/7/073013 (see pp. 25, 97, 178, 188, 191)

[NW10] MIGUEL NAVASCUS and HARALD WUNDERLICH A glance beyond the quantum model in: *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Science*, **466**:2115 (2010), 881–890 DOI: 10.1098/rspa.2009.0453 (see p. 25)

[Pal12] CARLOS PALAZUELOS Superactivation of Quantum Nonlocality in: *Phys. Rev. Lett.*, **109**: (19 2012), 190401 DOI: 10.1103/PhysRevLett.109.190401 (see pp. 172, 210)

[Paw+09] MARCIN PAWŁOWSKI, TOMASZ PATEREK, DAGOMIR KASZLIKOWSKI, VALERIO SCARANI, ANDREAS WINTER, and MAREK ŻUKOWSKI Information causality as a physical principle in: *Nature*, **461**: (7267 2009), 1101–1104 DOI: 10.1038/nature08400 (see p. 25)

[PB09] MARCIN PAWŁOWSKI and ČASLAV BRUKNER Monogamy of Bell's Inequality Violations in Nonsignaling Theories in: *Phys. Rev. Lett.*, **102**: (3 2009), 030403 DOI: 10.1103/PhysRevLett.102.030403 (see pp. 176, 179, 182)

[PC04] D. PORRAS and J. I. CIRAC Effective Quantum Spin Systems with Trapped Ions in: *Phys. Rev. Lett.*, **92**: (20 2004), 207901 DOI: 10.1103/PhysRevLett.92.207901 (see pp. 144, 209)

[Per96] ASHER PERES Separability Criterion for Density Matrices in: *Phys. Rev. Lett.*, **77**: (8 1996), 1413–1415 DOI: 10.1103/PhysRevLett.77.1413 (see pp. 3, 17)

[Pfa+14] W. PFAFF, B. J. HENSEN, H. BERNIEN, S. B. VAN DAM, M. S. BLOK, T. H. TAMINIAU, M. J. TIGGELMAN, R. N. SCHOUTEN, M. MARKHAM, D. J. TWITCHEN, and R. HANSON Unconditional quantum teleportation between distant solid-state quantum bits in: *Science*, **345**:6196 (2014), 532–535 DOI: 10.1126/science.1253512 (see p. 79)

[Pir+13] S. PIRONIO, LL. MASANES, A. LEVERRIER, and A. ACÍN Security of Device-Independent Quantum Key Distribution in the Bounded-Quantum-Storage Model in: *Phys. Rev. X*, **3**: (3 2013), 031007 DOI: 10.1103/PhysRevX.3.031007 (see pp. 3, 77, 177, 194, 195)

[Pir14] STEFANO PIRONIO All ClauserHorneShimonyHolt polytopes in: *Journal of Physics A: Mathematical and Theoretical*, **47**:42 (2014), 424020 DOI: 10.1088/1751-8113/47/42/424020 (see p. 27)

[Pop95] SANDU POPESCU Bell's Inequalities and Density Matrices: Revealing "Hidden" Nonlocality in: *Phys. Rev. Lett.*, **74**: (14 1995), 2619–2622 DOI: 10.1103/PhysRevLett.74.2619 (see pp. 172, 210)

[PR92] SANDU POPESCU and DANIEL ROHRLICH Generic quantum nonlocality in: *Physics Letters A*, **166**:5–6 (1992), 293–297 ISSN: 0375-9601 DOI: 10.1016/0375-9601(92)90711-T (see pp. 6, 79, 155)

[PR94] SANDU POPESCU and DANIEL ROHRLICH Quantum nonlocality as an axiom English in: *Foundations of Physics*, **24**:3 (1994), 379–385 ISSN: 0015-9018 DOI: 10.1007/BF02058098 (see pp. 24, 25)

[PS01] ITAMAR PITOWSKY and KARL SVOZIL Optimal tests of quantum nonlocality in: *Phys. Rev. A*, **64**: (1 2001), 014102 DOI: 10.1103/PhysRevA.64.014102 (see p. 27)

[PV10] KÁROLY F. PÁL and TAMÁS VÉRTESI Maximal violation of a bipartite three-setting, two-outcome Bell inequality using infinite-dimensional quantum systems in: *Phys. Rev. A*, **82**: (2 2010), 022116 DOI: 10.1103/PhysRevA.82.022116 (see pp. 138, 140)

[Pól37] G. PÓLYA Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und chemische Verbindungen German in: *Acta Mathematica*, **68**:1 (1937), 145–254 ISSN: 0001-5962 DOI: 10.1007/BF02546665 (see pp. 87, 130)

