DOCTORAL THESIS

Nonlocal Resources for Quantum Information Tasks

Entanglement versus Nonlocality and Randomness

Author:
Florian John CURCHOD

Supervisor:
Prof. Antonio ACÍN

UNIVERSITAT POLITÈCNICA
DE CATALUNYA
BARCELONATECH

ICFO
The Institute of Photonic Sciences

"*You clearly are not the best physicist I ever had in my group, but don't worry: you are okay at football.*"

Antonio Acín

"*You don't finish a thesis, it finishes you.*"

Mafalda L. Almeida

Abstract

This thesis focusses on the essential features of Quantum Theory that are systems in an entangled state and Bell nonlocal correlations. Here, we take the angle of a resource theory and are interested in understanding better how entanglement and nonlocality, first, relate to one another. Indeed, if entangled systems are necessary for the generation of nonlocal correlations, there nevertheless exist entangled systems that seem unable to do so. Quantitatively, it is also unclear whether "more" entanglement leads to "more" nonlocality and, related to that, which measures should be used as quantifiers. Second, entangled systems and nonlocal correlations have been identified as resources for information tasks with no classical equivalent such as the generation of true random numbers. It is then important to understand how the two quantum resources relate to other quantities generated in information tasks.

First, we show that entangled quantum systems are unbounded resources for the generation of certified random numbers by making sequences of measurements on them. This certification is achieved through the successive near maximal violation of a particular Bell inequality for each measurement in the sequence. Moreover, even the simplest two-qubit systems in an almost separable (pure) state achieve this unbounded randomness certification.

Second, we show that entanglement and nonlocality are seemingly put in a quantitative equivalence when using the *nonlocal volume* as measure. This measure is defined as the probability that a system in a given state generates nonlocal correlations when random measurements are performed on it. We prove that this measure satisfies natural properties for an operational measure of nonlocality. Then we show that, in all situations that we could explore, the most nonlocal state – as measured by the nonlocal volume – is always the maximally entangled state.

Third, we consider multipartite scenarios in which quantum systems are distributed to numerous parties. Note that it is in general harder to generate a system that is entangled between many parties rather than more systems entangled between fewer parties. In that spirit, we develop a framework and tools for the study of correlation depth, i.e. the minimal size of the resource – such as entangled systems – that is needed for the (re)production of the correlations.

Fourth, we study the equivalence between the multipartite notions of entanglement and of nonlocality. From an operational understanding of multipartite entanglement, we develop simple families of Bell inequalities that are very efficient for the detection of multipartite nonlocality of pure states.

Last, we study the utility of multipartite quantum correlations for the design of information protocols. We also identify novel features characteristic of these correlations.

The results of this thesis shed light on the interrelations in the triangle entanglement-nonlocality-randomness in Quantum Theory. By going beyond the standard approaches – by considering sequences of measurements on the systems or by considering a novel measure of nonlocality – we obtain insight on the quantitative relations between these three essential quantities. Our study of the multipartite scenario also helps in characterising and identifying multipartite correlations in a simple way. Finally, we also deepened our understanding of how entangled systems and nonlocal correlations, in particular multipartite ones, serve as resources for the design of information tasks with no classical equivalent.

Resumen

La física cuántica es drásticamente distinta de su análogo clásico. Por ejemplo, en principio es posible conocer con certidumbre el resultado de cualquier proceso clásico, si uno tiene un conocimiento perfecto de las condiciones iniciales del proceso y sus interacciones. Sin embargo, la física cuántica es intrínsecamente aleatoria: incluso con un control perfecto, el resultado de un proceso cuántico es, en general, probabilístico. El rango de posibilidades en términos de procesamiento de información también cambia cuando se codifica información en el estado de sistemas cuánticos. El estudio de todas estas nuevas posibilidades es el objeto de la teoría de la información cuántica.

Esta tesis se centra en dos fenómenos cuánticos responsables de parte del poder de la teoría de información cuántica: la existencia de sistemas físicos en estados entrelazados y de correlaciones de Bell no-locales. En primer lugar, y tomando el enfoque de una teoría de recursos, nuestro primer objetivo es comprender mejor cómo el entrelazamiento y la no-localidad se relacionan entre sí. De hecho, si bien es sabido que los sistemas entrelazados son necesarios para la generación de correlaciones no-locales, existen sin embargo sistemas entrelazados que parecen incapaces de hacerlo. Cuantitativamente, tampoco está claro si "más" entrelazamiento conduce a "más" no-localidad y qué medidas deben usarse como cuantificadores. En segundo lugar, los sistemas entrelazados y las correlaciones no-locales se han identificado como recursos para tareas de información sin ningún equivalente clásico, como por ejemplo la generación certificada de números aleatorios. Es por tanto importante comprender cómo los dos recursos cuánticos se relacionan con otras cantidades generadas en las tareas de información. El trabajo de la tesis, centrado alrededor de estas dos motivaciones, ha llevado a los resultados que se describen a continuación.

Primero, mostramos que los sistemas cuánticos entrelazados son recursos ilimitados para la generación de números aleatorios certificados a través de secuencias de medidas. Esta certificación se logra mediante la sucesiva violación, casi máxima, de una desigualdad de Bell particular para cada medición en la secuencia. Además, incluso los sistemas de dos qubits más simples, en un estado puro casi separable, logran esta certificación de aleatoriedad ilimitada.

En segundo lugar, mostramos que el entrelazamiento y la no-localidad se expresan, aparentemente, en una equivalencia cuantitativa cuando se utiliza el "volumen no-local" como cuantificador. El volumen no-local se define como la probabilidad de que un sistema en un estado dado genere correlaciones no-locales cuando se realizan mediciones aleatorias en él. Probamos que este cuantificador satisface las propiedades naturales de una medida operacional de no-localidad. Luego mostramos que, en todas las situaciones que podemos explorar, el estado más no-local, medido por el volumen no-local, es siempre el más entrelazado.

Finalmente, obtenemos varios resultados en escenarios multi-partitos en los que los sistemas cuánticos se distribuyen entre numerosos observadores. Desarrollamos un marco y herramientas para el estudio de la profundidad de correlación, es decir, el tamaño mínimo del recurso (por ejemplo, el entrelazamiento) que es necesario para la reproducción de las correlaciones. Además. estudiamos la equivalencia entre las nociones multi-partitas de entrelazamiento y de no-localidad, obteniendo familias sencillas de desigualdades de Bell que son muy eficientes para la detección de no-localidad multi-partita generada por sistemas en estados puros. Por último, estudiamos la utilidad de las correlaciones cuánticas multi-partitas para el diseño de protocolos de información.

Los resultados de esta tesis arrojan luz sobre las interrelaciones en el triángulo entrelazamiento/no-localidad/aleatoriedad en la teoría cuántica. Al ir más allá de los enfoques estándar, al considerar secuencias de mediciones en los sistemas o al considerar una nueva medida de no-localidad, obtenemos información sobre las relaciones cuantitativas entre estas tres cantidades esenciales. Nuestro estudio del escenario multi-partito también ayuda a caracterizar e identificar las correlaciones multi-partitas de una manera simple. Finalmente, profundizamos nuestra comprensión de cómo los sistemas entrelazados y las correlaciones no-locales, en particular multi-partitas, sirven como recursos para el diseño de tareas de información sin análogo clásico.

List of publications

- "Anonymous Quantum Nonlocality", Yeong-Cherng Liang, Florian John Curchod, Joseph Bowles, and Nicolas Gisin. Physical Review Letters 113, no. 13 (2014): 130401.

- "Quantifying multipartite nonlocality via the size of the resource", Florian John Curchod, Nicolas Gisin, and Yeong-Cherng Liang. Physical Review A 91, no. 1 (2015): 012121.

- "Unbounded randomness certification using sequences of measurements", Florian John Curchod, Markus Johansson, Remigiusz Augusiak, Matthew J. Hoban, Peter Wittek, and Antonio Acín. Physical Review A 95, no. 2 (2017): 020102.

- "Entangled systems are unbounded sources of nonlocal correlations and of certified random numbers", Florian John Curchod, Markus Johansson, Remigiusz Augusiak, Matty J. Hoban, Peter Wittek, and Antonio Acín. In LIPIcs-Leibniz International Proceedings in Informatics, vol. 73. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2018.

- "Towards an equivalence between maximal entanglement and maximal quantum nonlocality", Victoria Lipinska, Florian John Curchod, Alejandro Máttar, and Antonio Acín. New Journal of Physics, 20 063043 (2018).

- "A simple approach to genuine multipartite nonlocality of pure states", Florian John Curchod, Mafalda L. Almeida, and Antonio Acín. *To appear*.

Acknowledgements

First, I would like to thank you, the very famous Toni, for so many things that I can not decently put all of them here in the acknowledgements. I had a great time with you in front of the whiteboard, but also on the football field where I could enjoy your technique, speed and vision (ok, one of them is actually true). You also always took good care of putting the right person at the right moment in the office with me, thanks for that too. Like many before me, I will have the post-Toni blues.

Second, to my physics "grand-parents", Nicolas Gisin, Yeong-Cherng Liang and Denis Rosset, I can not thank you enough for introducing me to the field. A special thank to you, Yeong-Cherng, who really took (a lot of) time to help a simple master student.

Then, I would like to thank Andreas Winter, Maciej Lewenstein and Paul Skrzypczyk, for accepting to be part of the jury of my thesis. Toni was nice enough to let me choose my "dream team" and I feel sorry for imposing to people I like to read any thesis that is even remotely connected to multipartite nonlocality.

To my collaborators I didn't mention yet: Ale, Victoria, Markus, Remik, Matty, Mafalda, Peter, I thank you for letting me annoy you with my bees (yes, this is an apology Peter) and other related stuff. It was a pleasure to work with you!

To the first members of my office, Matty and Ariel, thanks for making sure that I had the best (I'm not sure I am using the right adjective here) atmosphere to start focussing hard on my PhD. To you Marti, that brought me to one of the best games I have ever seen! To Maciek, whom I owe all my futbolin skills to (and some yokes). To the other members of the group I don't see as often as I would like to: Ivan, Flavio, Senaida, Michal, Paul, Elsa, Bogna, Gonzalo, Alex, Zahrrrrra, Osvaldo, Janek, Christian, Joe, Dani, Karen, Matteo, Gaby, Erik, Dario, Chung-Yun, Patrick.

A special hug goes to my Liquid friends, Marcus, Claude, Stefan, for welcoming me and introducing me to the beauties (among other things) of Barcelona! To Leozinho and the local models you introduced to Nahla. To Bori and Alexia, I often remember both of you (for different reasons) when looking at a cereal bowl...

To these special moments that have made my PhD nicer: Marco for showing me part of Brazil, the Electrons Tropicals for showing me how football is played in Catalonia, Flapi for enjoying with me the other best game of my life (among many, many other things). To Flavien and Yann, and our endless search for the famous lost thermoclyde.

Seria um crime não mencionar Vovô e Vovó, que entraram num avião 5 minutos após todas as vezes que lhes pedimos apoio. Sou um dos raros sortudos que pode

dizer: passar 3 semanas convosco, num pequeno apartamento, é na realidade um prazer!

A mes parents, sans qui je ne serais rien. Avoir eu des enfants me fait réaliser combien de travail vous avez dû avoir. Malheureusement (pour vous), même en réalisant, un enfant ne change pas son attitude envers ses parents! En enooooorme kus voor me moeder, die zoveel voor haar kinderen gedan heeft. Ik heb ook een gedachte voor mijn Opa en Oma. A vous aussi, Jo et Sas, et les (encore) nombreux déguisements pourris qui nous attendent.

Finally, I would like to mention the three women of my life. Mafalda, I could never imagine that ponies come in so many colours, please never stop writing my career (and life) plans. Nahla et Zizo, vous voir grandir est la meilleure (et plus drôle) chose qui me soit jamais arrivée!

Contents

Chapter 1

Objectives and main results

Much of the excitement that surrounds Quantum Theory stems from the fact that it is very counter-intuitive. Indeed, our intuition is built on the events we experience on a daily basis and where most, if not all, quantum features disappear. In terms of information processing, the range of possibilities when information is encoded in quantum states drastically differ from what is achievable in a classical theory. For example, an unknown classical bit of information that is received can be read and copied at will. On the contrary, information encoded in a qubit – a quantum bit – can in general not be retrieved and copied with certainty, a result known as the no-cloning theorem [WZ82]. More than this, the amount of classical bits that are needed in order to fully describe the state of a single qubit is infinite!

Quantum Theory abandons many of the principles we believed to be essential to any physical theory. Intrinsically probabilistic, the outcome of a physical process can in general not be predicted even with perfect control over the initial conditions. Some quantities, such as the position of a particle and its velocity, can not be measured precisely at the same time: acquiring information about one will force uncertainty about the other.

More than a century after its inception, Quantum Theory is one of the most accurately tested physical theories. Nevertheless, some of its essential features – such as entanglement or quantum nonlocality – are still puzzling the community. The presence of entanglement, i.e. states of composite systems that can not be described by the states of their subsystems, leads to the phenomenon of nonlocality: measurements made on entangled quantum systems can produce correlations stronger than those of any classical theory. First seen as theoretical peculiarities, entanglement and non-locality are now essential resources in the field of Quantum Information Science. Indeed, they have been harnessed into powerful resources for information tasks with no classical counterpart: randomness certification, expansion and amplification [AM16; CK11; CR12; Pir+10], provably secure distribution of secret keys [BB84; Eke91], quantum teleportation [Ben+93] or testing devices without making assumptions about their internal functioning [MY98], for example.

The phenomenon of nonlocality exhibits itself through the correlations observed between the outcomes of distant measurements made on entangled particles. As such, it does not depend on the exact processes that were put into play to generate the correlations, but solely on the statistical properties of the correlations themselves. In particular, no assumption is made about the functioning of the measurement devices or about the underlying Hilbert spaces dimensions of the physical systems. This very abstract modelling of a physical set-up allows to draw conclusions in a *device-independent* manner [MY98; Ací+07; Ban13].

The benefit of taking such a minimalistic approach is two folded. On the one hand, we expect to deepen our understanding of the physical principles that are obeyed by the correlations observed in the quantum world. Quantum Theory was built as an ad hoc theory – whose predictive power has been confirmed numerous times – and we are still lacking an understanding in terms of operational principles, the "why" we observe what we observe. Comparing the correlations that can arise from measurements on quantum systems with the ones that can be generated in other theories, such as the classical or post-quantum ones, will help to single out Quantum Theory in terms of principles.

On the other hand, when designing information protocols that make use of the peculiarities of Quantum Theory as resources, the fewer assumptions that are made about the physical set-up the more robust the protocol in an adversarial picture. The device-independent paradigm allows one to build protocols with unprecedented level of security, as the number of assumptions that are made is minimal [MPA11; Ací+07; Eke91; AGM06; Pir+10].

1.1 Motivation

Understanding and characterising quantum nonlocal correlations is central not only to answer fundamental questions, but also for the implementations of information tasks where they have been identified as essential resources. In this view, it is crucial not only to improve our understanding of how they can be generated, but also to improve the methods for their identification or quantification. Given quantum nonlocal correlations, from a resource-theoretic point of view it is also interesting to understand how complex these correlations are for their (re)production.

Entangled quantum states are necessary for the generation of quantum nonlocal correlations, that in turn are needed in information tasks such as the generation of certified random numbers. It is then important to understand, first, how entanglement and nonlocality relate to one another. Second, to understand how entanglement and nonlocality relate to the quantities generated during information tasks such as certified random numbers. For example, is there a fundamental bound on the amount of randomness that can be certified from entangled systems? The answers to these questions will serve to understand what are the potentialities of Quantum Theory. As resources, it will also shed light on how powerful entanglement and nonlocal correlations are for the design of information tasks.

The two main axes of research of this thesis are: $i)$ understand better, at the fundamental level, how entanglement, nonlocality and other quantum features such as certified randomness relate to one another – both qualitatively and quantitatively; and $ii)$ understand better the potentiality of entanglement and of nonlocal correlations as resources for device-independent information tasks. For clarity, the precise lines of research of this thesis are outlined in the following.

□ **Improve the tools to identify nonlocal correlations.**
Today, the most common tool to witness the nonlocal character of the correlations generated in an experiment are Bell inequalities. A violation of these indeed serves to discard any possible classical explanation of the observed correlations. A Bell inequality can always be understood as an information task that can be achieved with greater probability when using quantum resources rather than classical ones. Bell inequalities are thus also useful to identify new information tasks in which quantum resources provide an advantage. In this context, it is important to continue designing new Bell inequalities for a better characterisation of quantum nonlocal correlations, but also in order to identify the nature of the advantages provided by Quantum Theory over the classical ones.

The observation of nonlocal correlations often serves as a certificate that the underlying processes were indeed making use of genuinely quantum resources [MY98], because it imposes constraints on any physical realisations compatible with the observed correlations. In particular, the violation of a Bell inequality has already been identified as useful for: randomness certification [CK11; CR12; Pir+10]; secure device-independent quantum key distribution [Ací+07; Eke91]; testing the functioning of a device without assumptions about its internal functioning [MY98]; as device-independent witness of entanglement [Ban14a]; obtaining lower bounds on the communication complexity of reproducing quantum correlations[Buh+10; Dam99; TB03; RT09].

□ **Improve our understanding of the relation between quantum entanglement and nonlocality.**
Entangled quantum systems are necessary for the generation of quantum nonlocal correlations. Nevertheless, it is still unclear whether all entangled systems can be used in order to generate nonlocal correlations. At the quantitative level, the relation

between the two quantum features is even more obscure. For instance, is *more* entanglement synonymous of *more* nonlocality? This question obviously depends on the measure that is used in order to quantify the nonlocality exhibited by quantum systems and the result typically depends on the choice that is made. Nevertheless, a shared feature of all measures used so far is that the most nonlocal states often are the ones that are not the most entangled [Aci+02; Ebe93; AGG05; BGS05; MS06]. Do these "anomalies" hint at the fact that one should not expect a quantitative equivalence between entanglement and nonlocality or rather that they appear as artefacts of the chosen measures?

In some particular cases, the qualitative equivalence between entanglement and nonlocality has been established. For instance, all physical systems in a pure entangled state can be used to generate nonlocal correlations [Gis91; PR92]. In many other situations, the question is subtler. For instance, some (mixed) quantum states can not display nonlocality whenever single measurements are performed on each copy [Wer89; Bar02]. They may nevertheless become able to generate nonlocal correlations when: sequences of measurements are being performed on each copy [Pop95] and/or many copies of the systems are measured together [Pal12] and/or the systems are combined with others that are also unable to display nonlocality [MLD08] and/or are put in a network [Cav+11]. The question of the equivalence between entanglement and nonlocality in general remains one of the most important open questions in the field of Quantum Information Theory.

□ **Identify information tasks whose success requires using quantum resources.**

As said, the use of quantum states as carrier of information and the phenomenon of nonlocality open a new range of possibilities in terms of information processing. Not only does it improve the performances in some existing tasks, but it also offers opportunities to perform some that were otherwise impossible. For example, in a classical theory it is impossible to generate truly random numbers as the theory is deterministic in its essence. On the contrary, Quantum Theory is intrinsically probabilistic. It thus offers the possibility to certify randomness, i.e. prove that the outcomes of measurements on quantum systems are unpredictable based on the statistical properties of the correlations only [CK11; CR12; Pir+10]. Another example is the one of distributing a secret key to distant parties in a secure way, a task of great importance in cryptography. Classical protocols for the distribution of keys rely on complexity assumptions. For instance, their security depends on the capacity of an adversary to factorize large numbers into prime ones, a task however known to be easy (solvable in polynomial time) for a quantum computer. Quantum key distribution offers the possibility to distribute secret keys in a provably secure way based on minimal assumptions, in particular none about the computational power of the adversary [Eke91]. Further, quantum key distribution can be performed in a device-independent manner [Ací+07], i.e. without relying on a faithful description of the parties' devices. One of the key objective of Quantum Information Theory is to identify these tasks where quantum resources prove useful, understand why and work on improving their experimental feasibility.

□ **Identify the limitations of quantum resources in information tasks.**
It is already clear that quantum resources, such as entangled systems, provide advantages in terms of what can be achieved in information tasks as compared to what can be done using classical resources. Nevertheless, there still exist fundamental bounds, or limitations, on what is achievable within Quantum Theory in terms of information processing. For example, since the state of a qubit requires an infinite amount of classical bits for its description, it is tempting to think that it can be used to transmit a very large amount of classical information. Nevertheless, it was found that a single qubit can be used for the transmission of at most a single bit of classical information [Hol73; SW97]. This question is closely related to the one of understanding which information principles bound the set of possible correlations achievable by making measurements on quantum systems. For example, the correlations generated in Quantum Theory seems to be optimal in terms of how much randomness can be certified through them, which is not the case in general when considering post-quantum theories [Tor+15].

As resources, it is important to understand exactly how powerful entangled systems and nonlocal correlations are. When bounds appear on the potentiality of quantum resources, it is important to distinguish the situation where these limitations derive from fundamental principles or appear as artefact of the set-up that is being considered. In the second case, it is then possible that the limitation can be lifted by extending the range of operations that are considered in the limited set-up. In that spirit, some entangled systems generate nonlocal correlations only when sequences of measurements are being performed on them and remain useless in the standard set-up with a single measurement in the sequence [Pop95].

□ **Characterise the complexity of nonlocal correlations for their (re)production.**
Quantifying the complexity of nonlocal correlations is useful for two reasons. First, it is imperative to understand how complicated given nonlocal correlations are for their experimental realisation, in particular when these are resources for information tasks. Measures of complexity could be the number of particles that need to be entangled together in a multipartite system [GTB05] or the degree of entanglement that is needed for the generation of the correlations [Woo98]. Obviously, the complexity of nonlocal correlations can be evaluated according to many criteria, the choice of which depends on the specific aim one is interested in.

Second, it is also of interest to compare the complexity of quantum nonlocal correlations when these are to be reproduced by other nonlocal resources. For example, how difficult is it to reproduce quantum nonlocal correlations when having access to post-quantum but nevertheless no-signalling resources[1] [BP05]? Also of interest is the amount of classical communication that needs to be exchanged in place of sharing entangled systems for the generation of specific nonlocal correlations – the communication complexity of the correlations [Buh+10; Dam99; TB03; RT09]. The goal is to understand how powerful quantum resources are as compared to the ones of other theories.

□ **Understand the advantages provided by *generalised scenarios*.**
The standard Bell scenario is the simplest set-up in which nonlocal correlations arise and, as such, as received most of the attention of the community so far. Some of its limitations are: a) correlations between two parties only are considered; b) the parties make a single measurement on the system they receive before discarding it; c) often projective measurements only are considered. The study of correlations in the standard scenario suffices to observe a quantum advantage over classical resources and its study has been extremely fruitful [Bela]. Nevertheless, there are many examples in which considering *generalised scenarios* – set-ups that go beyond the standard one – permits to achieve tasks that were otherwise impossible in the standard scenario. Generalised scenarios may consist in: i) the use of multipartite states distributed to many (more than two) observers, ii) performing sequences of measurements on the systems, iii) the use of general measurements (positive-operator valued measures). The use of multipartite systems has been shown to permit full randomness amplification [Gal+13; Bou+14], the use of sequences of measurements has been proved useful for the activation of hidden nonlocality [Pop95] and the use of general measurements allows for increased randomness certification for example [Ací+16]. In all these scenarios, not only is it possible to perform novel tasks but richer types of correlations also arise [Gal+14; Sve87; SS02; Ban+13; Gal+12].

Exploring generalised scenario also helps as tool to obtain insight on all the previously mentioned questions and research directions.

1.2 Main results

Entanglement and quantum nonlocality in bipartite states and beyond: towards a quantitative equivalence [Lip+18]. – Many Bell inequalities are maximally violated by non maximally entangled states only [Aci+02], even when considering states of arbitrary Hilbert space dimension [LVB11; VW11]. This phenomenon of obtaining more nonlocality from less entanglement is also observed for almost all other operational measures of nonlocality [Aci+02; Ebe93; AGG05;

[1] I.e. any resources which do not allow for infinite speed communication.

BGS05]. We study a recently proposed measure of nonlocality defined as the probability that a given state displays nonlocal correlations when subjected to random measurements, as witnessed by all possible Bell inequalities in a fixed scenario [Ros+17; Lia+10; FP15]. We first prove that this measure satisfies some natural properties for an operational measure of nonlocality. Second, we provide analytical and numerical results suggesting that this measure is a good candidate for a quantitative equivalence between entanglement and nonlocality for pure states. These results help understanding under which perspective one should recognise entanglement and nonlocality as quantitatively equivalent. In particular, it strengthens the idea that Bell inequalities should be considered as witnesses and not as quantifiers of nonlocality.

Entangled systems are unbounded resources for the generation of nonlocal correlations and of certified randomness [Cur+17; Cur+18]. – In the standard scenario, a single measurement is performed on the shares of a physical system before they are discarded and a fresh copy of the system is generated. Nonlocal correlations can thus be generated between the outcomes of two distant measurement and only a limited amount of randomness can be certified [Ací+16]. In particular, a system of two qubits can be used for the generation of *at most* four random bits. This raise the question of whether there exist fundamental bounds on the amount of randomness that can be certified from quantum systems. By considering sequences of measurements performed on the systems, we show that it is possible to generate an unbounded amount of certified randomness even from the simplest entangled systems, namely from two qubits that can be arbitrarily little entangled. The certification is achieved through the successive (near) maximal violation of a particular Bell inequality for each measurement in the sequence. An important ingredient for our construction is the use of weak measurements which allow tuning the trade-off between the amount of information that is extracted from the states and the state disturbance – i.e. entanglement destruction – that such a measurement causes. These results show that there is no fundamental limit on the amount of randomness that can be certified from entangled systems.

A simple approach to multipartite nonlocality from pure states [CAA18]. – In the multipartite set-up for the generation of nonlocality, where multipartite states are distributed to many (more than two) parties, richer correlations arise and novel quantum features appear [Hor+09; Gal+14; Sve87; SS02; Ban+13; Gal+12]. From an operational understanding of multipartite pure state entanglement, we develop simple families of Bell inequalities witnessing (genuine) multipartite nonlocality. We show that our families are very efficient to witness nonlocal correlations generated from pure states. We provide strong numerical evidence that all systems of three and four qubits in a genuine multipartite entangled (GME) pure state violate our families and thus generate genuine multipartite nonlocality (GMNL). Analytically, we show that almost all pure states of three qubits in a GME state generate GMNL, as witnessed by the violation of a single inequality. We also show that a large class of GME pure states violate a family of inequalities for any number of parties, even states that are almost separable. The operational meaning of our inequalities and their violations lead us to conjecture that these can be used to generalise Gisin's theorem for bipartite systems [Gis91] to the multipartite notions of entanglement and nonlocality: we suspect that all GME pure states are GMNL.

Quantifying multipartite nonlocality via the size of the resource [CGL15]. – When given correlations from an experiment or from a theory, it is desirable to determine the extent to which the participating parties would need to collaborate nonlocally – by sharing entangled systems for example – for their (re)production. We develop a framework to achieve this via the *minimal group size (MGS) of the resource*, i.e., the smallest number of parties that need to share a given type of nonlocal resource for the above-mentioned purpose. For example, certain correlations between four parties can be generated by sharing entangled systems that are entangled between three parties only. These correlations can be understood as simpler to generate than those that require the use of systems that are entangled between all the four parties together. They are nevertheless more complex than the ones where only bipartite entangled systems suffice. Other nonlocal resources can consist of arbitrary (post-quantum) no-signaling correlations or classical communication between subset(s) of the parties. Of course, the particular choice of resource that is made in general leads to different answers. With this in mind, we build a framework and tools for the study of the MGS of correlations. We also apply our techniques to specific examples where the MGS of the correlations can be determined. Our work allows for the quantification of multipartite correlations in a very natural and operational way.

Multipartite quantum nonlocal correlations are useful resources for novel device-independent information tasks [Lia+14]. – Novel properties exhibited by quantum nonlocal correlations in the multipartite scenario are identified and showed to be useful novel resources for information tasks. In particular, multipartite quantum correlations can exhibit a form of anonymity, allowing a party to perform an information task without revealing its identity. We also show that specific multipartite quantum nonlocal correlations can in principle be used for quantum key distribution in a device independent manner that is resilient to nearly arbitrary leakage of information to the adversary. We also propose a scheme to perform multipartite secret sharing between any two groups of parties. Our work also aims at showing that the multipartite extent to which correlations are nonlocal does not seem important for DI information tasks. One should rather focus on other interesting properties, such as perfect correlations between the parties, together with the fact that the correlations are nonlocal at all. To obtain these results, we also analyse the complexity of (re)producing specific quantum nonlocal correlations – in terms of minimal group size of the resources – when using post-quantum resources such as arbitrary no-signalling ones or classical communication between subset(s) of the parties. In particular, we show that the gap between quantum and post-quantum resources can be made arbitrarily large.

1.3 Outline of the thesis

The present thesis is organised as follows. The next chapter serves to introduce the background material supporting the results of this thesis. The chapters that follow are dedicated to the results obtained during the course of this thesis. Finally, I finish with a general overview of this thesis and future perspectives. The appendices serve as supporting material for the obtained results.

Chapter 2

Background

This chapter is devoted to an introduction of the topics central to the thesis. Its first section is devoted to entanglement, the second to the phenomenon of nonlocality, the third to entanglement and nonlocality in the multipartite set-up. Finally, the fourth section introduces several device-independent tasks relying on the generation of nonlocal correlations. In each section, the formalism, important existing results and tools useful in the scope of this thesis are exposed.

2.1 Quantum entanglement

"I would not call entanglement *one* but rather *the* characteristic trait of quantum mechanics, the one that enforces its entire departure from classical lines of thought."

E. Schrödinger, in [Sch35]

In 1935, Einstein, Podolski and Rosen (EPR) first note a peculiarity in the description of joint systems in Quantum Theory [EPR35]. Two particles that have once interacted can indeed be in an *entangled*[1] state when some physical quantities are conserved. By making different measurements on one of the particles in such an entangled state, it is possible to project the *other* particle into different states that can in principle be the eigenstates of observables that do not commute – this whatever the distance that separates the particles at the moment of the measurement. For example, by measuring one of the two entangled particles, one can project the other one into a state with definite position *or* with definite momentum without interacting with that second particle. By assuming that systems that are far apart can not influence each other instantaneously – the principle of locality – one comes to the conclusion that the second particle should have definite position *and* momentum, independently of the measurement that is being performed on the other particle. This contradiction between the local description of a physical system – that can not be

[1] EPR didn't use the word *entangled*, which was only later proposed by Schrödinger [Sch35].

an eigenstate of both the position and momentum operators – and the consequences of the global description of joint systems lead EPR to conclude that the description of physical systems in Quantum Theory could not be considered *complete*.

It is only much later that the paradox was resolved: measurements made on one of the two particles in an entangled state can indeed influence – at a distance and instantaneously – the results of measurements made on the second one! Such influences can nevertheless not be used to communicate faster than the speed of light and do thus not enter in conflict with the Theory of Relativity. Quantum Theory does not respect the principle of locality[2,3], a phenomenon known as *quantum nonlocality*. Quantum nonlocality is the main topic of interest of this thesis and we describe it in more detail in the next section. In the present section, we introduce the fundamental property of entanglement of the joint states of physical systems, which is necessary in order to generate nonlocal correlations.

2.1.1 Entanglement in bipartite systems

Two particles, A and B, that are in a pure state, are described by a joint quantum state $|\Psi\rangle_{AB} \in \mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}}$ – a vector living in the tensor product of the two local Hilbert spaces over the complex numbers for A and B. Such a bipartite pure state is said to be *separable* if it can be written as

$$|\Psi\rangle_{AB} = |\psi\rangle_A |\phi\rangle_B \tag{2.1}$$

for some $|\psi\rangle_A \in \mathcal{H}_{\mathcal{A}}$, $|\phi\rangle_B \in \mathcal{H}_{\mathcal{B}}$ that are two normalised quantum states and where we use the obvious abbreviation $|\psi\rangle_A|\phi\rangle_B \equiv |\psi\rangle_A \otimes |\phi\rangle_B$. Separable states (2.1) describe systems that can be understood as classical, in the sense that a measurement made on one of the particles does not change the state of the other.

On the contrary, there are states $|\Psi\rangle_{AB} \in \mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}}$ in Quantum Theory which do not allow for a decomposition of the form (2.1)

$$|\Psi\rangle_{AB} \neq |\psi\rangle_A |\phi\rangle_B \tag{2.2}$$

for any choice of (normalized) states $|\psi\rangle_A \in \mathcal{H}_{\mathcal{A}}$ and $|\phi\rangle_B \in \mathcal{H}_{\mathcal{B}}$. Such states are *entangled*: measurements on one of the subsystems can influence the state of

[2] To be exact, there are other ways to circumvent the paradox, such as allowing for faster than light signalling for example, but all these imply violating even stronger physical principles than the one of locality.

[3] We simplify the situation, in reality quantum correlations violate the principle of local *realism* (or, equivalently, local *causality* in Bell's terms), that is that an event is influenced deterministically by its immediate surroundings only.

the other. Physical systems in an entangled state, apart from being of fundamental interest, also are essential resources for many information tasks that are otherwise impossible with separable (or classical) states only. One can send more than one bit of information using the state of a single qubit[4] – called superdense coding [BW92] – or teleport the unknown state of one particle to another distant one using classical communication only – quantum teleportation [Ben+93]. Both these tasks fundamentally rely on the use of entangled systems. Furthermore, entangled systems are necessary for the generation of nonlocal correlations. This implies that any information tasks requiring nonlocal correlations to be generated also crucially relies on the possibility to distribute systems in an entangled state to distant observers.

Schmidt basis, concurrence and maximal entanglement

A pure quantum state $|\Psi\rangle_{AB} \in \mathbb{C}^d \otimes \mathbb{C}^d$ of two particles – a two-qudit pure state – can always be written in a particular choice of local bases as

$$|\Psi\rangle_{AB} = \sum_{i=0}^{d-1} \alpha_i |ii\rangle \tag{2.3}$$

with $\alpha_i \in \mathbb{R}_{\geq 0}\ \forall i$, $\sum_{i=0}^{d-1} \alpha_i^2 = 1$ and $\alpha_0 \geq \alpha_1 \geq ... \geq \alpha_{d-1}$. A pure bipartite state written in the form (2.3) is said to be in its Schmidt bases. In particular, a bipartite two-qubit pure state ($|\Psi\rangle_{AB} \in \mathbb{C}^2 \otimes \mathbb{C}^2$) is written as

$$|\Psi(\theta)\rangle_{AB} = \cos(\theta)|00\rangle + \sin(\theta)|11\rangle \tag{2.4}$$

for an angle $\theta \in [0, \frac{\pi}{4}]$.

The amount of entanglement in a pure state can be quantified with the help of a measure called the *concurrence* $\mathcal{C}(|\Psi\rangle_{AB}) : \mathbb{C}^d \otimes \mathbb{C}^d \to [0, 1]$. For any pure two qubit state $d = 2$, written in its Schmidt basis (2.4)

$$\mathcal{C}(|\Psi(\theta)\rangle_{AB}) = 2\cos(\theta)\sin(\theta) = \sin(2\theta) \tag{2.5}$$

implying that the amount of entanglement grows monotonically with the angle $\theta \in]0, \frac{\pi}{4}]$ and is zero only for the separable state with $\theta = 0$.

[4] In addition to the system in a qubit state that is sent, the parties also share (maximally) entangled systems which allow to enhance the amount of information the qubit system can carry between them.

A state of particular interest is the the maximally entangled one, with $\alpha_i = \frac{1}{\sqrt{d}} \forall i$ (2.3)

$$|\Phi^+\rangle_{AB} = \sum_{i=0}^{d-1} \frac{1}{\sqrt{d}} |ii\rangle \tag{2.6}$$

In the case of two qubits (2.4), it is the one maximising the concurrence (2.5) with $\theta = \frac{\pi}{4}$ in (2.4)

$$|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{2.7}$$

Mixed quantum states

In practice, noise in the set-up or imperfect knowledge make that the states of physical systems need to be described in the formalism of mixed states, which also allows for pure states to be represented. A mixed state ρ_{AB} is represented as an operator acting on the space $\mathcal{H}_A \otimes \mathcal{H}_B$[5] and is an hermitian, trace one, matrix. It can always be decomposed, and understood, as a probabilistic mixture of pure states

$$\rho_{AB} = \sum_i q_i |\Psi_i\rangle\langle\Psi_i|_{AB} \tag{2.8}$$

with q_i a probability distribution $q_i \in \mathbb{R}_{\geq 0} \;\; \forall i$ with $\sum_i q_i = 1$ and $|\Psi_i\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$ a valid pure (normalised) state for all i. Note that a mixed state that is not pure might allow for different decompositions (2.8). A simple condition to test the purity of a state ρ is

$$Tr(\rho^2) \begin{cases} = 1 & \Leftrightarrow \quad \rho \text{ is pure:} \quad \rho = |\Psi\rangle\langle\Psi|_{AB} \\ < 1 & \Leftrightarrow \quad \rho \text{ is mixed:} \quad \rho \neq |\Psi\rangle\langle\Psi|_{AB} \end{cases} \tag{2.9}$$

Mixed quantum states are not only useful as tools to deal with practical imperfection in the set-up – i.e. stemming from an incidental lack of knowledge – but also as essential objects originating from an intrinsic lack of knowledge in the formalism of Quantum Theory. Indeed, one can show that when a system is in a pure state $\rho_{AB} = |\Psi\rangle\langle\Psi|_{AB}$ (2.2), the purity of its subsystems, say $\rho_A = Tr_B(\rho_{AB})$ for example, can be computed in order to decide whether $|\Psi\rangle_{AB}$ is entangled or separable:

$$Tr(\rho_A^2) \begin{cases} = 1 & \Leftrightarrow \quad |\Psi\rangle_{AB} = |\psi\rangle_A|\phi\rangle_B \\ < 1 & \Leftrightarrow \quad |\Psi\rangle_{AB} \neq |\psi\rangle_A|\phi\rangle_B \end{cases} \tag{2.10}$$

[5] This is usually denoted $\rho \in B(\mathcal{H}_A \otimes \mathcal{H}_B)$, ρ acts on the Banach space associated to the Hilbert spaces $\mathcal{H}_A \otimes \mathcal{H}_B$.

Deciding whether a given pure state is entangled or not – the *separability problem* – can thus be achieved through the necessary and sufficient condition (2.10).

The definition of separable (2.1) and entangled pure states (2.2) generalise to density matrices (2.8). A mixed state ρ_{AB} is said to be separable if

$$\rho_{AB} = \sum_i g_i \sigma_A^i \otimes \gamma_B^i \tag{2.11}$$

where $g_i \in \mathbb{R}_{\geq 0}\ \forall i$ form a convex combination $\sum_i g_i = 1$ and $\sigma_A^i = |\psi_i\rangle\langle\psi_i|_A$ and $\gamma_B^i = |\phi_i\rangle\langle\phi_i|_B$ are valid (normalised) pure states for all i. The set of all separable states (2.11) acting on Hilbert spaces of dimension d is denoted $\mathcal{S}_d$ and is convex by construction. A mixed state (acting on Hilbert spaces of dimension d) that does not admit a decomposition of the form (2.11), $\rho \notin \mathcal{S}_d$, is said to be entangled.

The separability problem for mixed states ρ_{AB} (2.8) amounts to checking their membership to the set $\mathcal{S}_d$ of all separable states (2.11), i.e. deciding whether ρ_{AB} allows for a decomposition of the form (2.11). Solving the separability problem in general remains open and a necessary and sufficient criterion is known only for mixed two-qubit and qubit-qutrit states – acting on $\mathbb{C}^2 \otimes \mathbb{C}^2$ and in $\mathbb{C}^2 \otimes \mathbb{C}^3$ respectively [Per96]. Moreover, the separability problem was shown to be NP-hard in general [Gur04]. The task of witnessing entanglement – both in theory and in experiment – in quantum systems is of paramount importance in the field of Quantum Information Science, first as a question of fundamental interest but also for the characterisation of entanglement as a resource.

Entanglement witnesses

Another technique to identify entanglement in quantum states is the use of *entanglement witnesses*. Such a witness can be represented by an operator W acting on quantum states such that its expectation value

$$Tr(W\rho) < 0 \quad \Rightarrow \quad \rho \notin \mathcal{S}_d \tag{2.12}$$

identifies entanglement in the state. An entanglement witness can be understood as an hyperplane in the state space, the entire set of separable states lying on the positive side $Tr(W\rho) \geq 0$ of it. Note that there are also entangled states $\rho_{\text{ent}} \notin \mathcal{S}_d$ giving positive expectation values $Tr(W\rho_{\text{ent}}) \geq 0$, implying that the witness works as a sufficient but not necessary condition for entanglement.

On the other hand, in a situation where one would like to characterise the entanglement of an unknown state, it is then impossible to decide which entanglement witness – among a infinite set of them – to use, making the technique potentially

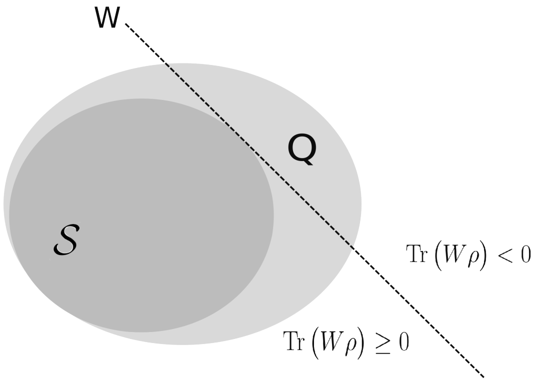
W
Q
S
$\mathrm{Tr}\left(W\rho\right) < 0$
$\mathrm{Tr}\left(W\rho\right) \geq 0$

FIGURE 2.1: An illustration of an entanglement witness W in the abstract space of quantum states. An entanglement witness is an hyperplane in that space and separates it into two half spaces, with the set of separable states S lying on the positive half. A negative expectation $Tr(W\rho) < 0$ serves as witness that the state is entangled $\rho \notin S$.

highly inefficient. Worse, imperfections in the measurement apparatuses or in prior knowledge of the state will potentially lead to false positives [Ros+12].

Local operations and classical communication

The maximally entangled pure state $|\Phi^{+}\rangle_{AB}$ (2.6) in a given dimension d can be transformed into *any* other state with the same (or lower) Hilbert space dimension by performing local operations on each subsystem and using classical communication (LOCC)[Nie99]. LOCC operations are the ones that do not increase the amount of entanglement (using any measure, for example the concurrence (2.5)). They can therefore be seen, from a theoretical point of view, as *free* resources. In that view, the maximally entangled state (2.6) plays a special role.