[RBG14] DENIS ROSSET, JEAN-DANIEL BANCAL, and NICOLAS GISIN Classifying 50 years of Bell inequalities in: *Journal of Physics A: Mathematical and Theoretical*, **47**:42 (2014), 424022 DOI: 10.1088/1751-8113/47/42/424022 http://www.faacets.com/ (see p. 27)

[Red27] J. HOWARD REDFIELD The Theory of Group-Reduced Distributions English in: *American Journal of Mathematics*, **49**:3 (1927), pp. 433–455 ISSN: 00029327 DOI: 10.2307/2370675 (see pp. 87, 130)

[RH14] RAVISHANKAR RAMANATHAN and PAWEŁ HORODECKI Strong Monogamies of No-Signaling Violations for Bipartite Correlation Bell Inequalities in: *Phys. Rev. Lett.*, **113**: (21 2014), 210403 DOI: 10.1103/PhysRevLett.113.210403 (see p. 176)

[SC10] NORBERT SCHUCH and J. IGNACIO CIRAC Matrix product state and mean-field solutions for one-dimensional systems can be found efficiently in: *Phys. Rev. A*, **82**: (1 2010), 012314 DOI: 10.1103/PhysRevA.82.012314 (see p. 209)

[Sch35] E. SCHRÖDINGER Discussion of Probability Relations between Separated Systems in: *Mathematical Proceedings of the Cambridge Philosophical Society*, **31**: (04 Oct. 1935), 555–563 ISSN: 1469-8064 DOI: 10.1017/S0305004100013554 (see pp. 11, 173)

[Sen+14] C. SENKO, P. RICHERME, J. SMITH, A. LEE, I. COHEN, A. RETZKER, and C. MONROE *Experimental Realization of a Quantum Integer-Spin Chain with Controllable Interactions* 2014 arXiv:1410.0937 (see p. 145)

[Sew+14] R. J. SEWELL, M. NAPOLITANO, N. BEHBOOD, G. COLANGELO, F. MARTIN CIURANA, and M. W. MITCHELL Ultrasensitive Atomic Spin Measurements with a Nonlinear Interferometer in: *Phys. Rev. X*, **4**: (2 2014), 021045 DOI: 10.1103/PhysRevX.4.021045 (see p. 145)

[SHH10] CHRISTOPH SPENGLER, MARCUS HUBER, and BEATRIX C HIESMAYR A composite parameterization of unitary groups, density matrices and subspaces in: *Journal of Physics A: Mathematical and Theoretical*, **43**:38 (2010), 385306 DOI: 10.1088/1751-8113/43/38/385306 (see p. 138)

[Sho94] P.W. SHOR "Algorithms for quantum computation: discrete logarithms and factoring" in: *Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on* 1994, 124–134 DOI: 10.1109/SFCS.1994.365700 (see p. 2)

[SKL07] JAN SAMSONOWICZ, MAREK KUŚ, and MACIEJ LEWENSTEIN Separability, entanglement, and full families of commuting normal matrices in: *Phys. Rev. A*, **76**: (2 2007), 022314 DOI: 10.1103/PhysRevA.76.022314 (see pp. 45, 54, 55, 72)

[SSŻ09] ŁUKASZ SKOWRONEK, ERLING STØRMER, and KAROL ŻYCZKOWSKI Cones of positive maps and their duality relations in: *Journal of Mathematical Physics*, **50**:6, 062106 (2009), – DOI: 10.1063/1.3155378 (see p. 19)

[Str+14] HELMUT STROBEL, WOLFGANG MUESSEL, DANIEL LINNEMANN, TILMAN ZIBOLD, DAVID B. HUME, LUCA PEZZ, AUGUSTO SMERZI, and MARKUS K. OBERTHALER Fisher information and entanglement of non-Gaussian spin states in: *Science*, **345**:6195 (2014), 424–427 DOI: 10.1126/science.1250147 (see p. 144)

[Stu99] J.F. STURM Using SeDuMi 1.02, a MATLAB toolbox for optimization over symmetric cones in: *Optimization Methods and Software*, **11–12**: (1999), 625–653 (see p. 192)

[Stø63] ERLING STØRMER Positive linear maps of operator algebras in: *Acta Math.*, **110**: (1963), 233–278 ISSN: 0001-5962 DOI: 10.1007/BF02391860 (see pp. 4, 17, 19, 49)

[SV86] MIKLOS SANTHA and UMESH V VAZIRANI Generating quasi-random sequences from semi-random sources in: *Journal of Computer and System Sciences*, **33**:1 (1986), 75–87 (see p. 197)