LOCC allow one to define entanglement in an operational way: entangled systems can not be prepared by two distant observers sharing separable states on which they make rounds of local operations (such as a measurement or unitary operation) followed by classical communication (such as sending to the other observer one's measurement outcome). In the same way, one can not increase the amount of entanglement in the states by means of LOCC. In order to create/increase entanglement one needs to perform global operations on the joint state of the systems.

2.2 Quantum Nonlocality

EPR were led to the conclusion of the incompleteness of Quantum Theory by *assuming* that any physical theory should respect the principle of locality: influences spread gradually through space-time. It is only much later, in 1965, that J. Bell formalised the concept of locality[6] and derived statistical constraints on any theory satisfying the principle [Bel01]. The inequalities that were obtained involve statistical correlations between the outcomes of local measurements made in distant locations. J. Bell showed that the correlations obtained by making local measurement on the subsystems of physical systems in an entangled state are stronger than those of any local (or classical) theory, as witnessed by a violation of his inequalities. The strength of J. Bell's results is to have turned a theoretical observation about the structure of a theory into measurable quantities, making it testable. More than 50 years later, so-called Bell inequalities have been used in numerous experiments confirming the nonlocal predictions made by Quantum Theory [Hen+15; FC72; ADR82; Giu+15; Sha+15]: entangled particles can influence each other at a distance through some "spooky action at a distance".

2.2.1 A Bell experiment

The simplest set-up for the generation of nonlocal correlations consists of two distant observers, A and B, that are being sent physical systems on which they perform measurements. The experiment is divided in rounds of measurements on the systems, which are repeated in order to estimate the joint conditional probabilities of the measurement outcomes.

Each round of the experiment, a fresh copy of a given bipartite system in a quantum state ρ is generated by a source and one of its parts is sent to each observer. Party A (respectively B) chooses one measurement from a set of m_A (m_B) possible ones, labelled by $x \in 0, 1, ..., m_A - 1$ ($y \in 0, 1, ..., m_B - 1$). Performing this measurement on its part of the system, it observes an outcome $a \in 0, 1, ..., O_A - 1$ ($b \in 0, 1, ..., O_B - 1$) among O_A (O_B) possible ones. In this thesis, the alphabet of the variables x, y, a, b is always taken to be finite. By repeating rounds of measurements on the parts of the copies of the shared systems, the parties gather data until they have a good estimate of the joint conditional probabilities $P(ab|xy)$ – hereafter called correlations.

Such an experiment with two parties is sufficient to discriminate between the predictions made by different physical theories. This comes from the fact that the

[6] Again, to be precise, he formalised the principle of local causality, i.e. that events are *deterministically* influenced by their immediate surroundings only.

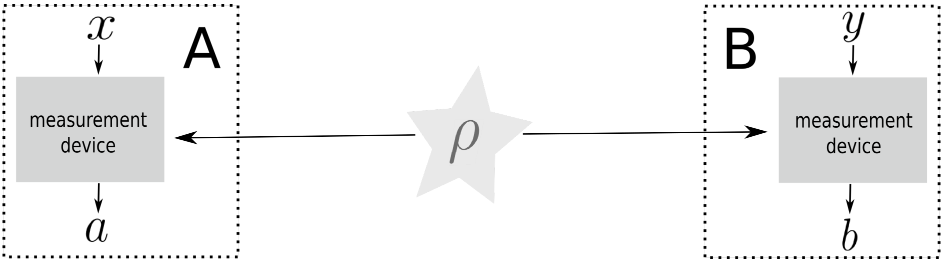

FIGURE 2.2: A round of a Bell experiment with two parties A and B. Each party receives half of a quantum system on which it, locally, performs one out of a possible set of measurements. The joint conditional outcome distribution of the measurements sometimes allows one to draw conclusions about the underlying processes, such as the entanglement properties of the state for example.

range of correlations that can, or not, be generated in a particular theory crucially depends on the structure of the theory itself.

The assumptions made in a Bell experiment

Several important assumptions are made on the physical set-up when performing a Bell test in order to draw the correct conclusions from the observed statistics [7]:

- **Independence of the measurement choices:** the measurement choice of each party, the inputs x, y, are independent variables at each round of the experiment. This is often referred to as the *freedom of choice* (of the inputs x and y) assumption.
- **No communication between the parties:** during each round of the experiment, communication between the two parties is forbidden. This can be implemented by making sure that the events of obtaining the outcomes a and b from the measurements by each party are space-like separated at each round of the experiment.

2.2.2 Local, quantum and no-signalling correlations

The range of possible correlations that can be generated depends on the particular theory that is being considered. The other way around, the study of correlations

[7] Several additional aspects may have to be addressed when implementing a Bell test in a laboratory, such as for example the problem of detection efficiencies or the need for the fair sampling assumption. We here restrict our attention to the assumptions that need to be made at the theoretical level only.

observed in an experiment offers insight on the properties that a theory should fulfil in order to be compatible with the observations.

Correlations from local influences

In a theory of local influences, correlations between space-like separated events can only be explained by a (possibly hidden) cause lying in their common past. Equivalently, one can understand that the parties A and B have access to *shared randomness* that was acquired before they perform a round of the experiment. Shared randomness can be obtained, for example, in a preparation phase where the two observers communicate to build a common list of numbers. These classical and possibly hidden variables shared in a common past are denoted by the variable λ and allow for (classical) correlations between the outcomes. In a single round of the experiment, correlations from local influences then ought to factorise on the additional knowledge of the variable λ

$$P(ab|xy) = P(a|x,\lambda)P(b|y,\lambda) \tag{2.13}$$

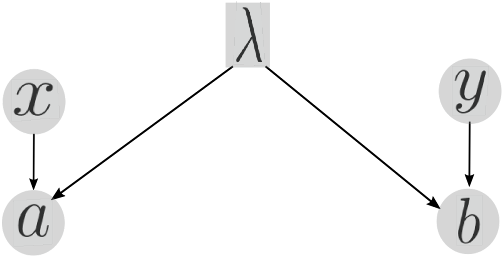

FIGURE 2.3: A graph of the possible causal influences between the variables of a Bell experiment in a local (or classical) theory. The measurement choice x (resp. y) can, locally, influence the outcome a (resp. b). Additionally, a classical (and possibly hidden) variable λ distributed in the past may also serve to correlate the outcomes. Such classical variable λ can also be understood as the two parties having access to shared randomness – a pre-established list of numbers they have in common.

The possible correlations that can be generated after many rounds of the experiment in a local theory are then those that can be decomposed as a probabilistic mixture of local correlations for one round (2.13)

$$P(ab|xy) = \sum_{\lambda} q_{\lambda} P(a|x,\lambda)P(b|y,\lambda) \tag{2.14}$$

for some distribution $q_\lambda \geq 0$ with $\sum_\lambda q_\lambda = 1$. Note that it can be shown that one can limit the alphabet of the variable λ to be finite when the variables of the measurement choices x, y and outcomes a, b are too, which will be the case throughout this thesis. We will refer to a Bell experiment with given alphabets m_A, m_B, O_A, O_B for the variables x, y, a, b as $[m_A, m_B, O_A, O_B]$. The set $\mathcal{L}$ of all correlations admitting a local decomposition (2.14) in a given set-up $[m_A, m_B, O_A, O_B]$ can be shown to be a polytope, that is a closed convex set with finite number of extremal points.

The set of quantum correlations

The correlations generated in a set-up $[m_A, m_B, O_A, O_B]$ when making local measurements on the shares of a joint physical system in a quantum state ρ_{AB} are described by Born's rule

$$P(ab|xy) = Tr(\rho_{AB} M_{a|x} \otimes N_{b|y}) \tag{2.15}$$

The measurement operators $M_{a|x}$ and $N_{b|y}$ are positive-operator valued measure (POVM) $M_{a|x} \geq 0$, $\forall a, x$ and $\sum_a M_{a|x} = \mathbb{1} \ \ \forall x$ (and similarly for $N_{b|y}$). They act, respectively, on $\mathcal{H}_\mathcal{A}$ and $\mathcal{H}_\mathcal{B}$. We come back later in more details on measurements in Quantum Theory, see 2.2.4. The set of all correlations of the form (2.15) in a particular set-up $[m_A, m_B, O_A, O_B]$ form the convex set of quantum correlations $\mathcal{Q}$. Note that the set of quantum correlations is not a polytope, as the number of extremal points is infinite.

The no-signalling principle and correlations

Quantum correlations (2.15) respect the no-signalling principle [Pr], which formalises the condition that measurements made on quantum systems should not be useable to transmit information at infinite speed. In a Bell experiment, this implies that the marginals $P_A(a|x)$ (and $P_B(b|y)$) of each party should be independent of the measurement choice y (x) of the other party. It could otherwise be used to send a signal instantaneously. Correlations $P(ab|xy)$ are said to be *no-signalling* when

$$\begin{aligned} P_A(a|x) \equiv P_A(a|xy) &= \sum_b P(ab|xy) \quad \forall y \\ P_B(b|y) \equiv P_B(b|xy) &= \sum_a P(ab|xy) \quad \forall x \end{aligned} \tag{2.16}$$

The set of all correlations in a set-up $[m_A, m_B, O_A, O_B]$ satisfying the conditions (2.16) is the set of no-signalling correlations $\mathcal{NS}$. The set $\mathcal{NS}$ is a convex polytope since it is defined only by a finite set of linear constraints (2.16), implying it has only a finite number of extremal points.

The study of no-signalling correlations lead the way into searching information principle(s) singling out quantum correlations from the set of possible ones. In fact, quantum correlations (2.15) satisfy the no-signalling conditions (2.16) and the principle seems so fundamental that one could be lead into thinking that the two sets of correlations are identical $\mathcal{Q} = \mathcal{NS}$. Interestingly, the quantum set of correlations is strictly included in the set of no-signalling correlations $\mathcal{Q} \subsetneq \mathcal{NS}$, implying that the no-signalling principle does not single out quantum correlations alone [PR94].

2.2.3 Bell inequalities

The polytope $\mathcal{L}$ of local correlations (2.14) in a given set-up $[m_A, m_B, O_A, O_B]$ can equivalently be described by a finite number of hyperplanes in the abstract space of correlations $P(ab|xy)$. Such hyperplanes take the form of inequalities $I_{\mathcal{L}}$ – linear combinations of the probabilities $P(ab|xy)$ – which are satisfied by all points $P(ab|xy) \in \mathcal{L}$

$$\begin{aligned} I_{\mathcal{L}}\big(P(ab|xy)\big) = \sum_{x,y,a,b} h^{x,y}_{a,b} P(ab|xy) \leq \mathrm{B}_{\mathcal{L}} \qquad & \forall P(ab|xy) \in \mathcal{L} \\ I_{\mathcal{L}}\big(P(ab|xy)\big) > \mathrm{B}_{\mathcal{L}} \quad \Rightarrow \quad & P(ab|xy) \notin \mathcal{L} \end{aligned} \tag{2.17}$$

where $\mathrm{B}_{\mathcal{L}} \in \mathbb{R}$ is the local bound – the maximal value of the inequality achievable by local correlations $P(ab|xy) \in \mathcal{L}$ (2.14) – and the numbers $h^{x,y}_{a,b} \in \mathbb{R}$ are the coefficient defining the specific inequality $I_{\mathcal{L}}$.

Bell inequalities are central for the study of nonlocal correlations and for the design of information processing tasks that are otherwise impossible. Their range of applications in the field of Quantum Information Science is enormous and the design of new useful Bell inequalities is a important task in the field.

Quantum nonlocality: the CHSH scenario

Quantum nonlocality refers to the fact that there exist inequalities of the form (2.17) and quantum correlations $P_{\mathcal{Q}}(ab|xy) \in \mathcal{Q}$ (2.15) such that $I_{\mathcal{L}}\big(P_{\mathcal{Q}}(ab|xy)\big) > \mathrm{B}_{\mathcal{L}}$ and thus $P_{\mathcal{Q}}(ab|xy) \notin \mathcal{L}$. This implies that quantum correlations can in general not be generated by a local (or classical) theory. Inequalities allowing for a quantum violation, thus witnessing quantum nonlocality, are called *Bell inequalities*.

The so-called Clauser-Horne-Shimony-Holt (CHSH) inequality [Cla+69] is the simplest and most widely used for witnessing nonlocality. In the scenario $[2,2,2,2]$ where both parties A and B have a dichotomic choice of two-outcome measurements ($x, y, a, b \in 0, 1$), it is the unique non-trivial hyperplane of the local set $\mathcal{L}$[8]. It reads

$$I_{CH}\big(P(ab|xy)\big) = \sum_{x,y,a,b} (-1)^{a \oplus b \oplus xy} P(ab|xy) \leq 2 \quad \forall P(ab|xy) \in \mathcal{L} \tag{2.18}$$

where $\oplus$ denotes the sum modulo 2 and the local bound $\mathrm{B}_{\mathcal{L}} = 2$. This inequality is often written using the expectation value of the product of the outcomes – the *correlators*

$$\langle A_x B_y \rangle = P(a = b|xy) - P(a \neq b|xy) \tag{2.19}$$

Written using these correlators, the CHSH inequality reads

$$\begin{aligned} I_{CHSH}\big(P(ab|xy)\big) = \langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle \leq 2 \\ \forall P(ab|xy) \in \mathcal{L} \end{aligned} \tag{2.20}$$

To see that indeed, $\mathcal{L} \subsetneq \mathcal{Q}$, we construct quantum correlations $P(ab|xy) \in \mathcal{Q}$ with $x, y, a, b \in 0, 1$ from measurements on the maximally entangled system of two qubits $|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ (2.7)

$$P(ab|xy) = Tr\big(M_{a|x} \otimes N_{b|y} |\Phi^+\rangle\langle\Phi^+|_{AB}\big)$$

$$\begin{aligned} M_{a|0} &= \frac{1}{2}(\mathbb{1} + (-1)^a \sigma_Z) \ \ ; \ \ N_{b|0} = \frac{1}{2}(\mathbb{1} + (-1)^b \frac{\sigma_Z + \sigma_X}{\sqrt{2}}) \\ M_{a|1} &= \frac{1}{2}(\mathbb{1} + (-1)^a \sigma_X) \ \ ; \ \ N_{b|1} = \frac{1}{2}(\mathbb{1} + (-1)^b \frac{\sigma_Z - \sigma_X}{\sqrt{2}}) \end{aligned} \tag{2.21}$$

giving the value $I_{CHSH}\big(P(ab|xy)\big) = 2\sqrt{2} > 2$, implying that $P(ab|xy) \notin \mathcal{L}$ and $\mathcal{L} \subsetneq \mathcal{Q}$, i.e. quantum nonlocality.

Interestingly, the set of quantum correlations is strictly included in the set of no-signalling correlations $\mathcal{Q} \subsetneq \mathcal{NS}$, implying that the no-signalling principle does not

[8] In addition to trivial inequalities of the form $P(ab|xy) \geq 0$

single out quantum correlations alone. This fact is best illustrated by considering the correlations $P_{PR}(ab|xy)$ with $x, y, a, b \in 0, 1$, also called the Popescu-Rohrlich (PR) correlations [Pr], respecting the rule

$$P_{PR}(ab|xy) = \begin{cases} \frac{1}{2} & \text{if } a \oplus b = xy \\ 0 & \text{otherwise} \end{cases} \tag{2.22}$$

where $\oplus$ denotes the sum modulo 2. It is easy to check that the correlations $P_{PR}(ab|xy)$ satisfy the conditions (2.16), but give a values $I_{CHSH}(P_{PR}(ab|xy)) = 4$ implying that they can not be realised using quantum resources $P_{PR}(ab|xy) \notin \mathcal{Q}$ (2.15). Indeed, Tsirelson has proven that the maximal value to the CHSH inequality (2.20) achievable by quantum correlations (2.15) is $\max_{\mathcal{Q}} I_{CHSH}(P(ab|xy)) = 2\sqrt{2} < 4$, which is realised uniquely by the quantum strategy (2.21).

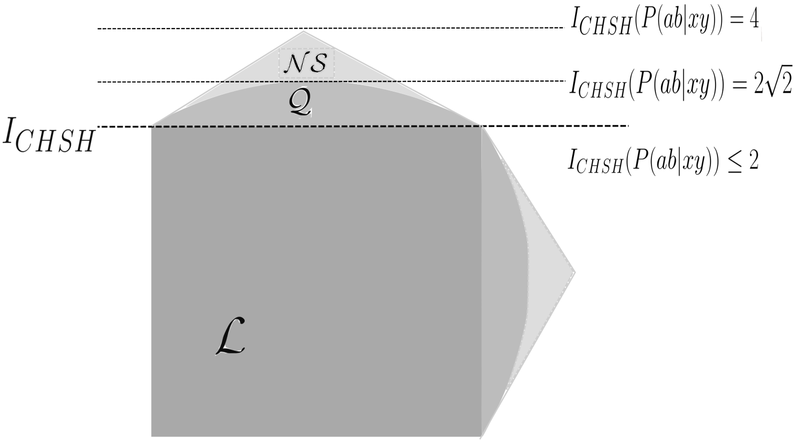

FIGURE 2.4: A representation of the sets of no-signalling, quantum and local correlations in a particular cut of the abstract space of correlations. The set of local correlations is strictly included in the set of quantum ones $\mathcal{L} \subset \mathcal{Q}$, which is in turn strictly included in the set of no-signalling ones $\mathcal{Q} \subset \mathcal{NS}$, as witnessed by the different values of the CHSH inequality.

The scenario $[2, 2, 2, 2]$ with two observers and dichotomic choice of two-outcome measurements is the only one in which the violation of the CHSH inequality[9] is both necessary and sufficient for correlations $P(ab|xy)$ to be nonlocal.

[9] One needs to consider the whole family of inequalities equivalent to the CHSH inequality (2.20), i.e. all the inequalities that can be obtained from the inequality by local relabelling of the variables.

In general, the set of local correlations for any number of measurement choices and outcomes has a richer structure with numerous inequivalent families of Bell inequalities [Pir14]. The violation of a particular Bell inequality is thus a sufficient condition, but not a necessary one in general. The full list (of finite size) of Bell inequalities for a specific scenario with a given number of measurement choices and outcomes x, y, a, b is a valuable resource: any correlations that are nonlocal necessarily violate at least one of these. Nevertheless, computing this full list for a specific scenario is in general a hard task and was only done in some specific cases with low number of measurement choices and outcomes (see [RBG14]).

Linear programming as an alternative to Bell inequalities

An alternative to the use of Bell inequalities for the detection of nonlocality is the use of linear programming to determine directly whether the correlations belong, or not, to the local set $\mathcal{L}$ in a given set-up $[m_A, m_B, O_A, O_B]$. One searches for a decomposition of some given correlations $P(ab|xy)$ into the extremal points – or *vertices* – of the local set $\mathcal{L}$. There is a finite number of vertices $i = 1, 2, ..., V$ only since the local set is a polytope. The vertices can be shown to be the ones that can be written as

$$P^i_{\text{ext}}(ab|xy) = \delta_{a=f^i_A(x)}\delta_{b=f^i_B(y)} \tag{2.23}$$

for some choice of $f^i_A : \{0, 1, ..., m_A - 1\} \to \{0, 1, ..., O_A - 1\}$ $(f^i_B : \{0, 1, ..., m_B - 1\} \to \{0, 1, ..., O_B - 1\})$, that is a function of the local input $x(y)$ and of the index i and $\delta_{a=f^i_A(x)} = \begin{cases} 1 & \text{if } a = f^i_A(x) \\ 0 & \text{otherwise} \end{cases}$ (and similarly for $\delta_{b=f^i_B(y)}$).

One can interpret expression (2.23) as the fact that the extremal strategies for local correlations are the those that come from local deterministic response functions: the outcome $a(b)$ is a deterministic function of the input $x(y)$ and of the variable i only. Any other local correlations in that set-up can then be obtained by a probabilistic mixture of these extremal strategies.

If the correlations $P(ab|xy)$ are written under the form of a column vector $\vec{P}(ab|xy)$, one is then interested in solving the problem:

$$\begin{aligned} &\text{Find} \qquad \vec{q} \in \mathbb{R}^V_{\geq 0} \quad \text{with} \quad \sum_{i=1}^{V} q_i = 1 \\ &\text{such that} \qquad \vec{P}(ab|xy) = \sum_{i=1}^{V} q_i \vec{P}^i_{\text{ext}}(ab|xy) \end{aligned} \tag{2.24}$$

If there exists a solution to the linear problem (2.24), then $P(ab|xy) \in \mathcal{L}$ and if not $P(ab|xy) \notin \mathcal{L}$, hence witnessing nonlocality of the correlations $P(ab|xy)$. Problem (2.24) can be solved by means of linear programming and is an efficient way to decide whether correlations are local for set-ups $[m_A, m_B, O_A, O_B]$ with small alphabet for the variables x, y, a, b.

On the other hand, the amount of vertices of the local set $\mathcal{L}$ grows exponentially fast with the number of measurement choices and outcomes, rapidly making an explicit decomposition of the correlations into them intractable.

2.2.4 Quantum measurements: POVM versus projective

Quantum correlations (2.15) in a Bell experiment 2.2.1 are made of two basic ingredients: quantum states and local measurements. A measurement is described in Quantum Theory by a positive-operator valued measure (POVM) $M_a \geq 0 \quad \forall a$ (for party A) such that

$$\sum_a M_a = \mathbb{1} \tag{2.25}$$

A restricted class of POVMs that is of particular interest are the measurements that are said to be projective. Such measurements, in addition to property (2.25), also satisfy

$$M_a^2 = M_a \quad \forall a \tag{2.26}$$

Interestingly, there are very few examples of situations related to nonlocality in which using general POVM measurements offers an advantage over projective ones. Several information tasks, such as obtaining a maximal amount of certified randomness from entangled systems, crucially depend on the use of POVM measurements [Ací+16]. The maximal violation of certain very specific Bell inequalities was also shown to require the use of POVMs measurements [VB10]. On the other hand, there is no known quantum entangled state that generates nonlocal correlations *only if* general measurements are being performed on it instead of projective ones.

For nonlocality, why are projective measurements almost always as powerful as general POVM ones? In that view, understanding in which tasks general POVM measurements outperform the subclass of projective ones is an interesting question of fundamental interest. We will see that the sequential scenario, where repeated measurements are being performed on the systems instead of a single one at each round of the experiment, offer a very natural situation in which one can not work without general (non-projective) POVM measurements.

2.2.5 Box world: a device-independent framework

In a Bell experiment 2.2.1, only a minimal modelling of the physical set-up is made. The objects of interest are the correlations $P(ab|xy)$ generated between the classical outcomes of distant measurements and not the exact underlying process that lead to their generation. In that sense, one can picture the two parties as each possessing a black box – representing their measurement device – which they interact with using a classical variable (the measurement choices x, y) and from which they observe the generation of another classical variable (the outcomes a, b). Somehow, the experiment is equivalent to using a classical computer to interact with a quantum device. One is then interested in drawing conclusions about the quantum devices based solely on the correlations observed "from the outside" between the classical variables x, y, a, b. This approach of picturing physical processes as black boxes is often referred to as *the box world*.

FIGURE 2.5: In the framework of *box world*, the two devices of a Bell experiment are seen as black boxes: no assumption is made about their internal functioning. One then interacts classically with the two boxes, by feeding each an input and observing an output from it. By repeating the procedure many times on two distant boxes, one can draw conclusions about the devices based solely on the generated correlations $P(ab|xy)$ between them.

Taking such a minimalist approach also offers the advantage of designing information protocols that are extremely secure in an adversarial picture. Indeed, representing processes as black boxes implies diminishing the number of assumptions that are made about the set-up, reducing the gap between theory and implementation. In particular, no assumptions are made regarding the Hilbert space dimension of the underlying states that are used nor on the nature of the measurement devices. The protocol's success is certified by the generation of certain (nonlocal) correlations only and not on how these were generated. This particular framework, based on the study of the statistical properties of the experiments, is called the *device-independent* framework and is the one that is followed in this thesis.

Nonlocality: a device-independent witness of entanglement

As said, entanglement is a necessary resource for the generation of quantum nonlocal correlations. This can be seen quite simply by noticing that the correlations generated by performing local measurements on a separable state $\rho_{\text{sep}} = \sum_i g_i \sigma_A^i \otimes \gamma_B^i$ (2.11) always give rise to local correlations (2.14)

$$\begin{aligned} P(ab|xy) &= Tr\left(\rho_{\text{sep}} M_{a|x} \otimes N_{b|y}\right) = Tr\Big(\sum_i g_i (\sigma_A^i \otimes \gamma_B^i)(M_{a|x} \otimes N_{b|y})\Big) \\ &= \sum_i g_i Tr\left(\sigma_A^i M_{a|x}\right) Tr\left(\gamma_B^i N_{b|y}\right) = \sum_i g_i P_A(a|x,i) P_B(b|y,i) \in \mathcal{L} \end{aligned} \tag{2.27}$$

independently of the Hilbert space dimension of the state or the local measurements M, N that were performed.

In the other direction, this implies that the observation of correlations $P(ab|xy) \notin \mathcal{L}$ is incompatible with the use of separable systems as the resource, hence that the systems on which the measurements were performed were entangled. The violation of a Bell inequality, and more generally the observation of Bell nonlocal correlations, thus serves as device-independent witness of entanglement (see also [Bra+13; Ter00]).

2.2.6 Entanglement versus nonlocality with two parties

The idea behind nonlocality – instantaneous influences at a distance – is already present in the formalism of Quantum Theory with the possibility for the state describing joint systems to be entangled. Nevertheless, quantum states are mathematical objects of the theory and not directly observable quantities. What can be observed are results, i.e. classical variables, of measurements performed on quantum states. In general, it is even possible to think that what we observe arises from different processes than the ones described by the Quantum Theory. In this thesis, if not explicitly stated otherwise, it is assumed that Quantum Theory indeed describes the observed world.

One could think that since quantum states already exhibit a (weaker) form of non-classicality, then it should be possible to make measurements on such states so as to exhibit nonlocal correlations between the outcomes of these measurements. If that were to be true, then entanglement and nonlocality could be understood as qualitatively equivalent.

Towards a qualitative equivalence

In the case of bipartite systems in an entangled pure state of any Hilbert space dimension (2.3), this qualitative equivalence was shown to hold by Gisin [Gis91]. Indeed, Gisin proved that it is always possible to find local measurements on any such entangled state to generate nonlocal correlations.

The case of mixed states is much subtler. As was shown by Werner, there exist mixed entangled states (2.8) that are unable to generate nonlocal correlations when performing (projective) measurements on them [Wer89]. This result was later extended to general measurements by Barrett [Bar02]. When the parties make local measurements on the copies of the state at each round of the experiment, entanglement and nonlocality are thus qualitatively different properties.

The situation gets more interesting when considering larger classes of local operations to be made on the subsystems of systems in an entangled state. Palazuelos considered (mixed) entangled states that can not generate nonlocal correlations in the standard Bell experiment – in which measurements are being performed on the shares of a single copy of the state. Palazuelos then showed that these states can be *super-activated* by making joint measurements on the shares of multiple copies of the state instead. By receiving multiple copies of the state instead of one only at each round of the experiment, the parties generate nonlocal correlations (see Fig. 2.8).

This result shows that it is in general important to consider all possible local operations in order to exploit the full potentiality of entangled states to generate nonlocal correlations.

Another possibility is to make a sequence of measurements, instead of a single measurement only, on each share of a copy of the state at each round. The sequential measurement scenario, that also allows one to generate nonlocal correlations from (mixed) entangled states that are otherwise unable to do so, is the subject of the next section (see Subsec. 2.2.7).

It is unknown whether there exists a class of local operations on quantum states such that all entangled states become able to display nonlocal correlations. In this view, exploring set-ups that go beyond the standard one with single measurements on each copy of the state is of fundamental importance.

Towards a quantitative equivalence

Second, at the quantitative level, it is important to understand whether "more" entanglement leads to "more" nonlocality. Tsireslon' originally showed that the maximal violation of the CHSH inequality (2.20) crucially requires the use of two-qubit systems in a maximally entangled state (2.7). It was then expected that the maximal violation of any Bell inequality requires maximal entanglement. Nevertheless, in [Aci+02], it was shown that some Bell inequalities are maximally violated only when making measurements on non maximally entangled states. This holds true even when considering states of arbitrary Hilbert space dimension [LVB11; VW11]. This *anomaly* of obtaining more nonlocality from less entangled states not only appears for the amount of violation of a particular Bell inequality, but also for other measures of nonlocality such as: the robustness of nonlocality to noise [Aci+02], losses [Ebe93], statistical strength of Bell tests [AGG05] and the simulation of quantum correlations with nonlocal resources [BGS05]. It is then desirable to understand if this apparent quantitative inequivalence between entanglement and nonlocality stems only as an artefact from the employed measure or, on the contrary, as a more fundamental phenomenon.

In chapter 3, we study anomalies using a natural and operational measure of nonlocality, defined as the probability that a given state generates nonlocal correlations when random measurements are performed on it.

2.2.7 The sequential measurement scenario

A Bell experiment such as the one described in 2.2.1 suffices to generate nonlocal correlations and, as such, has received most of the attention of researchers so far. Nevertheless, using bipartite systems, this scenario does not make use of the full capability of quantum states and local measurements in the sense that: $i)$ only single copies of the systems are measured at each round of the experiment and $ii)$ the shares of the systems are measured once by each party at each round. We have already seen in the previous section that going beyond point $i)$ offers advantages: some quantum states only exhibit their non-classical behaviour when the shares of multiple copies of the state are measured jointly. In this section, we focus on the *sequential measurement scenario*, in which the parts of a copy of the system are subjected to multiple measurements at each round of the experiment.

We here consider an intermediate situation where only one party, say B, makes a sequence of n measurements on its share of the system. Party A makes a single measurement in the sequence as in the standard Bell experiment. In the DI framework, party B is then pictured as possessing multiple measurement devices B_i, $i \in 1, 2, ..., n$ which are seen as black boxes (see Fig. 2.6). Each measurement choice (in the sequence) is labelled by y_i, $i \in 1,2,...,n$ and the corresponding outcomes by b_i, $i \in 1,2,...,n$. Remember that all variables x, y_i and a, b_i take their values within a finite alphabet. By making many rounds of measurements, the parties gather data until they obtain a good estimate of the joint conditional probabilities $P(a\vec{b}|x\vec{y}) \equiv \{P(ab_1b_2...b_n|xy_1y_2...y_n)\}_{x,y_1,y_2,...,y_n}$.

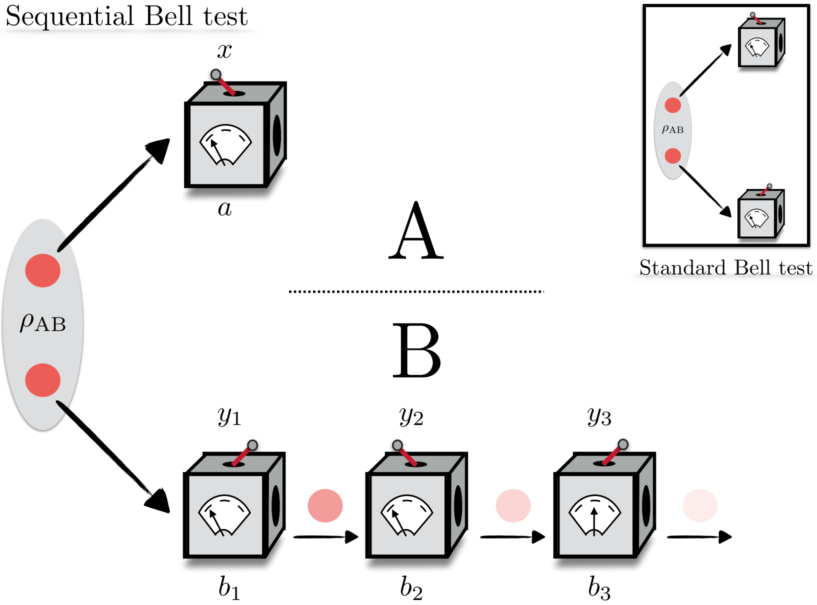

FIGURE 2.6: In a Bell experiment, at each round of the experiment the shares of a fresh copy of a quantum system are sent to the two parties. In the standard scenario, each party makes a single measurement on the share it receives. In the sequential scenario, party B makes multiple measurements on his share instead.

The sequential assumption: one-way signalling

The sequential measurement scenario takes its essence from the fact that a certain ordering of the measurements is assumed: measurement B_i happens *before* measurement B_j for $i < j$. Note that the freedom of choice assumption 2.2.1 is still valid: all measurement choices y_i of party B are assumed to be independent variables at each round of the experiment. Even if measurement B_j happens after B_i, the measurement choice y_j is assumed to be independent of the variables y_i, b_i generated in its past.

Mathematically, the sequential measurement assumption leads to the notion of one-way signalling: the outcome b_j of measurement B_j can depend on the variables

x_i, b_i of measurement B_i $i < j$. On the other hand, the outcome b_i of B_i can not depend on the variable x_j of B_j for $i < j$ or one could send a signal backwards in time. Correlations $P(a\vec{b}|x\vec{y})$ are said to be sequential – or one-way signalling – if

$$P(b_j|\vec{y}_j\vec{b}_{j-1}) \equiv \sum_{a,b_{j+1},b_{j+2},...,b_n} P(a\vec{b}|x\vec{y}) \qquad \forall b_j, \vec{y}_j, \vec{b}_{j-1} \quad \text{and} \quad \forall x, y_{l>j} \tag{2.28}$$

where we use the notation $\vec{b}_k = b_1, b_2, ..., b_k$. Note that we have also assumed standard no-signalling (2.16) between A and each B_i.

Local correlations in the sequential measurement scenario are a generalisation of the ones of the standard Bell experiment (2.13) with a single measurement in the sequence. Such correlations are the ones that can be obtained from classical (hidden) variables – or equivalently shared randomness – distributed to A and B (all B_i), together with communication from B_i to B_j for $i < j$ (see also Fig. 2.7)

$$P(a\vec{b}|x\vec{y}) = \sum_\lambda q_\lambda P(a|x\lambda) \prod_{i=1}^{n} P(b_i|\vec{y}_i\vec{b}_{i-1}\lambda)$$
$$= \sum_\lambda q_\lambda P(a|x\lambda) P(b_1|y_1\lambda) P(b_2|\vec{y}_2 b_1\lambda) ... P(b_i|\vec{y}_i\vec{b}_{i-1}\lambda) ... P(b_n| \ \ \vec{y}_n\vec{b}_{n-1}\lambda) \in \mathcal{L}_n^{\text{seq}} \tag{2.29}$$

with, again, $q_\lambda \geq 0 \ \forall\lambda$ and $\sum_\lambda q_\lambda = 1$. For $n = 1$, one recovers the standard definition of local correlations (2.13). Any correlations that can not be written in the form (2.29) for any choice of distribution of the variable λ and local response functions $P(a|x\lambda), P(b_i|\vec{y}_i\vec{b}_{i-1}\lambda)$ is said to be sequential nonlocal.

The set $\mathcal{L}_n^{\text{seq}}$ of local correlations (2.29) in the sequential scenario, for any number n of measurements in the sequence, also forms a polytope. Note, however, that due to the growing number of extremal points it is usually extremely difficult to characterise these local sets with the help of linear programming (see sec. 2.2.3).

Post-measurement states and Kraus operators

The whole point of considering sequences of measurements instead of single ones resides in the fact that one makes further use of the post-measurement systems as potential resources. In the standard Bell experiment the systems are, at each round, measured only once before a new round starts and that a fresh copy of the system is sent to the parties. There are two main reasons why sequences of measurements have not attracted much attention so far: $a)$ in a laboratory, a measurement usually is destructive, i.e. the particle(s) that was measured is not available subsequently; $b)$

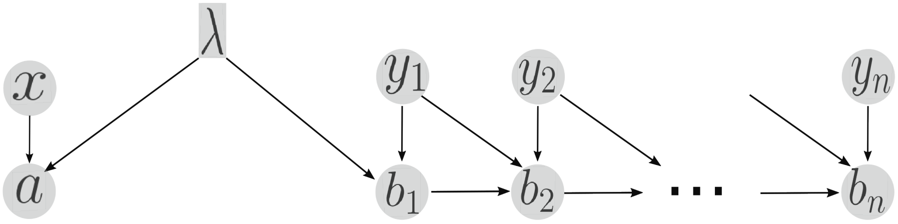

FIGURE 2.7: A graph of the causal influences in a local theory between the variables of a sequential Bell experiment. Each input y_i can influence, locally, the outcome b_i but also the outcomes generated *later* b_j $j > i$. Nevertheless, the inputs are still assumed to be independent variables. Additionally, the outcomes might be correlated using the the shared classical variable λ.

we have seen that in almost all situations, projective measurements (2.26) perform just as well as general POVMs (see 2.2.4), it is then often useless to consider these last ones.

Measurements in Quantum Theory can be represented using the formalism of Kraus operators, with which it is also possible to represent general POVMs. Nevertheless, Kraus operators additionally allow to compute the state of the post-measurement system. A measurement N with d outcomes is represented by a set of d matrices N_b – the Kraus operators

$$N_b, \quad b = 1, 2, ..., d \qquad \text{s.t.} \qquad \sum_{b=1}^{d} N_b^\dagger N_b = \mathbb{1} \tag{2.30}$$

that, when performed on a state $\rho_B \in B(\mathcal{H}^d)$, give outcome $b \in 1, 2, ..., d$ with probability

$$p(b|\rho_B) = Tr\big(\rho_B N_b^\dagger N_b\big) \tag{2.31}$$

The formalism of POVMs (2.25) is simply obtained by considering each POVM element $P_b = N_b^\dagger N_b$ and projective measurements (2.26) are the ones for which $P_b P_b = P_b \ \forall b$.

The formalism of Kraus operators, contrary to the one of POVMs, allows to compute the state $\rho'_B(b)$ *after* a measurement N for which outcome b was obtained

$$\rho'_B(b) = \frac{N_b \rho_B N_b^\dagger}{p(b|\rho_B)} \tag{2.32}$$

The states $\rho'_B(b)$ can then be measured another time, thus potentially serving as the resource again.

Clearly, measurements that are useful to generate multiple nonlocal correlations in a sequence preserve some entanglement in the system. If the initial system ρ_{AB} is entangled between A and B_1, one would like the post-measurement system $\rho'_{AB}(b_1)$ (after B_1's measurement) to be entangled between A and B_2 too, at least for one outcome b_1. If the first measurement of B_1 destroys all entanglement in the system, then there is no hope to use it as subsequent resource to generate nonlocal correlations between A and B_2.

Rank one Kraus operators

$$N_b = \alpha |b\rangle\langle b| \quad \forall b \tag{2.33}$$

$b = 1, 2, ..., d$ of $\mathcal{H}^d$ and $\alpha \in [-1, 1]$ destroy all entanglement in any initial state $\rho_{AB} = \sum_j q_j |\Psi_j\rangle\langle\Psi_j|_{AB} \in B(\mathcal{H}^d \otimes \mathcal{H}^d)$. The post-measurement state for each outcome b is thus a convex mixture of separable states. This implies that one should go beyond rank one Kraus operators, in particular rank one projective measurements, to retain entanglement in the post-measurement system.

Some results making use of sequences of measurements

Werner showed that there exist some mixed entangled states that are unable to generate nonlocal correlations when each copy of the system is subjected to a projective measurement [Wer89]. These states nevertheless generate nonlocal correlations when performing sequences of (non-projective) measurements on each copy of the state [Pop95]. This result was later generalised to mixed states that do not exhibit nonlocal correlations when a single general (POVM) measurement is made on each copy of the state [Hir+13], but that do with sequences of measurements instead. This phenomenon of obtaining nonlocality from systems only when sequences of measurements are being performed on them is called *hidden nonlocality*.

Until now, it was unknown whether sequences of measurements can provide with advantages in device-independent information tasks. In some sense, is it possible to use sequences of measurement to do more than just reveal the nonlocal

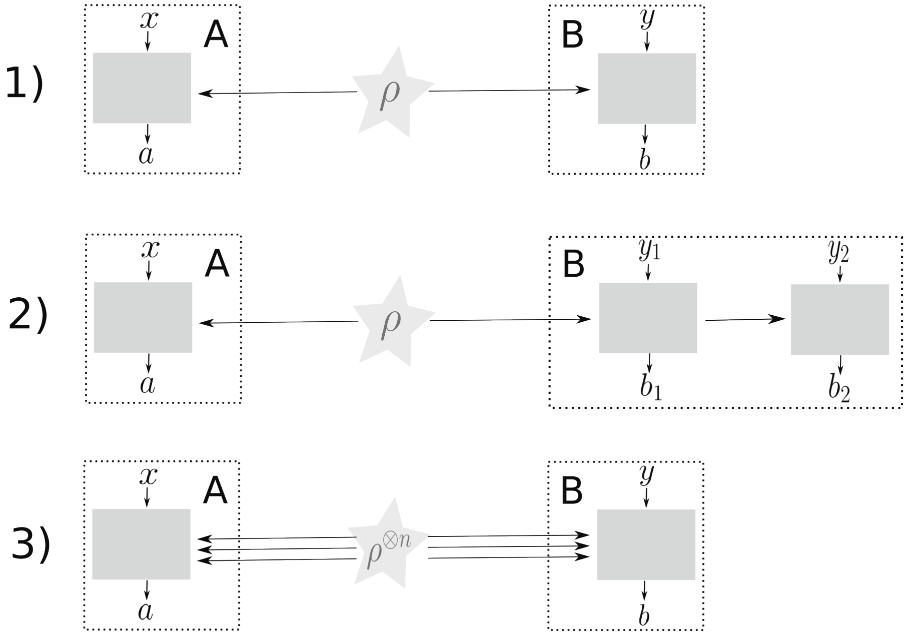

FIGURE 2.8: 1) The standard Bell scenario, where the parties each make a single measurement on each copy of the system at each round. 2) The sequential scenario, where one of the parties (B) makes two measurements in a row on his share of the copy of the system at each round. 3) The multi-copy scenario, where the parties receive the shares of multiple copies of the system at each round, which they measure jointly. One can understand scenarios 2) and 3) as ones in which larger sets of local operations are allowed. Some quantum systems in a entangled mixed state generate nonlocal correlations only in the scenario 2) or 3).

behaviour of some very specific quantum states?

In chapter 4, we consider the use of sequences of measurements for certifying randomness.

2.3 Multipartite entanglement and nonlocality

Resources such as systems in an entangled state naturally come in more complex configurations than in the simpler bipartite scenario. In the multipartite scenario, one considers that more than two observers share physical systems in a joint quantum state. The notions of entanglement and non-locality become richer in this scenario [Hor+09; GTB05; Sve87; SS02; Gal+12; Ban+13]. For example, multipartite systems can be in a genuine multipartite entangled (GME) state, a stronger form of entanglement where all the particles of a physical system are entangled with each other, not only subsets of them. Such GME systems – and only them – can generate strong correlations that can not be reproduced by any local theory, even if additional non-local resources are available to subsets of the observers [Sve87]. Multipartite non-local correlations have already been used, for example: to discard causal influences that spread at a faster than light, but finite speed [Ban]; for randomness amplification under a minimal set of assumptions [Gal+13; Bou+14]; to detect the non-local behaviour of ground states of Hamiltonians appearing naturally in condensed matter physics [Tur+14]. However, much remains to be explored in this scenario.

This section introduces the novel notions of entanglement and of nonlocality that appear when multiple (more than two) parties share systems in an entangled state. The section follows the lines of the ones on bipartite entanglement 2.1 and nonlocality 2.2. We start with the basic definitions of multipartite entanglement both for pure and mixed states and the different approaches for the quantification of the multipartite extent to which multipartite states can be entangled. Second, we focus on the novel notions of multipartite nonlocality that appear and how to quantify and/or reproduce these correlations. Finally, we expose what is known about the relation between entanglement and nonlocality in the multipartite scenario and the use of multipartite resources for DI information tasks.

2.3.1 Multipartite entanglement

Physical systems distributed to multiple observers can be in different entangled quantum states that are richer than the ones of bipartite systems. For example, a system made of three particles can be in a state in which two of the three parties A_1, A_2, A_3 only are entangled $|\Psi\rangle_{A_1A_2A_3} = |\phi_+\rangle_{A_1A_2}|\psi\rangle_{A_3}$. If such a state clearly exhibits some entanglement, it is nevertheless lacking some genuinely multipartite feature since party C does not share entanglement with the other parties. With three parties, a new hierarchy of multipartite entanglement appears: $i)$ fully separable states which do not require any form of entanglement; $ii)$ states that require entanglement between two of the three parties only and; $iii)$ states which are entangled between all three parties. Contrary to the bipartite scenario, multipartite states allow for some hybrid form of entanglement where some subsets of parties only are entangled.

In that spirit, in a set-up with n parties A_r, $r = 1,2,...,n$, a pure state $|\Psi\rangle_n \equiv |\Psi\rangle_{A_1A_2...A_n} \in \mathcal{H}^d \otimes \mathcal{H}^d \otimes ... \otimes \mathcal{H}^d$ is said to be fully separable if

$$|\Psi\rangle_n^{\text{sep}} = |\psi_1\rangle_{A_1}|\psi_2\rangle_{A_2}...|\psi_n\rangle_{A_n} \tag{2.34}$$

and entangled otherwise. Similarly, an $n-$partite mixed entangled state ρ_n is fully separable if it can be written as a convex mixture of fully separable pure states (2.34)

$$\begin{aligned}\rho_n^{\text{sep}} &= \sum_i q_i \bigotimes_{r=1}^{n} |\psi_{r,i}\rangle\langle\psi_{r,i}|_{A_r} \\ &= \sum_i q_i |\psi_{1,i}\rangle\langle\psi_{1,i}|_{A_1} \otimes |\psi_{2,i}\rangle\langle\psi_{2,i}|_{A_2} \otimes ...\otimes|\psi_{n,i}\rangle\langle\psi_{n,i}|_{A_n}\end{aligned} \tag{2.35}$$

with $\sum_i q_i = 1$ and $q_i \geq 0 \ \forall i$. A state ρ_n that does not allow for a decomposition of the form (2.35) for any distribution of the variable i and of choice of local states $|\psi_{r,i}\rangle_{A_r}$ is said to be entangled.

Multipartite entangled states: $m-$separability

As said, multipartite states exhibit richer forms of entanglement than in the bipartite set-up. One of the approaches to capture the extent to which subsystems in a joint quantum state are entangled together is through the notion of $m-$separability, which refines the bipartite notion of separability to multipartite states [Hor+09]. An $m-$separable pure state $|\Psi\rangle_n^{m-\text{sep}}$ – for a given $m \leq n$ – is a state which is separable between (at least) m groups of parties

$$|\Psi\rangle_n^{m-\text{sep}} = \bigotimes_{r=1}^{m} |\psi_r\rangle_{k_r} \tag{2.36}$$

with each state $|\psi_r\rangle_{k_r}$ being defined on the Hilbert space of a subset k_r of the n parties. The variable k defines a partitioning of the n parties into m pairwise disjoint and non-empty groups k_r, $r = 1,2,...,m$, $k_r \cap k_s = \emptyset \ \forall r \neq s$ and such that $\sum_{r=1}^{m} |k_r| = n$.

For example, a four-partite, 3-separable, pure state $|\Psi\rangle_4^{3-\text{sep}}$ can only be entangled between two parties at most since it be decomposed as $|\Psi\rangle_4^{3-\text{sep}} = |\psi\rangle_{A_sA_t}|\psi\rangle_{A_u}|\psi\rangle_{A_v}$

for some quadruple s, t, u, v. In that case, the partitioning is $k_1 = \{A_s A_t\}$, $k_2 = \{A_u\}$ and $k_3 = \{A_v\}$. An $n-$partite state that is $n-$separable is fully separable (2.34).

The idea is that an $n-$partite state $|\Psi\rangle_n$ which can be decomposed as (2.36) for a given m is then less multipartite entangled than another state $|\Phi\rangle_n$ which can not. A special class of states are the ones that do not allow for a decomposition of the form (2.36) even for $m = 2$

$$|\Psi\rangle_n \neq |\psi_1\rangle_{k_1} |\psi_2\rangle_{k_2} \tag{2.37}$$

for any bipartition of the n parties k_1, k_2 and any choice of states $|\psi_i\rangle_{k_i}$. These states require entanglement to be present between all the n parties and are called *genuine multipartite entangled.*

Similarly to the case of full separability, a mixed state ρ is $m-$separable if it can be decomposed as a convex mixture of $m-$separable pure states (2.36)

$$\rho_n^{m-\text{sep}} = \sum_i q_i |\Psi_i\rangle\langle\Psi_i|_n^{m-\text{sep}} \tag{2.38}$$

with $\sum\limits_i q_i = 1, q_i \geq 0$.

A genuine multipartite entangled mixed state is a state ρ_n which does not allow for a decomposition (2.38) even for $m = 2$

$$\rho_n \neq \sum_i q_i |\Psi_i\rangle\langle\Psi_i|_n^{2-\text{sep}} \tag{2.39}$$

for any choice of the distribution of the variable q, $q_i \leq 0$ and $\sum\limits_i q_i = 1$ and any 2-separable states $|\Psi_i\rangle_n^{2-\text{sep}}$ (sometimes also termed biseparable).

The operational meaning of $m-$separability is clear and analogous to the bipartite one: a state ρ_n that is not $m-$separable for some $m < n$ can not be prepared by the n parties gathering into m groups, within which they can perform any (joint) operations and use classical communication between the groups. A state that is not $m-$separable then exhibits entanglement between at least $m + 1$ groups of parties. Obviously, a state that is $m-$separable is also $(m-1)-$separable and a state that is not $m-$separable is not $(m+1)-$separable either.

Quantifying multipartite entanglement: Entanglement depth

The notion of $m-$separability captures a multipartite aspect of classicality in the sense that the state is separable across m groups of parties at least. Between these groups of parties, entanglement is thus absent and can not be used as resource in a device-independent task for example. On the other hand, and following this definition, a state with bipartite entanglement between multiple pairs of parties might be more entangled than a state in which a single group of three parties only are entangled together. Nevertheless, it is in general difficult to generate entanglement between an increasing number of parties. Another natural measure of the multipartite extent to which a state is entangled is the minimal number of parties which need to be entangled together in order to generate the state. The *entanglement depth* of a pure states $|\Psi\rangle_n$ captures this aspect of multipartite entanglement [GTB05]. A pure state having an entanglement depth of m can be decomposed as

$$\begin{aligned} |\Psi\rangle_n^{m-\text{depth}} &= \bigotimes_i |\psi_i\rangle_{k_i} \\ \text{if and only if} \quad & \max_{|k_i|} \geq m \end{aligned} \tag{2.40}$$

In other words, if one is able to generate entanglement between *at most* a certain number m of parties, then one can hope to produce at best multipartite systems with an entanglement depth of m.

Similarly, a mixed entangled state $\rho_n^{m-\text{depth}}$ with an entanglement depth of m can be decomposed as a convex mixture of pure states of entanglement depth m

$$\rho_n^{m-\text{depth}} = \sum_i q_i |\Psi_i\rangle\langle\Psi_i|_n^{m-\text{depth}} \tag{2.41}$$

for some distribution of i, $\sum_i q_i = 1$, $q_i \geq 0$ and some states $|\Psi_i\rangle_n^{m-\text{depth}}$.

In that spirit, a fully separable state ρ_n (2.35) has an entanglement depth of $m = 1$ and a genuine multipartite entangled state (2.37) of $m = n$, i.e. requires all parties to be entangled together.

2.3.2 Multipartite nonlocality

Similarly to entanglement, many novel features appear exclusive to the multipartite scenario when generating nonlocal correlations between multiple observers instead of two. For example, and contrary to the bipartite scenario, some Bell inequalities in the multipartite scenario can be saturated by quantum correlations, enabling full randomness amplification under minimal assumptions [Gal+13; Bou+14]. It was also found that an information principle, if any, that singles out quantum correlations necessarily involves multipartite considerations [Fri+13].

A multipartite Bell experiment

In a multipartite Bell experiment, $n > 2$ parties make rounds of measurements on the copies of a multipartite quantum system. Each party A_i $i = 1, 2, ..., n$, at each round of the experiment, chooses to make a measurement labelled by $x_i \in \{0, 1, ..., m_{A_i} - 1\}$ on the share of the system it receives. It then obtains an outcomes $a_i \in \{0, 1, ..., O_{A_i} - 1\}$ from that measurement. In this thesis, the number of measurement choices and outcomes of all parties are taken to be dichotomous $x_i, a_i \in \{0, 1\}$ if not explicitly stated otherwise. Making many rounds of measurements serves to compute a good estimate of the correlations $P(\vec{a}_n|\vec{x}_n) \equiv P(a_1a_2...a_n|x_1x_2...x_n)$. In the DI picture, one is interested in drawing conclusions about the underlying processes generating the correlations from the statistical properties of the correlations only.

The definitions of multipartite nonlocality

The notions and definitions of multipartite nonlocality basically follow the same constructions as for entanglement, up to interesting peculiarities.

In analogy to fully separable states, fully local correlations $P_{\text{loc}}(\vec{a}_n|\vec{x}_n)$ are the ones that factorise with respect to all parties on the additional knowledge of a classical variable λ

$$\begin{aligned} P_{\text{loc}}(\vec{a}_n|\vec{x}_n) &= \sum_{\lambda} q_{\lambda} \prod_{i=1}^{n} P(a_i|x_i, \lambda) \\ &= \sum_{\lambda} q_{\lambda} P(a_1|x_1, \lambda) P(a_2|x_2, \lambda) ... P(a_n|x_n, \lambda) \end{aligned} \tag{2.42}$$

$\sum_{\lambda} q_{\lambda} = 1$ and $q_{\lambda} \geq 0 \ \forall \lambda$. The set of all fully local correlations $\mathcal{L}_n$ (2.42) form a polytope which can equivalently be described by a finite set of inequalities that are satisfied by all correlations belonging to the set – which then serve as Bell inequalities in the multipartite scenario.

Fully local correlations (2.42) can be understood as those which can be generated by all the parties using shared randomness λ only (that is generated before the parties make their measurement choices x_i). Equivalently, and in analogy to bipartite nonlocality, fully local correlations can be understood as those coming from local measurements made on fully separable state (2.35) since

$$\begin{aligned} & Tr\left(M_{a_1|x_1} \otimes M_{a_2|x_2} \otimes ... \otimes M_{a_n|x_n} \rho_n^{\text{sep}}\right) \\ = & \sum_i q_i Tr\left(M_{a_1|x_1} \otimes M_{a_2|x_2} \otimes ... \otimes M_{a_n|x_n} |\psi_i\rangle\langle\psi_i|_{A_1} \otimes |\psi_i\rangle\langle\psi_i|_{A_2} \otimes ... \otimes |\psi_i\rangle\langle\psi_i|_{A_n}\right) \\ = & \sum_i q_i Tr\left(M_{a_1|x_1}|\psi_i\rangle\langle\psi_i|_{A_1}\right) Tr\left(M_{a_2|x_2}|\psi_i\rangle\langle\psi_i|_{A_2}\right) ... Tr\left(M_{a_n|x_n}|\psi_i\rangle\langle\psi_i|_{A_n}\right) \\ = & \sum_i q_i P(a_1|x_1, i) P(a_2|x_2, i) ... P(a_n|x_n, i) \in \mathcal{L}_n \end{aligned} \tag{2.43}$$

In particular, (2.43) implies that any correlations that are not fully local (2.42) can not have been generated from local measurements on a fully separable state. The violation of a Bell inequality defining the set $\mathcal{L}_n$ thus serves as a device-independent witness of entanglement – or non full separability (2.35) – of the state.

As for entanglement, multipartite correlations can exhibit stronger form of nonlocality characteristic of the multipartite scenario. Indeed, nonlocal correlations can be generated in an $n-$party scenario by two parties only sharing entangled states on which they make suitable measurements. Such correlations, even if nonlocal, do not capture the essence of multipartite nonlocality as the nonlocality is in effect bipartite. In analogy with the definition of $m-$separability (2.38) and of entanglement depth (2.41), one can quantify the multipartite extent of nonlocal correlations with notions such as $m-$way locality and correlations depth.

The multipartite extent of correlations: m-way (non)locality

The idea of $m-$separability for systems in an entangled state can be generalised to capture the multipartite extent of correlations. The first to introduce, indirectly, the notion of $m-$way locality was Svetlichny[Sve87; SS02][10]. In the spirit of his work, extremal correlations $P^{\text{ext}}_{\text{m-way}}(\vec{a}_n|\vec{x}_n)$ are said to be $m-$way local if they can be decomposed into a product of m groups of parties

$$P^{\text{ext}}_{\text{m-way}}(\vec{a}_n|\vec{x}_n) = \prod_{r=1}^{m} P(\vec{a}_{k_r}|\vec{x}_{k_r}) \tag{2.44}$$

with, as for multipartite entanglement, a partitioning of the n parties labelled by the variable k: $k_r,\ \ r = 1, 2, ..., m,\ \sum_{r=1}^{m} |k_r| = n$ and $k_s \cap k_t = \emptyset\ \ \forall s \neq t$. We also used the notation $\vec{a}_{k_r} = \{a_i | i \in k_r\}$. The terms $P(\vec{a}_{k_r}|\vec{x}_{k_r})$ in (2.44) of the parties inside a group k_r are, in Sveltichny's definition, allowed to be arbitrary (i.e. normalised

[10] We use the name $m-$way (non)locality that was introduced in [Ban+13; Ban+09].

and positive only) outcome distributions of the $|k_r|$ parties in the group k_r.

General, i.e. not necessarily extremal, correlations that are $m-$way local can be decomposed as convex mixture of extremal, $m-$way local correlations (2.44)

$$P_{\text{m-way}}(\vec{a}_n|\vec{x}_n) = \sum_{\lambda} q_\lambda P^{\text{ext}}_{\text{m-way}}(\vec{a}_n|\vec{x}_n, \lambda) \tag{2.45}$$

for some distribution of the variable λ, $\sum_{\lambda} q_\lambda = 1$ and $q_\lambda \geq 0 \ \forall \lambda$. A decomposition that does not allow for a decomposition (2.45) for a given m is said to be $m-$way nonlocal. In particular, there are strong nonlocal correlations that can not be decomposed as (2.45) even for $m = 2$

$$P(\vec{a}_n|\vec{x}_n) \neq \sum_{\lambda} q_\lambda P^{\text{ext}}_{\text{2-way}}(\vec{a}_n|\vec{x}_n, \lambda) \tag{2.46}$$

for any choice of distribution q_λ, $q_\lambda \geq 0$ and $\sum_{\lambda} q_\lambda = 1$. Correlations (2.46) are said to be *genuine multipartite nonlocal* as nonlocality is somehow "everywhere". In that sense, such genuinely multipartite nonlocal correlations requires all the parties to group together $m = 1$ and $|k_1| = n$ in order to (re)produce the correlations. Remark that if $m = 1$, any probability distribution $P(\vec{a}_n|\vec{x}_n)$ can be decomposed as (2.45).

Interestingly, it is possible to make local measurements on systems in a genuine multipartite entangled state (2.39) such that the generated correlations are genuine multipartite nonlocal (2.46) for any number n of parties [Ban+09; Ban+11]. In the other direction, the generation of $m-$way nonlocal correlations (2.45) serves as DI witness of non $m-$separability (2.38) – i.e. of entanglement between $m+1$ groups – in the underlying systems that were used.

It was shown in [Gal+12] that the definition of $m-$local correlations (2.45) in the sense of Svetlichny – i.e. where the terms $P(\vec{a}_{k_r}|\vec{x}_{k_r})$ are unconstrained (yet normalised) probabilities – does not allow for an operational meaning. To avoid operational problems, one can constrain further the terms $P(\vec{a}_{k_r}|\vec{x}_{k_r})$ to be no-signalling (see 2.2.2).

An operational meaning of multipartite correlations: no-signalling resources within subsets of parties

Following the ideas introduced and developed in [Gal+12] and in [Ban+13], one can define a hierarchy of multipartite correlation by constraining the correlations

$P(\vec{a}_{k_r}|\vec{x}_{k_r})$ that are allowed between the parties within a group k_r of parties

$$\begin{aligned} P_{\text{m-way}}(\vec{a}_n|\vec{x}_n) &= \sum_\lambda q_\lambda P^{\text{ext}}_{\text{m-way}}(\vec{a}_n|\vec{x}_n,\lambda) \\ \text{where} \qquad P^{\text{ext}}_{\text{m-way}}(\vec{a}_n|\vec{x}_n,\lambda) &= \prod_{r=1}^{m} P(\vec{a}_{k_r}|\vec{x}_{k_r},\lambda) \end{aligned} \tag{2.47}$$

- **m−way quantum correlations.–** can be decomposed as in (2.47) by the n parties grouping into m groups and where entanglement is allowed within the groups only

  $$P(\vec{a}_{k_r}|\vec{x}_{k_r},\lambda) = Tr(\rho^\lambda_{k_r} \bigotimes_{i\in k_r} M_{a_i|x_i,\lambda}) \tag{2.48}$$

  i.e. all the correlations that can be generated from local measurements on $m-$separable states. For a given m, the set $\mathcal{Q}_{m-way}$ of all $m-$way quantum correlations is a convex set. Quantum correlations $P(ab|xy) \notin \mathcal{Q}_{m-way}$ must have been generated using states that are not $m-$separable, hence witnessing $m+1$ multipartite entanglement in a DI manner.

- **m−way no-signalling correlations.–** can be decomposed as (2.47) where each term $P(\vec{a}_{k_r}|\vec{x}_{k_r},\lambda)$ is restricted by the no-signalling principle (see 2.2.2) only between the $|k_r|$ parties

  $$P(a_i|x_i,\lambda) \equiv \sum_{\substack{a_j \\ j\in k_r, j\neq i}} P(\vec{a}_{k_r}|\vec{x}_{k_r},\lambda) \qquad \forall k_r, i\in k_r, a_i, \vec{x}_{k_r}, \lambda \tag{2.49}$$

  On the other hand, two parties that do not belong to the same group can be correlated using the shared randomness λ only. $m-$way no-signalling correlations are thus the ones that can be generated by the n parties making m groups, within which the parties can share post-quantum but nevertheless no-signalling resources.

  For any $m \leq n$, the set of $m-$way no-signalling correlations $\mathcal{NS}_{m-way}$ that can be generated is a polytope. Since quantum correlations satisfy the no-signalling principle, one gets that for any given $n, m \leq n$: $\mathcal{Q}_{m-way} \subseteq \mathcal{NS}_{m-way}$. Hence,

  $$P(ab|xy) \notin \mathcal{NS}_{m-way} \qquad \Rightarrow \qquad P(ab|xy) \notin \mathcal{Q}_{m-way} \tag{2.50}$$

  which also enables one to witness $m+1$ entanglement in a DI manner $P(ab|xy) \notin \mathcal{Q}_{m-way}$ and using linear programming only.

In this work, to avoid operational problems in the definitions of multipartite nonlocality, we will work with the no-signalling (NS) definition described above

(2.3.2). Correlations $P(\vec{a}_n|\vec{x}_n) \notin \mathcal{NS}_{m-way}$ are then said to be $m - way$ nonlocal. Note that since $\mathcal{NS}_{m-way} \subseteq \mathcal{S}_{m-way}$, witnessing $m - way$ Sveltichny nonlocality serves to witness $m - way$ nonlocality

$$P(\vec{a}_n|\vec{x}_n) \notin \mathcal{S}_{m-way} \qquad \Rightarrow \qquad P(ab|xy) \notin \mathcal{NS}_{m-way} \tag{2.51}$$

This last fact (2.51) proves useful since it is easy to compute the extremal points of the polytope $\mathcal{S}_{m-way}$, but hard to get the ones of $\mathcal{NS}_{m-way}$ in general. This makes the condition $P(\vec{a}_n|\vec{x}_n) \notin \mathcal{S}_{m-way}$ often easier to check that $P(\vec{a}_n|\vec{x}_n) \notin \mathcal{NS}_{m-way}$.

All the sets $\mathcal{R}_{m-way}$, $\mathcal{R} \in \{\mathcal{Q}, \mathcal{NS}, \mathcal{S}\}$ ($\mathcal{Q}_{m-way} \subseteq \mathcal{NS}_{m-way} \subseteq \mathcal{S}_{m-way}$) can be understood, from a resource-theoretic point of view, as disjoint groups of parties having access to a given type of nonlocal resource in order to generate correlations. In all cases, parties that do not belong to the same groups are only correlated classically, imposing additional limitations on the possible correlations that can be generated.

Correlation depth and minimal group size

The study of $m-$way locality has been very fruitful, in particular to characterise genuine multipartite nonlocality and thus witness genuine multipartite entanglement in a DI manner (using $m = 2$) [Sve87; Ban+12; Aol+12; Gal+12; Ban+13; Col+02b; JLM05; Ban+11; Che+11]. Nevertheless, in general it is difficult to generate systems that are entangled between a large number of parties and easier to generate many systems that are only entangled between fewer parties. In that sense, it is often not the number of groups that can be made, but rather the size of these groups – and thus of the system in an entangled state – that is needed that should serve as figure of merit. If one can generate entanglement between a given number m of parties, it is then interesting to understand what correlations can be (re)produced by using these nonlocal resources. If an information protocol requires the generation of a specific type of correlations, what is the minimal size of the resource that is needed in order to generate these correlations?

In chapter 6, we study these questions and quantify, for a resource $\mathcal{R} \in \{\mathcal{Q}, \mathcal{NS}, \mathcal{S}\}$, the minimal amount of parties that need to group together in order to (re)produce given correlations. To this end, we develop a framework that generalises the concept of entanglement depth to correlations.

Multipartite entanglement versus multipartite nonlocality

Analogously to the bipartite set-up, understanding the relation between multipartite entanglement and nonlocality is a topic of fundamental interest in the field of Quantum Information Theory. Nevertheless, we have seen that the notions of entanglement and of nonlocality become richer in the multipartite scenario: $i)$ parties can be entangled/nonlocal between subsets of parties only and $ii)$ the definitions of multipartite nonlocality crucially depend on what nonlocal resources are allowed within the subsets (or groups) of parties. In this light, there are many questions of interest and numerous directions to explore in the multipartite scenario.

All multipartite systems in a pure entangled state were shown to be able to generate nonlocal correlations [PR92; GG16]. More precisely, all states that are not fully separable (2.34) can generate non fully local correlations (2.42) for any number of parties. On the other hand, these results have the caveat of not capturing the notions of multipartite entanglement and nonlocality as these are essentially bipartite.

For pure states only, it is still unknown whether all genuine multipartite entangled (GME) states are able to generate genuine multipartite nonlocal (GMNL) correlations. Only in the case of three parties was the question answered affirmatively in [Che+14; Che+04]. Nevertheless, witnessing nonlocality in these works requires Hardy-type paradoxes [Har93], making it untestable in an experiment. For any number of parties n, the equivalence between GME and GMNL for pure states is yet to be proven.

For mixed states, the situation is analogous to the bipartite case. Some GME states (2.39) were shown to be unable to generate GMNL correlations (2.47) for all n [Aug+15]. This implies that GME and GMNL are qualitatively inequivalent. There even exist GME mixed states that were shown to be able to generate fully local correlations (2.42) only [Bow+16], strengthening the previous result.

More generally, it would be even more interesting to understand better the exact link between states that are not $m-$separable (2.36, 2.38) and the generation of correlations that are $m-$way nonlocal (2.47), both for pure and mixed states. Similarly, another direction to explore is the link between entanglement depth and correlations depth.

In chapter 5, we focus on understanding better the relation between GME pure states and GMNL correlations. We then also extend our study and results further to the relation between $m-$separable states and $m-$way nonlocal correlations.

Understanding the relation between entanglement and nonlocality, both in the bipartite and in the multipartite set-up, can be seen as a task of purely fundamental interest. On the other hand, some DI information tasks can be performed only when designing protocols making use of multipartite resources [Gal+13; Ban; Bou+14; Tur+14]. One of these tasks is full randomness amplification, in which one allows the initial source of randomness to be arbitrarily, yet not completely, correlated to an adversary. This task requires the generation of correlations that algebraically saturate a Bell inequality, which can not be achieved in the bipartite set-up. The maximal violation of, for example, the Mermin inequality with three parties $n = 3$ allows one to achieve full randomness amplification [Gal+13; Bou+14]. This result is even valid against an adversary that is not limited by the laws of Quantum Theory, but that is only unable to signal faster than light.

In chapter 7, we study multipartite nonlocal correlations and their use in DI information tasks such as quantum key distribution (DIQKD) or secret sharing.

2.4 Entanglement and nonlocality: resources for device-independent information tasks

Despite their fundamental nature, the study of nonlocal correlations – and thus indirectly of entangled systems – has lead to very fruitful advances in our information processing capabilities (see [Bru+14]). The violation of a Bell inequality can always be understood as a particular information task in which quantum resources outperform classical ones. Usually, the nonlocal properties of the correlations serve as certificate that the processes in the experiment truly make use of quantum states and measurements, guaranteeing that the outcomes indeed exhibit some desired property – that they are truly random for example.

As explained in section 2.2.5, the observation of nonlocal correlations only requires minimal assumptions to be made about physical set-up, allowing to draw conclusions in a device-independent (DI) manner. For that reason, the implementation of an information protocol in the DI framework reaches unprecedented levels of security in an adversarial picture, since the gap between theory and experiment is made smaller. The price for obtaining such level of security is that the correlations that need to be generated are typically more demanding experimentally than in a framework in which one relies on more assumptions, such as a faithful description of the measurement devices.

This section introduces two important information tasks based on nonlocal correlations between distant observers. The first one, on which we give a particular focus in this thesis, is devoted to *randomness certification*. The provably secure distribution of secret keys – *device-independent quantum key distribution* (DIQKD) is the subject of the second part of this section.

2.4.1 Information tasks in an adversarial picture

Before describing randomness certification and DIQKD in more details, it is useful to understand in which framework the security of these tasks is asserted. Two honest parties, A and B, perform a Bell experiment 2.2.1 in the DI framework. They thus rely only on the generated statistics $P_{\text{obs}}(ab|xy)$ and on the minimal assumptions described in 2.2.1 to draw conclusions. The two parties do not want to rely on any assumption regarding the functioning of their devices – which they see as black boxes – and the success of the information task should be independent of the actual implementation generating the observed statistics.

In addition to the two trusted parties, the experiment is pictured as being performed in the presence of a third and malicious party E that compromises the security of the protocol. The objective of the adversary E is to break the security of the protocol that the two parties wish to perform without being detected. To this end, E shares, at each round of the experiment, a tripartite state ρ_{ABE} of which $\rho_{AB} = Tr_E(\rho_{ABE})$ is used to generate the statistics observed between the two honest parties (see Fig. 2.9). This implies that E might share entanglement – and thus be strongly correlated – with parties A and B. Moreover, A and B do not make any assumption about the functioning of their measurement devices or the distributed states. These might even be – in the worse case scenario – plotting against them in the adversary's advantage. In that sense, the states that are prepared and the measurements that are being made on these can be understood as being the optimal ones for the adversary's cause. Nevertheless, these need to be compatible with the observed statistics or the adversary's presence would be detected and the protocol aborted. Crucially, the constrain on E to reproduce the observed correlations, in addition to the assumption that are made in a Bell experiment, are sufficient to put bounds on the adversary's capabilities in attacking the security of the tasks.

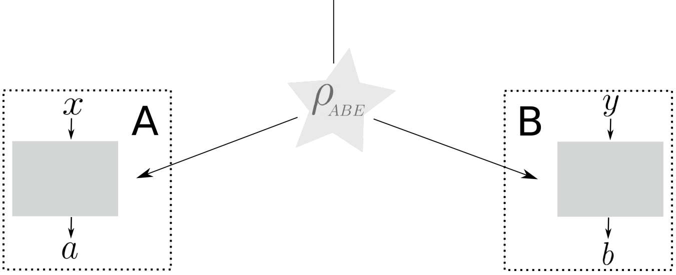

FIGURE 2.9: In the adversarial picture, the Bell experiment between A and B is imagined as being performed in the presence of a third and malicious party E. This adversary is modelled in a very abstract, minimalistic, way. In particular, it may prepare the joint state ρ_{ABE} of which $\rho_{AB} = Tr_E(\rho_{ABE})$ is used to generate the observed correlations $P_{\text{obs}}(ab|xy)$ and thus be correlated to A and B. If one can certify that such an adversary can not compromise the security of the task, then the task is cryptographically secure.

For the sake of clarity, one can find in table 2.1 a comparison of what are the premises the honest parties A and B can rely on for the security proofs and compare them with the adversary E's capabilities.

Parties A and B	**Adversary E**
Can rely on the fact that the experiment respects the assumptions made during a Bell test, see 2.2.1.	Can design the state and measurements that are used by A and B during the experiment, without violating the assumptions of a Bell test.
Can rely on the observed correlations $P_{\text{obs}}(ab\|xy)$.	Can use on a finer description of the observed correlations $P_{\text{obs}}(ab\|xy) = \sum_e q_e P(ab\|xye)$.
Can rely on the assumption that the experiment is *shielded* from the outside: the outcomes a, b are obtained by the parties and are not communicated to the adversary after their generation.	Respects the laws of Quantum Mechanics, i.e. $P(ab\|xye)P(e) = Tr_{ABE}(\rho_{ABE} M_{a\|x} \otimes N_{b\|y} \otimes E_e)$, where ρ_{ABE} is a valid quantum state and $M_{a\|x}$, $N_{b\|y}$ and E_e valid quantum measurements (2.2.4) for all e.

TABLE 2.1

Remark that one assumption was added to the ones made in a Bell experiment: the *shielding assumption*. This assumption refers to the fact that the outcomes (a, b in the case of a Bell experiment) of the devices should not be communicated to the adversary after their generation and each is known only to the party that observes it.

2.4.2 Randomness certification

The concept of randomness has always attracted a lot of attention and has been at the centre of many fields of research ranging from philosophy and mathematics to evolutionary biology. The generation of good random numbers is of paramount importance for tasks such as quantum cryptography, but also for numerical simulations when using the Monte-Carlo technique for example.

In any experiment, two types of randomness coexist: $i)$ the apparent one, that stems from a lack of control or knowledge about the underlying processes and $ii)$ the intrinsic one, that can not be removed even with perfect control over the initial conditions or over the processes. Classical theory is intrinsically deterministic and, as such, only allows for the first type of randomness. With perfect knowledge of the initial conditions one can in principle predict the outcome of any physical process.

Quantum Theory is intrinsically random. Even if one knows all variables of a physical set-up, in general the two types of randomness coexist in an experiment making use of quantum objects.

In this thesis, the notion of randomness we focus on is the cryptographic one: a random number is a number that is private and unpredictable by the hypothetical adversary we modelled in section 2.4.1. Such random numbers necessarily stem from intrinsically random processes.

A random number is unpredictable and private

As said, two notions are crucial to the concept of a random number we are interested in: its unpredictability and its privacy. To illustrate why these two notions are important, consider the situation where one uses a first random number generator (RNG) to obtain a list of random numbers. This list is then put inside a second device that, then, outputs the numbers on the list. Now, suppose that the first RNG is truly built on a random process, i.e. the numbers it outputs are random numbers when they are generated. Nevertheless, their presence on the list makes them predictable at the exit of the second RNG to an adversary having made a copy of that list.

Moreover, suppose that one makes a projective measurement on one of the parts of a system in a maximally entangled two-qubits state $|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ (2.7). Quantum Theory predicts that the two outcomes of this measurement occur with probability half, i.e. are completely unpredictable. One could thus be tempted in using these outcomes as random numbers. Nevertheless, an adversary E that makes measurements on the other share of the system can in general obtain an outcome that is correlated to the one obtained from the other share. If the outcomes of such measurements can be considered as coming from a truly unpredictable process, they are nevertheless correlated to each other, i.e. the adversary has at least partial knowledge of it. Public randomness, random numbers made accessible to everyone, is another example of randomness that is not cryptographically secure.

The outcomes of measurements whose statistics violate a Bell inequality can be proven to be both private and coming from a truly unpredictable process, overcoming the potential problems mentioned in the two previous examples. Relying on minimal assumptions about the set-up, device-independent randomness certification is the only way known today to generate such random numbers.

The guessing probability

A way to quantify the randomness, or unpredictability, of the outcomes generated in a Bell experiment is through *guessing probabilities*. The *observed guessing probability* corresponds to the probability to guess correctly the outcome pair a, b, given only the observed correlations $P_{\text{obs}}(ab|xy)$. For some particular choices of measurement settings $x = \bar{x}, y = \bar{y}$, it is

$$G_{\text{obs}}(\bar{x}, \bar{y}, P_{\text{obs}}(ab|xy)) = \max_{ab} P_{\text{obs}}(ab|\bar{x}\bar{y}) \tag{2.52}$$

This predictability of the outcomes, based on $P_{\text{obs}}(ab|xy)$ only, is the one of parties A and B.

In the adversarial picture we have described, the adversary may possess a finer description of the observed correlations $P_{\text{obs}}(ab|xy) = \sum_{e} q_e P(ab|xye)$. This, in general, implies that it also has greater predictive power of the outcomes. In order to obtain quantitative bounds on the adversary's predictive power, one defines the *device-independent guessing probability* of the outcomes a, b of given observed correlations $P_{\text{obs}}(ab|xy)$ by

$$G(\bar{x}, \bar{y}, P_{\text{obs}}(ab|xy)) = \max_{\substack{q_e, P(ab|xye) \\ \to P_{\text{obs}}(ab|xy)}} \sum_{e} q_e G_{\text{obs}}(\bar{x}, \bar{y}, P(ab|xye)) \tag{2.53}$$

where the maximisation means that the adversary can choose the optimal realisation of $P_{\text{obs}}(ab|xy) = \sum_{e} q_e P(ab|xye)$. Moreover, we assume that the adversary respects the laws of Quantum Theory, i.e. that

$$P(ab|xye) = Tr\big(M^e_{a|x} \otimes N^e_{b|y} |\psi_e\rangle\langle\psi_e|_{AB}\big) \tag{2.54}$$

where $M^e_{a|x}, N^e_{b|y}$ are valid quantum measurements and $|\psi_e\rangle_{AB}$ valid states for all e.

The operational meaning of the guessing probability (2.53) is clear: the adversary has access to the optimal decomposition of the observed correlations in extremal realisations $P_{\text{obs}}(ab|xy) = \sum_e q_e P(ab|xye)$ and guesses the most likely outcomes for each of the extremal realisations $\max_{ab} P(ab|\bar{x}\bar{y}e))$. This guessing probability (2.53) clearly gives an upper bound on the predictive power of the adversary, hence allowing for the certification of randomness as long as $G(\bar{x}, \bar{y}, P_{\text{obs}}(ab|xy)) < 1$.

The amount of randomness, measured in bits r, that can be certified in a Bell experiment is then quantified through the min entropy

$$r = H_\infty(\bar{x}, \bar{y}, P_{\text{obs}}(ab|xy)) = -\log_2(G(\bar{x}, \bar{y}, P_{\text{obs}}(ab|xy))) \tag{2.55}$$

A guessing probability $G(\bar{x}, \bar{y}, P_{\text{obs}}(ab|xy)) = (\frac{1}{2})^r$ allowing to certify the generation of r random bits.

Extremal correlations $P^{\text{ext}}_{\text{obs}}(ab|xy)$ – correlations that do not allow for different decompositions – are of particular interest for the task of randomness certification. Indeed, for these there is a unique $e = \bar{e}$ such that $q_{\bar{e}} = 1$ in $P^{\text{ext}}_{\text{obs}}(ab|xy) = \sum_e q_e P(ab|xye)$ and the optimisation problem in (2.53) simplifies to

$$G(\bar{x}, \bar{y}, P^{\text{ext}}_{\text{obs}}(ab|xy)) = G_{\text{obs}}(\bar{x}, \bar{y}, P^{\text{ext}}_{\text{obs}}(ab|xy)) = \max_{ab} P^{\text{ext}}_{\text{obs}}(ab|xy) \tag{2.56}$$

i.e. the observed guessing probability of the honest parties and the DI guessing probability of the adversary E coincide for extremal correlations.

Bell nonlocality as witness of randomness

The outcomes generated in a Bell experiment can be certified to be at least partially random given that the observed correlations violate a Bell inequality. For this, one does not need to assume that the correlations are generated through quantum processes, but only that these respect the no-signalling principle [CR12] (see sec. 2.2.2). Quantum correlations are only a particular case since they satisfy the principle. Interestingly, one does thus not need to assume that the world is described by the laws of quantum mechanics in order to be able to generate randomness. Assuming that the correlations respect the no-signalling principle is sufficient for that purpose.

On the other hand, it seems that Quantum Theory is somehow optimal – as compared to post-quantum but no-signalling theories for example – in order to generate certified random number [Tor+15]: in any scenario, one can in principle find quantum correlations from which all the outcomes are certified to be random. On the contrary, in a no-signalling theory one of the outcomes can always be predicted once the other outcomes are known. This puts limitations on the amount of randomness generated in a Bell experiment in such a theory, unlike in Quantum Theory.

The optimisation problem (2.53) to obtain bounds on the predictive power of E can be relaxed into the one where, instead of demanding to the adversary to reproduce the full observed statistics $P_{\text{obs}}(ab|xy)$, one asks only that a particular Bell inequality violation

$$I_{\mathcal{L}}\left(P_{\text{obs}}(ab|xy)\right) = \sum_{x,y,a,b} h^{x,y}_{a,b} P_{\text{obs}}(ab|xy) = \text{B}_{\text{obs}} \tag{2.57}$$

is reproduced:

$$G(\bar{x},\bar{y},P_{\text{obs}}(ab|xy)) = \max_{\substack{q_e,P(ab|xye)\\ \to\sum_e q_e B_e = B_{\text{obs}}}} \sum_e q_e G_{\text{obs}}(\bar{x},\bar{y},P(ab|xye)) \tag{2.58}$$

where $B_e = I_{\mathcal{L}}\left(P(ab|xye)\right)$. The result of the optimisation problem (2.58) is an upper bound on the one of (2.53), as the constraints on the adversary are being relaxed. Crucially, in many cases this relaxed problem is sufficient to obtain non trivial upper bounds on the guessing power of the adversary and thus to certify the generation of random numbers.

For the generation of randomness using the outcomes of a Bell experiment, the rounds of measurements on the systems are divided into two sets: $i)$ rounds that serve to build the statistics $P_{\text{obs}}(ab|xy)$ violating a Bell inequality, their number depends on the quality of the estimate one desires to obtain; and $ii)$ rounds in which the outcomes serve to generate randomness. The rounds $i)$ serve to certify properties of the set-up through the study of the generated statistics, often by observing a given Bell inequality violation. In some sense a given portion of the statistics is sacrificed to obtain the guarantee that the outcomes from the rest of the rounds can indeed be used to generate random numbers.

Local randomness in a Bell test

Randomness certification is usually performed as a single user task, i.e. the two boxes performing the Bell test are held by a single observer. In this case, the two outcomes can be used as random numbers. Nevertheless, in a cryptographic set-up the user might have access to one of the outcomes of the Bell experiment only.

Instead of using both outcomes a, b at a round of the experiment to generate randomness, one can disregard one of them and focus on generating randomness from the other outcome only – from b for example. Outcome a is still crucial to compute the observed correlations, but is not used as random number. In this case, the goal is to certify that the adversary E can not predict the outcome b, which is quantified through the local DI guessing probability

$$\begin{aligned} G(\bar{y}, P_{\text{obs}}(ab|xy)) &= \max_{\substack{q_e, P(ab|xye) \\ \to P_{\text{obs}}(ab|xy)}} \sum_e q_e G_{\text{obs}}(\bar{y}, P(ab|xye)) \\ &= \max_{\substack{q_e, P(ab|xye) \\ \to P_{\text{obs}}(ab|xy)}} \sum_e q_e \max_b P_B(b|\bar{y}e) \end{aligned} \tag{2.59}$$

where $P_B(b|\bar{y}e) = \sum_a P(ab|x\bar{y}e) \;\; \forall x, e$ is the marginal of party B for each extremal distribution.

Again, one can relax the problem into the one where the adversary is only required to reproduce a particular Bell inequality violation

$$G(\bar{y}, P_{\text{obs}}(ab|xy)) = \max_{\substack{q_e, P(ab|xye) \\ \to \sum_e q_e B_e = B_{\text{obs}}}} \sum_e q_e G_{\text{obs}}(\bar{y}, P(ab|xye)) \tag{2.60}$$

where $B_e = I_{\mathcal{L}}\left(P(ab|xye)\right)$ and $\sum_e q_e B_e = I_{\mathcal{L}}\left(P_{\text{obs}}(ab|xy)\right)$.