[Sve87] GEORGE SVETLICHNY Distinguishing three-body from two-body nonseparability by a Bell-type inequality in: *Phys. Rev. D*, **35**: (10 1987), 3066–3069 DOI: 10.1103/PhysRevD.35.3066 (see pp. 27, 171)

[TA06] GÉZA TÓTH and ANTONIO ACÍN Genuine tripartite entangled states with a local hidden-variable model in: *Phys. Rev. A*, **74**: (3 2006), 030306 DOI: 10.1103/PhysRevA.74.030306 (see pp. 6, 160, 172)

[Ter00] BARBARA M. TERHAL Bell inequalities and the separability criterion in: *Physics Letters A*, **271**:5–6 (2000), 319–326 ISSN: 0375-9601 DOI: 10.1016/S0375-9601(00)00401-1 (see p. 18)

[TG09] GÉZA TÓTH and OTFRIED GÜHNE Entanglement and Permutational Symmetry in: *Phys. Rev. Lett.*, **102**: (17 2009), 170503 DOI: 10.1103/PhysRevLett.102.170503 (see pp. 4, 34, 49)

[TH00] BARBARA M. TERHAL and PAWEŁ HORODECKI Schmidt number for density matrices in: *Phys. Rev. A*, **61**: (4 2000), 040301 DOI: 10.1103/PhysRevA.61.040301 (see p. 16)

[Ton09] BEN TONER Monogamy of non-local quantum correlations in: *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Science*, **465**:2101 (2009), 59–69 DOI: 10.1098/rspa.2008.0149 (see pp. 29, 176)

[Tur+12] J. TURA, R. AUGUSIAK, P. HYLLUS, M. KUŚ, J. SAMSONOWICZ, and M. LEWENSTEIN Four-qubit entangled symmetric states with positive partial transpositions in: *Phys. Rev. A*, **85**: (6 2012), 060302 DOI: 10.1103/PhysRevA.85.060302 Published as a Rapid Communication (see pp. 7, 10, 35, 36, 49, 60)

[Tur+14a] J. TURA, R. AUGUSIAK, A. B. SAINZ, T. VÉRTESI, M. LEWENSTEIN, and A. ACÍN Detecting nonlocality in many-body quantum states in: *Science*, **344**:6189 (2014), 1256–1258 DOI: 10.1126/science.1247715 (see pp. 8, 10, 81, 82, 110, 119, 250, 252)

[Tur+14b] J TURA, A B SAINZ, T VÉRTESI, A ACÍN, M LEWENSTEIN, and R AUGUSIAK Translationally invariant multipartite Bell inequalities involving only two-body correlators in: *Journal of Physics A: Mathematical and Theoretical*, **47**:42 (2014), 424024 DOI: 10.1088/1751-8113/47/42/424024 Part of the special issue *50 years of Bell's Theorem* (see pp. 8, 10, 82, 84, 138)

[Tur+15a] J. TURA, A. B. SAINZ, T. GRASS, R. AUGUSIAK, A ACÍN, and M. LEWENSTEIN *Entanglement and Nonlocality in Many-Body Systems: a primer* 2015 arXiv:1501.02733. To be published in the Proceedings of the International School of Physics *Enrico Fermi* 2014, Course 191 - Quantum Matter at Ultralow Temperatures (see pp. 9, 10, 79, 82)

[Tur+15b] J. TURA, R. AUGUSIAK, A. B. SAINZ, B. LÜCKE, C. KLEMPT, M. LEWENSTEIN, and A. ACÍN *Nonlocality in many-body quantum systems detected with two-body correlators* 2015 arXiv : 1505.06740. To be submitted to Communications in Mathematical Physics (see pp. 8, 10, 79, 82)

[TV06] BENJAMIN TONER and FRANK VERSTRAETE *Monogamy of Bell correlations and Tsirelson's bound* 2006 arXiv:quant-ph/0611001 (see pp. 29, 105, 118, 136, 176, 188–190)

[VB12] TAMÁS VÉRTESI and NICOLAS BRUNNER Quantum Nonlocality Does Not Imply Entanglement Distillability in: *Phys. Rev. Lett.*, **108**: (3 2012), 030403 DOI: 10.1103/PhysRevLett.108.030403 (see pp. 34, 35)

[VB14] TAMAS VÉRTESI and NICOLAS BRUNNER Disproving the Peres conjecture by showing Bell nonlocality from bound entanglement in: *Nature Communications*, **5**: (2014), 5297 DOI: 10.1038/ncomms6297 (see p. 34)