In both cases (2.59) and (2.60), the amount of randomness that is generated at each round of the experiment is quantified through the min entropy

$$r = H_\infty(\bar{y}, P_{\text{obs}}(ab|xy)) = -\log_2(G(\bar{y}, P_{\text{obs}}(ab|xy))) \tag{2.61}$$

Randomness versus entanglement and nonlocality

We have seen that a necessary and sufficient condition to certify randomness in the outcomes of a Bell experiment is that the generated correlations $P_{\text{obs}}(ab|xy)$ violate a Bell inequality. In that sense, randomness and nonlocality are qualitatively equivalent. As entanglement is necessary for the generation of nonlocal correlations, it is in turn necessary – but not sufficient – for the generation of random outcomes.

At the quantitative level, the exact relation between entanglement, nonlocality and randomness is more intricate. In the simplest $[2,2,2,2]$ Bell scenario (with two dichotomic choices of two-outcome measurements), it is known that one can use almost separable states and still be able to generate perfectly random bits locally. This means that $G(\bar{y}, P_{\text{obs}}(ab|xy)) = \frac{1}{2}$ (2.59) or $r = 1$ at each round used for the generation of randomness. Entanglement and randomness are thus quantitatively inequivalent in that sense, since weak entanglement suffices to generate perfect randomness. What is more, generating observed correlations $P_{\text{obs}}(ab|xy)$ that lie arbitrarily close to the set of local correlations – whose correlations have predictable outcomes – can be used to generate perfect randomness. Entanglement, nonlocality and randomness are thus quantitatively inequivalent.

Interestingly, it is known that correlations generated from measurements on two-qudit systems (in $\mathcal{H}^d \otimes \mathcal{H}^d$ (2.3)) in a pure state can be simulated by using local measurement with *at most* $O_A = O_B = d^2$ outcomes each [DPP05]. In that light, the worse case scenario for the adversary E is to have to reproduce the observed correlations using measurements with d^2 outcomes locally. This, in turn, limits to $r = -\log_2(\frac{1}{d^2}) = 2\log(d)$ bits the randomness that can be generated from a qudit system at each round. By combining the two local outcomes a, b, there is thus a fundamental bound of $r = 4\log(d)$ which can be obtained from each two-qudit state at each round used for randomness generation when single measurements are being performed on each copy of the state. In the particular case of systems of two qubits, one can generate *at most* $4log_2(2) = 4$ bits of randomness at each round used for randomness generation. For two-qubit systems in a maximally entangled pure state only, it was shown how to certify the maximal amount of 2 local random bits in [Ací+16].

These results raise the question of whether there exist fundamental bounds on the amount of randomness that can be generated from quantum systems.

In chapter 4, this is the question we consider and use sequences of measurements on the systems at each round of the experiment. This allows us to explore further the limitations on the amount of randomness that can be certified from quantum systems. We show that an unbounded amount of randomness can be certified from quantum systems by performing sequences of measurements.

2.4.3 Device-independent quantum key distribution

The second information task that we focus on is the one of distributing secret keys to distant observers. This task can be achieved in a provably secure way only when using quantum resources [BB84; Eke91]. The generated secret keys can then be used to secure the communication of a message between parties – called quantum cryptography. In reality, secure communication between parties can be achieved classically, given that they share a key that has the same size as the message they wish to encrypt, through a procedure called *one-time pad*. The only missing element in order to establish secure communication using classical resources is the generation of secret keys between the parties. This is (yet) doable securely only when using quantum systems. Moreover, one can also perform device-independent quantum key distribution (DIQKD) from the outcomes of measurements whose statistics violate a Bell inequality.

The task of producing secret keys can be understood as two parties generating random outcomes a, b – i.e. certify that these are uncorrelated to an hypothetical adversary E – that are nevertheless correlated between each other, $a = b$ for example. The correlated and random outcomes then serve as key, which can be used to encrypt the message. Performing DIQKD allows one to design protocols whose security is maximal. The actual implementation generating the observed statistics is of no importance, but crucially requires the generation of nonlocal correlations. The secret keys are thus built from the outcomes of a Bell experiment whose observed correlations violate a Bell inequality, as proposed in [Ací+07] and based on the ideas in the previous works [MY98] and [BHK05]. General security proofs for these protocols were later obtained in [VV14; MS16; AF+18].

As for randomness certification, a portion of the rounds of the experiment serves to build an estimate of the behaviours of the devices through the observed correlations $P_{\text{obs}}(ab|xy)$. From a good estimate $P_{\text{obs}}(ab|xy)$ violating a Bell inequality, one then obtains a certificate of security for the rounds that serve for the generation of the secret key.

DIQKD: the CHSH inequality and the maximally entangled state

In this thesis, we are not interested in building a protocol implementing DIQKD that would have, for example, a certain resistance to noise or imperfections. In that sense, we study only perfect implementations with maximal violation of a Bell inequality in order to draw theoretical conclusions about the fundamental aspect of DIQKD from the Quantum Information Theory perspective. With that particular aim in mind, we describe DIQKD through the particular case of the maximal violation of the CHSH inequality.

By performing measurements on a maximally entangled system of two qubits $|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ (2.7)

$$P_{\text{obs}}(ab|xy) = Tr\big(M_{a|x} \otimes N_{b|y} |\Phi^+\rangle\langle\Phi^+|_{AB}\big)$$

$$\begin{aligned} M_{a|0} &= \frac{1}{2}(\mathbb{1} + (-1)^a \sigma_Z) \ \ ; \ \ N_{b|0} = \frac{1}{2}(\mathbb{1} + (-1)^b \frac{\sigma_Z + \sigma_X}{\sqrt{2}}) \\ M_{a|1} &= \frac{1}{2}(\mathbb{1} + (-1)^a \sigma_X) \ \ ; \ \ N_{b|1} = \frac{1}{2}(\mathbb{1} + (-1)^b \frac{\sigma_Z - \sigma_X}{\sqrt{2}}) \end{aligned} \tag{2.62}$$

one obtains the maximal value $I_{CHSH}\big(P_{\text{obs}}(ab|xy)\big) = 2\sqrt{2} > 2$, implying that $P(ab|xy) \notin \mathcal{L}$ is nonlocal. In particular, $P_{\text{obs}}(ab|xy)$ is also extremal and the local outcome a for $x = 0$ defines a perfect random bit

$$\begin{aligned} G(\bar{x} = 0, P_{\text{obs}}(ab|xy)) &= G_{\text{obs}}(\bar{x} = 0, P_{\text{obs}}(ab|xy)) \\ &= \max_a \sum_b P_{\text{obs}}(ab|\bar{x}y) = \frac{1}{2} \end{aligned} \tag{2.63}$$

Now, party B can in addition make a projective $N_{b|y=2} = \frac{1}{2}(\mathbb{1} + (-1)^b \sigma_Z)$ measurement on his share the maximally entangled system $|\Phi^+\rangle_{AB}$, obtaining $b = a$

$$P_{\text{obs}}(a = b|02) = 1 \tag{2.64}$$

i.e. they share two correlated but yet random bits $a = b$ that serve to build the secret key.

2.5 End of the background

We have now finished introducing the basic ingredients necessary for the development of the results obtained during the course of this thesis. The following chapters expose these results and are mostly modelled on the published articles.

Chapter 3

Towards an equivalence between maximal entanglement and maximal quantum nonlocality

While all bipartite pure entangled states are known to generate correlations violating a Bell inequality, and are therefore nonlocal, the quantitative relation between pure-state entanglement and nonlocality is poorly understood (see Sec. 2.2.6). In fact, some Bell inequalities are maximally violated by non-maximally entangled states and this phenomenon is also observed for other operational measures of nonlocality. In this chapter, we study a recently proposed measure of nonlocality defined as the probability that a pure state displays nonlocal correlations when subjected to random measurements. We first prove that this measure satisfies some natural properties for an operational measure of nonlocality. Then, we show that for pure states of two qubits the measure is monotonic with entanglement for all correlation two-outcome Bell inequalities: for all these inequalities, the more the state is entangled, the larger the probability to violate them when random measurements are performed. Finally, we extend our results to the multipartite setting.

Our work represents the first analytical results of a measure seemingly putting entanglement and nonlocality in a quantitative equivalence. Complementary numerical evidence is provided for the cases which we could not approach analytically. This is the first chapter presenting the results that were obtained during the thesis and is based on [Lip+18].

3.1 Introduction

Early work by Tsirelson demonstrated that the maximal quantum violation of the Clauser-Horne-Shimony-Holt (CHSH) inequality [Cla+69] can only be achieved when making measurements on a two-qubit maximally entangled state [Cir80]. It was then natural to expect maximal entanglement to be indispensable to retrieve the maximal quantum violation of Bell inequalities. However, subsequent examples showed this intuition to be wrong: the maximal quantum violation of certain Bell inequalities crucially requires partial entanglement [Aci+02], even when considering states of arbitrary Hilbert space dimension [LVB11; VW11]. Furthermore, the phenomenon of obtaining more nonlocality from less entanglement for pure states happened to occur not only for the amount of violation of a given Bell inequality. It was also observed for other measures of nonlocality, such as the robustness of nonlocality to noise [Aci+02], losses [Ebe93], statistical strength of Bell tests [AGG05] and the simulation of quantum correlations with nonlocal resources [BGS05]. This apparent inequivalence of pure-state entanglement and nonlocality was dubbed *anomaly* in [MS06] and this is the terminology adopted here.

Even if there is no fundamental requirement for maximal entanglement and maximal nonlocality to be in one to one correspondence, it is desirable to understand if these anomalies appear only as artefacts of the measure that is used. In that sense, it would be interesting to come up with an operational measure of quantum nonlocality that would be maximized by maximally entangled states. A step in this direction was made in [FP15], where the authors gave numerical results suggesting that the anomaly originally observed in [Aci+02] with two-qutrit states violating maximally the Collins-Gisin-Linden-Massar-Popescu (CGLMP) Bell inequality [Col+02a] disappears when considering a novel measure of nonlocality. For a given (pure) quantum state $|\psi\rangle$, the value of the measure is the probability of violating a specific Bell inequality when random projective measurements are performed on the state. A state $|\psi_1\rangle$ is more nonlocal than a state $|\psi_2\rangle$, in the sense of the measure studied in [FP15], if by making random measurements on $|\psi_1\rangle$ there is a higher chance of generating nonlocal correlations than on $|\psi_2\rangle$. This is the type of measure of nonlocality that we study here, which we name *nonlocal volume*. More specifically, the authors of [FP15] numerically showed that the probability of violating the three-outcome CGLMP inequality with random projective measurements is maximal among all pure two-qutrit states when using a maximally entangled state. Thus, the new quantifier removes the original anomaly between entanglement and nonlocality identified in [Aci+02] for the CGLMP inequality with three outputs. Note that the probability of finding nonlocal correlations for qubit states was initially considered in [Lia+10].

While the above study offers a promising insight into a potential measure of nonlocality for which the original anomaly disappears, several crucial aspects were not addressed there. The main limitation of this measure is that a single Bell inequality is used to witness nonlocality in the correlations. But apart from the simplest Bell-CHSH case, in any Bell scenario there are many inequivalent families of Bell inequalities. It is, then, unclear why a single inequality should be tested and preferred over the rest. In the context of the nonlocality measure, this limitation was lifted later when the authors of [Ros+17] extended the numerical search of [FP15] without assuming any *a priori* fixed Bell inequality. Instead, they considered all the possible Bell inequalities in a given Bell scenario. Note that this approach is equivalent to checking whether the given correlations are nonlocal independently of a specific Bell inequality, which provides a much more operational result. They then performed an intense numerical exploration of many different Bell setups, seeing that in all of them the largest value of the nonlocal volume was obtained for the maximally entangled state.

All this numerical evidence suggests that the nonlocal volume, that is, the probability of generating nonlocal correlations when performing random local measurements on a quantum state, is a good candidate for a measure of nonlocality without anomalies. On the other hand, to our knowledge almost no analytical results are known using this new measure. The only analytical results we are aware of concern the simplest scenario for quantum nonlocality with its unique CHSH inequality [Lia+10; Ros+17], where it is known that the nonlocal volume is a monotone of entanglement: the more entangled the state, the bigger its probability to violate a CHSH inequality with random measurements made on it. The nonlocal volume for the maximally entangled state of two qubits only was computed analytically in [Lia+10] and was found to be $2(\pi - 3) \approx 28.32\%$. The reason why so little is known so far about the nonlocal volume is that it is hard to deal with it in analytically as one typically needs to solve complicated integrals.

In this chapter, we give the first analytical results connecting maximal entanglement and nonlocality in terms of the nonlocal volume. We start by defining properly the measure and proving that it indeed has many of the desirable properties as measure of nonlocality for quantum states. Specifically, we show that it is invariant under local unitaries (LU) applied by each party on the state, that its value is strictly positive for all pure bipartite entangled states and that its value tends to one in the limit of infinite measurement settings, as expected.

We then prove that no anomaly can occur for two-qubit states when considering scenarios based on *correlation inequalities* (or XOR games [Cle+04; BV13]) involving any number of projective two-outcome measurements per site. More generally, we show that these particular inequalities are monotonic with the amount of entanglement in two-qubit pure states: the more the entanglement in the state, the larger its probability of violating these Bell inequalities when random measurements are made on it. This implies, in particular, that the maximally entangled state is always the most nonlocal according to this measure in these scenarios. We show that our results extend to the multipartite scenario for the Greenberger-Horne-Zeilinger (GHZ) family of states $\cos(\theta)|0...0\rangle + \sin(\theta)|1...1\rangle$. Finally, we demonstrate by providing explicit examples that our proof technique cannot be extended to scenarios involving two-output Bell inequalities with marginal terms.

3.2 The nonlocal volume

We work in the standard bipartite Bell scenario $[m_A, m_B, o_A, o_B]$ that we described in Sec. 2.2.1, where the two parties generate the correlations $P(ab|xy)$ from many rounds of measurements. The measurements each party performs are described by a set of orthogonal projectors $\{M_{a|x}\}_{x=0,1,\ldots,m_A-1}$ and $\{N_{b|y}\}_{y=0,1,\ldots,m_B-1}$ that sum up to the identity $\sum_{a=0}^{o_A-1} M_{a|x} = \sum_{b=0}^{o_B-1} N_{b|y} = \mathbb{1} \;\; \forall x, y$ (see Sec. 2.2.4).

Now, consider a quantum system shared by A and B in a pure state of two qubits written in its Schmidt basis (2.4):

$$|\psi_\theta\rangle = \cos(\theta)\,|00\rangle + \sin(\theta)\,|11\rangle \tag{3.1}$$

parametrized by the angle $\theta \in [0, \frac{\pi}{4}]$. Gisin showed that one can find local measurements on any state of the form (3.1) with $\theta > 0$ such that the generated correlations are nonlocal [Gis91]. A natural question is then: which one among all the states $|\psi_\theta\rangle$ is the *most* nonlocal, in the sense of giving the largest Bell inequality violation? The question is troublesome as the answer typically depends on the scenario and on the Bell inequality considered. The situation simplifies in the setup with two dichotomic-outcome measurements per side, where the violation of the CHSH inequality alone is both necessary and sufficient to witness nonlocality. The state maximally violating the CHSH inequality upon optimization over the measurements is the maximally entangled state $|\phi^+\rangle$ ($\theta = \pi/4$ in (3.1)) [Cir80]. In fact, in this case there even exists a monotonous relation between entanglement and nonlocality [HHH95]: the more entangled the state is, the more it violates the CHSH inequality.

Intuitively, one could expect a similar monotonous relation between entanglement and nonlocality to hold for inequalities in broader scenarios, for Bell tests involving more measurement choices and/or outcomes, or even in full generality. In [Aci+02], however, it was found that the CGLMP inequality [Col+02a] with $o_A = o_B = 3$ outcomes and with a two-qutrit state of the form $|\psi_3^\gamma\rangle = \frac{1}{\sqrt{2+\gamma^2}}(|00\rangle + \gamma|11\rangle + |22\rangle)$ with $\gamma \simeq 0.79$ achieves a higher violation than obtained with the two-qutrit maximally entangled state $|\phi_3^+\rangle = \frac{1}{\sqrt{3}}(|00\rangle + |11\rangle + |22\rangle)$. Furthermore, this anomaly of obtaining more nonlocality from less entanglement happened to occur for states of arbitrary dimension [ZG08], and for other measures of nonlocality as well [Ebe93; AGG05; BGS05]. Note that most of the previous results were not rigorous proofs of the existence of an anomaly, as they mostly consisted of numerical searches. But subsequent works, such as [LVB11; NPA08; VW11], proved some of these results analytically.

As mentioned, to fix the original anomaly detected in [Aci+02], the authors of [FP15] considered a measure of nonlocality defined by the probability that the correlations generated from randomly chosen measurements made on a given state $|\psi\rangle$ violate any Bell inequality by any extent. More formally, one defines the set of variables Ω parametrizing all the measurements that two parties may perform. For instance, a two-outcome projective measurement $M_{a|x} \equiv M_{a|x}(\omega_1, \omega_2)$ can be parametrized by two angles ω_1, ω_2 in the Bloch sphere. For all the measurement parameters in Ω one then needs to check whether the generated behavior from the state $|\psi\rangle$ is nonlocal. The parameters that do lead to measurements giving nonlocal correlations when made on $|\psi\rangle$ can be arranged in the set $\mathcal{V}(|\psi\rangle)$. We are interested in calculating the relative volume of the set $\mathcal{V}(|\psi\rangle)$ with respect to the volume of the whole set Ω. The reason for it is that it can be directly interpreted as the probability of obtaining nonlocal correlations with random measurements, i.e. $P_{NL}(|\psi\rangle) = \frac{\text{vol}(\mathcal{V}(|\psi\rangle))}{\text{vol}(\Omega)}$. Note that the exact value of this probability depends on the value of the volumes, which, in turn, is a function of the measure chosen to sample the measurements. As discussed below, for projective measurements the sampling is naturally defined by the Haar measure, which is the only measure invariant under unitary operations. Moreover, we remark that some of our results are valid for any choice of measure.

Equivalently, the nonlocal volume can be obtained by considering the following quantity

$$P_{NL}(|\psi\rangle) = \int \mathrm{d}\Omega f(|\psi\rangle, \Omega), \tag{3.2}$$

where we integrate over the measurement parameters Ω according to the Haar measure. The function $f(|\psi\rangle, \Omega)$ is an indicator function that takes the value 1 whenever the generated behavior is nonlocal and 0 otherwise:

$$f(|\psi\rangle, \Omega) = \begin{cases} 1 & \text{if } p(ab|xy) \text{ is nonlocal} \\ 0 & \text{otherwise} \end{cases} \tag{3.3}$$

Using this definition, the potential nonlocality of the generated behaviors $p(ab|xy) = Tr(|\psi\rangle\langle\psi| M_{a|x} \otimes M_{b|y})$ (3.3) can be understood as witnessed by *all possible* Bell inequalities for a given scenario. Note that this is equivalent to checking whether some given correlations admit a local decomposition (**??**). In that sense, the violation of a Bell inequality should be understood as a witness of nonlocality only, and not as a quantifier. Seen as witnesses, it is then important to consider the full set of possible inequalities in a setup, as it would otherwise be possible for nonlocal correlations to go undetected and lead to an underestimation of the nonlocal volume.

In general, explicitly evaluating the integral in (3.2) can be highly demanding. So far, analytical results exist only in the simplest bipartite case and for the CHSH inequality [Lia+10; Ros+17]. Nonetheless, the numerical results of [FP15; Ros+17] strongly suggest that the above measure may be able to remove the anomaly between nonlocality and entanglement. Indeed, extensive numerical computations show that the maximally entangled state is the one achieving the highest probability of obtaining nonlocal correlations with random measurements in all the explored cases.

3.3 Properties of the measure

The nonlocal volume (3.2) aims at measuring how nonlocal pure states are in order to compare them. As such, we clearly want this measure to fulfill a basic set of conditions to consider it an operational measure of nonlocality. In this section we list some of the desired properties and formally prove that the nonlocal volume satisfies them.

Property 1. *The nonlocal volume (3.2) is invariant under local unitaries applied on the state if one uses the Haar measure for the integration:*

$$P_{NL}(V_1 \otimes V_2 \, \rho \, V_1^\dagger \otimes V_2^\dagger) = P_{NL}(\rho) \qquad \forall \; V_1, V_2 \tag{3.4}$$

where V_1, V_2 are local unitary transformations applied by the parties to their share of the state.

Proof.

$$\begin{aligned} &P_{NL}(V_1 \otimes V_2 \, \rho \, V_1^\dagger \otimes V_2^\dagger) \\ &= \int \mathrm{d}\Omega f(V_1 \otimes V_2 \, \rho \, V_1^\dagger \otimes V_2^\dagger, \Omega) \end{aligned} \tag{3.5}$$

Now, using the cyclicity of the trace operator:

$$\begin{aligned} &Tr(V_1 \otimes V_2 \, \rho \, V_1^\dagger \otimes V_2^\dagger M_{a|x}^\Omega \otimes N_{b|y}^\Omega) \\ &= Tr(\rho \, V_1^\dagger M_{a|x}^\Omega V_1 \otimes V_2^\dagger N_{b|y}^\Omega V_2) \end{aligned} \tag{3.6}$$

Finally, making the substitution $\Omega \to \Omega'$ such that $M_{a|x}^{\Omega'} \otimes N_{b|y}^{\Omega'} = V_1^\dagger M_{a|x}^\Omega V_1 \otimes V_2^\dagger N_{b|y}^\Omega V_2$ and the fact that, if using the Haar measure, $\mathrm{d}\Omega' = \mathrm{d}\Omega$ (the elements of integration are invariant under LU) leads to the desired result. □

Property 2. *For all pure bipartite entangled states $|\psi\rangle_{ent}$ in a setup with at least two choices of two-outcome measurements, the nonlocal volume* (3.2) *is strictly positive:*

$$P_{NL}(|\psi\rangle_{ent}) > 0 \tag{3.7}$$

and thus:

$$P_{NL}(|\psi\rangle) = 0 \tag{3.8}$$

if and only if the state $|\psi\rangle$ is separable.

Proof. To see this, first consider the space Ω of parameters parameterizing all the local measurements. For example, a two-outcome projective measurement on a qubit state can be parameterized by two angles ω_1, ω_2 in the Bloch sphere. From [Gis91], we know that for any pure entangled state $|\psi\rangle_{\text{ent}}$ (of any dimension) there exist certain values of the parameters such that the measurements performed on the state generate correlations that are nonlocal in the simplest setup with $x, y, a, b = 1, 2$, i.e. $\mathcal{V}(|\leftarrow\rangle_{\text{ent}}) \neq \emptyset$. We still need to show that the set of parameters leading to nonlocal correlations $\mathcal{V}(|\leftarrow\rangle_{\text{ent}})$ is not of volume zero. Note that since the local correlations form a closed set, for any fixed state the set of measurement parameters leading to local correlations (**??**) is also closed. This implies that the (disjoint) sets of parameters leading to nonlocal correlations are open. In particular there is always a ball around any nonlocal point in this space of parameters that contains parameters leading to nonlocal correlations as well. For any fixed pure entangled state is then clear that starting from any nonlocal quantum correlations one can slightly perturb all the parameters ω and still generate nonlocal correlations. □

Property 3. *For any pure bipartite entangled state $|\psi\rangle_{ent}$, the nonlocal volume* (3.2) *tends to unity when the number of measurement choices tends to infinity:*

$$P_{NL}(|\psi\rangle_{ent}) \xrightarrow[m_B \to \infty]{m_A \to \infty} 1 \tag{3.9}$$

Proof. From property (2), we know that for the pure state $|\psi\rangle_{\text{ent}}$ and in the setup with $x, y, a, b = 1, 2$ the nonlocal volume is strictly larger than zero $P_{NL}(|\psi\rangle_{\text{ent}}) = \epsilon > 0$. The probability that the generated correlations $\{p(ab|xy)\}_{x,y=1,2}$ are local for random measurements is then $P_{\text{loc}} = 1 - P_{NL} = 1 - \epsilon$. Now, with additional measurement settings, say $x = 3, 4$ and $y = 3, 4$, the correlations $\{p(ab|xy)\}_{x,y=3,4}$ also has a probability $P_{\text{loc}} = 1 - \epsilon$ of being local, independently of $\{p(ab|xy)\}_{x,y=1,2}$. By repeating the argument and thus increasing the number of measurements choices, the probability that *all* two-settings correlations $\{p(ab|xy)\}_{x,y=2k-1,2k}$ with $k = 1, 2, ...$ are local is:

$$P^k_{\text{loc}}(|\psi\rangle_{\text{ent}}) = (1 - \epsilon)^k \tag{3.10}$$

Remark that if any of these two-settings correlations are nonlocal, then clearly the full correlations also is nonlocal. This implies that

$$P_{NL}(|\psi\rangle_{\text{ent}}) \geq 1 - P^k_{\text{loc}}(|\psi\rangle_{\text{ent}}) = 1 - (1-\epsilon)^k \xrightarrow{k\to\infty} 1, \tag{3.11}$$

which means that the lower bound on P_{NL} goes to 1 as $k \to \infty$. Moreover, we have that $k \to \infty$ implies $m_A, m_B \to \infty$, which yields the desired result. □

Note that the numerical evidence suggesting Property 3 of the nonlocal volume had been found in [Ros+17; Sha+12].

Finally, let us comment on the generalisation of properties 2 and 3 to bipartite mixed entangled states that are nonlocal, i.e. mixed states for which one can find local measurements such that the generated correlations violate a Bell inequality. Clearly, if the mentioned measurements can be found in a scenario involving finite numbers of measurements settings m_A, m_B, then one can obtain properties similar to 2 and 3 for a given mixed nonlocal state ρ. In a scenario with at least m_A and m_B settings – instead of $m_A, m_B = 2$ for a pure entangled state, $P_{NL}(\rho) > 0$ since one can always slightly perturb the mentioned measurements and still generate nonlocal correlations. This observation comes from the fact that the set of local correlations is also closed in that scenario. Property 3 also holds for any mixed nonlocal state and only the proof needs to be adapted. One now considers k disjoints sets consisting of m_A, m_B measurements each (instead of $m_A, m_B = 2$ for pure entangled states) and by taking k large enough the probability that *all* the correlations $\{p(ab|xy)\}^{x=(k-1)m_A,(k-1)m_A+1,\ldots,km_A-1}_{y=(k-1)m_B,(k-1)m_B+1,\ldots,km_B-1}$ for k = 1,2,... are local tends to zero, implying that the probability of the full correlations being nonlocal tends to one with growing k.

3.4 The nonlocal volume using correlation Bell inequalities is a monotone of entanglement

Having proven some of the properties of the measure (3.2), we proceed to analyzing the nonlocal volume of different entangled states. We are still unable to compute $P_{NL}(|\psi\rangle)$ explicitly from Definition 3.2. Therefore, we approach the problem alternatively and study whether there exist inclusion relations among the sets $\mathcal{V}(|\psi\rangle)$ of measurements leading to nonlocal correlations when made on different states. Indeed, if the set of measurements $\mathcal{V}(|\psi_1\rangle)$ leading to nonlocal correlations on the state $|\psi_1\rangle$ is *included* in the set $\mathcal{V}(|\psi_2\rangle)$ for the state $|\psi_2\rangle$, $\mathcal{V}(|\psi_1\rangle) \subseteq \mathcal{V}(|\psi_2\rangle)$, then obviously $P_{NL}(|\psi_1\rangle) \leq P_{NL}(|\psi_2\rangle)$. Crucially, we show that in many situations, namely when witnessing nonlocality with correlation (see below (3.13)) inequalities only, the set of measurements $\mathcal{V}(|\psi_{\theta_1}\rangle)$ leading to nonlocal correlations on a pure two-qubit entangled state $|\psi_{\theta_1}\rangle$ is included in the set $\mathcal{V}(|\psi_{\theta_2}\rangle)$ if $|\psi_{\theta_1}\rangle$ is less entangled than $|\psi_{\theta_2}\rangle$. We thus prove that the nonlocal volume of correlation Bell inequalities is a monotone of entanglement in the case of qubit states and two-outcome projective measurements.

We work in Bell scenarios with two-outcome measurements and any number of measurement settings per party. Labeling the measurements outcomes $a, b = \pm 1$, the correlations in this scenario can be parametrized as

$$p(ab|xy) = \frac{1}{4}\left(1 + a\langle A_x\rangle + b\langle B_y\rangle + ab\langle A_x B_y\rangle\right), \tag{3.12}$$

where $\langle A_x\rangle = \sum_{a=\pm 1} a\ p_A(a|x)$ are Alice's local expectation value depending on her marginal distribution $p_A(a|x) = \sum_b p(ab|xy)$, and similarly for Bob's $\langle B_y\rangle$. The terms $\langle A_x B_y\rangle = \sum_{a,b=\pm 1} ab\ p(ab|xy)$ are known as two-body correlators. In this scenario, correlation or full-correlator Bell inequalities (or even *XOR* games) for two outcomes are those in which only these last terms appear and hence can be written as

$$\hat{I}^{\langle..\rangle} = \sum_{xy} g_{xy}\langle A_x B_y\rangle \leq g_{\text{loc}} \tag{3.13}$$

where g_{loc} is the local bound.

For any correlation Bell inequality $I^{\langle..\rangle}$ and for local measurements $M_{a|x}$ and $N_{b|y}$, one can define the associated Bell operator (acting at the level of the states):

$$B_{I^{\langle..\rangle}} = \sum_{xy} g_{xy} A_x \otimes B_y, \tag{3.14}$$

where we defined the observables $A_x = M_{+1|x} - M_{-1|x}$, $B_y = N_{+1|y} - N_{-1|y}$. For a given state ρ, the value of the Bell inequality then reads

$$I^{\langle..\rangle}(\rho) = Tr(\rho B_{I^{\langle..\rangle}}). \tag{3.15}$$

Next, we present our main result under the form of a theorem. Our result holds for any number of 2-outcome projective measurements performed by Alice and Bob.

Theorem 1. *Consider any correlation Bell inequality* $\hat{I}^{\langle..\rangle} = \sum_{xy} g_{xy}\langle A_x B_y\rangle \leq$

g_{loc} (3.13) *with* g_{loc} *being the local bound. A and B measure the local observables* $\{A_x\}$ *and* $\{B_y\}$ *respectively, defining the associated Bell operator* $B_I^{\langle..\rangle} = \sum_{xy} g_{xy} A_x \otimes B_y$ (3.15)*. Consider two pure two qubit states* $|\psi_{\theta_1}\rangle$ *and* $|\psi_{\theta_2}\rangle$ *with* $\theta_1, \theta_2 \in [0, \frac{\pi}{4}]$ (3.1) *and* $\theta_2 > \theta_1$ *such that* $|\psi_{\theta_1}\rangle$ *violates the inequality, that is* $Tr(|\Psi_{\theta_1}\rangle\langle\Psi_{\theta_1}|\,\hat{B}_{I^{\langle..\rangle}}) > g_{\text{loc}}$*. Then:*

$$Tr(|\Psi_{\theta_2}\rangle\langle\Psi_{\theta_2}|\,\hat{B}_{I^{\langle..\rangle}}) > Tr(|\Psi_{\theta_1}\rangle\langle\Psi_{\theta_1}|\,\hat{B}_{I^{\langle..\rangle}}). \tag{3.16}$$

In words, if a correlation Bell inequality $I^{\langle..\rangle}$ is violated by correlations generated when A and B measure the local observables $\{A_x\}$ and $\{B_y\}$ respectively on a pure partially entangled two qubit state $|\psi_{\theta_1}\rangle$, then the same inequality with the same measurements gives a strictly larger violation when acting on any other pure entangled two qubit state $|\psi_{\theta_2}\rangle$ with more entanglement $\theta_2 > \theta_1$.

Proof. Observe that $|\psi_\theta\rangle$ can always be written as

$$|\psi_\theta\rangle = \left(\tfrac{\cos\theta+\sin\theta}{\sqrt{2}}\mathbb{1} + \tfrac{\cos\theta-\sin\theta}{\sqrt{2}}\sigma_z\right) \otimes \mathbb{1}\,|\phi^+\rangle. \tag{3.17}$$

Denote by $\hat{B}_{I^{\langle..\rangle}}$ the Bell operator associated to the inequality $I^{\langle..\rangle}$ (3.14) for the given local measurements. Since the inequality $I^{\langle..\rangle}$ contains only full-body correlators, it does not involve marginal terms and thus the decomposition of the Bell operator $\hat{B}_{I^{\langle..\rangle}}$ in the Pauli basis does not contain terms proportional to $\mathbb{1}\otimes\mathbb{1}$, $\mathbb{1}\otimes\sigma_i$ and $\sigma_i\otimes\mathbb{1}$, for $i = x, y, z$. Using this fact and expression (3.17), the Bell violation for state (3.17), $b_\theta \equiv Tr(|\psi_\theta\rangle\langle\psi_\theta|\,|\hat{B}_{I^{\langle..\rangle}})$, reads

$$b_\theta = \frac{b_+ + b_-}{2} + \frac{\sin 2\theta}{2}(b_+ - b_-) > g_{\text{loc}}, \tag{3.18}$$

where $b_\pm \equiv \langle\phi^\pm|\hat{B}_{I^{\langle..\rangle}}|\phi^\pm\rangle$ denotes the expectation value of $\hat{B}_{I^{\langle..\rangle}}$ on the maximally entangled state $|\phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$.

By hypothesis we have that when $\theta = \theta_1$

$$b_{\theta_1} \equiv Tr(|\psi_{\theta_1}\rangle\langle\psi_{\theta_1}|\hat{B}_{I^{\langle..\rangle}}) > g_{\text{loc}}, \tag{3.19}$$

The term $\frac{b_+ + b_-}{2}$ can be understood (by linearity of the trace) as the expectation value of $\hat{B}_{I^{\langle..\rangle}}$ on the separable state

$$\frac{1}{2}(|00\rangle\langle00| + |11\rangle\langle11|) \tag{3.20}$$

and is thus necessarily smaller or equal to g_{loc}. But since $\sin 2\theta$ is positive for $\theta \in [0, \frac{\pi}{4}]$, Eq. (3.18) necessarily implies that $b_+ > b_-$. Now, because of this property and the fact that $\sin 2\theta$ is monotonically increasing for $\theta \in [0, \frac{\pi}{4}]$, the proof of the theorem follows. □

Put differently, the theorem shows that when using correlation Bell inequalities $\hat{I}^{\langle .. \rangle}$ (3.13) only to witness nonlocal correlations, the set of measurements $\mathcal{V}^{\langle .. \rangle}(|\psi_{\theta_1}\rangle)$ generating nonlocal behaviors when performed on $|\psi_{\theta_1}\rangle$ is included in the set of measurements $\mathcal{V}^{\langle .. \rangle}(|\psi_{\theta_2}\rangle)$ leading to nonlocal correlations when performed on any state $|\psi_{\theta_2}\rangle$ with more entanglement $\theta_2 > \theta_1$. This, in particular, implies that no anomaly can ever occur in these cases.

We now want to show that the inclusion relation $\mathcal{V}^{\langle .. \rangle}(|\psi_{\theta_1}\rangle) \subset \mathcal{V}^{\langle .. \rangle}(|\psi_{\theta_2}\rangle)$ is strict. In the setup with two measurement choice with two outcomes, the violation of the CHSH inequality

$$\langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle \leq 2 \tag{3.21}$$

is both necessary and sufficient for witnessing nonlocality in the correlation. In that scenario one can check that A and B measuring the following observables:

$$\begin{aligned} A_{x=0} &= \sigma_x \qquad & B_{y=0} &= \cos(\xi)\sigma_x + \sin(\xi)\sigma_z \\ A_{x=1} &= \sigma_z \qquad & B_{y=1} &= \cos(\xi)\sigma_x - \sin(\xi)\sigma_z \end{aligned} \tag{3.22}$$

with $\xi \in [0, \frac{\pi}{2}]$ on a pure two qubit state $|\psi_\theta\rangle$ (3.1) gives:

$$\text{CHSH}(\theta, \xi) = 2\Big(\sin(\xi) + \sin(2\theta)\cos(\xi) \Big) \tag{3.23}$$

which for $\theta = \frac{\pi}{4}$ and all $\xi > 0$ is larger than 2 (the local bound). Now, for another value of θ, the inequality is violated if

$$\sin(2\theta) > \frac{1 - \sin(\xi)}{\cos(\xi)} \tag{3.24}$$

implying in particular that for any $\theta_2 > \theta_1$ – i.e. $\sin(2\theta_2) > \sin(2\theta_1)$ – one can find an angle $\bar{\xi}$ such that $\text{CHSH}(\theta_2, \bar{\xi}) > 2$ but $\text{CHSH}(\theta_1, \bar{\xi}) \leq 2$. In the end, this allows us to conclude that the inclusion of sets is strict

$$\mathcal{V}^{\langle .. \rangle}(|\psi_{\theta_1}\rangle) \subset \mathcal{V}^{\langle .. \rangle}(|\psi_{\theta_2}\rangle), \tag{3.25}$$

Consequently, and in the spirit of definition (3.2), it follows that:

$$P_{\text{NL}}^{\langle .. \rangle}(|\psi_{\theta_1}\rangle) \leq P_{\text{NL}}^{\langle .. \rangle}(|\psi_{\theta_2}\rangle) \leq P_{\text{NL}}^{\langle .. \rangle}(|\phi^+\rangle), \tag{3.26}$$

where $P_{\mathrm{NL}}^{\langle \cdot,\cdot \rangle}(|\psi_{\theta_1}\rangle)$ is defined in the same fashion as in (3.2), but assuming that nonlocal correlations may only be witnessed by correlation inequalities. Crucially, and in sound contrast with previous works [LVB11; FP15; Ros+17], our results are valid for any number of measurement settings, and – interestingly – as well as for any measurement sampling in (3.2) (not only for the Haar measure). It is also worth noting that in many scenarios facet inequalities — those delimiting the local set $\mathcal{L}$ — are correlation inequalities, meaning that our result applies to a very broad class of inequalities [WW01b] in any scenario [Pir14; WW01a; Ban+09; Lia+15; CLG14].

Furthermore, our result enables us to draw conclusions beyond the fundamental study of the relation between entanglement and nonlocality. In a situation where one wants to check whether given measurements are useful to violate a correlation Bell inequality with two-qubit states, a necessary and sufficient condition is that they generate nonlocal correlations when performed on the maximally entangled state. Indeed, if the measurements do not generate nonlocality with the maximally entangled state, they will not generate nonlocality with any other less entangled state. What is more, since the maximally entangled state is the one with the highest probability to reveal nonlocality (up to any extend), it is the best choice to succeed in any Bell test using correlation inequalities and two-qubit states with poor control over the measurement bases. This is of particular interest for experimental setups where aligning reference frames is troublesome.

Before concluding, we would like to connect this result with previous works. Tsirelson showed that the maximal violation of a two-outcome correlation Bell inequality is obtained for a maximally entangled state [Tsi93]. However, this state is not necessarily of two qubits. In fact, there are known examples of two-outcome correlation Bell inequalities whose maximal violation requires systems of dimension larger than 2 [VP08]. When discussing qubits, the maximal violation of correlation Bell inequalities is obtained by a maximally entangled state, as the Bell operator is always diagonal in a given Bell basis. Recall, however, that this has a priori no implications for the nonlocal volume, as maximal violation and nonlocal volume are unrelated quantities. For example, the maximally entangled state does not give the maximal violation of the CGLMP inequality, but it does maximise the nonlocal volume. Note, however, that our theorem goes beyond proving that the maximal qubit violation is obtained by a Bell state: for fixed Schmidt bases, which do not necessarily coincide with those of the maximally entangled state providing the maximal qubit violation, the largest violation is obtained by a maximally entangled state.

3.5 Possible bipartite generalisations of the result

Our next objective is to discuss possible extensions of our result. In 3.4 we made three important assumptions: *i)* the Bell inequality is a correlation inequality, *i.e.* without marginal terms (single-body correlators), *ii)* only two-qubit pure states were considered, and *iii)* only extremal (thus projective) measurements were considered.

As far as assumption *i)* is concerned, a numerical search provided us with an analytical counter-example consisting of measurements generating correlations violating a Bell inequality when performed on $|\psi_\theta\rangle$ for $\theta = \frac{3\pi}{16}$ but generating local correlations when performed on $|\phi^+\rangle$ in the $[3,4,2,2]$ scenario. We verified that the violated Bell inequality indeed contains marginal terms $\langle A_x\rangle$ and $\langle B_y\rangle$ as expected. We refer the reader to A.1 for the exact construction. This counterexample closes the possibility to generalize our theorem onto general Bell inequalities including single-body correlators. Therefore, the sets $\mathcal{V}(|\psi_\theta\rangle)$ and $\mathcal{V}(|\phi_+\rangle)$ are not contained one into another and we can not conclude on the relation between $P_{NL}(|\psi_\theta\rangle)$ and $P_{NL}(|\phi^+\rangle)$ based on inclusion relations between these sets.

As it is impossible to prove an analog of our main theorem for general two-outcome Bell inequalities including marginals, we numerically computed the value of the nonlocal volume (3.2) for arbitrary two-qubit states and different Bell scenarios. In fig. 3.1, we provide numerical evidence for a wide range of scenarios that indicate that the probability of generating nonlocal correlations from random measurements is always the largest when measuring the maximally entangled state. We conjecture that the relation $P_{NL}(|\psi_\theta\rangle) \leq P_{NL}(|\phi^+\rangle)$ (3.2) holds in general. Note that similar numerical results were obtained in [Ros+17].

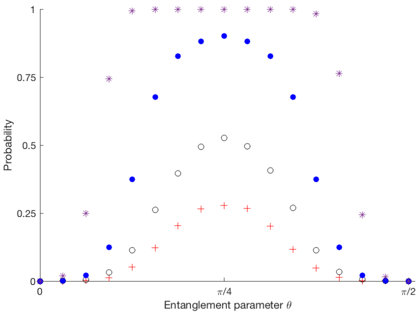

FIGURE 3.1: Probability of obtaining nonlocal correlations with uniformly random measurements as a function of the entanglement parameter θ. For clarity of the image the range of θ has been extended to $\frac{\pi}{2}$ due to symmetry of the state $|\psi_\theta\rangle$. Measurement scenarios: $(+)$ – [2,2,2,2], $(\circ)$ – [2,3,2,2], $(\bullet)$ – [3,4,2,2], $(*)$ – [8,8,2,2].

In order to relax assumption *ii)* one can study states in systems of arbitrary dimension $\mathbb{C}^d \times \mathbb{C}^d$. Note that in these systems, the ordering induced between entangled states is partial at the single-copy level, as there are pairs of states that can not be deterministically transformed one into another in either way by local operations and classical communication (LOCC) [Nie99]. So, it is unclear which entanglement quantifier would be a good candidate to be in correspondence with the nonlocal volume. The most natural candidate is the entanglement entropy, but it is a quantity that becomes especially relevant in the many-copy regime [PR97]. Despite all these issues, there is a clear notion of maximally entangled state. Thus, the most natural working conjecture is that this state maximizes the nonlocal volume. Numerical searches already performed in [Ros+17] indicate that this may be the case. More precisely, the authors considered states $\frac{1}{\sqrt{2+\gamma^2}}(|00\rangle + \gamma|11\rangle + |22\rangle)$ with parameter $\gamma \in [0,1]$ and found that the highest probability of obtaining nonlocality with randomly sampled measurements occurs for $\gamma = 1$. It is also interesting to consider weaker variants of this conjecture that may be easier to attack. For instance there is a notion of correlation function and correlation Bell inequality for scenarios involving measurements of more than two outputs [Col+02a; Sal+17]. Understanding whether Theorem 1 generalizes to this partial case deserves further investigation.

As for assumption *iii)*, extending our study to general measurements beyond projective is also interesting. Note, however, that in this case, it is less clear what the natural way of sampling measurements should be.

3.6 The nonlocal volume in the multipartite scenario

So far our analysis has focused on bipartite settings. Extending the problem to the multipartite case is also interesting and first numerical steps in this direction were presented in [Lia+10; Ros+17]. Here we provide the first analytical results. Note that in the multipartite case there is no notion of maximally entangled state [AVC03]. So it is not clear which state should be the natural candidate to maximise the nonlocal volume and it could even happen that the optimal state varies with the number of parties. In the following however we show that in a restricted multipartite scenario, it is possible to generalize our main result and conclude about the monotonicity of the measure for specific families of states and correlation Bell inequalities.

In a multipartite scenario, n parties share an entangled system of many particles (see more details in Sec. 2.3). Each party A_i, $i = 1, ..., n$, performs a local measurement on its share of the system with measurement choice labelled $x_i = 1, ..., m_{A_i}$ and (dichotomic) outcome $a_i = 0, 1$. As before, the measurements each party performs are described by a set of orthogonal projectors $\{M^{(i)}_{a_i|x_i}\}$, which generate joint conditional probabilities $P(\vec{a}|\vec{x}) \equiv \{p(a_1 \dots a_n | x_1 \dots x_n)\}$.

Then, $p(\vec{a}|\vec{x}) \equiv p(a_1 \ldots a_n|x_1 \ldots x_n) = Tr(M^{(1)}_{a_1|x_1} \otimes \ldots \otimes M^{(n)}_{a_n|x_n} \rho)$. As in the bipartite scenario, a Bell inequality is a linear combination of the probabilities $\hat{I}^{\langle n \rangle}(P(ab|xy)) \equiv \sum\limits_{a_1 \ldots a_n x_1 \ldots x_n} g^{x_1 \ldots x_n}_{a_1 \ldots a_n} p(\vec{a}|\vec{x})$ and corresponds to a Bell operator acting at the level of the states $\hat{B}_{I^{\langle n \rangle}} = \sum\limits_{a_1 \ldots a_n x_1 \ldots x_n} g^{x_1 \ldots x_n}_{a_1 \ldots a_n} M^{(1)}_{a_1|x_1} \otimes \ldots \otimes M^{(n)}_{a_n|x_n}$.

For two-outcome measurements only, we can define full-body correlators

$$\langle A_{x_1} \ldots A_{x_n} \rangle = \sum_{a_1 \ldots a_n = 0,1} (-1)^{\sum\limits_{i=1}^{n} a_i} p(\vec{a}|\vec{x}), \tag{3.27}$$

and a correlation inequality (inequality with n-body correlators)

$$I^{\langle n \rangle} = \sum_{x_1 \ldots x_n} \tilde{g}_{x_1 \ldots x_n} \langle A_{x_1} \ldots A_{x_n} \rangle. \tag{3.28}$$

As we mentioned, it is much harder in the multipartite setting to order (pure) states in terms of how entangled they are. To avoid the problem, we focus on a natural generalization of the bipartite pure states $|\phi_\theta\rangle$ (3.1)

$$|\Psi^n_\theta\rangle = \cos\theta |0\rangle^{\otimes n} + \sin\theta |1\rangle^{\otimes n}, \tag{3.29}$$

where θ is the entanglement parameter whose value runs again from 0 to $\pi/4$. The maximally entangled state of this family, with $\theta = \frac{\pi}{4}$, is the GHZ state $|\mathrm{GHZ}^n\rangle \equiv |\Psi^n_{\theta=\frac{\pi}{4}}\rangle$ as any other state in the family can be deterministically reached from it by LOCC.

We now generalize Theorem 1 to the multipartite setup for an even number of parties, correlation Bell inequalities and pure states in the GHZ family (3.29).

Theorem 2. *Consider a correlation Bell inequality $I^{\langle n \rangle} = \sum\limits_{x_1 \ldots x_n} \tilde{g}_{x_1 \ldots x_n} \langle A_{x_1} \ldots A_{x_n} \rangle \leq g_{\mathrm{loc}}$ with g_{loc} being the local bound. Assume that the number of parties n is even. Each party measures, locally, the observable $\{A^{(i)}_{x_i} \equiv M^{(i)}_{a_i=0|x_i} - M^{(i)}_{a_i=1|x_i}\}$, defining the associated Bell operator $\hat{B}_{I^{\langle n \rangle}} = \sum\limits_{x_1 x_2 \ldots x_n} g_{x_1 x_2 \ldots x_n} \otimes^n_{i=1} A^{(i)}_{x_i}$. For any two pure multipartite qubit states $|\Psi^n_{\theta_1}\rangle$, $|\Psi^n_{\theta_2}\rangle$ with $\theta_1, \theta_2 \in [0, \frac{\pi}{4}]$ (3.1) and $\theta_2 > \theta_1$, if $Tr(\left|\Psi^n_{\theta_1}\right\rangle\!\left\langle\Psi^n_{\theta_1}\right| \hat{B}_{I^{\langle \cdot \cdot \rangle}}) > g_{\mathrm{loc}}$ then:*

$$Tr(\left|\Psi^n_{\theta_2}\right\rangle\!\left\langle\Psi^n_{\theta_2}\right| \hat{B}_{I^{\langle n \rangle}}) > Tr(\left|\Psi^n_{\theta_1}\right\rangle\!\left\langle\Psi^n_{\theta_1}\right| \hat{B}_{I^{\langle n \rangle}}) \tag{3.30}$$

In particular, the theorem implies that if the state $|\Psi^n_{\theta_1}\rangle$ violates the Bell inequality when given measurements are being made on it, the state $|\Psi^n_{\theta_2}\rangle$ does so too with the same measurements.

Proof. The proof of the above statement follows the structure of the proof of Theorem 1. By assumption we have that

$$b^n_{\theta_1} \equiv Tr(|\Psi^n_{\theta_1}\rangle\langle\Psi^n_{\theta_1}|\,\hat{B}_{I^{\langle n\rangle}}) > g_{\text{loc}} \tag{3.31}$$

As before, we can write, without loss of generality, that

$$\begin{aligned}|\Psi^n_{\theta_1}\rangle = \left(\tfrac{\cos\theta_1+\sin\theta_1}{\sqrt{2}}\mathbb{1} + \tfrac{\cos\theta_1-\sin\theta_1}{\sqrt{2}}\sigma_z\right)\\ \otimes\underbrace{\mathbb{1}\otimes\ldots\otimes\mathbb{1}}_{n-1}|GHZ^n\rangle\end{aligned} \tag{3.32}$$

Now, the Bell operator can be decomposed in the Pauli basis as

$$\hat{B}_{I^{\langle n\rangle}} = \sum_{\mathbf{i}=1}^{3} c_{i_1\ldots i_n}\sigma_{i_1}\otimes\ldots\otimes\sigma_{i_N} \tag{3.33}$$

where σ_{i_j} denotes one of the Pauli operators $\sigma_x, \sigma_y, \sigma_z$ of j-th party. Note that the inequality $I^{\langle n\rangle}$ is a correlation inequality, therefore in the above decomposition (3.33) none of the operators σ_{i_j} can be $\mathbb{1}$. Using this fact and expression (3.32), the left hand-side of (3.31) can be written as

$$b^n_{\theta_1} = \frac{b^n_+ + b^n_-}{2} + \frac{\sin 2\theta_1}{2}(b^n_+ - b^n_-) > g_{\text{loc}}, \tag{3.34}$$

where $b^n_+ \equiv \langle GHZ^n|\hat{B}_{I^{\langle n\rangle}}|GHZ^n\rangle$ denotes the expectation value of $\hat{B}_{I^{\langle n\rangle}}$ on the maximally entangled GHZ state, and similarly $b^n_- \equiv \langle GHZ^n_-|\hat{B}_{I^{\langle n\rangle}}|GHZ^n_-\rangle$ for the GHZ state with a relative $-$ sign. Note that this decomposition holds if and only if the number of parties n is even – as it can be verified that all the cross terms involving $\underbrace{\mathbb{1}\otimes\sigma_{i_1}\otimes\ldots\otimes\sigma_{i_n}}_{n}$ disappear only when n is even.

Similarly to the proof of Theorem 1, observe that the term $\frac{b^n_+ + b^n_-}{2}$ from (3.34) is the expectation value of $\hat{B}_{I^{\langle n\rangle}}$ on a separable state, $\frac{1}{2}(|0\ldots0\rangle\langle0\ldots0| + |1\ldots1\rangle\langle1\ldots1|)$, and therefore it is necessarily smaller or equal to g_{loc}. Since by assumption $b^n_{\theta_1} > g_{\text{loc}}$, it follows that $b^n_+ > b^n_-$ since $\sin(2\theta_1) > 0$ for all $\theta_1 \in [0, \frac{\pi}{4}]$.

□

Interestingly, in the multipartite scenario the implications of Theorem 2 become richer than those of Theorem 1 in the bipartite scenario. Specifically, in the multipartite scenario there exist other notions of nonlocality, giving rise to a hierarchy of multipartite correlations as captured by notions such as k-producibility or correlation depth [Ban+09; CGL15]. Observe, however, that in the proof of Theorem 2 our derivation is independent of the type of multipartite nonlocality that is witnessed by the violation of a given correlation Bell inequality. This observation is possible due to the fact that the term $\frac{b_+^n - b_-^n}{2}$ in (3.34) is the expectation value of the inequality on a fully separable state $\frac{1}{2}(|0\dots0\rangle\langle0\dots0| + |1\dots1\rangle\langle1\dots1|)$. Hence, this term alone can not violate any Bell inequality as the generated correlations are (fully) local. Therefore, our theorem applies to any type of generalized multipartite nonlocality. In particular, if some measurements lead to k-partite nonlocal correlations violating a correlation Bell inequality when made on the state $|\Psi_{\theta_1}^n\rangle$, they also generate k-partite nonlocal correlations on any state $|\Psi_{\theta_2}^n\rangle$ with $\theta_2 \geq \theta_1$.

In light of the above theorem, when using correlation n-partite inequalities to witness nonlocality, for even n, the set of measurements leading to nonlocal behaviors when performed on $|\Psi_{\theta_1}^n\rangle$ is included in the set of measurements leading to nonlocal correlations when made on $|\Psi_{\theta_2}^n\rangle$ if $\theta_2 > \theta_1$. In particular, the set of measurements leading to nonlocal correlations on the maximally entangled state $|GHZ^n\rangle$ is the largest

$$\mathcal{V}_{\langle n\rangle}(|\Psi_\theta^n\rangle) \subseteq \mathcal{V}_{\langle n\rangle}(|GHZ^n\rangle). \tag{3.35}$$

where $\mathcal{V}_{\langle n\rangle}$ denotes the set of measurements leading to nonlocal behaviors exhibited with correlation inequalities. In the end, the nonlocal volume (3.2) is always maximised by the maximally entangled n-partite GHZ state (3.29)

$$P_{\langle n\rangle}(|\Psi_\theta^n\rangle) \leq P_{\langle n\rangle}(|GHZ^n\rangle). \tag{3.36}$$

Note that these results are consistent with the numerical findings of [Ros+17]. We leave open the problem of proving Theorem 2 for an odd number of parties.

3.7 Conclusions

The nonlocal volume is a measure of nonlocality with a clear operational meaning that seems to establish a one-to-one correspondence between maximal entanglement and maximal quantum nonlocality. Based on the existing results, it is tempting to conjecture that in bipartite systems the maximally entangled state maximizes the nonlocal volume, which would solve the anomaly observed between entanglement and nonlocality when using other measures. In our work, we provide the first analytical results in this direction. Solving the problem in full generality appears challenging because the nonlocal volume is a rather hard function to deal with. Beyond analytical results, it is also worth performing more numerical searches supporting the conjecture, by extending it to more complex scenarios involving more measurements, outputs, or non-projective measurements. The multipartite case is quite unexplored and also contains intriguing questions.

Before concluding, we would like to briefly mention that no anomalies can be seen in the case of steering, where one of the parties has control over the state received and over the measurements performed [WJD07; SNC14]. In this framework one can see that the set of measurements leading to steering on a partially entangled state is always included in the set of measurements doing the same on the maximally entangled one. This observation holds for any number of measurements, any type of measurements and any dimension d. In fact, the probability to violate a steering inequality is always 1 for any pure entangled states, since the set of compatible measurements has mesure zero and therefore random measurements always produce a violation of a steering inequality when performed on any pure entangled state [CS16].

Chapter 4

Unbounded randomness certification using sequences of measurements

When making single measurements on the parts of quantum systems at each round of a Bell experiment, only a limited amount of randomness can be certified from the generated outcomes. Indeed, from systems in an entangled states in an Hilbert space $|\psi\rangle \in \mathcal{H}^d \otimes \mathcal{H}^d$, one can hope to generate *at most* $r = 4\log_2(d)$ certified random bits, i.e. $r = 4$ bits from two qubits systems (see Sec. 2.4.2). Does this imply that there is a fundamental bound on the amount of certified randomness that can be generated from measurements on quantum systems?

In this chapter, we consider the scenario where one of the parties, B, performs sequences of measurements on the system it receives at each round of a Bell experiment as explained in Sec. 2.2.7. We show that the bounds on randomness from single measurements can be lifted and obtain *any* amount of certified random numbers from entangled pairs of qubits in a pure state. This is achieved by making sequences of weak measurements on one of the shares of each copy of the system. Moreover, the systems can be arbitrarily weakly entangled. The certification is achieved by near-maximal violation of a particular Bell inequality for each measurement in the sequence. Quantum systems in an almost separable state and of the lowest possible Hilbert space dimension – $d = 2$, i.e. two-qubit systems – are thus unbounded sources of certified random numbers and of nonlocal correlations in a sequence.

This chapter is based on the two articles [Cur+17; Cur+18].

4.1 Introduction

Imagine the following situation where, contrary to the device-independent approach that we follow in this thesis, one has perfect control over the functioning of the device generating randomness. An entangled state initially prepared in the Pauli-Z basis, i.e., a σ_z eigenstate $|0\rangle$ or $|1\rangle$, is measured in the Pauli-X, or σ_x basis $|\pm\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$. The outcome of this measurement is perfectly random and the post-measurement state is now one of the two eigenstates of the Pauli-X basis $|\pm\rangle$. If the device now measures this new state in the original Pauli-Z basis, the outcome of this new measurement is again random and one of the σ_z eigenstates is obtained. A device alternating between measurements in those two orthogonal basis thus allows one to obtain any amount of random bits from a single system as input.

Of course, this way of generating randomness can never be trusted, as one can always design a classical device (with deterministic outcomes – a local model) that has the same behavior as the device we described, i.e., their outputs are indistinguishable. To *certify* randomness one needs the generation of non-local correlations, that can not be simulated with classical resources. But is it nevertheless possible to use this idea of measuring a state repeatedly, in a scheme exploiting nonlocality, to obtain more random numbers and beat the bounds on randomness certification? Clearly, certifying more randomness by making sequences of measurements on the same state depends on whether one is able to produce sequences of non-local correlations between distant observers, as otherwise no additional randomness can be certified. One of the obstacles to this is that if local (projective) measurements are used to generate the non-local correlations, the entanglement in the state is destroyed. Then the post-measurement state is separable and thus cannot be further used to generate nonlocality or to certify randomness. A challenge is therefore to come up with measurements that do not destroy all the entanglement in the state but nevertheless generate non-local correlations. With such measurements the post-measurement state will still be a potential resource for the generation of more non-local correlations and certified randomness.

Bell tests with sequences of measurements have received less attention in the literature than the standard ones with a single measurement round despite the novel features in this scenario [Gal+14], as for example the phenomenon known as hidden nonlocality [Pop95] (for more details, see sec. 2.2.7). In our work we show that they prove useful in the task of randomness certification, which also provides another example [Ací+16] where general measurements can overcome limitations of projective ones, the first example of their usefulness in a DI information task. More precisely, we describe a scheme where any number m of random bits are certified using a sequence of $n > m$ consecutive measurements on the same system. This work thus shows that the bound of $4\log_2 d$ random bits in the standard scenario can be overcome in the sequential scenario, where it is impossible to establish any bound. The unbounded randomness is certified by a near-maximal violation of a particular Bell inequality for each measurement in the sequence. Moreover, for any finite amount of certified randomness, our scheme has a finite (yet very small) noise robustness. Our results show that entangled systems are an unbounded resource for the generation of certified random numbers and of non-local correlations in a sequence.

4.2 The sequential measurements scenario

Before presenting our results, let us remind the scenario we work in and that we developed in more details in sec. 2.2.7. We carry over many of the features from the standard scenario except that now we allow party B to make multiple measurements in a sequence on his share of the state. One can visualize this as in Fig. 4.1 where B is split up into several Bs, each one corresponding to a measurement made on the state and labeled by B_i, $i \in \{1,2,..,n\}$, where n is the total number of measurements made in the sequence. Each B_i makes one measurement and the post-measurement state is sent to B_{i+1}. We organize the Bobs such that B_i is doing his measurement *before* B_j for $i < j$. Thus in principle B_j can receive the information about the inputs and outputs of previous measurements B_i for all $i < j$(see fig. 4.1 and sec. 2.2.5).

They generate statistics from multiple runs of the experiment to obtain the observed probability distribution P_{obs} with elements $p_{\text{obs}}(a,\vec{b}|x,\vec{y})$. This distribution P_{obs} lives inside the set of quantum correlations Q_n^{sequ} obtained from measurements on quantum states in a sequence as we described. This set is convex and thus can be described in terms of its extreme points, denoted P_{ext}, and any P_{obs} can be written as $P_{\text{obs}} = \sum_{\text{ext}} q_{\text{ext}} P_{\text{ext}}$, where $\sum_{\text{ext}} q_{\text{ext}} = 1$ and every $q_{\text{ext}} \geq 0$.

4.3 Randomness certification: from the standard to the sequential scenario

As in the standard scenario with a single measurement in the sequence (see Sec. 2.4.2), one can quantify the amount of randomness in the set-up with sequences of measurements. From studying the outcome statistics *only* we can bound E's predictive power by allowing it to have complete knowledge of how P_{obs} is decomposed into extreme points, i.e., it knows the probability distribution q_{ext} over extreme points P_{ext}. This predictive power is quantified via the *sequential device-independent guessing probability* (DIGP) [AMP12] where we fix the particular input string $y_1^0, y_2^0, .., y_n^0 \equiv \vec{y}^0$ for which E has to guess the outputs $\vec{b}$. The sequential

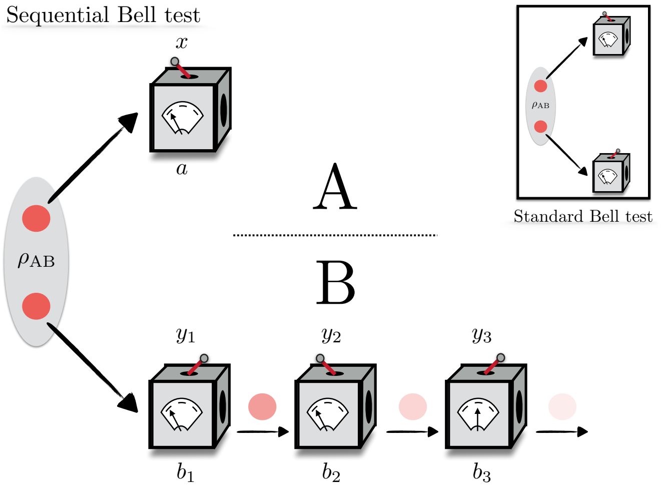

FIGURE 4.1: The standard scenario, where parties A and B make a single quantum measurement on their share of the state and discard it versus the sequential scenario where the second party B makes multiple measurements on his share.

DIGP, denoted by $G(\vec{y}^0, P_{\text{obs}})$, is then calculated as the optimal solution to the following optimization problem [Tor+15; NSPS14]:

$$G(\vec{y}^0, P_{\text{obs}}) = \max_{\{q_{\text{ext}}, P_{\text{ext}}\}} \sum_{\text{ext}} q_{\text{ext}} \max_{\vec{b}} p_{\text{ext}}(\vec{b}|\vec{y}^0)$$

subject to:

$$p_{\text{ext}}(\vec{b}|\vec{y}^0) = \sum_a p_{\text{ext}}(a, \vec{b}|x, \vec{y}^0), \qquad \forall x \tag{4.1}$$

$$P_{\text{obs}} = \sum_{\text{ext}} q_{\text{ext}} P_{\text{ext}}, \qquad P_{\text{ext}} \in \mathcal{Q}_n^{\text{sequ}}. \tag{4.2}$$

The operational meaning of this quantity is clear: E has a complete description of the observed correlations in terms of extreme points. It then guesses the most probable outcome for each extreme point. The standard scenario with a single measurement at each round $n = 1$ can also be represented in this formalism by simply considering that $\vec{b} = b$ and $\vec{y}^{(0)} = y^{(0)}$, recovering the standard non-sequential DIGP (2.53) of sec. 2.4.2. To quantify the amount of bits of randomness that is certified, we use the *min entropy* $H(\vec{y}^0, P_{\text{obs}}) = -\log_2 G(\vec{y}^0, P_{\text{obs}})$ which returns m bits of randomness if $G(\vec{y}^0, P_{\text{obs}}) = 2^{-m}$. The amount of bits of randomness quantified in this way is the figure of merit in this work and our goal is to obtain as many bits as possible from the systems.

Note that certifying randomness can be understood as splitting the rounds of the Bell experiment in two: $i)$ rounds that serve to build the statistics P_{obs} violating a

Bell inequality, their number depends on the quality of the estimate one desires to obtain; and $ii)$ rounds in which the outcomes serve to generate randomness. The rounds $i)$ serve to certify properties of the set-up through the study of the generated statistics, often by observing a given Bell inequality violation. In some sense, a given portion of the rounds is sacrificed to obtain a certificate that the outcomes from the rest of the rounds can indeed be used to generate random numbers. Here, we are interested in obtaining as much randomness from measurements on quantum systems when the round serves to generate randomness only. A more general approach would consist in studying how much randomness *on average* can be obtained from the outcomes by also taking into account the sacrificed rounds.

Before presenting proceeding further, it is worth explaining why the causal constraints imposed by the sequential scenario make it stronger than in a standard Bell experiment with one measurement in the sequence. At first sight, one could be tempted to group all the measurements in the sequence into a single box receiving an input string $\vec{y}_n$ to output another string $\vec{b}_n$, as in a standard Bell test. However, in general a sequence of measurements can not be represented as a single measurement. To understand this, note that in the sequential scenario the outcome b_i can depend only on variables produced in its past, namely the input choices $\vec{y}_i$ and the outcomes $\vec{b}_{i-1}$ that were *previously* obtained. However, a single measurement box instead of the sequence receives all inputs and produces all outputs at once. In particular, outcome b_i can now be a function of input choices $y_{j>i}$ and outcomes $b_{j>i}$ that are produced in the *future*. That is, such a big box may violate the physical constraints coming from the sequential arrangement and the assumption that signaling from the future to the past is impossible. These additional causality constraints further limit the adversary E's predictability with respect to a standard Bell test and are responsible for the unbounded amount of certified randomness.

An important part of this work is contained in the appendices B.1, where we develop a framework and tools for the study of the DIGP in a sequence and derive general properties of the guessing probability (4.2), summarised in the form of theorems 3 and 4. Let us stress here that these results are not limited to the guessing probability used in this work but are general properties of guessing probabilities. For the sake of simplicity, we give here a subset of these results only.

The remaining of this subsection is more technical and one can pass directly to subsection "Making non-destructive measurements on qubit states" 4.4 without loosing comprehension of the main results.

For a single measurement on each system (i.e. a sequence of $n = 1$ measurement), which corresponds to the standard Bell scenario and $\mathcal{Q} \equiv \mathcal{Q}_1^{\text{sequ}}$ the set of quantum correlations for a single measurement on each subsystem we have that:

Proposition 1. *The function $G(y^0, P_{obs})$ on the set of quantum distributions $\mathcal{Q}$ is continuous in the interior of $\mathcal{Q}$.*

Proposition 2. *The function $G(y^0, P_{obs})$ is continuous at any extremal point of $\mathcal{Q}$.*

The proofs of these two propositions are based mostly on general properties of concave functions [Roc70] and of concave roof extensions in particular [BL13], and can be found in section B.2 of the appendices. In other words the guessing probability for a single measurement is continuous everywhere except possibly at some points that lie on the surface of the quantum set but that are not extremal. An example of such a discontinuity can be obtained from the measurements described in [Pir+10] for a state with arbitrarily little entanglement. The joint conditional probability distribution (introduced below, see (4.6)) corresponding to those measurements made on such a state has $G(y^0, P_{obs}) = 1/2$ and is at the same time arbitrarily close to a joint conditional probability distribution corresponding to measurements on a product state with $G(y^0, P_{obs}) = 1$, i.e., a local point. The key is that this local point is not extremal, it lies somewhere on the surface of the local (and quantum) set but can be decomposed into other extremal (local) points, i.e. is not a vertex of the local polytope. Discontinuities of $G(y^0, P_{\text{obs}})$ can thus appear only at the boundary between extremal points and non-extremal points lying on the surface of the set, and in the rest of the set it is continuous.

In general – and in particular in our work – the optimization problem (4.2) can be relaxed to an optimization where instead of insisting on $P_{\text{obs}} = \sum_{\text{ext}} q_{\text{ext}} P_{\text{ext}}$ (4.2), one only imposes that the observed statistics P_{obs} give a particular Bell inequality violation [Pir+10]. The optimal solution to this new problem is an upper bound to the optimal solution of (4.2). Crucially, this relaxation often gives non trivial bounds as shown in our case for example. From now on, every time we refer to a guessing probability we refer to this relaxation of the problem to a particular Bell inequality violation.

Now, we consider a Bell expression I with its maximal value t_{max} on the quantum set $\mathcal{Q}$. We define the hyperplane H_t to contain the elements of $\mathcal{Q}$ for which the value of I is $t \leq t_{\text{max}}$ and further we define the restriction $G(y^0, P_{\text{obs}})_t$ of $G(y^0, P_{\text{obs}})$ to the intersection of H_t with $\mathcal{Q}$ and let $\max G(y^0, P_{\text{obs}})_t$ be the maximum of the guessing probability on this intersection. From Propositions 1 and 2 we can show that:

Theorem 3. *If the intersection of $H_{t_{max}}$ with $\mathcal{Q}$ is a single (thus extremal) point, there exists a $t_c < t_{max}$ such that $G(y^0, P_{obs})_t$ is a continuous function of t for $t_c \leq t \leq t_{max}$*

The proof of this theorem can be found in section B.3 of the appendices. In the other case, if the intersection of $H_{t_{\max}}$ with $\mathcal{Q}$ has more than one point, it also contains a set of non-extremal points of $\mathcal{Q}$ and therefore a discontinuity of $G(y^0, P_{\text{obs}})_t$ at $t_{\max}$ can not be ruled out by theorem (3). In other words, if the violation of a particular Bell inequality I is achieved by a unique quantum point (as for example the following (4.5)), the guessing probability close to that point is continuous.

Until now, we have considered the continuity properties of the guessing probability in the standard scenario with a single measurement in the sequence. We would like to extend those results to the guessing probability in the sequential measurement scenario with $n \geq 2$ measurements being made on the subsystems. Remember that we split party B into many B_i, so that party B_i makes the ith measurement on the system. The measurement setting of B_i is y_i and its outcome b_i (see Fig. 1). In our work, we will always take $y_i \in \{0, 1\}$ and $b_i \in \{0, 1\}$, but the following results can be generalized to any number of inputs and outcomes (they may even be different for each measurement in the sequence).

Consider the joint conditional probability distributions $P^i_{\text{obs}}(a, b_i | x, \vec{y}_i, \vec{b}_{i-1})$, $\vec{y}_i = y_1, y_2, ..., y_i$ and $\vec{b}_{i-1} = b_1, b_2, ..., b_{i-1}$, between A and each B_i. That is, the joint conditional probability distribution between A and B_i conditioned on what happened before the ith measurement, namely the input choices $\vec{y}_{i-1}$ and the outcomes $\vec{b}_{i-1}$ that were obtained *before* measurement i. There are n of those joint conditional probability distributions living in $\mathcal{Q}$ that can be obtained directly from the whole probability distribution for the sequence $P_{\text{obs}}(a\vec{b}|x\vec{y})$ living in $\mathcal{Q}_n^{\text{sequ}}$. Now suppose that we play, for each distribution $P^i_{\text{obs}}(a, b_i | x, \vec{y}_i, \vec{b}_{i-1})$, a Bell game I_i such that $I_i(P_i(a, b_i | x, \vec{y}_i, \vec{b}_{i-1})) = t_i \leq t_i^{\max}$, where $t_i^{\max}$ is the maximum of I_i over the set $\mathcal{Q}$.

Theorem 4. *Suppose that each joint conditional probability distribution $P^i_{obs}(a, b_i | x, \vec{y}_i, \vec{b}_{i-1})$ between A and B_i in the sequence is such that $I_i(P_i(a, b_i | x, \vec{y}_i, \vec{b}_{i-1})) = t_i$ and consider the limit where each $t_i \to t_i^{max}$. Suppose also that for each i, $G_i(y_i^0, P^i_{obs}(a, b_i | x, \vec{y}_i, \vec{b}_{i-1}))$ attains its smallest possible value at $t_i = t_i^{max}$. Then if the maximal value t_i^{max} of each I_i is achieved in a unique quantum point in $\mathcal{Q}$:*

$$G(\vec{y}^0, P_{obs}(a\vec{b}|x\vec{y})) \to \prod_{i=1}^{n} G_i(y_i^0, P^i_{obs}(a, b_i | x, \vec{y}_i, \vec{b}_{i-1})) \tag{4.3}$$

where $G_i(y_i^0, P^i_{\text{obs}}(a, b_i | x, \vec{y}_i, \vec{b}_{i-1}))$ is the (non sequential) relaxed guessing probability (4.2) of an adversary E trying to guess outcome b_i for input y_i^0 from the observed joint probability distribution $P^i_{\text{obs}}(a, b_i | x, \vec{y}_i, \vec{b}_{i-1})$). The proof of this theorem can be found in appendices B.4 and B.5. In other words, if each measurement in the sequence taken separately – thus not seen as in a sequence – leads to correlations close enough to the unique maximal violation of inequality I_i between A and B_i only, and if this maximal violation corresponds to the minimal possible guessing probability for b_i, then the guessing probability for the whole sequence tends to the product of the individual guessing probabilities of the outcomes b_i.

4.4 Making non-destructive measurements on qubit states

A and B share the two-qubit pure state (2.4)

$$|\psi(\theta)\rangle = \cos(\theta)|00\rangle + \sin(\theta)|11\rangle \tag{4.4}$$

that for all $\theta \in]0, \pi/4]$ is entangled. In Ref. [AMP12], a family of Bell inequalities was introduced:

$$I_\theta = \beta\langle\mathbb{B}_0\rangle + \langle\mathbb{A}_0\mathbb{B}_0\rangle + \langle\mathbb{A}_1\mathbb{B}_0\rangle + \langle\mathbb{A}_0\mathbb{B}_1\rangle - \langle\mathbb{A}_1\mathbb{B}_1\rangle \tag{4.5}$$

where $\beta = 2\cos(2\theta)/[1+\sin^2(2\theta)]^{1/2}$, $\langle\mathbb{B}_y\rangle = p(b=+1|y) - p(b=-1|y)$ and $\langle\mathbb{A}_x\mathbb{B}_y\rangle = p(a=b|xy) - p(a\neq b|xy)$ for x, $y \in \{0,1\}$. This family of inequalities has the following two useful properties: first, its maximal quantum violation, $I_\theta^{\max} = 2\sqrt{2}\sqrt{1+\beta^2/4}$, is obtained by measuring the state (4.4) with measurements:

$$\begin{aligned} \mathbb{A}_0 &= \cos\mu\,\sigma_z + \sin\mu\,\sigma_x, & \mathbb{B}_0 &= \sigma_z, \\ \mathbb{A}_1 &= \cos\mu\,\sigma_z - \sin\mu\,\sigma_x, & \mathbb{B}_1 &= \sigma_x, \end{aligned} \tag{4.6}$$

where $\tan\mu = \sin(2\theta)$. Second, when maximally violated, the inequality certifies one bit of local randomness on Bob's side for his second measurement choice $y^0 = 1$: $G(y^0 = 1, P_{\text{obs}}^{\max}) = 1/2$ [AMP12]. These observations are possible because the maximal violation is *uniquely* achieved by the probability distribution $P_{\text{obs}}^{\max}$ that arises from the previously-described state and measurements (4.4) and (4.6). Therefore, for the maximal violation, $P_{\text{obs}}^{\max} = P_{\text{ext}}$ in (4.2) and the guessing probability for input choice $y^0 = 1$ is equal to $1/2$.

However, as we said in general we may not get correlations that maximally violate our Bell inequality but give a violation that is only close to maximal. Nevertheless, using theorem 3 one gets that the guessing probability is a continuous function of the value of the inequality close to the maximal violation. This implies in the particular case we are studying that:

$$I_\theta \to I_\theta^{max} \quad \Rightarrow \quad G(y^0 = 1, P_{\text{obs}}) \to \frac{1}{2}. \tag{4.7}$$

In section 4.6, we also provide a numerical upper bound on the guessing probability $G(y^0 = 1, P_{obs})$ by a concave function of the value of I_θ.

Bell inequalities (4.5) are the first main ingredient in our sequential construction below. The second one is the use of general, non-projective measurements. Indeed, if B_1 performs a projective measurement on the shared entangled state, the resulting post-measurement state, now shared between Alice and B_2, is separable and thus useless for randomness production. Consequently, one needs to consider non-projective measurements to retain some entanglement in the system for the subsequent measurements. For this purpose, let us introduce the following two-outcome quantum measurement (written in the formalism of Kraus operators, see sec. 2.2.7 for more details):

$$M_{\pm 1}(\xi) = \cos\xi |\pm\rangle\langle\pm| + \sin\xi |\mp\rangle\langle\mp| \tag{4.8}$$

corresponding to the two outcomes $\{\pm 1\}$. This measurement $\hat{\sigma}_x(\xi) \equiv \{M_{+1}^\dagger M_{+1}, M_{-1}^\dagger M_{-1}\}$ can be understood as a generalization of the projective measurement σ_x. It varies from being projective (for $\xi = 0$) to being non-interacting (for $\xi = \pi/4$). One can verify that measuring an entangled state (4.4) for $\xi \in]0, \pi/4]$ (non-projective measurement) the post-measurement state still retains some entanglement, irrespectively of the outcome. Therefore, by tuning the parameter ξ we are able to vary the destruction of the entanglement of the state at the gain of extracting information from it: the closer to being a projective measurement, the lower the entanglement in the post-measurement state, but the bigger the violation of the initial Bell inequality.

4.5 A scheme for unbounded certified random numbers

We now combine the previous observations to demonstrate our main result. First, let us recall that, as shown in [AMP12], one can obtain one bit of randomness from any pure entangled two qubit state, irrespective of the amount of entanglement in it. Moreover, one can verify that approximately one random bit can be certified if the measurements are close to the ones in Eq. (4.6) (in the sense that $\hat{\sigma}_x(\xi)$ is close to a measurement of σ_x for $\mathbb{B}_1$ in Eq. (4.6)) since I_θ is then close to $I_\theta^{\max}$ in Eq. (4.7). Second, the measurement in Eq. (4.8) is only close to projective for ξ close to zero and leaves entanglement in the post-measurement state between Alice and Bob, which is thus still useful for randomness certification.

By repeated use of these two properties we can certify the production of an unbounded amount of random bits from a single pair of entangled qubits. We now formally describe this process in which Alice makes a single measurement on her share of the state, whereas Bob makes a sequence of n measurements on his.

Each B_i chooses between measurements of σ_z and $\hat{\sigma}_x(\xi_i)$ (4.8) for inputs $y_i = 0$ and $y_i = 1$, respectively, with outcomes $b_i \in \{\pm 1\}$. The parameter ξ_i is fixed before the beginning of the experiment. The initial entangled state shared between A and B, before B_1's measurement, is $|\psi^{(1)}(\theta_1)\rangle$ (see Eq. (4.4) with $\theta = \theta_1$). If the first non-projective measurement of the operator $\hat{\sigma}_x(\xi_1)$ is made by B_1 on the initial state $|\psi^{(1)}(\theta_1)\rangle$, the post-measurement state is of the form

$$|\psi^{(2)}_{b_1}(\theta_1,\xi_1)\rangle = U_A^{b_1}(\theta_1,\xi_1) \otimes V_B^{b_1}(\theta_1,\xi_1)(c|00\rangle + s|11\rangle), \tag{4.9}$$

where $c = \cos(\theta_{b_1}(\theta_1,\xi_1))$ and $s = \sin(\theta_{b_1}(\theta_1,\xi_1))$ and the two unitaries, $U_A^{b_1}(\theta_1,\xi_1)$ and $V_B^{b_1}(\theta_1,\xi_1)$, and angle $\theta_{b_1}(\theta_1,\xi_i) \in]0,\pi/4]$ depend on the first outcome b_1 and the angles θ_1 and ξ_1.

After his measurement, B_1 applies the unitary $(V_B^{b_1})^\dagger$, conditioned on his outcome b_1, on the post-measurement state going to B_2. This allows B_2 to use the same two measurements $\hat{\sigma}(\xi_2)$ and σ_z independently of the outcome b_1 since the unitary $(V_B^{b_1})$ is canceled in (4.9). This last procedure will be applied by each B_i after his measurement, before sending the post-measurement state to the next B_{i+1}. If the system passed through *only* the non-projective measurements, the state received by B_i can be one of 2^{i-1} potential states, depending on all of the previous B_j's ($j < i$) outcomes (one for each combination $\vec{b}_{i-1} \equiv (b_1, b_2, .., b_{i-1})$ of outcomes obtained by the previous B_j, these can be computed *before* the beginning of the experiment). Any of these states can be written as:

$$|\psi^{(i)}_{\vec{b}_{i-1}}\rangle = U_A^{\vec{b}_{i-1}} \otimes \mathbb{1}_B \left[\cos(\theta_{\vec{b}_{i-1}})|00\rangle + \sin(\theta_{\vec{b}_{i-1}})|11\rangle\right], \tag{4.10}$$

where the angles $\theta_{\vec{b}_{i-1}}$ and the matrix $U_A^{\vec{b}_{i-1}}$ both depend on the outcomes $\vec{b}_{i-1}$, on the initial angle θ_1 and the angles ξ_j of the previous B_j's with $j < i$. In the notation, we will always omit the dependence on the angles θ_1 and $\xi_1, \xi_2, .., \xi_j$ since these are fixed *before* the beginning of the experiment. For each of these different potential states with angle $\theta_{\vec{b}_{i-1}}$, Alice adds two measurements to her input choices, where for $k \in \{0,1\}$, these are measurements of the observables $\mathbb{A}_k^{\vec{b}_{i-1}}$ which are defined as

$$U_A^{\vec{b}_{i-1}} \left[\cos(\mu_{\vec{b}_{i-1}})\sigma_z + (-1)^k \sin(\mu_{\vec{b}_{i-1}})\sigma_x\right] (U_A^{\vec{b}_{i-1}})^\dagger, \tag{4.11}$$

where $\tan(\mu_{\vec{b}_{i-1}}) = \sin(2\theta_{\vec{b}_{i-1}})$, depending on the specific state $|\psi^{(i)}_{\vec{b}_{i-1}}\rangle$ (4.10).

We are now ready to describe how the scheme certifies randomness. The measurement operator $\hat{\sigma}_x(\xi_i)$ can be made arbitrarily close to σ_x by choosing ξ_i sufficiently small. This brings the outcome statistics for measurements $\hat{\sigma}_x(\xi_i), \sigma_z$ on Bob's side and $\mathbb{A}_0^{\vec{b}_{i-1}}, \mathbb{A}_1^{\vec{b}_{i-1}}$ on Alice's side on the state in Eq. (4.10), arbitrarily close to the statistics for the measurements in Eq. (4.6) and a state of the form in Eq. (4.4), for $\theta = \theta_{\vec{b}_{i-1}}$. Therefore, the inequality $I_{\theta_{\vec{b}_{i-1}}}$ for Alice and B_i as defined in (4.5) can be made arbitrarily close to its maximal violation. This in turn guarantees that the guessing probability, $G(y_i^0 = 1, P_{obs})$ can be made arbitrarily close to $1/2$. Note that this guessing probability does not only describe the instances when Alice chooses the measurements $\mathbb{A}_j^{\vec{b}_{i-1}}$. Since Eve does not know Alice's measurement choices in advance she cannot use a strategy that gives higher predictive power for the instances when Alice chooses other measurements. Finally, by making $G(y_i^0 = 1, P_{obs})$ sufficiently close to $1/2$ for each i (by choosing each ξ_i sufficiently close to 0) the DIGP $G(\vec{y}_n^0, P_{obs})$ can, by continuity, be made arbitrarily close to 2^{-n} (see appendices B.4 and B.5 for more formal proofs of these statements).

At the end, Bob can produce m random bits by a suitably chosen sequence $\hat{\sigma}_x(\xi_i)$, $i \in \{1,2,..,n\}$, of $n > m$ measurements. The certification only requires that each B_i occasionally chooses the projective measurement σ_z so that a good estimate of the whole statistics P_{obs} can be constructed. Note that Bob can choose σ_z with probability γ_i and $\hat{\sigma}_x(\xi_i)$ with probability $1 - \gamma_i$ for γ_i as close to zero as he wants. Finally, note that the value of *each* inequality $I_{\theta_{\vec{b}_{i-1}}}$ between each B_i and A can be made as close as wanted to the maximal value $I^{\max}_{\theta_{\vec{b}_{i-1}}}$. Therefore, we can certify randomness for each measurement B_i in the sequence at the expense of increasing the number of measurements that Alice chooses from.