[Vet+10] E. VETSCH, D. REITZ, G. SAGUÉ, R. SCHMIDT, S. T. DAWKINS, and A. RAUSCHENBEUTEL Optical Interface Created by Laser-Cooled Atoms Trapped in the Evanescent Field Surrounding an Optical Nanofiber in: *Phys. Rev. Lett.*, **104**: (20 2010), 203603 DOI: 10.1103/PhysRevLett.104.203603 (see p. 145)

[VW01] K. G. H. VOLLBRECHT and R. F. WERNER Entanglement measures under symmetry in: *Phys. Rev. A*, **64**: (6 2001), 062307 DOI: 10.1103/PhysRevA.64.062307 (see p. 35)

[Wen+13] A. N. Wenz, G. Zürn, S. Murmann, I. Brouzos, T. Lompe, and S. Jochim From Few to Many: Observing the Formation of a Fermi Sea One Atom at a Time in: *Science*, **342**:6157 (2013), 457–460 DOI: 10.1126/science.1240516 (see p. 144)

[Wer89] Reinhard F. Werner Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model in: *Phys. Rev. A*, **40**: (8 1989), 4277–4281 DOI: 10.1103/PhysRevA.40.4277 (see pp. 6, 13, 14, 30, 79, 155–157, 169)

[WG03] Tzu-Chieh Wei and Paul M. Goldbart Geometric measure of entanglement and applications to bipartite and multipartite quantum states in: *Phys. Rev. A*, **68**: (4 2003), 042307 DOI: 10.1103/PhysRevA.68.042307 (see p. 133)

[WJD07] H. M. Wiseman, S. J. Jones, and A. C. Doherty Steering, Entanglement, Nonlocality, and the Einstein-Podolsky-Rosen Paradox in: *Phys. Rev. Lett.*, **98**: (14 2007), 140402 DOI: 10.1103/PhysRevLett.98.140402 (see p. 173)

[WNŻ12] Marcin Wieśniak, Mohamed Nawareg, and Marek Żukowski N-particle nonclassicality without N-particle correlations in: *Phys. Rev. A*, **86**: (4 2012), 042339 DOI: 10.1103/PhysRevA.86.042339 (see p. 81)

[Wor76] S.L. Woronowicz Positive maps of low dimensional matrix algebras in: *Reports on Mathematical Physics*, **10**:2 (1976), 165–183 ISSN: 0034-4877 DOI: 10.1016/0034-4877(76)90038-0 (see pp. 4, 17, 19, 49)

[WW01] Reinhard F. Werner and Michael M. Wolf Bell inequalities and entanglement in: *Quantum Inf. Comput.*, **1**:3 (2001), 1–25 ISSN: 1533-7146 (see p. 138)

[Zho+11] Jing Zhou, Yong Hu, Xu-Bo Zou, and Guang-Can Guo Ground-state preparation of arbitrarily multipartite Dicke states in the one-dimensional ferromagnetic spin-$\frac{1}{2}$ chain in: *Phys. Rev. A*, **84**: (4 2011), 042324 DOI: 10.1103/PhysRevA.84.042324 (see p. 117)

[ZR10] HASHEM ZOUBI and HELMUT RITSCH Hybrid quantum system of a nanofiber mode coupled to two chains of optically trapped atoms in: *New Journal of Physics*, **12**:10 (2010), 103014 DOI: 10.1088/1367-2630/12/10/103014 (see p. 145)

[Zür+13] G. ZÜRN, A. N. WENZ, S. MURMANN, A. BERGSCHNEIDER, T. LOMPE, and S. JOCHIM Pairing in Few-Fermion Systems with Attractive Interactions in: *Phys. Rev. Lett.*, **111**: (17 2013), 175302 DOI: 10.1103/PhysRevLett.111.175302 (see p. 144)

[Bri+12] BRITTON JOSEPH W., SAWYER BRIAN C., KEITH ADAM C., WANG C.-C. JOSEPH, FREERICKS JAMES K., UYS HERMANN, BIERCUK MICHAEL J., and BOLLINGER JOHN J. Engineered two-dimensional Ising interactions in a trapped-ion quantum simulator with hundreds of spins in: *Nature*, **484**:7395 (2012) 10.1038/nature10981, 489492 ISSN: 0028-0836 DOI: 10.1038/nature10981 (see pp. 144, 209)