This protocol can also be used to certify any finite amount of randomness with some small but strictly non-zero noise robustness. Indeed, assume the goal is to certify m random bits. One can then run the protocol for $m' > m$ bits. By continuity, when adding a small but finite amount of noise the protocol will certify m random bits. Of course, the noise robustness tends to zero with the number of certified random bits. However, we expect this to be the case for any protocol. This conjecture is based on the following argument: each measurement of a particle of finite dimension can produce only a finite amount of randomness. Thus, to get unbounded randomness, an infinite number of measurements are needed. Moreover, a measurement that is very close to non-interacting is unlikely to produce nonlocal correlations and is thus useless to certify randomness. It therefore appears quite likely that, in the infinite limit, any sequence of local measurements that are useful for randomness certification will destroy all the entanglement in the state, so that the resulting noise resistance tends to zero. We therefore expect that, while quantitative improvements over our protocol in terms of noise robustness can be expected, from a qualitative point of view it goes as far as possible.

4.6 Numerical bounds on the amount of violation of the family of Bell inequalities of [AMP12] and the certified randomness

Let us now explain some numerical results that should provide some quantitative intuition on the relation between the amount of violation of the family of inequalities (4.5) and the amount of random bits certified by this violation. This allows one to evaluate how close the value I_θ of the inequalities (4.5) should be to the maximal one I_θ^{max} in order to certify close to one perfect random bit from the statistics for one measurement $n = 1$.

Our numercial bounds apply to a larger family of Bell inequalities than the I_θ (4.5), namely the following two-parameter class of Bell inequalities:

$$I_{\alpha,\beta} := \beta\langle\mathbb{B}_0\rangle + \alpha(\langle\mathbb{A}_0\mathbb{B}_0\rangle + \langle\mathbb{A}_1\mathbb{B}_0\rangle) + \langle\mathbb{A}_0\mathbb{B}_1\rangle - \langle\mathbb{A}_1\mathbb{B}_1\rangle \leq \beta + 2\alpha \quad (4.12)$$

where $\alpha \geq 1$ and $\beta \geq 0$ such that $\alpha\beta < 2$. For $\alpha = 1$ the above class reproduces the family of Bell inequalities (4.5) with $\beta = 2\cos(2\theta)/[1+\sin^2(2\theta)]^{1/2}$. In [AMP12] it was proved that the maximal quantum value $I_{\alpha,\beta}^{\max}$ for these inequalities is given by:

$$I_{\alpha,\beta}^{\max} = \sqrt{(1+\alpha^2)(4+\beta^2)}. \quad (4.13)$$

Now, we conjecture that the following inequality is satisfied by $I_{\alpha\beta}$:

$$I_{\alpha,\beta}^2 + (2-\alpha\beta)^2\langle\mathbb{B}_1\rangle^2 \leq (1+\alpha^2)(4+\beta^2). \quad (4.14)$$

We have numerically evaluated this inequality for various values of α and β by maximizing its left-hand side over general one-qubit measurements $\mathbb{A}_i = \vec{m}_i \cdot \vec{\sigma}$ and $\mathbb{B}_i = \vec{n}_i \cdot \vec{\sigma}$ with $\vec{m}_i, \vec{n}_i \in \mathbb{R}^3$ such that $|\vec{m}_i| = |\vec{n}_i| = 1$ for $i = 0, 1$, and two-qubit pure entangled states that can always be written as

$$|\psi\rangle = \cos(\theta)|00\rangle + \sin(\theta)|11\rangle \quad (4.15)$$

with $\theta \in [0, \pi/2]$ now being independent of β. The obtained values were always smaller than or equal to the right-hand side of (4.14). Notice that in the case of Bell scenarios with two dichotomic measurements one can always optimize expression like the above one over qubit measurements and states (see e.g. Ref. [AMP12]).

From (4.14), it is easy to obtain an upper bound on the expectation value:

$$|\langle \mathbb{B}_1 \rangle| \leq \frac{\sqrt{(1+\alpha^2)(4+\beta^2) - I^2_{\alpha,\beta}}}{2-\alpha\beta} = \frac{\sqrt{(I^{\max}_{\alpha,\beta})^2 - I^2_{\alpha,\beta}}}{2-\alpha\beta}, \tag{4.16}$$

which, due to the fact that the right-hand side of the above is a concave function in $I_{\alpha,\beta}$, implies an upper bound on the guessing probability:

$$G(y^0 = 1, P_{obs}) \leq \frac{1}{2} + \frac{\sqrt{(I^{\max}_{\alpha,\beta})^2 - I^2_{\alpha,\beta}}}{2(2-\alpha\beta)} \equiv f(I_{\alpha\beta}). \tag{4.17}$$

In the particular case of maximal violation of the inequality $I_{\alpha\beta}$ (4.12) – which saturates inequality (4.14), this bound implies that the outcome of the first Bob's measurement is completely unpredictable, $G(y^0 = 1, P_{obs}) = 1/2$. Our numerical bound is thus tight at the maximal quantum violation of the inequality, but also when $I_{\alpha\beta}$ attains its classical value $2\alpha + \beta$, for which $G(y^0 = 1, P_{\text{obs}}) = 1$. In general, however, the bound (4.17) is not tight. Still, it provides a good bound on the guessing probability in terms of the amount of violation of $I_{\alpha\beta}$ (4.12) and thus also of the family of inequalities I_θ (4.5) we were using in our scheme.

Let us finally consider the case of $\alpha = 1$ and $\beta = 2\cos(2\theta)/[1+\sin^2(2\theta)]^{1/2}$, which results in the Bell inequality (4.5) considered in the main text. Figure 4.3 presents the bound (4.17) for three values of θ, in particular for $\theta = \pi/4$ which corresponds to the CHSH Bell inequality. This should provide one with an intuition of how close quantitatively to the maximal violation I_θ^{max} the observed value I_θ should be in order to get close to one perfect local bit of randomness ($G(y = 1, P_{obs}) \to 1/2$) for a state with a given angle θ.

4.7 The amount of certified randomness as a function of the strength of the measurement

In this section we analyse with the help of numerical tools the dependency of the certified randomness from the violation of the family of Bell inequalities (4.5) on the strength parameter ξ of the measurements $\hat{\sigma}_x(\xi) = cos(2\xi)\sigma_x$ (4.8). For example, what is the maximal value of the parameter ξ – i.e. the minimal strength of the

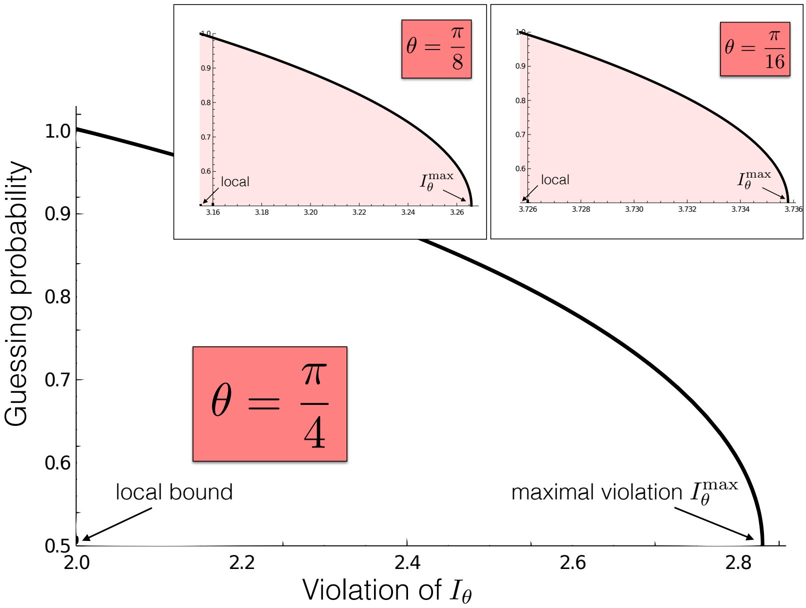

FIGURE 4.2: Our numerical upper bounds on the guessing probability in function of the violation of I_θ for $\theta = \frac{\pi}{4}, \frac{\pi}{8}, \frac{\pi}{16}$, where $I_{\theta=\frac{\pi}{4}} = \text{CHSH}$. One can see that these are tight both at the maximal violation of the inequality and at its local bound.

measurement –such that we can generate nonlocal correlations (and thus randomness) from this measurement on an entangled state of the form $|\psi(\theta)\rangle$ (4.4)? Do less entangled states need stronger measurement to unveil their nonlocal behaviour?

To answer these questions, we have been using semi-definite programming (SDP) techniques as explained in [BSS14; NSPS14] to obtain numerical upper bounds on the guessing probabilities (4.2). One can find the computational details – presented in a pedagogical way – online at `https://github.com/peterwittek/ipython-note` `blob/master/Unbounded_randomness.ipynb`. Here we work in the standard scenario with only one measurement $n = 1$ in the sequence. We used states of the form (4.4):

$$|\psi(\theta)\rangle = \cos(\theta)|00\rangle + \sin(\theta)|11\rangle \tag{4.18}$$

and measurements (4.6):

$$\begin{aligned} \mathbb{A}_0 = \cos\mu\,\sigma_z + \sin\mu\,\sigma_x, \qquad & \mathbb{B}_0 = \sigma_z, \\ \mathbb{A}_1 = \cos\mu\,\sigma_z - \sin\mu\,\sigma_x, \qquad & \mathbb{B}_1 = \hat{\sigma}_x(\xi) = cos(2\xi)\sigma_x, \end{aligned} \tag{4.19}$$

where $tan(\mu) = sin(2\theta)$. These measurements correspond to the ones in our scheme for an unbounded amount of randomness and where the second measurement $y = 1$ of B is the tunable version $\hat{\sigma}_x(\xi) \equiv \{M^{\dagger}_{+1}M_{+1}, M^{\dagger}_{-1}M_{-1}\}$ of Eq. (4.8):

$$M_{\pm 1}(\xi) = \cos\xi|\pm\rangle\langle\pm| + \sin\xi|\mp\rangle\langle\mp|, \tag{4.20}$$

with $\xi \in [0, \frac{\pi}{4}]$. For example, if the parameter $\xi = 0$, the four (projective) measurements in Eq. (4.19) on any quantum state $|\psi(\theta)\rangle$ with angle θ (4.18) generates a behavior P^{θ}_{obs} leading to the maximal violation of the inequality I_{θ} (4.5) for the same value of θ. This implies that extremal nonlocal correlations are generated and from the results of [AMP12] we know that one perfect random bit – equivalently $G(y^0 = 1, P^{\theta}_{obs}) = \frac{1}{2}$ – is produced. This corresponds to the strongest (projective) version of the measurements. Now, as we increase the parameter $\xi > 0$ of B's $y = 1$ measurement, $\hat{\sigma}_x(\xi)$ gets weaker, the generated correlations cease to be extremal and less than one random bit is produced. At some point, at a particular value $\xi^{\theta}_{\max}$ the measurement of B is so weak that we expect the generated correlations to become local. This exact value might depend on the amount of entanglement θ in the state. The bounds obtained by SDP indicate that this dependency on the angle θ of the maximal value $\xi^{\theta}_{\max}$ is unexpectedly small. As we vary the angle θ, the minimal required strength of the measurement to generate a nonlocal behavior P^{θ}_{obs} stays within a narrow interval: $\xi^{\theta}_{\max} \in [0.519, 0.576]$ for $\theta \in [\frac{\pi}{32}, \frac{\pi}{4}]$. Nevertheless, as ξ increases the lower bounds on the certified randomness rapidly decreases, with a more rapid decrease for smaller θ.

One can find our results in the form of a graph Fig.4.3. A complete tables with our results for the different states and bounds on the guessing probabilities can be found in the appendices B.6.

In the end, we are interested primarily in the amount of certified randomness from P^{θ}_{obs} *close to* the maximal violation of I_{θ}, corresponding to $\xi \to 0$. There, the SDP solutions indicate that the correlations resisting the best to the weakening of the measurement $\xi > 0$ are the ones coming from the measurements made on the maximally entangled state. Indeed, if the bounds are close to the actual values of certified randomness it is quite clear from the numerical results that the more the state is entangled ($\theta \to \frac{\pi}{4}$) the better it resists. The less entangled states ($\theta \to 0$) appear to generate exponentially less randomness when the parameter ξ increases, or equivalently when the correlations cease to be extremal. This tells us that even though our scheme certifies an unbounded amount of randomness from states $|\psi(\theta)\rangle$ with any nonzero amount of entanglement, i.e. any $\theta > 0$, it is preferential from a practical point of view to use the maximally entangled state as the initial state.

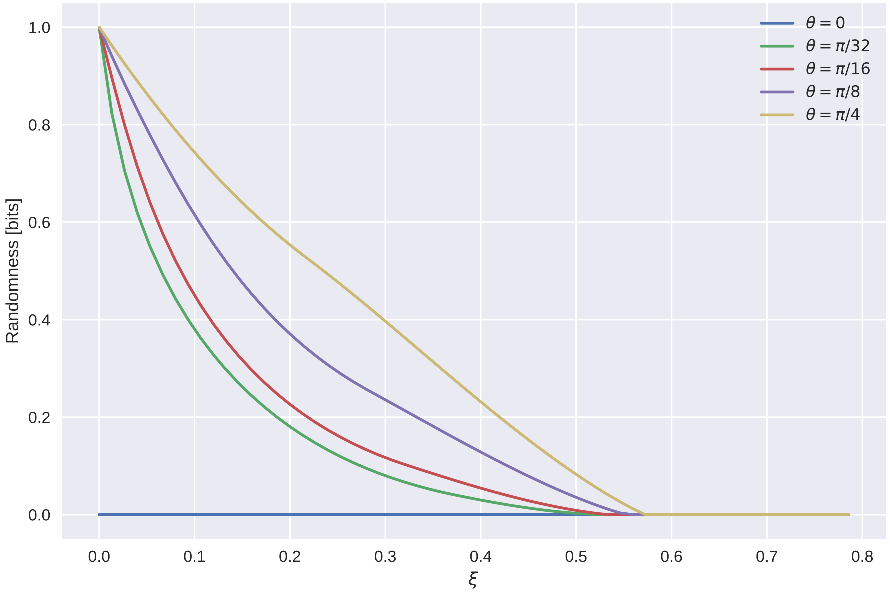

FIGURE 4.3: Lower bounds on the amount of randomness certified from the quantum state (4.4) with angles $\theta = 0, \frac{\pi}{32}, \frac{\pi}{16}, \frac{\pi}{8}, \frac{\pi}{4}$ as function of the strength of the measurement ξ. The measurement is projective for $\xi = 0$ – which certifies the maximal amount of randomness – and is non interacting with the system when $\xi = \frac{\pi}{4}$. It is intriguing to see that for the cases of $\frac{\pi}{32} \leq \theta \leq \frac{\pi}{4}$ considered the generated behavior become local in a small interval $\xi_{\max} \in [0.519, 0.576]$.

4.8 Conclusion

We have presented a scheme for certifying an unbounded amount of random bits from pairs of entangled qubits in the scenario where one of the qubits is subjected to a sequence of measurements. The measurements do not completely destroy the entanglement but map the state to another pure entangled two-qubit state (with reduced entanglement). Our main result made use of the fact that every measurement in Bob's sequence generated an almost-maximally non-local output distribution (in the sense of violating some Bell inequality almost maximally). In Ref. [Sil+15], a sequence of non-local correlations is obtained from pairs of qubits, showing that the nonlocality of a state can be shared between many parties. While it also considers sequences of measurements, one can show that the correlations obtained in their work do not generate more certified randomness than the simple standard single measurement scenario. Indeed, the maximum of randomness is achieved when all but one measurements do not interact with the particle and their scheme is thus optimal when coinciding with a single measurement one. In our work, we overcome this limitation by producing (almost) extremal correlations for each measurement in the sequence, which is a fundamental property of potential further use for many other device-independent quantum information tasks (in particular for randomness certification). Our work is in many respects a proof-of-principle result: First, it requires an exponentially increasing number of measurements on Alice's side, namely $\sum_{i=1}^{n} 2^i = 2(2^n - 1)$ measurement choices for n measurements in the sequence. Second, the result is based on a continuity argument and there is no control on the noise robustness. All these issues deserve further investigation. Finally, it is worth exploring how to design device-independent randomness generation protocols involving sequences of measurements. However, the sequential scenario is much more demanding from an implementation point of view, because it requires quantum non-demolition measurements. It is then unclear whether with present or near future technology sequential protocols will provide a significant practical advantage over simpler protocols based on standard Bell tests. However, the first experimental works observing non-local correlations in the sequential scenario have recently been reported [Sch+17; Hu+16]. In any case, the main implications of our work are fundamental: It shows that pairs of pure entangled qubits are potentially unbounded sources of certifiable random bits when performing sequences of measurements on it.

We have also provided numerical results that gives us an insight on the resistance to imperfections of a potential protocol that implements our scheme. For a single measurement in the sequence, we have given numerical bounds on how the certified randomness diminishes as the generated correlations cease to be extremal. Second, we have also explored how the certified randomness diminishes when the strength of the measurement is lowering. This allows us to expect that any potential protocol trying to implement our scheme for a finite amount of randomness starting from an entangled system has an advantage in using the maximally entangled one. It is clear from our numerical results that this state offers the best resistance to imperfections. So, while it is true that even arbitrarily little entangled states are a source of unbounded certified randomness, more entanglement offers an advantage in terms of resistance to imperfections.

It would also be interesting to explore whether an unbounded amount of randomness can be obtained versus a post-quantum adversary E, only constrained by the no-signaling condition, trying to guess the outcomes of the measurements. Or, on the contrary, is the amount of certified randomness against no-signaling adversaries bounded also in the sequential scenario? Our conjecture is that the amount of randomness that can be certified is limited in this case. Indeed, the fact that the no-signaling set – consisting of all correlations constrained only by the no-signaling conditions – does not have a continuous set of extremal points (it is a polytope) makes it impossible to obtain a sequence of extremal probability distributions in a sequence as the one that we could obtain in the quantum case. A different approach thus needs to be taken. It is really the fact that the quantum set has curved boundaries made of extremal quantum behaviours that allowed to derive the results of this chapter.

Chapter 5

A simple approach to genuine multipartite nonlocality of pure states

In this chapter, we study the relation between the different notions of multipartite entanglement and multipartite nonlocality. In particular, we focus on the equivalence between genuine multipartite entanglement (GME) and genuine multipartite nonlocality (GMNL) for pure states. From an operational understanding of multipartite (pure state) entanglement, we develop a method to construct simple families of Bell inequalities witnessing different types of multipartite nonlocality. We show, analytically, that our families witnessing GMNL are violated by large classes of GME pure states for any number of parties. In particular, even GME states that are almost separable can violate our inequalities for any number of parties. In the tripartite scenario, we show analytically that all three-qubit systems in a GME pure state, that is symmetrical to the permutation of two of the three parties, violate a single Bell inequality witnessing GMNL. Complementary to our analytical results, numerical evidence is provided that all three and four partite qubit systems in a GME pure state also violate a single of our inequalities and are hence GMNL.

These results, together with the operational meaning of our inequalities, lead us to conjecture that our families of Bell inequalities can be used to show that all GME pure states display GMNL.

The work exposed in this section is based on [CAA18].

5.1 Introduction

Nonlocal correlations have been extensively studied in the simplest scenario of bipartite systems (see Sec. 2.2), which is sufficient to obtain powerful resources for information tasks with no classical equivalent (see Sec. 2.4). Multipartite scenarios

– consisting of set-ups with at least three parties – have received far less attention due to their greater complexity. They offer, however, a much richer source of correlations than the bipartite set-up, and have already been proven useful for several tasks [Sve87; SS02; Gal+12; Ban+13; Ban14a; Gal+13; Ban14b; Bou+14; Tur+14]. For more details on the multipartite scenario, see Sec. 2.3. Either for a better use of the potential provided by multipartite systems, which might be particularly interesting for tasks on quantum networks, or simply to explore scenarios that go beyond the standard bipartite set-up, the study of multipartite scenarios is nowadays a central problem.

Two-particle systems in a pure quantum state display a straighforward relation between entanglement and nonlocality: all pure entangled two-particle states are nonlocal [Gis91]. This result has been extended to the multipartite scenario [PR92; GG16], with the caveat that the used definitions of entanglement and nonlocality only require two parties of the multipartite system to be non-classically correlated. In order to grasp the full potential of many-body systems, it is necessary to consider genuinely multipartite definitions of entanglement and nonlocality, where all the parties of a system are engaged, instead of only subsets of them. *Genuine multipartite entangled (GME)* states (2.39) are necessary to generate *genuine multipartite nonlocal (GMNL)* correlations (2.46) (see more details in Sec. 2.3). It is a long-standing open question whether entanglement in pure states is sufficient to observe nonlocality, in the genuinely multipartite sense. Can all pure GME states generate GMNL correlations, for any number of particles? So far, it is known that this holds for systems of three particles in a pure GME state [YO13; Che+14]. This result relies, however, on the use of genuine tripartite Hardy-type paradoxes [Har93], which have the drawback of not allowing for experimental realisations, contrary to nonlocal correlations detected by the violation of a Bell inequality[1].

In this work, we make steps forward to prove the equivalence between GME of pure states and GMNL in full generality. To do so, we develop a technique to build families of Bell inequalities that witness GMNL for any number of observers. These families of Bell inequalities have a very clear operational meaning and capture essential features of multipartite nonlocality. We show analytically that a large class of GME pure states violate our inequalities for any number of parties, even states that are almost separable. In the tripartite scenario, we also show that almost

[1] Contrary to the violation of a Bell inequality, the realisation of a Hardy-type paradox relies on strong conditions of the form $P(ab|xy) = 0$ for some values of a, b, x, y. Such conditions are impossible to meet in an experiment, where even the smallest imperfections lead to values $P(ab|xy) = \epsilon > 0$. Realisations that are close to the optimal ones of a Hardy paradox are likely to remain nonlocal, but will further require the use of a Bell inequality as witness. It is moreover unclear which Bell inequality should be used in that case.

all GME pure state violate our inequalities. We extend these analytical results by providing numerical evidence that all three-qubit and four-qubit systems in a GME pure state violate our inequalities. The strength of our construction to detect the multipartite nonlocality generated from pure states – in addition to the strong operational meaning of our construction – lead us to conjecture that one of our family of Bell inequalities can be used to generalise Gisin's theorem: all GME pure states are GMNL.

Finally, we extend our results to the richer notions of multipartite nonlocality as captured by the notion of $m-$way (non)locality (see Sec. 2.3.2).

5.2 The tripartite scenario

We are here interested in genuinely multipartite definitions of entanglement and nonlocality (2.39), (2.46), which we recall here briefly for the sake of clarity. As first noticed by Svetlichny [Sve87], distributions generated in a tripartite scenario lead to stronger notions of nonlocality. Consider for instance a relaxation of the locality assumption, where pairs of parties are now allowed to group together and share nonlocal resources. This type of hybrid local/nonlocal models leads to joint conditional probability distributions

$$\begin{aligned} & P_{2/1}(a_1a_2a_3|x_1x_2x_3) = \\ = & \sum_{\lambda_1} q_1(\lambda_1)P_{A_1A_2}(a_1a_2|x_1,x_2,\lambda_1)P_{A_3}(a_3|x_3,\lambda_1) \\ + & \sum_{\lambda_2} q_2(\lambda_2)P_{A_1A_3}(a_1a_3|x_1,x_3,\lambda_2)P_{A_2}(a_2|x_2,\lambda_2) \\ + & \sum_{\lambda_3} q_3(\lambda_3)P_{A_2A_3}(a_2a_3|x_2,x_3,\lambda_3)P_{A_1}(a_1|x_1,\lambda_3) \end{aligned} \tag{5.1}$$

with $q_i(\lambda_i) \geq 0$ and $\sum\limits_{i,\lambda_i} q_i(\lambda_i) = 1$. Distributions $P(a_1a_2a_3|x_1x_2x_3)$ that cannot be decomposed in the form (5.1) are named *genuine tripartite nonlocal*. Remember that the choice of nonlocal resource inside a group of parties leads to different definitions of genuine multipartite nonlocality (see Sec. 2.3.2). As explained, in this thesis the distributions $P_{A_iA_j}(a_ia_j|x_i,x_j,\lambda)$ satisfy the no-signalling principle [PR94], which implies that the marginals $P(a_i|x_i,\lambda) = P(a_i|x_i,x_j,\lambda) = \sum_{a_j} P(a_ia_j|x_ix_j,\lambda)$, $\forall x_j$, are well defined for all λ.

A system of three particles is said to be in a genuine tripartite entangled pure state if it can not be decomposed as $|\psi_{123}\rangle = |\phi_{ij}\rangle|\phi_k\rangle$, where ijk is any combination of the particles (2.39). One can easily verify that local measurements on biseparable states always lead to a hybrid joint distribution (5.1).

In the bipartite scenario, when each party have two choices of two-outcome measurements, i.e. $x_i, a_i \in \{0,1\}$ for $i = 1,2$, the violation of the CHSH inequality is both necessary and sufficient for $P(a_1a_2|x_1x_2)$ to be nonlocal [Chs; Fro81; Fin82]. This is also the inequality used to show that all pure states of two particles are nonlocal [Gis91]. Here we write a variation of the CHSH inequality,

$$I^{A_1A_2} = P(00|00) - P(01|01) - P(10|10) - P(00|11) \leq 0 \tag{5.2}$$

which is equivalent to the standard expression

$$\text{CHSH} = \langle A_0B_0\rangle + \langle A_1B_0\rangle + \langle A_0B_1\rangle - \langle A_1B_1\rangle \leq 2 \tag{5.3}$$

for no-signaling distributions and where $\langle A_xB_y\rangle = \sum_{ab} P(a = b|xy) - P(a \neq b|xy)$.

5.3 Bell inequalities witnessing genuine tripartite nonlocality

Our two inequalities witnessing genuine tripartite nonlocality use CHSH inequalities (5.2) as building blocks and can be written as

$$I^{A_1A_2A_3}_{\text{sym}} = I^{A_1A_2}_{0|0} + I^{A_1A_3}_{0|0} + I^{A_2A_3}_{0|0} - P(000|000) \leq 0 \tag{5.4}$$

$$I^{A_1A_2A_3}_{①} = I^{A_1A_2}_{0|0} + I^{A_1A_3}_{0|0} - P(000|000) \leq 0 \tag{5.5}$$

and where

$$\begin{aligned} I^{A_1A_2}_{0|0} \equiv P(000|000) - P(010|010) - P(100|100) \\ -P(000|110) \end{aligned} \tag{5.6}$$

is a *lifting* [Pir05] of the inequality $I^{A_1A_2}$ to the tripartite scenario, by setting observer A_3 to measurement $x_3 = 0$ and outcome $a_3 = 0$. Lifted inequalities $I^{A_1A_3}_{0|0}$ and $I^{A_2A_3}_{0|0}$ are built in a similar way. Note that the local bound of the lifted inequalities is the same as the original one, $I^{A_iA_j}_{0|0} \leq 0$. See Appendix C.1 for more details on lifted Bell inequalities. Inequality $I^{A_1A_2A_3}_{\text{sym}}$ belongs to class 6 of [Ban+13], where strong numerical evidence was provided indicating that all 3-qubit systems in a GME pure state could generate distributions violating it. Although we already know from [Ban+13] that this inequality detects genuine tripartite nonlocality, we present here a proof that will be useful for understanding the generalisation to n parties.

Theorem 5. *The Bell inequalities $I_{sym}^{A_1A_2A_3}$ (5.4) and $I_{①}^{A_1A_2A_3}$ (5.5) are witnesses of genuine tripartite nonlocality.*

Proof. We want to show that any hybrid distribution (5.1) satisfies $I_{\text{sym}}^{A_1A_2A_3} \leq 0$ and $I_{①}^{A_1A_2A_3} \leq 0$, hence only genuine tripartite nonlocal correlations can violate these inequalities. A basic element of our proof if that

$$I_{0|0}^{A_iA_j}\left(P_{A_jA_k}(a_ja_k|x_jx_k)P_{A_i}(a_i|x_i)\right) \leq 0 \tag{5.7}$$

for any triplet $i,j,k \in \{1,2,3\}$ with $i \neq j \neq k \neq i$ and for any extremal hybrid distribution $P_{A_jA_k}(a_ja_k|x_jx_k)P_{A_i}(a_i|x_i)$. This comes from the fact that the (lifted) inequality $I_{0|0}^{A_iA_j}$ can only be violated if parties A_i and A_j are non-classically correlated, which is not the case when the correlations allow for a decomposition of the form $P_{A_jA_k}(a_ja_k|x_jx_k)P_{A_i}(a_i|x_i)$. Also notice that

$$\begin{aligned}\bar{I}_{0|0}^{A_iA_j} \equiv & I_{0|0}^{A_iA_j} - P(000|000) = \\ = -P(010|010) - & P(100|100) - P(000|110) \leq 0\end{aligned} \tag{5.8}$$

holds for any normalised probability distribution (that is, even a post-quantum one). For completeness, in Appendix C.1 we add a brief review on lifting Bell inequalites and in particular a rigorous proof of statement (5.7).

We now first expose the proof for $I_{\text{sym}}^{A_1A_2A_3}$ and notice that the inequality is invariant under permutations of parties. This, together with the convexity of (5.1) allows us to restrict, without loss of generality, to show that

$$I_{\text{sym}}^{A_1A_2A_3}(P_{A_1A_2}(a_1a_2|x_1x_2)P_{A_3}(a_3|x_3)) \leq 0 \tag{5.9}$$

Now, for correlations $P_{A_1A_2}(a_1a_2|x_1x_2)P_{A_3}(a_3|x_3)$ we have that $I_{0|0}^{A_1A_3} \leq 0$ and $I_{0|0}^{A_2A_3} \leq 0$ from (5.7). Therefore,

$$I_{\text{sym}}^{A_1A_2A_3}(P_{A_1A_2}(a_1a_2|x_1x_2)P_{A_3}(a_3|x_3)) \leq I_{0|0}^{A_1A_2} - P(000|000) = \bar{I}_{0|0}^{A_1A_2} \leq 0 \tag{5.10}$$

which ends the proof for the symmetrical family $I_{\text{sym}}^{A_1A_2A_3}$.

The proof for the second family $I_{\textcircled{1}}^{A_1A_2A_3}$ follows the same steps as for the symmetrical $I_{\text{sym}}^{A_1A_2A_3}$ one. This time, since the inequality is not invariant under permutations of parties we need to prove that

$$I_{\textcircled{1}}^{A_1A_2A_3}(P_{A_iA_j}(a_ia_j|x_ix_j)P_{A_k}(a_k|x_k)) \leq 0 \tag{5.11}$$

for any hybrid correlations $P_{A_iA_j}(a_ia_j|x_ix_j)P_{A_k}(a_k|x_k)$. Now, since (5.7) and (5.8) hold for any combination of the three parties

$$I_{\textcircled{1}}^{A_1A_2A_3}(P_{A_iA_j}(a_ia_j|x_ix_j)P_{A_k}(a_k|x_k)) \ \leq \ I_{0|0}^{A_iA_j} - P(000|000) \ = \ \bar{I}_{0|0}^{A_iA_j} \ \leq \ 0 \tag{5.12}$$

This finishes the proof for the second family $I_{\textcircled{1}}^{A_1A_2A_3}$. □

Notice that the idea behind our construction can be extended to build a two parameter family of inequalities that also witness genuine multipartite nonlocality between three parties

$$I_{\mu,\nu}^{A_1A_2A_3} = I_{0|0}^{A_1A_2} + \mu I_{0|0}^{A_1A_3} + \nu I_{0|0}^{A_2A_3} - P(000|000) \leq 0 \tag{5.13}$$

for $\mu, \nu \in [0,1]$[2]. Indeed, one can use property (5.7) as in the proof of Theorem 5 to see that (5.13) holds

$$I_{\mu,\nu}^{A_1A_2A_3}(P_{A_iA_j}(a_ia_j|x_ix_j)P_{A_k}(a_k|x_k)) \leq I_{0|0}^{A_iA_j} - P(000|000) = \bar{I}_{0|0}^{A_iA_j} \leq 0 \tag{5.14}$$

It is interesting to observe that the local strategy where every party always obtains outcome $a_i = 1$ for any measurement x_i saturate both inequalities $I_{\textcircled{1}}^{A_1A_2A_3} = 0$ and $I_{\text{sym}}^{A_1A_2A_3} = 0$. This implies that the local and hybrid bounds of our inequalities coincide.

We now use the non symmetrical family of inequalities $I_{\textcircled{1}}^{A_1A_2A_3}$ (5.5) to show that a very large class of three-qubit *GME* pure states are GMNL. In [Ací+00], it was shown that all systems of three qubits in a pure state could be written as

$$|\Psi_3\rangle = h_0|000\rangle + h_1e^{i\phi}|100\rangle + h_2|101\rangle + h_3|110\rangle + h_4|111\rangle \tag{5.15}$$

where $h_i \in \mathbb{R}_+$, $\sum\limits_i h_i^2 = 1$ and $\phi \in [0,\pi]$.

[2] Note that the combination $\mu = \nu = 0$ is not a Bell inequality any more.

Theorem 6. *For all tripartite pure states* (5.15) *that are GME and for which $h_2 = h_3$ – i.e. that are symmetrical with respect to permutation of two parties among the three $A_2 \leftrightarrow A_3$*[3] *– one can find measurements such that the generated correlations violate inequality $I_{①}^{A_1A_2A_3} > 0$* (5.5)*, hence generating GMNL correlations.*

Proof. The full proof of theorem 6 can be found in appendix C.4. The main line of it goes as follows. Both the (projective) measurements of parties A_2 and A_3 are chosen to be the same $\langle m_{a_2|x_2}| = \langle m_{a_3|x_3}|\ \forall a_2 = a_3$ and $x_2 = x_3$. This makes the whole correlations $P(a_1a_2a_3|x_1x_2x_3)$ symmetrical with respect to the permutation $A_2 \leftrightarrow A_3$ too as both the state and the measurements used are. This symmetry also implies that the two prepared states $|\psi_{0|0}^{A_1A_2}\rangle = |\psi_{0|0}^{A_1A_3}\rangle$ are the same, where the state $|\psi_{0|0}^{A_1A_2}\rangle$ between A_1 and A_2 is the state prepared by party A_3 making the projection $\langle m_{a_3=0|x_3=0}|$ on $|\Psi_3\rangle$ (5.15)

$$|\psi_{0|0}^{A_1A_2}\rangle \propto \mathbb{1}_{A_1} \otimes \mathbb{1}_{A_2} \otimes \langle m_{a_3=0|x_3=0}||\Psi_3\rangle \tag{5.16}$$

and similarly for $|\psi_{0|0}^{A_1A_3}\rangle$. So far, we can always tune the measurements $\langle m_{a_2=0|x_2=0}| = \langle m_{a_3=0|x_3=0}|$ such that the prepared states $|\psi_{0|0}^{A_1A_2}\rangle = |\psi_{0|0}^{A_1A_3}\rangle$ are entangled [PR92], but not maximally. In the end, all these symmetries, in particular that $I_{0|0}^{A_1A_2} = I_{0|0}^{A_1A_3}$ allow us to simplify

$$\begin{aligned} I_{①}^{A_1A_2A_3} &= I_{0|0}^{A_1A_2} + I_{0|0}^{A_1A_3} - P(000|000) = 2I_{0|0}^{A_1A_2} - P(000|000) \\ &= P(000|000) - 2P(010|010) - 2P(100|100) - 2P(000|110) \end{aligned} \tag{5.17}$$

Finally, we show that one can always realise

$$\begin{aligned} P(000|000) &> 0 \\ P(010|010) = P(100|100) = P(000|110) &= 0 \end{aligned} \tag{5.18}$$

by choosing the measurements on the prepared state $|\psi_{0|0}^{A_1A_2}\rangle$ (that is entangled, but not maximally) as for a violation of the Hardy paradox [Har93]. Note that it is a family of measurements on a non-maximally entangled state $|\psi_{0|0}^{A_1A_2}\rangle$ that can be chosen such that the generated correlations satisfy (5.18): one can choose freely[4] the first measurement, say $\langle m_{a_2=0|x_2=0}|$, and always find three other measurements $\langle m_{a_2=0|x_2=1}|, \langle m_{a_1=0|x_1=0}|, \langle m_{a_1=0|x_1=1}|$ such that (5.18) is satisfied. Now since

[3] I.e. for which $h_0, h_4 > 0, h_2 = h_3$

[4] To be exact, for any pure (non maximally) entangled state $|\psi_{0|0}^{A_1A_2}\rangle$ the measurement can not be chosen completely freely: there is one point in the full space of measurements that is not allowed. Being only a point in the full space, this does not affect the proof. More details can be found in App. C.5.

measurement $\langle m_{a_2=0|x_2=0}|$ is free, it can be tuned in order to be compatible with the condition to prepare a state $|\psi_{0|0}^{A_1A_3}\rangle$ $(= |\psi_{0|0}^{A_1A_2}\rangle)$ that is non-maximally entangled. □

Theorem 6 implies that all three qubit systems in a GME pure state, that are in addition symmetrical to the permutation of two out of the three parties $A_i \leftrightarrow A_j,\ i \neq j$, are GMNL. Note that the fact that tripartite systems in a GME pure state are GMNL was already proven in [Che+14; Che+04]. On the other hand, their construction relies on the violation of two families of Hardy-like paradox witnessing GMNL, making it untestable in an experiment. We were unable to prove that our inequality $I_{①}^{A_1A_2A_3}$ (5.5) can be violated by all GME three qubit pure states (5.15) (else than numerically).

5.4 General multipartite scenario

Let us briefly recall the important definitions that we need in the multipartite scenario (see Sec. 2.3.2 for more details). Consider $n \geq 3$ distant observers performing local measurements $\vec{x} = (x_1, \dots, x_n)$ and obtaining outcomes $\vec{a} = (a_1, \dots, a_n)$. A distribution $P(\vec{a}|\vec{x})$ is said to be *biseparable* if

$$P_{2\text{-sep}}(\vec{a}|\vec{x}) = \sum_g \sum_{\lambda_g} q_g(\lambda_g) P(\vec{a}_g|\vec{x}_g, \lambda_g) P(\vec{a}_{\bar{g}}|\vec{x}_{\bar{g}}, \lambda_g) \tag{5.19}$$

where $\sum_g \sum_{\lambda_g} q_g(\lambda_g) = 1$, $q_g(\lambda_g) \geq 0$ and g is a group consisting of a particular subset of the n observers and $\bar{g}$ its complement. We label the string of measurement choices (resp. outcomes) of the observers belonging to the group g as $\vec{x}_g$ $(\vec{a}_g)$. For example, for $n = 3$ there are only three possible inequivalent ways of making two groups: $(g_1 = A_1A_2, \bar{g}_1 = A_3)$, $(g_2 = A_1A_3, \bar{g}_2 = A_2)$ and $(g_3 = A_2A_3, \bar{g}_3 = A_1)$, leading to a decomposition of the form (5.1). Distributions that can not be written according to the decomposition (5.19) are *genuine multipartite nonlocal*. Again, local measurements on pure biseparable states, which for pure states can be written as $|\psi_{1\dots n}\rangle = |\phi_g\rangle|\phi_{\bar{g}}\rangle$ for some splitting $g/\bar{g}$ of the particles, always lead to biseparable joint distributions (5.19). Genuine multipartite entanglement is necessary to observe genuine multipartite nonlocality.

5.5 Bell inequalities witnessing genuine multipartite nonlocality

The generalisation of inequalities $I_{\text{sym}}^{A_1A_2A_3}$ (5.4) and $I_{①}^{A_1A_2A_3}$ (5.5) to any number of parties gives two distinct families of Bell inequalities that can be written in a simple form:

$$I_{\text{sym}}^{A_1\ldots A_n} = \sum_{i=1}^{n-1}\sum_{j>i}^{n} I_{\vec{0}|\vec{0}}^{A_iA_j} - \binom{n-1}{2} P(\vec{0}|\vec{0}) \leq 0 \tag{5.20}$$

$$I_{①}^{A_1\ldots A_n} = \sum_{j>1}^{n} I_{\vec{0}|\vec{0}}^{A_1A_j} - (n-2)P(\vec{0}|\vec{0}) \leq 0 \tag{5.21}$$

where $\binom{n-1}{2} = \frac{(n-1)(n-2)}{2}$ and we take the freedom of writing $\vec{0} \equiv (0,0,...,0)$, the size of the string should be obvious in the context. Similarly to (5.6), $I_{\vec{0}|\vec{0}}^{A_iA_j}$ is a lifting of inequality $I^{A_iA_j}$ (5.2) to n observers by setting the remaining $n-2$ observers to have their measurement and outcome set to 0:

$$\begin{aligned} I_{\vec{0}|\vec{0}}^{A_iA_j} &= P(0_i0_j\vec{0}|0_i0_j\vec{0}) - P(1_i0_j\vec{0}|1_i0_j\vec{0}) \\ &-P(0_i1_j\vec{0}|0_i1_j\vec{0}) - P(0_i0_j\vec{0}|1_i1_j\vec{0})\,. \end{aligned} \tag{5.22}$$

The operational meaning of these inequalities is the following: $a)$ for the symmetrical family (5.20), more than $\binom{n-1}{2}$ different pairs of parties A_iA_j should be able to win a lifted inequality (conditioned on the remaining $n-2$ parties' input and outcomes $x_k = a_k = 0 \ \ \forall k \neq i,j$); and $b)$ the inequalities "centered" on A_1 (5.21), more than $n-2$ different pair of parties A_1A_j should win a lifted inequality (conditioned on the remaining $n-2$ parties' input and outcomes $x_k = a_k = 0 \ \ \forall k \neq 1,j$).

Theorem 7. *The Bell inequalities $I_{sym}^{A_1\ldots A_n}$ (5.20) and $I_{①}^{A_1\ldots A_n}$ (5.21) are witnesses of genuine multipartite nonlocality for all $n \geq 3$.*

Proof. Here we only provide an outline, the detailed proof can be found in Appendix C.2.1. The idea is similar to the one for three parties and, again, we start with the symmetrical family $I_{\text{sym}}^{A_1\ldots A_n}$ (5.20). We want to show that all biseparable distributions (5.19) for n parties satisfy $I_{\text{sym}}^{A_1\ldots A_n} \leq 0$. Again, by convexity, it is enough to verify it for extremal biseparable distributions

$$I_{\text{sym}}^{A_1\ldots A_n}\left(P(\vec{a}_g|\vec{x}_g)P(\vec{a}_{\bar{g}}|\vec{x}_{\bar{g}})\right) \leq 0\,. \tag{5.23}$$

If parties A_i and A_j belong to different groups, they are only classically correlated and therefore $I_{\vec{0}|\vec{0}}^{A_iA_j} \leq 0$. Then, the only terms that can give a positive contribution to (5.23) are terms $I_{\vec{0}|\vec{0}}^{A_iA_j}$ where parties A_i and A_j belong to the same group. Now the trick is to kill these positive contributions by subtracting enough $P(\vec{0}|\vec{0})$ terms since, similarly to $n = 3$ (5.8),

$$\bar{I}_{\vec{0}|\vec{0}}^{A_iA_j} \equiv I_{\vec{0}|\vec{0}}^{A_iA_j} - P(\vec{0}|\vec{0}) \leq 0 \tag{5.24}$$

for any probability distributions. In general, if the first group g consists of m parties and $\bar{g}$ of $n-m$, a total number of $\binom{m}{2} + \binom{n-m}{2}$ inequalites $I_{\vec{0}|\vec{0}}^{A_iA_j}$ can in principle be positive. The largest number of pairs is obtained by putting $n-1$ parties in one group[5], which means $\binom{n-1}{2}$ potentially positive terms $I_{\vec{0}|\vec{0}}^{A_iA_j}$. Then,

$$\begin{gathered} I_{\text{sym}}^{A_1...A_n}\left(P(\vec{a}_g|\vec{x}_g)P(\vec{a}_{\bar{g}}|\vec{x}_{\bar{g}})\right) \leq \\ \sum_{i=1}^{n-2}\sum_{j>i}^{n-1} I_{\vec{0}|\vec{0}}^{A_iA_j} - \binom{n-1}{2} P(\vec{0}|\vec{0}) = \sum_{i=1}^{n-2}\sum_{j>i}^{n-1} \bar{I}_{\vec{0}|\vec{0}}^{A_iA_j} \leq 0 \end{gathered} \tag{5.25}$$

where we used the fact that $I_{\text{sym}}^{A_1...A_n}$ is invariant under permutations of parties to consider the specific partition $g = \{1,..,n-1\}$ and $\bar{g} = \{n\}$. This finishes the proof for the symmetrical family $I_{\text{sym}}^{A_1...A_n}$.

The proof for the non symmetrical family $I_{①}^{A_1...A_n}$ (5.21) follows the same idea. Using (5.24), any biseparable distribution (5.19) with m parties in the first group g containing party A_1 and $n-m$ in the other group $\bar{g}$ gives

$$I_{①}^{A_1...A_n}\left(P(\vec{a}_g|\vec{x}_g)P(\vec{a}_{\bar{g}}|\vec{x}_{\bar{g}})\right) \leq \sum_{j\in g} I_{\vec{0}|\vec{0}}^{A_1A_j} - (n-2)P(\vec{0}|\vec{0}) \leq \sum_{j\in g} \bar{I}_{\vec{0}|\vec{0}}^{A_1A_j} \leq 0 \tag{5.26}$$

since there are at most $n-2$ parties together with party A_1 in the first group g.

□

One can understand a violation of the families (5.21) and (5.20) of inequalities in the following way: GMNL correlations are the only ones for which it is potentially possible to violate a lifted inequality $I_{\vec{0}|\vec{0}}^{A_iA_j}$ between *all* pairs of parties, as they are the ones where all the parties share nonlocal resources with all the others.

[5] One can check that $\binom{n-1}{2} > \binom{m}{2} + \binom{n-m}{2}$ $\forall m \geq 2$.

Biseparable correlations (5.19) are limited in this sense, as many parties are only classically correlated to the parties that are in a different group and thus numerous lifted inequalities $I_{\vec{0}|\vec{0}}^{A_iA_j}$ cannot be violated. We give an illustration of that argument in Fig. 5.1.

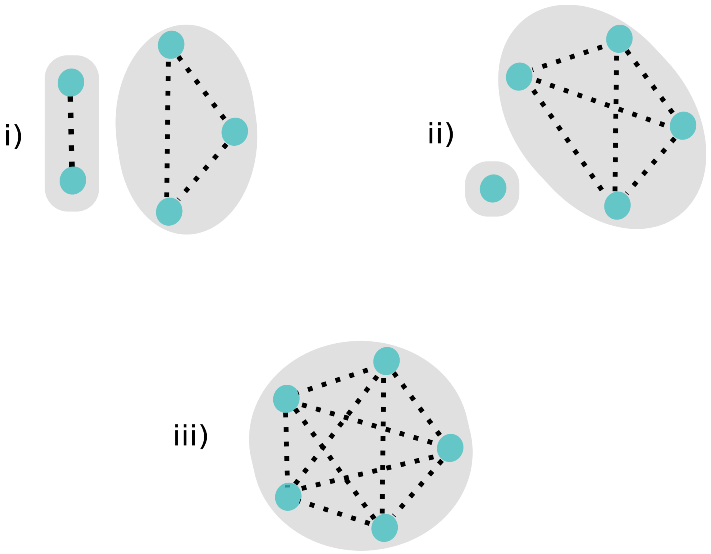

FIGURE 5.1: An abstract representation of five parties (the blue balls) arranged into groups (the grey areas). Two parties inside the same group can potentially violate a lifted inequality $I_{\vec{0}|\vec{0}}^{A_iA_j}$ (as represented by a dashed line between them). *i)* Two groups of parties $|g| = 2; |\bar{g}| = 3$, giving a distribution of the form $P(\vec{a}|\vec{x}) = P(a_1a_2|x_1x_2)P(a_3a_4a_5|x_3x_4x_5)$ and a maximum number of $\binom{2}{2} + \binom{3}{2} = 4$ violated inequalities $I_{\vec{0}|\vec{0}}^{A_iA_j} > 0$. *ii)* Two groups of parties $|g| = 1; |\bar{g}| = 4$, for $\binom{4}{2} = 6$ potentially violated inequalities $I_{\vec{0}|\vec{0}}^{A_iA_j} > 0$. *iii)* GMNL: all parties are in the same group and thus $\binom{5}{2} = 10$ inequalities can be violated. Only *iii)* can violate $I_{\text{sym}}^{A_1\ldots A_5} = \sum\limits_{i=1}^{4}\sum\limits_{j>i}^{5} I_{\vec{0}|\vec{0}}^{A_iA_j} - 6P(\vec{0}|\vec{0})$ since $I_{\vec{0}|\vec{0}}^{A_iA_j} - P(\vec{0}|\vec{0}) \leq 0$.

More insight on the rich structure of the symmetrical family of inequalities (5.20) is given by noticing that they can also be written in a recursive form for $n \geq 3$

$$I_{\text{sym}}^{A_1A_2\ldots A_n} = \sum_{i=1}^{n} I_{0|0}^{\text{all}\setminus A_i} - (n-2)P(\vec{0}|\vec{0}) \leq 0 \tag{5.27}$$

where $I_{0|0}^{\text{all}\backslash A_i}$ is the symmetrical inequality for $n-1$ observers lifted to n of them with observer A_i's input and outcome set to 0. Note that for $n=3$, $I_{0|0}^{\text{all}\backslash A_i}$ corresponds to the CHSH inequality lifted to 3 parties (5.6). The proof of the equivalence between the direct expression (5.20) and the recursive one (5.27) can be found in Appendix C.2.2.

In other words, operationally a violation of the symmetrical family $I_{\text{sym}}^{A_1 A_2 \dots A_n}$ can also be understood as a violation of more than $n-2$ inequalities $I_{0|0}^{\text{all}\backslash A_i}$ between $n-1$ parties lifted to n parties – instead of $\binom{n-1}{2}$ bipartite ones $I_{\vec{0}|\vec{0}}^{A_i A_j}$ lifted to n parties. Since this argument can be used recursively, one concludes that GMNL correlations violating our inequalities violate numerous inequalities between subset of m parties lifted to n parties, for all m.

Observe that, similar to the tripartite case, the generalised families $I_{\text{sym}}^{A_1 \dots A_n}$ (5.20) and $I_{①}^{A_1 \dots A_n}$ (5.21) are also saturated by local distributions. The local strategy is the same as for $n=3$: every party A_i outputs $a_i=1$ for all measurements x_i. This implies that the local and biseparable bounds of our families of inequalities coincide for all n.

5.6 Pure GME states and GMNL detected by our inequalities

The operational meaning of our families of Bell inequalities is clear: $a)$ any distribution that violates $I_{\text{sym}}^{A_1 \dots A_n}$ (5.20) needs to be capable of violating more than $\binom{n-1}{2}$ lifted CHSH inequalities $I_{\vec{0}|\vec{0}}^{A_i A_j}$ between different observers A_i and A_j; and $b)$ any distribution that violates $I_{①}^{A_1 \dots A_n}$ (5.21) violates more than $n-2$ lifted CHSH inequalities $I_{\vec{0}|\vec{0}}^{A_1 A_j}$ between A_1 and different observers A_j. Only GMNL correlations, where all pairs of parties can potentially be correlated nonlocally, are able to do this.

Let us now return to our main question: can we always find local measurements on *any* pure GME state that generate GMNL correlations? Our Bell inequalities seem fit for prove this result since for any pure GME state, there exist local projections on *any* $n-2$ parties that leave the remaining two in a pure entangled state [PR92], which can in turn be used to violate the CHSH inequality [Gis91]. The main difficulty in proving the result in full generality is to find local measurements that simultaneously perform the desired projections but are also fit to violate the CHSH terms. For $n = 2$ our two families of inequalities coincide with the CHSH inequality, which was used to prove the equivalence between nonlocality and pure state entanglement [Gis91]. For $n = 3$, there is numerical evidence that this holds for GME three-qubits pure states [Ban+13] using the symmetrical family $I_{\text{sym}}^{A_1 A_2 A_3}$ (5.5).

We extend these results to the scenario with $n = 4$ observers, where we obtained numerical evidence that all 4-qubit systems in a pure GME state generate distributions violating the symmetrical family of inequality $I_{\text{sym}}^{A_1 A_2 A_3}$ (5.20).

Moreover, we use our symmetrical family of inequalities $I_{\text{sym}}^{A_1 \ldots A_n}$ (5.20) to show analytically that a large class of pure GME states of the greenberger1989going family [GHZ89] can generate GMNL correlations for all number of observers $n \geq 3$.

Theorem 8. *All pure GME states of the form*

$$|greenberger1989going^n\rangle_\theta = \cos\theta|0\rangle^{\otimes n} - \sin\theta|1\rangle^{\otimes n} \tag{5.28}$$

with $\theta \in]0, \frac{\pi}{4}[$ *violate the Bell inequality* $I_{sym}^{A_1 \ldots A_n}$ (5.20) *for all* $n \geq 3$. *All observers* A_i *make the same projective measurements,* $\langle m_{a_i|x_i}| = \langle m_{a|x}|$, *defined by*

$$\begin{aligned} \langle m_{0|x}| &= \cos\alpha_x \langle 0| + \sin\alpha_x \langle 1| \\ \langle m_{1|x}| &= \sin\alpha_x \langle 0| - \cos\alpha_x \langle 1| \end{aligned} \tag{5.29}$$

where

$$\begin{aligned} \alpha_0 &= \arctan(\tan^{-\frac{3}{3n-4}}(\theta)) \\ \alpha_1 &= -\arctan(\tan^{-\frac{1}{3n-4}}(\theta)) \,. \end{aligned} \tag{5.30}$$

In other words, all states of the form (5.28) *that are GME are GMNL.*

Proof. A detailed proof of this theorem can be found in Appendix C.3 and is constructive. The key point is to impose that the local measurements to be the same for every observer, which makes the joint outcome distribution invariant under permutations of the parties (since the state $|greenberger1989going^n\rangle_\theta$ (5.28) is too). This symmetry simplifies the problem and allowed us to find an analytical solution. □

Interestingly, the only pure GME state of this family for which our construction fails is the maximally entangled state ($\theta = \pi/4$), which is already known to generate GMNL for any number of observers [Ban+09]. We have however found, numerically, several sets of measurements on this state that lead to distributions violating our inequality, but the amount of symmetries is reduced. Interestingly, Theorem 8 implies that even states that are almost separable ($\theta \to 0$) can be used to generate GMNL correlations for any number of observers.

A larger class of symmetrical states, including the ones of (5.28), was shown to be GMNL for all n in [Che+14; Che+04]. Nervetheless, their construction is based on Hardy-like paradoxes witnessing GMNL, making the test impossible in an experiment.

5.7 Using other inequalities as seed for the construction

The construction was so far done using as "seed" the CHSH inequality $I^{A_1A_2}$ (5.2) to build our families of inequalities by using the lifted inequalities $I^{A_iA_j}_{\vec{0}|\vec{0}}$. However, the construction can be applied to other inequalities. Indeed, any inequality that can be written as

$$I^{A_1A_2}(P(ab|xy)) = P(00|00) - \sum_{\substack{a,b,x,y \\ \neq 0,0,0,0}} \beta^{x,y}_{a,b} P(ab|xy) \leq 0 \tag{5.31}$$

such that $\beta^{x,y}_{a,b} \geq 0 \ \forall a,b,x,y \neq 0,0,0,0$ is useful. To see that, note that the only important ingredient in all our proofs is that $I^{A_1A_2} - P(00|00) \leq 0$ (for any probability distribution), which is true for any inequality which can be written as (5.31):

$$\bar{I}^{A_1A_2} \equiv I^{A_1A_2} - P(00|00) = - \sum_{\substack{a,b,x,y \\ \neq 0,0,0,0}} \beta^{x,y}_{a,b} P(ab|xy) \leq 0 \tag{5.32}$$

In particular, (5.32) also implies that $\bar{I}^{A_iA_j}_{\vec{0}|\vec{0}} = I^{A_iA_j}_{\vec{0}|\vec{0}} - P(\vec{0}|\vec{0}) \leq 0$ once the original inequality is lifted to more parties. The rest of this section is devoted such examples of inequalities that can be used for the construction.

The tilted CHSH inequality.– as first example, we write the "tilted CHSH" inequality $I^{A_1A_2}_{\beta}$ that was introduced in [AMP12] (with $\alpha = 1$) as

$$I^{A_1A_2}_{\beta} = P(00|00) - P(01|01) - P(10|10) - P(00|11) - \frac{\beta}{2} P_{A_1}(1|0) \leq 0 \tag{5.33}$$

where $P_{A_1}(a_1|x_1) = \sum_{a_2} P(a_1a_2|x_1x_2)\ \ \forall x_2$ is the marginal distribution of party A_1 and $\beta \geq 0$. As said, similarly to $\bar{I}^{A_iA_j}_{\vec{0}|\vec{0}} \leq 0$ (5.24) from the CHSH inequality (5.2)

$$\begin{aligned}\bar{I}^{A_iA_j}_{\beta,\vec{0}|\vec{0}} \equiv& I^{A_1A_2}_{\beta,\vec{0}|\vec{0}} - P(\vec{0}|\vec{0})\\ = -P(\vec{0}1_j|\vec{0}1_j) - P(1_i\vec{0}|1_i\vec{0}) - P(\vec{0}|1_i1_j\vec{0}) - &\sum_{a_j} \frac{\beta}{2} P(1_ia_j\vec{0}|\vec{0}) \leq 0\end{aligned} \tag{5.34}$$

where $\bar{I}^{A_1A_2}_{\beta,\vec{0}|\vec{0}}$ is a lifting of inequality $I^{A_1A_2}_{\beta}$ (5.33) to n parties similarly to the lifting $I^{A_1A_2}_{\vec{0}|\vec{0}}$ to n parties of the CHSH inequality $I^{A_1A_2}$. The term $\sum_{a_j} \frac{\beta}{2} P(1_ia_j\vec{0}|\vec{0})$ is the marginal $P_{A_i}(1|0) = \sum_{a_j} P_{A_iA_j}(1a_2|0x_2)\ \ \forall x_2$ of party A_i lifted to n parties.

Starting from the new seed $I^{A_1A_2}_{\beta}$ (5.33), we construct two new families of GMNL witnesses for any number n of parties

Theorem 9. *The families of inequalities*

$$I^{A_1\ldots A_n}_{\beta,sym} = \sum_{i=1}^{n-1}\sum_{j>i}^{n} I^{A_iA_j}_{\beta,\vec{0}|\vec{0}} - \binom{n-1}{2} P(\vec{0}|\vec{0}) \leq 0 \tag{5.35}$$

$$I^{A_1\ldots A_n}_{\beta,①} = \sum_{j>1}^{n} I^{A_1A_j}_{\beta,\vec{0}|\vec{0}} - (n-2)P(\vec{0}|\vec{0}) \leq 0 \tag{5.36}$$

witness GMNL for any number n of parties.

Proof. The proof that these two families of inequalities indeed witness GMNL for all n is exactly the same as for the families (5.20) and (5.21), except one needs to use property $\bar{I}^{A_1A_2}_{\beta,\vec{0}|\vec{0}} \leq 0$ (5.34) instead of $\bar{I}^{A_iA_j}_{\vec{0}|\vec{0}} \leq 0$ (5.24). □

A tripartite inequality as seed.– as a second example, we show that one can also start from a seed that is an inequality for more parties instead of a bipartite one. We found that the inequality for $n = 3$ parties – that witnesses GMNL in tripartite correlations – that belongs to the class number 5 of [Ban+13] could be written as

$$\begin{aligned}I^{A_1A_2A_3}_{\text{tri}} =& P(000|000) - P(010|111) - P(000|011)\\ -P(001|001) - P(100|110) - &P(010|010) - P(100|100) \leq 0\end{aligned} \tag{5.37}$$

Implying that $I^{A_1A_2A_3}_{\text{tri}} - P(000|000) \leq 0$ and $I^{A_1A_2A_3}_{\text{tri},\vec{0}|\vec{0}} - P(\vec{0}|\vec{0}) \leq 0$ for any probability distribution as desired. This allows us to construct, again, two new families of Bell inequalities witnessing GMNL for any $n \geq 3$

Theorem 10. *The families of inequalities*

$$I^{A_1\ldots A_n}_{tri,sym}=\sum_{i=1}^{n-2}\sum_{j>i}^{n-1}\sum_{k>j}^{n}I^{A_iA_jA_k}_{tri,\vec{0}|\vec{0}}-\binom{n-1}{3}P(\vec{0}|\vec{0})\leq 0 \tag{5.38}$$

$$I^{A_1\ldots A_n}_{tri,①②}=\sum_{j>2}^{n}I^{A_1A_2A_j}_{tri,\vec{0}|\vec{0}}-(n-3)P(\vec{0}|\vec{0})\leq 0 \tag{5.39}$$

witness GMNL for any number n of parties.

Proof. This time, a biseparable probability distribution (5.19) can violate at most $\binom{n-1}{3}$ inequalities $I^{A_iA_jA_k}_{\text{tri},\vec{0}|\vec{0}}$ between three different parties. This comes from the fact that the best for a biseparable distribution is a grouping $g=\{1,2,...,n-1\}$, $\bar{g}=\{n\}$ of the parties, allowing a maximum of $\binom{n-1}{3}$ to potentially violate the inequality $I^{A_iA_jA_k}_{\text{tri},\vec{0}|\vec{0}}$. Hence the family (5.38).

Second, there are at most $n-3$ inequalities $I^{A_1A_2A_j}_{\text{tri},\vec{0}|\vec{0}}$ that can potentially be violated for a grouping $g=\{1,2,...,n-1\}$, $\bar{g}=\{n\}$ of the parties. Hence the family (5.39). □

It would obviously be interesting to explore to which extent the inequalities that can be built – as the ones in (5.35),(5.36), (5.38) and (5.39) – are useful in order to witness GMNL from GME states. We leave this direction of research open for further work. Finally, it would also be insightful to consider inequalities $I^{A_1A_2}$ as seeds for our construction that allow for more measurement choices and/or outcomes and that satisfy the condition $I^{A_1A_2}-P(00|00)\leq 0$.

5.8 Constructing $m-$way multipartite nonlocality witnesses with our techniques

For a given inequality as seed for the construction, one can also build families to witness intermediate types of multipartite nonlocality, rather than GMNL only. Indeed, in the multipartite scenario it is possible to define a hierarchy of multipartite correlations taking into account the multipartite extent to which these are nonlocal. This can be measured, for example, by notions such as $m-$way (non)locality or $m-$separability of correlations [Ban+13; Ban+09] (see more details in Sec. 2.3.2). Instead of asking whether given correlations can be decomposed into (convex mixtures) of two groups as in (5.19), one can ask whether the correlations can be decomposed into m groups. Correlations that are decomposable into $m<n$ groups are then less multipartite nonlocal than other correlations that can not.

Correlations $P(\vec{a}|\vec{x})$ are said to be $m-$separable (or $m-$way local), i.e. decomposable into m groups, if

$$P_{\text{m-sep}}(\vec{a}|\vec{x}) = \sum_{k}\sum_{\lambda_k} q_k(\lambda_k) \prod_{i=1}^{m} P(\vec{a}_{k_i}|\vec{x}_{k_i}, \lambda_k) \tag{5.40}$$

where $\sum\limits_{k}\sum\limits_{\lambda_k} q_k(\lambda_k) = 1$, $q_k(\lambda_k) \geq 0$. This time, the variable k defines a *grouping* of the n parties into m pairwise disjoint and non-empty groups: $|k_i| > 0 \ \forall i$, $k_i \cap k_j = \emptyset \ \forall i \neq j$ and $\sum\limits_{i=1}^{m} |k_i| = n$. Biseparable correlations (5.19) for $m = 2$ can be decomposed into (convex mixtures of) two group of parties $k_1 = g$ and $k_2 = \bar{g}$.

Now, from any seed inequality $I^{A_1A_2}$ such that $I^{A_1A_2} - P(00|00) \leq 0$ (for any correlations), we have that

Theorem 11. *The families of inequalities for n parties*

$$I^{A_1\ldots A_n}_{m\text{-}sep,sym} = \sum_{i=1}^{n-1}\sum_{j>i}^{n} I^{A_iA_j}_{\vec{0}|\vec{0}} - \binom{n+1-m}{2} P(\vec{0}|\vec{0}) \leq 0 \tag{5.41}$$

$$I^{A_1\ldots A_n}_{m\text{-}sep,\textcircled{1}} = \sum_{j>1}^{n} I^{A_1A_j}_{m,\vec{0}|\vec{0}} - (n-m)P(\vec{0}|\vec{0}) \leq 0 \tag{5.42}$$

witness $m-$way nonlocality – or non $m-$separability – for all $n, m < n$.

Proof. The proofs follow the same line as the proofs for the other families of inequalities we have already constructed. By making m groups instead of 2, one needs to count the maximum number of pairs of parties A_iA_j that can be made inside all the m groups for the family (5.41). Indeed, only such pair of parties A_iA_j in the same group can potentially violate a lifted inequality $I^{A_iA_j}_{\vec{0}|\vec{0}}$. The best way to group n parties into m groups, in order to maximise the number of such pairs of parties, is to put $n-m+1$ parties into one group and the remaining $m-1$ ones into one group each. In this way, a maximum amount of $\binom{n+1-m}{2}$ inequalities $I^{A_iA_j}_{\vec{0}|\vec{0}}$ can potentially be violated, but these can be cancelled by the $\binom{n+1-m}{2}P(\vec{0}|\vec{0})$ terms in (5.41) since $I^{A_iA_j}_{\vec{0}|\vec{0}} - P(\vec{0}|\vec{0}) \leq 0$.

For the family (5.42), one needs to count the maximum number of pair A_1A_j that can be made inside the group containing party A_1. By putting the maximal number of $n-m$ parties, plus party A_1, in one group, one gets that a maximum number of $n-m$ pairs A_1A_j can be formed. This implies that a maximum amount of $n-m$ inequalities $I_{\vec{0}|\vec{0}}^{A_iA_j}$ can potentially be violated, but these are cancelled by the $(n-m)P(\vec{0}|\vec{0})$ term in (5.42) since $I_{\vec{0}|\vec{0}}^{A_iA_j} - P(\vec{0}|\vec{0}) \leq 0$. □

5.9 Conclusion

In this work, we have first designed two new families of multipartite Bell inequalities, for any number of parties $n \geq 3$, where many different pairs of parties are asked to violate a lifted CHSH game. The idea is that only GMNL distributions are capable of violating a sufficiently large number of lifted CHSH inequality in order to observe a violation of our inequalities. The intuition behind this observation is based on an intuition found in [Pop95]: GME pure states are the ones for which one can find projections on any $n-2$ parties leaving the remaining two parties in a pure entangled state. This state can then be used for the violation of the CHSH inequality for that pair. Using these families, we have analytically found local measurements on states of the form $\cos\theta|0\rangle^{\otimes n} - \sin\theta|1\rangle^{\otimes n}$ that generate GMNL distributions in the whole range of parameter θ where the states are GME (except for $\theta = \pi/4$, which are already known to be GMNL [Ban+09]). We also found numerical evidence that all 4-qubit systems in a GME pure state violate our symmetrical inequality $I_{\text{sym}}^{A_1\ldots A_4}$ (5.23), extending the evidence for 3-qubits [Ban+13]. For systems of three qubits in a GME pure state, we have also shown that all states that are invariant under the permutation of two of the three parties violate our second family of inequalities $I_{①}^{A_1A_2A_3}$ (5.5). These results, together with the operational meaning of our inequalities, lead us to conjecture that these families can be used to show that all GME pure states display GMNL.

Apart from a proof in full generality, which seems not straightforward, it would be interesting to extend our results to more families of GME pure states. A possibility is to study the multipartite W-state, $|W_n\rangle = \frac{1}{\sqrt{n}}\sum_{i=1}^{n}|1\rangle_i \otimes_{j\neq i}|0\rangle_j$, for which we already managed to obtain, numerically, violations up to $n=5$. It would also be interesting to use further the characterisation of all 3-qubit systems in a pure state [Aci+01] to obtain an analytical proof that our inequality for $n=3$ detects GMNL when these states are GME by detecting also the states which have no symmetries. Further numerical exploration, for more observers or systems of larger dimensions, is another possibility.

In parallel, it would be interesting to explore the strength of the witnesses of $m-$way nonlocality (see 5.8) by, for example, using numerical techniques to obtain violation from states that are not GME. More generally, it would be interesting to understand the link between $m-$separability (of states) and $m-$way nonlocality, both for pure and mixed states.

Finally, we have seen that our method to construct families of Bell inequalities is very fertile and can be used to obtain many other families witnessing multipartite nonlocality. By using a different seed than the CHSH inequality, for instance a Bell inequality for more settings or outcomes, or even for more parties, one can generate inequalities fit to detect GMNL in a whole range of different scenarios. We also expect that our families of inequalities with various seeds, such as the tilted CHSH inequality (5.33), can be used to self-test certain classes of multipartite entangled pure states.

Chapter 6

Quantifying multipartite nonlocality via the size of the resource

When given correlations from an experiment or from a theory, it is desirable to determine the extent to which the participating parties would need to collaborate nonlocally for its (re)production. Here, we develop a framework for the study of the correlations' depth, which we study in terms of the *minimal group size* (MGS) of the resource needed for the above-mentioned purpose. Indeed, it is often harder to produce nonlocal resources between numerous parties rather than numerous copies of a smaller nonlocal resource between fewer parties – as is often the case for multipartite entangled systems.

We provide a general recipe — based on the lifting of Bell-like inequalities — to construct MGS witnesses for non-signalling resources starting from *any* Bell inequality. En route to illustrating the applicability of this recipe, we also show that when restricted to the space of full-correlation functions, non-signalling resources are as powerful as unconstrained signalling resources. Explicit examples of correlations where their MGS can be determined using this recipe and other numerical techniques are provided.

The work exposed in this chapter is based on the results published in [CGL15].

6.1 Introduction

Far, prior investigations on multipartite nonlocal correlations have focused predominantly on the notion of m-way (non)locality (2.47), namely, the possibility to reproduce them when the parties are separated into m groups [Ban+09] — specifically two groups [Sve87; Ban+12; Aol+12; Gal+12; Ban+13; Col+02b; JLM05;

Ban+11; Che+11] — and where the usage of some nonlocal resource $\mathcal{R}$ is only allowed within each group (see sec. 2.3.2). While this has been a fruitful approach for the detection of genuine multipartite nonlocality, and hence genuine multipartite entanglement in a device-independent setting [Ban11; PV11; Mor+13; Ban+12], it is however not always applicable to the detection of genuine multipartite nonlocality among a *subset* of participating parties. To manifest this shortcoming, let us consider a 4-partite correlation $\vec{P} = \{P(\vec{a}|\vec{x})\} = \{P(a_1a_2a_3a_4|x_1x_2x_3x_4)\}$ of getting measurement outcome (output) a_i for the i-th party given the measurement setting (input) x_i. A specific kind of biseparable correlation in this scenario takes the form of

$$\begin{aligned} P(\vec{a}|\vec{x}) = &\sum_\lambda q_\lambda P^{\mathcal{R}}_\lambda(a_1a_2|x_1x_2)P^{\mathcal{R}}_\lambda(a_3a_4|x_3x_4) \\ &+ \sum_\mu q_\mu P^{\mathcal{R}}_\mu(a_1a_3|x_1x_3)P^{\mathcal{R}}_\mu(a_2a_4|x_2x_4) \\ &+ \sum_\nu q_\nu P^{\mathcal{R}}_\nu(a_1a_4|x_2x_3)P^{\mathcal{R}}_\nu(a_2a_3|x_2x_3), \end{aligned} \tag{6.1}$$

where $P^{\mathcal{R}}_i(a_ja_k|x_jx_k)$ is some 2-partite distribution allowed by the resource $\mathcal{R}$, while q_λ, q_μ and q_ν are non-negative, normalized weights. If $\vec{P}$ *cannot* be written in the form of Eq. (6.1), the production of this correlation clearly requires at least 3 out of the 4 participating parties to collaborate nonlocally via $\mathcal{R}$. If moreover, nonlocal collaboration between 3 parties is sufficient, we see that $\vec{P}$ is thus biseparable, i.e., producible by parties separated into (convex mixtures of) two groups, see Fig. 6.1. In other words, the multipartite nonlocality contained in $\vec{P}$ cannot be detected by the conventional approach of detecting non-biseparability. Indeed, with the conventional (m-separability) approach, one only makes a distinction between the number of groups, but not the size, i.e., the number of parties involved in each group.

To determine the extent to which participating parties would need to collaborate nonlocally in a general scenario, it thus seems more natural to quantify multipartite nonlocality in terms of the *minimal group size* (MGS), i.e., the smallest number of parties required to collaborate nonlocally in reproducing some nonlocal correlation. In this work, we develop the formalism necessary for the study of MGS, or correlation depth in analogy to the study of entanglement, see sec. 2.3.1. Clearly, this approach provides information complementary to the one of m-way locality on how $\mathcal{R}$ has to be distributed/ shared among the participating parties in order to reproduce some given correlation. The aim of this work is to give a state-of-the-art exposition of this approach and to provide a general technique for the construction of MGS witnesses.

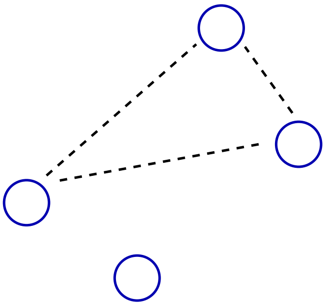

FIGURE 6.1: Schematic diagram showing a situation where the conventional approach of non-biseparability fails to detect the multipartite nonlocality present in the correlation. Here, the dashed lines joining the three circles symbolically represent the nonlocal collaboration between the three parties. Since the fourth party is only correlated with the rest through shared randomness, the overall correlation is biseparable.

6.2 Minimal group size, k-producibility and multipartite nonlocality

Correlations satisfying Eq. (6.1) are 2-producible whereas a correlation $\vec{P} = \{P(\vec{a}|\vec{x})\}$ satisfying

$$\begin{aligned} P(\vec{a}|\vec{x}) = &\sum_{\lambda} q_{\lambda} P_{\lambda}^{\mathcal{R}}(a_1a_2a_3|x_1x_2x_3)P_{\lambda}^{\mathcal{R}}(a_4|x_4) \\ &+ \sum_{\mu} q_{\mu} P_{\mu}^{\mathcal{R}}(a_1a_2a_4|x_1x_2x_4)P_{\mu}^{\mathcal{R}}(a_3|x_3) \\ &+ \sum_{\nu} q_{\nu} P_{\nu}^{\mathcal{R}}(a_1a_3a_4|x_1x_3x_4)P_{\nu}^{\mathcal{R}}(a_2|x_2) \\ &+ \sum_{\theta} q_{\theta} P_{\theta}^{\mathcal{R}}(a_2a_3a_4|x_2x_3x_4)P_{\theta}^{\mathcal{R}}(a_1|x_1). \end{aligned} \tag{6.2}$$

are only 3-producible. General 3-producible correlations, however, may involve convex combination of correlations of the form of Eq. (6.1) and of Eq. (6.2). Obviously, k-producibility implies k'-producibility for all $k' > k$. Using the above terminologies, we thus say that $\vec{P}$ is *genuinely* k-partite nonlocal[1] or having a MGS of k if $\vec{P}$ is k-producible but not $(k-1)$- producible. For example, a 4-partite correlation that satisfies Eq. (6.1) but violates a Bell inequality is 2-producible but not

[1] To conform with existing terminologies in the literature, when $\mathcal{R}$ refers to a quantum resource, we say that $\vec{P}$ must have arisen from a genuinely k-partite entangled state instead of $\vec{P}$ exhibits genuine k-partite nonlocality.

1-producible, and hence genuinely 2-partite nonlocal. Similarly, a 4-partite correlation that is 3-producible but not decomposable in the form of Eq. (6.1) is genuinely 3-partite nonlocal.

A few other remarks are now in order. Firstly, the above definition can be seen as a generalization of existing notions of genuine k-partite nonlocality for an n=k-partite scenario [Ban+13] to an n-partite scenario where $n \geq k$. It is worth noting that the question of whether given correlations $\vec{P}$ can be produced by having *at most* k parties in one group (k-producibility) is not completely independent from the question of whether $\vec{P}$ can be produced by separating the n parties into *at least* m groups (m-way locality (2.47)). For instance, k-producible correlations $\vec{P}$ are m-way local for some $m \geq \lceil \frac{n}{k} \rceil$; likewise, if $\vec{P}$ are m-way local, these are also k-producible for some $k \geq \lceil \frac{n}{m} \rceil$. Thus, the smallest n for which these descriptions become inequivalent is $n = 4$. Finally, any multipartite correlations that can not be produced by SR, or equivalently that is nonlocal or not 1-producible, is genuinely k-partite nonlocal for some $k \geq 2$.

6.2.1 Characterization of the sets of k-partite $\mathcal{R}$-producible correlations

While the bulk of the above discussion is independent of the choice of the nonlocal resource $\mathcal{R}$, it is worth reminding some features that are pertinent to specific resources. A more detailed discussion of these topics can be found in sec. 2.3.2. In this context, four commonly discussed nonlocal resources $\mathcal{R}$ are: (1) $\mathcal{Q}$: (local measurements on) an entangled quantum state of unrestricted Hilbert space dimension, (2) $\mathcal{NS}$: a post-quantum, but non-signalling [PR94; Bar+05] resource,[2] (3) $\mathcal{T}$ [Gal+12; Ban+13]: a time-ordered, one-way classical signalling resource[3] and (4) $\mathcal{S}$ [Sve87] : a Svetlichny resource.[4] Note that each resource $\mathcal{R}$ above is strictly[5] stronger than the preceding one(s), in the sense that $\mathcal{R}$ can be used to produce all correlations arising from the preceding resource(s) [Gal+12; Ban+13]. As a result,

[2] Such a resource only allows correlations where their marginal distributions for *any* subset of parties are independent of the input of the complementary subset of parties.

[3] The correlations allowed by such a resource is referred to as time-ordered bilocal in Ref. [Gal+12].

[4] The Svetlichny resource allows the parties in a group to use any joint strategy and hence to produce any correlation that is only constrained by the normalization of probabilities. In some cases, such a resource can be realized by allowing multiple rounds of classical communications among the parties but in others, such a resource may not have a well-defined physical meaning, see Refs. [Gal+12; Ban+13] for a discussion.

[5] To see the "strictly" part, one can construct, for each type of resources $\mathcal{R}$, correlations violating the Guess Your Neighbour's Input (GYNI) inequality introduced in [**GYNI**] up to different extents (except for $\mathcal{L} \subset \mathcal{Q}$, which refers to quantum nonlocality).

we have the strict inclusion relations,

$$\mathcal{L} \subset \mathcal{Q} \subset \mathcal{NS} \subset \mathcal{T} \subset \mathcal{S}, \tag{6.3}$$

with $\mathcal{L}$ being a local resource, provided by SR alone. Hence, a correlation $\vec{P}$ that is k-partite $\mathcal{Q}$-producible is also a member of the set of k-partite $\mathcal{R}$-producible correlations (henceforth denoted by $\mathcal{R}_{n,k}$) for $\mathcal{R} \in \{\mathcal{NS}, \mathcal{T}, \mathcal{S}\}$. Conversely, a correlation that is *not* in $\mathcal{S}_{n,k}$ is also not in $\mathcal{R}_{n,k}$ for $\mathcal{R} \in \{\mathcal{Q}, \mathcal{NS}, \mathcal{T}\}$, see Fig. 6.2. Formally, these implications are summarized as follows:

$$\vec{P} \in \mathcal{Q}_{n,k} \Rightarrow \vec{P} \in \mathcal{R}_{n,k} \quad \text{for all} \quad \mathcal{R} \in \{\mathcal{NS}, \mathcal{T}, \mathcal{S}\}, \tag{6.4a}$$

$$\vec{P} \notin \mathcal{S}_{n,k} \Rightarrow \vec{P} \notin \mathcal{R}_{n,k} \quad \text{for all} \quad \mathcal{R} \in \{\mathcal{Q}, \mathcal{NS}, \mathcal{T}\}. \tag{6.4b}$$

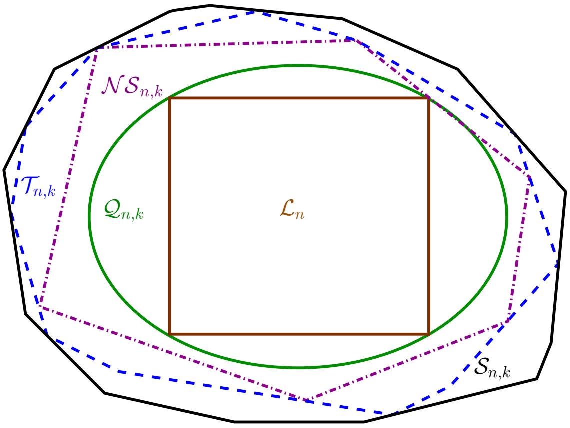

FIGURE 6.2: (Color online) Schematic diagram showing the inclusion relations of the various sets of $\mathcal{R}_{n,k}$, cf. Eq. (6.3) and Eq. (6.4). The smallest of these sets is $\mathcal{L}_n$ [depicted as the (brown) rectangle], followed by $\mathcal{Q}_{n,k}$ [depicted as the (green) oval], followed by $\mathcal{NS}_{n,k}$ [with boundary marked by the (magenta) dashed-dotted line], followed by $\mathcal{T}_{n,k}$ [with boundary marked by the (blue) dashed line]. Finally, the k-producible Svetlichny set $\mathcal{S}_{n,k}$ is represented by the outermost (black) solid polygon.

More generally, we note that independent of the nonlocal resource $\mathcal{R} \in \{\mathcal{Q}, \mathcal{NS}, \mathcal{T}, \mathcal{S}\}$, the set $\mathcal{R}_{n,k}$ is convex. Moreover, for the case when $\mathcal{R} \in \{\mathcal{NS}, \mathcal{T}, \mathcal{S}\}$, $\mathcal{R}_{n,k}$ is even a convex polytope [Ban+13], i.e., a convex set having only a finite number of extreme points [Grü+67] and thus can be equivalently specified through a finite number of Bell-like inequalities (corresponding to the facets of the respective polytope). Determining if a given correlation $\vec{P}$ is inside $\mathcal{R}_{n,k}$, and hence producible by the respective resource can thus be decided via a linear program [BV04], or through the violation of one of those Bell-like inequalities defining the polytope. In the simplest 2-input, 2-output scenario where $\mathcal{R} = \mathcal{NS}$, the set $\mathcal{NS}_{3,2}$ has been completely characterized in Ref. [Ban+13] whereas a superset of $\mathcal{NS}_{4,2}$ has also been characterized in Ref. [CLG14] (see also Ref. [Cur13]). If $\mathcal{R} = \mathcal{Q}$, i.e., a quantum resource, then the set $\mathcal{R}_{n,k}$ is no longer a convex polytope. Determining if a given $\vec{P}$ is in $\mathcal{Q}_{n,n-1}$ can nonetheless be achieved by solving a hierarchy of semidefinite programs [BV04] described in Ref. [Ban11]. More generally, determining if any given $\vec{P}$ is in $\mathcal{Q}_{n,k}$ can be achieved — to some extent — by solving a variant of the hierarchy of semidefinite programs described in Ref. [Mor+13] (see Ref. [Lia+15] for details).

However, regardless of $\mathcal{R}$, it is generally formidable to solve the aforementioned linear/ semidefinite programs by *brute force* even on a computer for relatively simple scenarios. Implications such as those summarized in Eq. (6.4) are thus useful to bear in mind for subsequent discussions. For example, if $\vec{P}$ violates an n-partite Svetlichny inequality — a Bell-like inequality that holds for a general Svetlichny resource — then it is not $(n-1)$-producible for all $\mathcal{R}$. In other words, the correlation $\vec{P}$ exhibits genuine n-partite nonlocality (and hence can only be produced, if at all, by a genuinely n-partite entangled state) and has an MGS of n. A generic correlation $\vec{P}$, evidently, will have an MGS that depends on the resource under consideration, as we now illustrate by explicit examples in the following subsections.