[Cav+11] CAVALCANTI DANIEL, ALMEIDA MAFALDA L., SCARANI VALERIO, and ACÍN ANTONIO Quantum networks reveal quantum nonlocality in: *Nat Commun*, **2**: (2011) 10.1038/ncomms1193, 184 DOI: 10.1038/ncomms1193 (see pp. 172, 210)

[Eck+08] ECKERT KAI, ROMERO-ISART ORIOL, RODRIGUEZ MIRTA, LEWENSTEIN MACIEJ, POLZIK EUGENE S., and SANPERA ANNA Quantum non-demolition detection of strongly correlated systems in: *Nat Phys*, **4**:1 (2008) 10.1038/nphys776, 5054 ISSN: 1745-2473 DOI: 10.1038/nphys776 (see pp. 145, 209)

[Fri+08] FRIEDENAUER A., SCHMITZ H., GLUECKERT J. T., PORRAS D., and SCHAETZ T. Simulating a quantum magnet with trapped ions in: *Nat Phys*, **4**:10 (2008) 10.1038/nphys1032, 757761 ISSN: 1745-2473 DOI: 10.1038/nphys1032 (see p. 144)

[Gob+14] GOBAN A., HUNG C.-L., YU S.-P., HOOD J.D., MUNIZ J.A., LEE J.H., MARTIN M.J., MCCLUNG A.C., CHOI K.S., CHANG D.E., PAINTER O., and KIMBLE

H.J. Atomlight interactions in photonic crystals in: *Nat Commun*, **5**: (2014) DOI: 10.1038/ncomms480810.1038/ncomms4808 (see p. 145)

[Kim+10] KIM K., CHANG M.-S., KORENBLIT S., ISLAM R., EDWARDS E. E., FREERICKS J. K., LIN G.-D., DUAN L.-M., and MONROE C. Quantum simulation of frustrated Ising spins with trapped ions in: *Nature*, **465**:7298 (2010), 590593 ISSN: 0028-0836 DOI: 10.1038/nature09071 (see p. 144)

[Lyd+10] LYDERSEN LARS, WIECHERS CARLOS, WITTMANN CHRISTOFFER, ELSER DOMINIQUE, SKAAR JOHANNES, and MAKAROV VADIM Hacking commercial quantum cryptography systems by tailored bright illumination in: *Nat Photon*, **4**:10 (2010) 10.1038/nphoton.2010.214, 686–689 ISSN: 1749-4885 DOI: 10.1038/nphoton.2010.214 (see p. 2)

[Nap+11] NAPOLITANO M., KOSCHORRECK M., DUBOST B., BEHBOOD N., SEWELL R. J., and MITCHELL M. W. Interaction-based quantum metrology showing scaling beyond the Heisenberg limit in: *Nature*, **471**:7339 (2011) 10.1038/nature09778, 486489 ISSN: 0028-0836 DOI: 10.1038/nature09778 (see pp. 145, 209)

[Ost+02] OSTERLOH A., AMICO LUIGI, FALCI G., and FAZIO ROSARIO Scaling of entanglement close to a quantum phase transition in: *Nature*, **416**:6881 (2002) 10.1038/416608a, 608–610 ISSN: 0028-0836 DOI: 10.1038/416608a (see p. 5)

[Pir+10] PIRONIO S., ACÍN A., MASSAR S., DE LA GIRODAY A. BOYER, MATSUKEVICH D. N., MAUNZ P., OLMSCHENK S., HAYES D., LUO L., MANNING T. A., and MONROE C. Random numbers certified by Bell's theorem in: *Nature*, **464**:7291 (2010) 10.1038/nature09008, 1021–1024 ISSN: 0028-0836 DOI: 10.1038/nature09008 (see pp. 3, 77)

[Sor+01] SORENSEN A., DUAN L.-M., CIRAC J. I., and ZOLLER P. Many-particle entanglement with Bose-Einstein conden-

sates in: *Nature*, **409**:6816 (2001) 10.1038/35051038, 6366 ISSN: 0028-0836 DOI: 10.1038/35051038 (see p. 144)

[Śli03] CEZARY ŚLIWA Symmetries of the Bell correlation inequalities in: *Physics Letters A*, **317**:34 (2003), 165 –168 ISSN: 0375-9601 DOI: 10.1016/S0375-9601(03)01115-0 (see pp. 27, 81)

[ŻB02] MAREK ŻUKOWSKI and ČASLAV BRUKNER Bell's Theorem for General *N*-Qubit States in: *Phys. Rev. Lett.*, **88**: (21 2002), 210401 DOI: 10.1103/PhysRevLett.88.210401 (see pp. 80, 81)