6.2.2 An example of a genuinely 3-partite $\mathcal{NS}$ nonlocal correlation in a 4-partite scenario

The Greenberger-Horne-Zeilinger (GHZ) state [GHZ89; Mer90b] between n parties is defined as follow :

$$|\mathrm{GHZ_n}\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes \mathrm{n}} + |1\rangle^{\otimes \mathrm{n}}), \tag{6.5}$$

where $|0\rangle$ and $|1\rangle$ are, respectively, the eigenstate of the Pauli matrix σ_z with eigenvalue $+1$ and -1. Consider the following equal-weight mixture of three parties sharing $|\mathrm{GHZ_3}\rangle$ and one party holding $|-\rangle$:

$$\rho = \frac{1}{4}\left(|\mathrm{GHZ_3}\rangle\langle\mathrm{GHZ_3}| \otimes |-\rangle\langle-| + \circlearrowright\right) \tag{6.6}$$

where $|-\rangle$ is the eigenstate of the Pauli matrix σ_x with eigenvalue -1, and we have used $\circlearrowright$ to denote similar terms which must be included to ensure that the expression involved is invariant under arbitrary permutation of parties. This quantum state could be prepared, for instance, by distributing uniformly randomly $|\mathrm{GHZ_3}\rangle$ to any of the three parties and $|-\rangle$ to the remaining one. By construction, ρ does not have genuine 4-partite entanglement. Hence, any correlation $\vec{P}$ derived by performing local measurement on ρ must be a member of $\mathcal{Q}_{4,3}$ and by Eq. (6.4a), also $\mathcal{R}_{4,3}$.

Now, consider the case where all parties measure the following dichotomic observables,

$$\begin{aligned} A_0 = B_0 = C_0 = D_0 &= -\frac{\sqrt{3}}{2}\sigma_x + \frac{1}{2}\sigma_y, \\ A_1 = B_1 = C_1 = D_1 &= -\frac{\sqrt{3}}{2}\sigma_x - \frac{1}{2}\sigma_y. \end{aligned} \tag{6.7}$$

It can be shown that that the resulting correlation $\vec{P}$ violates the following Bell inequality which must be satisfied by all correlations from $\mathcal{NS}_{4,2}$ [CLG14]:

$$\begin{aligned} \mathcal{I} = &-12\langle A_0\rangle - 3\langle A_1\rangle - 2\langle A_0B_0\rangle + 6\langle A_0B_1\rangle \\ &- 3\langle A_1B_1\rangle + 13\langle A_0B_0C_0\rangle - 3\langle A_1B_0C_0\rangle \\ &- 11\langle A_1B_1C_0\rangle + 14\langle A_1B_1C_1\rangle + 22\langle A_0B_0C_0D_0\rangle \\ &- 15\langle A_0B_0C_0D_1\rangle - 10\langle A_1B_1C_0D_0\rangle \\ &- 7\langle A_1B_1C_1D_0\rangle + 21\langle A_1B_1C_1D_1\rangle + \circlearrowright \\ &\overset{\mathcal{NS}_{4,2}}{\leq} 105, \end{aligned} \tag{6.8}$$

giving a quantum value of 117.8827. This implies that the correlation $\vec{P}$ is also genuinely 3-partite nonlocal, or having an MGS of 3 for $\mathcal{R} \in \{\mathcal{Q}, \mathcal{NS}\}$.

Interestingly, it can be shown that $\vec{P}$ *does not* lie in any of the 3-partite $\mathcal{NS}$-producible set corresponding to a fixed partition. This, together with the fact that $\vec{P}$ is 3-partite $\mathcal{NS}$-producible means that the generation of $\vec{P}$ requires classical mixtures of different partitions of the 4 participating parties into 2 groups, one of them containing three parties and sharing an $\mathcal{NS}$ resource. It is also worth noting that all *tripartite* marginal correlations of $\vec{P}$ are verifiably 1-producible (hence satisfying the complete set of Bell inequalities for this scenario given in Ref. [Śli03]). In other words, although $\vec{P}$ is genuinely 3-partite $\mathcal{NS}$-nonlocal, this 3-partite nonlocality cannot be revealed by studying each of the four tripartite marginal correlations individually. Neither can this multipartite nonlocality be manifested by analysing the biseparability (or 2−way locality (2.47)) of the 4-partite correlation since this more conventional approach can not distinguish correlation of the form of Eq. (6.1) and those of the form of Eq. (6.2).

In the above example, we were able to determine the MGS of the correlation for the quantum, and a general non-signalling resource. For the Svetlichny resource, we could also show — by solving some linear program — that the very same correlations is inside the set $\mathcal{S}_{4,2}$, and thus only exhibits an MGS of 2. However, due to the computational complexity involved in solving the corresponding linear program for the 1-way signalling resource $\mathcal{T}$, we were not able to determine precisely its MGS. Apart from correlations that violate an n-partite Svetlichny inequality (in which case MGS $= n$ for all resources) or correlations that are local (in which case MGS $= 1$), one may thus wonder if there exist other n-partite correlations $\vec{P}$ which have an MGS that can be fully characterized for all the different resources. We now provide examples of this kind in the next section.

6.2.3 A family of n-partite examples with fully characterized MGS

In chapter 7 (based on [Lia+14]), we show that if all n parties either measure the σ_x or the σ_y observable on the n-partite state $|\mathrm{GHZ_n}\rangle$, Eq. (6.5), the resulting correlation has an MGS of $\lceil \frac{n}{2} \rceil$ for $\mathcal{R} \in \{\mathcal{NS}, \mathcal{T}, \mathcal{S}\}$ whenever n is odd or $\frac{n}{2}$ is even. On the other hand, if we restrict ourselves to a quantum resource, then for all odd $n \geq 3$, it follows from the result of Ref. [Lia+14] that the corresponding MGS is n, demonstrating a large gap between the size of the resource required to reproduce these correlations when using a quantum and a post-quantum non-signalling (or a classical but signalling) resource. To prove these results, a general $\mathcal{NS}$ biseparable decomposition of the aforementioned correlation is provided for arbitrary partitioning of the n parties into two groups, thus establishing that these correlations are $\lceil \frac{n}{2} \rceil$-producible for $\mathcal{R} \in \{\mathcal{NS}, \mathcal{T}, \mathcal{S}\}$. Then to prove that these correlations are *not* $(\lceil \frac{n}{2} \rceil - 1)$-producible for the same set of resources, it was shown in Ref. [Lia+14] that except for even n with odd $\frac{n}{2}$, these correlations are not 3-separable, i.e., cannot be reproduced by a separation of the n parties into 3 groups. As for $\mathcal{R} = \mathcal{Q}$, an MGS = n for odd n [Lia+14] follows from the fact that the corresponding correlation violates a device-independent witness for genuine n-partite entanglement [Ban11; Ban+12] constructed from the Mermin-Ardehali-Belinskii-Klyshko (MABK) Bell expression [Mer90a; Ard92; RS91; Belb; GBP98]. In the case of even n, result recently established in Ref. [Lia+15] (based on earlier work of Ref. [NKI02]) allows one to conclude that the above-mentioned GHZ correlations has an MGS of at least $n - 1$ (for $\mathcal{R} = \mathcal{Q}$).

6.3 Witnessing non-k-producibility using Bell-like inequalities

Evidently, as discussed in Sec. 6.2, Bell-like inequalities are very useful tools for determining (or at least lower-bounding) the MGS of given correlations by certifying its non-k-producibility. For example, all Bell-like inequalities that have been derived — based on the non-biseparability (2.46) approach [Sve87; Ban+12; Aol+12; Gal+12; Ban+13; Col+02b; JLM05; Ban+11; Che+11] — to detect genuine n-partite nonlocality can be used as witnesses for non-$(n-1)$-producibility for the respective resources. It is however unrealistic to hope to find *all* such Bell-like inequalities by solving the polytope describing the convex set $\mathcal{R}_{n,k}$ even for relatively small n and k. But all is not lost and in this section, we recall from Ref. [Pir05] the technique of lifting — originally developed for Bell inequalities that witness Bell-nonlocality — and show that it can also be used to construct Bell-like inequality for arbitrary $\mathcal{R}_{n',k}$ (where $n' > n$ and $\mathcal{R} \in \{\mathcal{Q}, \mathcal{NS}\}$) starting from *any* given Bell-like inequality for $\mathcal{R}_{n,k}$. Before that, let us first make a digression and point out the usefulness of a non-signalling resource in simulating a general correlation.

6.3.1 All extremal full-correlation functions can be simulated with non-signalling strategies

In an n-partite, m-input, ℓ-output Bell scenario, the set of full-correlation functions defined in Ref. [Ban+12] consists of the following $\ell\, m^n$ joint conditional probability distributions:

$$\{P([\mathbf{a}_{\vec{x}}]_\ell = r)\}_{r=0}^{\ell-1} \tag{6.9a}$$

where $[X]_\ell := X \mod \ell$,

$$P([\mathbf{a}_{\vec{x}}]_\ell = r) = \sum_{\vec{a}} P(\vec{a}|\vec{x})\, \delta_{\sum_i a_i \bmod \ell, r}, \tag{6.9b}$$

and $\delta_{a,b}$ is the Kronecker delta of a and b. Note that due to the normalization conditions, only $(\ell-1)\, m^n$ of these joint conditional probability distributions are independent. Moreover, in the case where there are only two possible outcomes, i.e., $\ell = 2$, it is easy to see that the above definition of full-correlation functions is equivalent to the conventional one defined by the expectation value of the product of ± 1 outcomes.

We now present a mathematical fact about the space of correlations spanned by the set of full-correlation functions defined in Eq. (6.9).

Theorem 12. *When restricted to the set of full-correlation functions given in Eq.* (6.9)*, all extremal strategies achievable by an n-partite Svetlichny resource $\mathcal{S}_n$ are also achievable using an n-partite non-signalling resource $\mathcal{NS}_n$. Thus, in the subspace spanned by full-correlation functions, the three sets of correlations $\mathcal{S}_n$, $\mathcal{T}_n$, and $\mathcal{NS}_n$ become identical.*

One can find the proof of this theorem in Appendix D.1. Let us remind that the Svetlichny resource is the most powerful nonlocal resource, and is only constrained by the normalization of probability distributions. In other words, $\mathcal{S}_n$ is basically the set of normalized n-partite correlations. The importance of Theorem 12 is that when restricted to the set of coarse-grained measurement statistics represented by the set of full-correlation functions, cf Eq. (6.9a), one also can not make a distinction between $\mathcal{NS}_n$ and the set of normalized conditional probability distributions. Note that for binary-outcome full-correlation functions arising from the Bell singlet state, the coincidence between $\mathcal{S}_2$ and $\mathcal{NS}_2$ was already anticipated from the results of Ref. [Cer+05]. In fact, an alternative proof of Theorem 12 for the special case of binary-outcome full-correlation functions can be found, e.g., in Theorem 12 of Ref. [Qui12].

It is also worth noting that the definition of full-correlation functions is not unique, nevertheless, numerous Bell-like inequalities can be written in terms of the correlation functions defined in Eq. (6.9), see e.g., Ref. [Ban+12]. In this regard, note also the following corollary of Theorem 12, which allows us to relate Bell-like inequalities for $\mathcal{NS}_{n,k}$ with those of $\mathcal{R}_{n,k}$ for $\mathcal{R} \in \{\mathcal{T}, \mathcal{S}\}$.

Corollary 1. *Let $\mathcal{I}^{\mathcal{R}}_{n,k}$ be a tight, full-correlation Bell-like inequality that holds for $\mathcal{R} \in \{\mathcal{T}, \mathcal{S}\}$, i.e.,*

$$\mathcal{I}^{\mathcal{R}}_{n,k} : \sum_{\vec{x}} \sum_{r=0}^{\ell-1} \beta^r_{\vec{x}} P([\mathbf{a}_{\vec{x}}]_\ell = r) \overset{\mathcal{R}_{n,k}}{\leq} B^{\mathcal{R}}_{n,k}, \tag{6.10}$$

and there exists $P(\vec{a}|\vec{x}) \in \mathcal{R}_{n,k}$ such that inequality (6.10) becomes an equality, then there also exists $P(\vec{a}|\vec{x}) \in \mathcal{NS}_{n,k}$ such that inequality (6.10) becomes an equality. In other words,

$$\sum_{\vec{x}} \sum_{r=0}^{\ell-1} \beta^r_{\vec{x}} P([\mathbf{a}_{\vec{x}}]_\ell = r) \overset{\mathcal{NS}_{n,k}}{\leq} B^{\mathcal{R}}_{n,k}, \tag{6.11}$$

is also a tight, *full-correlation Bell-like inequality that holds for $\mathcal{R} = \mathcal{NS}$.*

The proof of the above corollary can be found in Appendix D.2. The corollary tells us that if we restrict ourselves to Bell-like inequalities that only involve linear combination of full-correlation functions, Eq. (6.9), then we cannot distinguish between correlations that are k-producible with respect to any of the resource $\mathcal{R} \in \{\mathcal{NS}, \mathcal{T}, \mathcal{S}\}$. In other words, for any given n and k and in the subspace of measurement statistics spanned by the set of full-correlation functions, cf. Eq. (6.9), the three sets of correlations $\mathcal{NS}_{n,k}$, $\mathcal{T}_{n,k}$ and $\mathcal{S}_{n,k}$ become identical. It is worth bearing this fact in mind in order to appreciate the generality of the upcoming theorem.

6.3.2 Lifting of Bell-like inequalities

The *lifting* of Bell inequalities was first discussed by Pironio in Ref. [Pir05]. Essentially, it is a technique that allows one to extend any (facet-defining) Bell inequality of a given scenario to a more complex scenario (involving more parties and/or inputs and/or outputs). In this work, we are only interested in the lifting of Bell-like inequalities to a scenario involving more parties. In this case, a lifted Bell inequality corresponds to a witness of nonlocality where the nonlocal behavior of a subset of, say n, of the parties becomes apparent after conditioning on a specific combination of measurement settings and outcomes from the complementary subset of h parties.[6]

More concretely, let us denote a specific combination of the measurement settings and measurement outcomes of the h parties, respectively, by $\vec{s}$ and $\vec{o}$. It can then be shown that if the $(n+h)$-partite correlation $P(\vec{a},\vec{o}|\vec{x},\vec{s})$ is 1-producible (and non-vanishing[7]), so is the conditional distribution given by:

$$\tilde{P}^{|\vec{o},\vec{s}}(\vec{a}|\vec{x}) = \frac{P(\vec{a},\vec{o}|\vec{x},\vec{s})}{\sum_{\vec{a}} P(\vec{a},\vec{o}|\vec{x},\vec{s})}. \tag{6.12}$$

An immediate implication of this is that a Bell inequality that is defined for an n-partite scenario can be trivially extended to any $(n+h)$-partite scenarios by considering specific measurement settings $\vec{s}$ and outcomes $\vec{o}$ for the h parties.

As an example consider the well known Clauser-Horne-Shimony-Holt [Cla+69] Bell inequality applicable to a scenario involving two parties, each performing two binary-outcome measurements:

$$\sum_{x_1,x_2,a_1,a_2=0}^{1} (-1)^{a_1+a_2+x_1x_2} P(a_1a_2|x_1x_2) \overset{\text{Ł}}{\leq} 2. \tag{6.13}$$

Lifting this inequality to the scenario of 3 parties and with the 3rd party getting a *specific* measurement outcome o_3 given the *specific* measurement setting s_3 gives the following lifted CHSH Bell inequality:

$$\begin{aligned} &\sum_{x_1,x_2,a_1,a_2=0}^{1} (-1)^{a_1+a_2+x_1x_2} P(a_1a_2o_3|x_1x_2s_3) \\ &- 2P(o_3|s_3) \overset{\text{Ł}}{\leq} 0. \end{aligned} \tag{6.14}$$

Lifting the CHSH Bell inequality to an arbitrary number of $n > 2$ parties can be carried out analogously. In Ref. [Pir05], it was shown that such a procedure not only generates a legitimate Bell inequality but even one that preserves the facet-defining property of the original Bell inequality.

[6] This particular kind of lifting has been applied to show, for instance, a stronger version of Bell's theorem, see, e.g., Ref. [Ban14b; Bar+13].

[7] If the distribution vanishes, the conditional distribution given in Eq. (6.12) is ill-defined.

6.3.3 A general recipe for the construction of non-k-producible witnesses

We shall now demonstrate how lifting may be used as a general technique for the construction of Bell-like inequalities for $\mathcal{R}_{n',k}$ starting from one for $\mathcal{R}_{n,k}$ where n' is an arbitrary integer greater than n and $\mathcal{R}$ is a resource that respects the non-signalling constraints. To this end, we note that, without loss of generality, a (linear) Bell-like inequality for a non-signalling-respecting $\mathcal{R}_{n,k}$ can always be written in the form of:

$$I_n = \sum_{\vec{a},\vec{x}} \beta_{\vec{x}}^{\vec{a}} P(\vec{a}|\vec{x}) \overset{\mathcal{R}_{n,k}}{\leq} 0, \tag{6.15}$$

where $\beta_{\vec{x}}^{\vec{a}}$ is some real-valued function of $\vec{a}$ and $\vec{x}$. Our main observation is that the lifting of I_n to a scenario involving arbitrary $n' > n$ parties is also a legitimate Bell-like inequality for $\mathcal{R}_{n',k}$, as summarized more formally in the following theorem.

Theorem 13. *If I_n is a Bell-like inequality satisfied by all correlations in $\mathcal{R}_{n,k} \in \{\mathcal{Q}, \mathcal{NS}\}$, i.e., Eq. (6.15) holds for all $P(\vec{a}|\vec{x}) \in \mathcal{R}_{n,k}$, then*

$$I_{n+h} = \sum_{\vec{a},\vec{x}} \beta_{\vec{x}}^{\vec{a}} P(\vec{a},\vec{o}|\vec{x},\vec{s}) \overset{\mathcal{R}_{n+h,k}}{\leq} 0, \tag{6.16}$$

meaning that the lifted inequality holds for all $P(\vec{a},\vec{o}|\vec{x},\vec{s}) \in \mathcal{R}_{n+h,k}$ where $h \geq 1$, whilst $\vec{o}$ and $\vec{s}$ refer, respectively, to arbitrary but fixed *combination of measurement outcomes and measurement settings for the h additional parties.*

A proof of this theorem can be found in Appendix D.3. Clearly, one can see Theorem 13 as a partial generalization of the results presented in [Pir05] from $\mathcal{R}_{n,1}$ to $\mathcal{R}_{n,k}$ whenever $\mathcal{R} \in \{\mathcal{Q}, \mathcal{NS}\}$. As for $\mathcal{R} \in \{\mathcal{T}, \mathcal{S}\}$, we know from Corollary 1 and Theorem 13 that any full-correlation Bell-like inequality valid for $\mathcal{R}_{n,k}$ can also be lifted as a Bell-like inequality for $\mathcal{NS}_{n',k}$ in the extended scenarios. Unfortunately, the theorem in general does not apply to the signalling resource $\mathcal{S}$ (as well as $\mathcal{T}$). To see this, consider the tripartite Svetlichny inequality (writtten in the form given in [Ban+12]):

$$I_{\mathcal{S},3} = \sum_{\vec{x},\vec{a}} \beta_{\mathcal{S},3,\vec{x}}^{\vec{a}} P(a_1a_2a_3|x_1x_2x_3) - 4 \overset{\mathcal{S}_{3,2}}{\leq} 0, \tag{6.17a}$$

$$\beta_{\mathcal{S},3,\vec{x}}^{\vec{a}} = (-1)^{\sum_i a_i + \left\lfloor \frac{\sum_i x_i - 1}{2} \right\rfloor}. \tag{6.17b}$$

If Theorem 13 were to be applicable for a Svetlichny resource, we would expect, for instance, that the following inequality

$$\begin{aligned} I_{\mathcal{S},4} = &\sum_{\vec{x},\vec{a}} \beta^{\vec{a}}_{\mathcal{S},3,\vec{x}} P(a_1a_2a_3, o_4 = 0|x_1x_2x_3, s_4 = 0) \\ &-4\sum_{\vec{a}} P(a_1a_2a_3, o_4 = 0|x_1'x_2'x_3', s_4 = 0) \leq 0, \end{aligned} \tag{6.18}$$

to hold true for $\mathcal{S}_{4,2}$ and for some arbitrary choice of $x_1', x_2', x_3' = \{0, 1\}$. One can, however, easily verify that this is not the case. For instance, with $x_1' = x_2' = x_3' = 0$, the Svetlichny strategy from $\mathcal{S}_{4,2}$:

$$\begin{aligned} a_1 &= 1 - \delta_{x_1,1}\delta_{x_2,1}, \quad a_2 = 1, \\ a_3 &= a_4 = 1 - \delta_{x_3,1}\delta_{x_4,0}, \end{aligned} \tag{6.19}$$

gives vanishing contribution to the second term in Eq. (6.18) but an overall value of 4 for $I_{\mathcal{S},4}$, clearly violating inequality (6.18).

Despite the above remark, let us stress once more that there is still wide applicability of Theorem 13. For example, *each* of the Bell-like inequalities obtained for $\mathcal{NS}_{3,2}$ and $\mathcal{NS}_{4,2}$ in Refs. [Ban+13; CLG14] can now be used to construct witnesses showing MGS ≥ 3 (for the $\mathcal{NS}$ resource) for arbitrary number of parties. Thanks to Corollary 1, the families of k-partite Svetlichny inequalities obtained in Refs. [Col+02b; JLM05; Ban+11; Che+11; Ban+12] can similarly be extended to detect genuine $\mathcal{NS}$ k-partite nonlocality in an arbitrary $n > k$ partite scenario. Likewise, *each* device-independent witness for genuine k-partite entanglement obtained in Ref. [Ban11; Ban+12; PV11] can now be applied to witness genuine k-partite entanglement in an arbitrary $n > k$ partite scenario. Of course, it remains to show that Bell-like inequalities generated with the help of Theorem 13 could indeed be useful, and this is what shall show next with a very simple example.

6.3.4 An example where a lifted Bell-like inequality can be used to determine MGS

Consider the following four-partite mixed state:

$$\rho = v\,|\mathrm{GHZ}_3\rangle\langle\mathrm{GHZ}_3| \otimes |0\rangle\langle 0| + (1-v)\frac{\mathbb{1}}{2^3} \otimes |1\rangle\langle 1|, \tag{6.20}$$

where $v \in (0, 1]$, and $|0\rangle$, $|1\rangle$ are again the eigenstates of σ_z. Since ρ is *biseparable*, regardless of which local measurements are performed on ρ, the resulting correlations must be in $\mathcal{Q}_{4,3}$ and thus having MGS ≤ 3 for all $\mathcal{R}$ [cf. Eq. (6.4a)]. Clearly, from Eq. (6.20), we see that the entanglement of ρ lies entirely within the first three subsystems. Let us denote these systems by A, B, and C respectively. For $v \leq \frac{1}{5}$, it is known that the tripartite reduced density matrix $\rho_{\text{ABC}} = v\,|\text{GHZ}_3\rangle\langle\text{GHZ}_3| + (1-v)\frac{\mathbb{1}}{2^3}$ is fully separable (2.35) [DC00] and thus not capable of violating any Bell inequalities. Nonetheless, in what follows, we shall show that a lifted Bell-like inequality can indeed be used to show that certain correlation derived from ρ indeed exhibits MGS $= 3$ for all $v \neq 0$, thus showing that the generation of such a correlation quantum mechanically indeed requires at least tripartite entanglement.

To this end, consider now the following dichotomic observables,

$$\begin{gathered} A_0 = \sigma_x, \quad A_1 = \sigma_y, \\ B_0 = \frac{1}{\sqrt{2}}(\sigma_x - \sigma_y), \quad B_1 = \frac{1}{\sqrt{2}}(\sigma_x + \sigma_y), \\ C_0 = -\sigma_y, \quad C_1 = \sigma_x, \end{gathered} \tag{6.21}$$

and the tripartite Svetlichny inequality given in Eq. (6.17). It is known that by measuring the local observables $\{A_i, B_i, C_i\}_{i=0,1}$ given in Eq. (6.21) on $|\text{GHZ}_3\rangle$, one obtains correlation $\vec{P}$ that violates $I_{\mathcal{S},3}$ maximally.

Note that by Corollary 1 and the fact that Eq. (6.17) is a full-correlation Bell-like inequality, we know that inequality (6.17) still holds and can be saturated even if we now consider only correlations in $\mathcal{NS}_{3,2}$, i.e.,

$$I_{\mathcal{NS},3} = \sum_{\vec{x},\vec{a}} \beta^{\vec{a}}_{\mathcal{S},3,\vec{x}}\, P(a_1a_2a_3|x_1x_2x_3) - 4 \overset{\mathcal{NS}_{3,2}}{\leq} 0. \tag{6.22}$$

Lifting the inequality $I_{\mathcal{NS},3}$ to the specific case where the 4th party performs the 0-th measurement and getting the 0-th outcome, one obtains the inequality:

$$\begin{aligned} I^{|s_4=o_4=0}_{\mathcal{NS},3} &= \sum_{\vec{x},\vec{a}} \beta^{\vec{a}}_{\mathcal{NS},3,\vec{x}} P(a_1a_2a_3, o_4 = 0|x_1x_2x_3, s_4 = 0) \\ &\quad - 4P(o_4 = 0|s_4 = 0) \overset{\mathcal{NS}_{4,2}}{\leq} 0. \end{aligned} \tag{6.23}$$

Let us now identify the 0-th measurement of the fourth party by σ_z and the 0-th outcome by a successful projection onto the eigenstate $|0\rangle$. Together with the measurements specified in Eq. (6.21), one finds that for all $0 < v \leq 1$, the resulting correlation derived from ρ must also violate inequality (6.23). To see this, it suffices to note that (i) for $v \neq 0$, the probability of successfully projecting the fourth system onto $|0\rangle$ is strictly greater than zero and (ii) conditioning on a successful projection, the conditional state for ABC is simply $|\text{GHZ}_3\rangle$ which, as mentioned above, violates $I_{\mathcal{NS},3}$ inequality maximally. The aforementioned correlation thus exhibits MGS stronger than that allowed in $\mathcal{NS}_{4.2}$ which, by Eq. (6.4b), implies that it has MGS ≥ 3 for all $\mathcal{R} \in \{\mathcal{Q}, \mathcal{NS}\}$. Combining this with the biseparability of ρ mentioned above, we see that this particular correlation has exactly MGS = 3.

6.4 Conclusion

To investigate the extent to which participating parties would need to collaborate nonlocally in a multipartite Bell experiment 2.3.2, we have introduced the notion of *minimal group size* (MGS), i.e., the smallest number of nonlocally-correlated parties required to reproduce a given nonlocal correlation $\vec{P}$. We believe that this more general notion of genuine multipartite nonlocality inspired by k-producibility (or entanglement depth) [GTB05] from the studies of multipartite entanglement will be a fruitful approach towards a better understanding of multipartite nonlocality.

As an illustration, we presented, in a four-partite scenario, some genuine tripartite nonlocal correlation where the multipartite nonlocality *cannot* be detected through the conventional m-way (non)locality approach 2.3.2. Nonetheless, as first demonstrated in Ref. [Lia+14] (see chapter 7), and further elaborated in this paper, the biseparability approach – i.e. $m-$way locality for $m = 2$ – can in some cases provide tight lower bound on the MGS. In fact, for the family of n-partite correlations presented in Ref. [Lia+14], it was even found that their MGS for a quantum resource is n whereas that for a general non-signalling (or even an unrestricted signalling) resource is $\lceil \frac{n}{2} \rceil$, giving an increasing gap between their MGS as n increases. Could there be a bigger gap between the MGS of a nonlocal correlation with respect to a quantum resource and a general (non-)signalling resource? In particular, does there exist a multipartite nonlocal quantum correlation which requires genuine n-partite entangled state for its production but nonetheless only an MGS of 2 if one is allowed to exploit a signalling, or even a non-signalling but post-quantum resource? The answer to these questions would certainly shed light on how quantum entanglement help in a different aspect of communication complexity, namely, how many communicating parties we can replace by quantum entanglement.

We also demonstrated how the technique of lifting [Pir05] — originally presented in the context of Bell inequality (for 1-producibility) — can be applied to generate new MGS witnesses starting from one involving a smaller number of parties. This generalizes partially the result of Ref. [Pir05] and provides a useful recipe for the construction of MGS witnesses (with respect to a non-signalling, e.g., a quantum resource) for an arbitrary n-partite scenario. Moreover, we have found that for the complete list of 185 facet-defining Bell-like inequalities of $\mathcal{NS}_{3,2}$ given in Ref. [Ban+13], the corresponding MGS witnesses of $\mathcal{NS}_{4,2}$ generated from lifting still correspond to a *facet* [Grü+67] of the polytope in the more complex scenario.

Likewise, when these 185 lifted inequalities, as well as the 13,479 facet-defining inequalities obtained in Ref. [CLG14] are lifted to the 5-partite scenario, it can again be verified that they correspond to facets of the $\mathcal{NS}_{5,2}$ polytope. Based on these observations, we conjecture that — as with standard Bell inequalities — the procedure of lifting, when applied to a facet-defining inequality of $\mathcal{NS}_{n,k}$, also generates a facet of $\mathcal{NS}_{n',k}$ in the extended scenario involving $n' > n$ parties.

Unfortunately, a naive application of lifting to signalling resources generally does not always result in legitimate MGS witnesses in the extended scenario. Nevertheless, the possibility to simulate all possible *full-correlation functions* [Ban+12] using only non-signalling resources — as we show in Appendix D.1 — allows us to apply the recipe to Bell-like inequalities originally derived for Svetlichny resources [Ban+12; Sve87; Col+02b; JLM05; Ban+11; Che+11] and construct MGS witnesses for non-signalling resources in *any* extended scenario. It is also conceivable that an analogous witness-generating technique may be found for signalling resources, a problem that we shall leave for future research.

Evidently, on top of Bell-like inequalities that one may construct using the aforementioned technique, it is natural to ask if there exist simple family of non-k-producible witnesses for arbitrary number of parties. In this regard, we note that a family of such witnesses for a quantum resource (as well as a general non-signalling resource) has recently been identified [Lia+15]. Similar results for other resources, especially one that is either *optimal* (in the sense of being facet-defining) for the respective convex polytope, or one that involves a small number of terms to be measured experimentally, would certainly be desirable.

Finally, let us stress that while we have discussed MGS mostly in the context of reproducing certain nonlocal correlations, these values for the post-quantum non-signalling resource, as well as for signalling resources also provide insight on the difficulty in reproducing certain correlations using quantum resources. In this sense, evaluation of the MGS for a given correlation may give an indication on how difficult it is to produce certain Bell-inequality violating correlations in the laboratory: the larger the value of MGS, the more systems need to be entangled together in their generation.

Chapter 7

Anonymous Quantum Nonlocality

In this chapter, we study multipartite nonlocal correlations and their use in device-independent (DI) information tasks. We show that these can indeed provide advantages in some tasks, such as DI quantum key distribution (DIQKD) or secret sharing between any two groups of parties. We study correlations whose generation requires only subsets of the parties to share nonlocal resources – such as entangled systems – but which exhibit other interesting features. Such correlations already provide with the necessary properties for information tasks. *Anonymous* nonlocality is such a feature proper to multipartite correlations, allowing a subset of parties to generate nonlocal correlations – and thus achieve an information task – without revealing their identity. Our work thus provides additional evidence that multipartite nonlocal correlations are useful for DI information tasks. On the other hand, there is no apparent reason to focus on the multipartite extend of the nonlocal correlations, but rather on the fact that these are nonlocal at all.

From a resource-theoretic perspective, our results also imply that the gap between quantum and post-quantum resources (such as no-signalling ones) – in terms of resources size or correlations depth – for the (re)production of nonlocal correlations can be made arbitrarily large.

This chapter is based on the results obtained in [Lia+14].

7.1 Biseparable correlations and anonymous nonlocality

In contrast to genuine multipartite nonlocal correlations (2.46), correlations that are biseparable, cf. Eq. (2.45) with $m = 2$, receive almost no attention. Apart from being a tool in the derivation of Bell-type inequalities for genuine multipartite nonlocality, is this kind of correlations interesting in its own right? Here, we answer this question affirmatively via the phenomenon of *anonymous nonlocality* (ANL), an intriguing feature that is only present in biseparable correlations. We will also provide evidence showing that ANL can be a powerful resource, allowing one to design device-independent quantum cryptographic protocols that can guard against a particular kind of attack by any post-quantum, but no-signalling adversary.

To appreciate the peculiarity manifested by ANL, let us start by considering the simplest, tripartite scenario. Clearly, among the subsets of correlations that can are biseparable, are those that satisfy:

$$P(\vec{a}|\vec{x}) = \sum_{\nu} p_\nu P_\nu(a_1|x_1)\, P_\nu^{\mathcal{R}}(a_2a_3|x_2x_3), \tag{7.1a}$$

$$= \sum_{\mu} p_\mu\, P_\mu(a_2|x_2) P_\mu^{\mathcal{R}}(a_1a_3|x_1x_3), \tag{7.1b}$$

$$= \sum_{\lambda} p_\lambda\, P_\lambda(a_3|x_3) P_\lambda^{\mathcal{R}}(a_1a_2|x_1x_2), \tag{7.1c}$$

where $p_\nu, p_\mu, p_\lambda \geq 0$ for all ν, μ and λ, but in contrast with Eq.(2.45), we now have $\sum_\nu p_\nu = \sum_\mu p_\mu = \sum_\lambda p_\lambda = 1$. Eqs. (7.1a)–(7.1c) imply that the correlation can be produced *without* having any nonlocal collaboration between the isolated party and the remaining two parties (as a group). Naively, one may thus expect that all correlations satisfying these equations must also be Bell-local (henceforth abbreviated as local). However, there exist [VB12] quantum correlations that satisfy Eqs. (7.1a)–(7.1c) as well as:

$$P(\vec{a}|\vec{x}) \neq \sum_{\theta} p_\theta\, P_\theta(a_1|x_1) P_\theta(a_2|x_2) P_\theta(a_3|x_3), \tag{7.1d}$$

for *any* conditional distributions $P_\theta(a_i|x_i)$ and *any* normalized weights p_θ. In other words, $\vec{P}$ satisfying Eq. (7.1) is nonlocal but this nonlocality is (i) not genuinely tripartite (it is biseparable) (ii) not attributable to any of the two-partite marginals[1] and (iii) not attributable to any bipartition of the three parties. The nonlocality present in *any* correlations satisfying Eq. (7.1) is thus in some sense nowhere to be found!

We now provide a very simple example of correlation satisfying Eq. (7.1), and more generally the property of being (1) nonlocal and (2) biseparable with respect to all bipartitions in an arbitrary n-partite scenario. Consider the n-partite Greenberger-Horne-Zeilinger (GHZ) state [GHZ89] $|\mathrm{GHZ_n}\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes \mathrm{n}} + |1\rangle^{\otimes \mathrm{n}})$ and the local measurement of σ_x and σ_y. The resulting correlation is

$$P(\vec{a}|\vec{x}) = P^n_{\mathrm{GHZ}}(\vec{a}|\vec{x}) = \frac{1}{2^n}\left[1 + \cos\left(\mathbf{x}\frac{\pi}{2}\right)\prod_{i=1}^{n} a_i\right], \tag{7.2}$$

where $\mathbf{x} = \sum_i x_i$, and we have identified $x_i = 0\,(1)$ as the $\sigma_x(\sigma_y)$ measurement

[1] Eqs. (7.1a)–(7.1c) imply that all marginals are local.

(see, eg. Eq. (23) of [WLB11]). In Appendix E.1, we show that *for all* $n \geq 3$, n-partite correlations of the form of Eq. (7.2) admit a biseparable decomposition with respect to *any* partitioning of the n parties into two groups. Specifically for $n = 3$, this decomposition, cf. Eq. (7.1a), involves $p_\nu = \frac{1}{4}$ for all ν, $P_\nu(a_1|x_1) = 0, 1$ and $P_\nu^{\mathcal{R}}(a_2a_3|x_2x_3)$ is the correlation associated with the so-called Popescu-Rohrlich (PR) box (2.27) — a hypothetical, stronger-than-quantum, but non-signalling resource.[2] To see that these correlations are nonlocal, it suffices to note that Eq. (7.2) violates the Mermin-Bell inequality [Mer90a; Ard92; RS91; Belb; GBP98] (even maximally [WW00] for all odd $n \geq 3$). See Appendix E.2.

Consider now an alternative way to understand the nonlocality associated with Eq. (7.1). Operationally, Eq. (7.1c) implies that $\vec{P}$ can be produced by, e.g., party 1 signalling classically to party 2, and all parties responding according to the information that they received and some predefined strategy λ. By symmetry of Eqs. (7.1a)–(7.1c), the same can be achieved by having only nonlocal collaboration between any two out of the three parties. Thus, while the correlation can be produced by having only a *definite subset* of parties collaborating nonlocally, the identity of these nonlocally collaborating parties is *anonymous* to an outsider who only has access to $\vec{P}$. Indeed, even if an outsider is given the promise that a *fixed* subset of the parties have collaborated nonlocally, it is impossible for him to tell if, say, party 1 and 2 have collaborated nonlocally in generating $\vec{P}$. Importantly, the anonymity present in these correlations differs from the case where a *classical mixture* of the different bipartitions is necessary, cf. Fig. 7.1 (see [CLG14; Lia+14] for examples of such classical anonymity). In this latter case, it is indeed possible to identify the parties that *must have* collaborated nonlocally, even though this identification is generally not possible at any single run of the experiment.

As remarked above, for all $n \geq 3$, the GHZ correlations of Eq. (7.2) are nonlocal but can nevertheless be produced by splitting the parties into *any* two groups, and disallowing any nonlocal collaboration between these groups. Thus, the anonymity present in these correlations is even more striking in the $n > 3$ scenarios: not only are the groups of parties sharing $\mathcal{R}$ unidentifiable in an unambiguous manner, even the *size* of the groups are also not identifiable (see Fig. 7.2). For example, when

[2] In the *tripartite* scenario, the biseparability of the GHZ correlation was also discovered independently in [PBS11] (see also [Cer02; MPR04]).

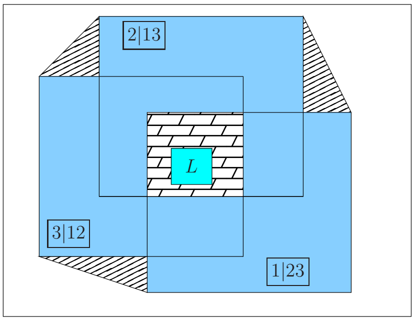

FIGURE 7.1: (Color online) Schematic representation of the various sets of tripartite correlations. Correlations biseparable with respect to party i in one group and parties j and k in the other lie in the (light blue) rectangle labelled by "$i|jk$". The convex hull of the three biseparable sets "$i|jk$" where $i, j, k \in \{1, 2, 3\}$ is represented by the filled convex region and gives the set of all biseparable correlations. The blank region between the outermost box and the filled convex region represents correlations that are genuinely tripartite nonlocal. Intersection of the three biseparable subsets "$i|jk$" gives correlations satisfying Eqs. (7.1a)–(7.1c); its subset featuring ANL is the tiled region while local correlations lie in the (cyan) rectangle L. Hatched regions represent biseparable correlations where classical mixture of different bipartitions is necessary for their production.

$n = 4$, the correlation satisfy:

$$P(\vec{a}|\vec{x}) = \sum_{\lambda_1} q_{\lambda_1} P_{\lambda_1}(a_1|x_1) P^{\mathcal{R}}_{\lambda_1}(a_2a_3a_4|x_2x_3x_4), \tag{7.3a}$$

$$= \sum_{\lambda_2} q_{\lambda_2} P_{\lambda_2}(a_2|x_2) P^{\mathcal{R}}_{\lambda_2}(a_1a_3a_4|x_1x_3x_4), \tag{7.3b}$$

$$= \cdots, \tag{7.3c}$$

$$= \sum_{\mu_3} q_{\mu_3} P^{\mathcal{R}}_{\mu_3}(a_1a_4|x_1x_4) P^{\mathcal{R}}_{\mu_3}(a_2a_3|x_2x_3), \tag{7.3d}$$

$$P(\vec{a}|\vec{x}) \neq \sum_{\theta} q_\theta \prod_{i=1}^{4} P_\theta(a_i|x_i), \tag{7.3e}$$

where $\sum_{\lambda_i} p_{\lambda_i} = \sum_{\mu_j} p_{\mu_j} = 1$, $p_i \geq 0$ for all i, j, and "$\cdots$" indicates other possible biseparable decompositions that have been omitted. From Eq. (7.3), we see that the 4-partite GHZ correlation could have been produced by having *any* three parties collaborating nonlocally, or *any* two groups of two parties collaborating nonlocally within each group. From the correlation itself, it is simply impossible to distinguish these possibilities apart (Fig. 7.2).

Let us now briefly comment on the relationship between ANL and multipartite

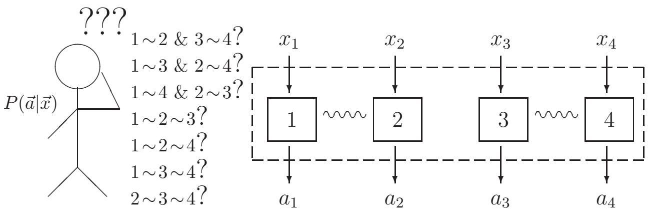

FIGURE 7.2: ANL in the 4-partite scenario. Each participating party is abstractly represented by a box labelled by the party number. The correlations were produced by having parties 1 & 2, as well as 3 & 4 collaborated nonlocally (symbolized by "∼"). To an outsider who only has access to $\vec{a}$ and $\vec{x}$, even if one is given the promise that the correlations were produced by the four parties separated into two fixed groups, it is impossible to tell which actual partitioning of the parties generated these correlations.

entanglement. Clearly, one expects that there must also be features analogous to ANL in the studies of multipartite entanglement. Indeed, the first of such examples dates back to the three-qubit bound entangled [HHH98] SHIFT state [Ben+99] where its entanglement was dubbed *delocalized* [DiV+03] since it is separable with respect to all bipartitions, yet not fully separable. A more recent example [VB12] involves a three-qubit bound entangled state which even violates a Bell inequality, thus giving also an example of anonymous quantum correlation. An important difference between their example and the tripartite case of our GHZ example is that their correlation can be produced by a biseparable tripartite entangled state whereas ours necessarily requires a genuinely tripartite entangled state. More generally, for all odd $n \geq 3$, we show in Appendix E.3 that the correlations of Eq. (7.2) can only be produced by genuinely n-partite entangled state. Our examples thus show that the generation of ANL does not require delocalized entanglement.

7.2 Perfect correlations with uniform marginals

From Eq. (7.2), we see that whenever an odd number of parties measure in the σ_y basis, the product of outcomes $\prod_i a_i$ gives ±1 with equal probability, otherwise it is either perfectly correlated or perfectly anti-correlated. Moreover, it follows from Eq. (7.2) that all marginal distributions of these correlations are uniformly random. Next, we present two quantum cryptography protocols that exploit these strong but anonymous correlations.

7.2.1 Application I: multipartite secret sharing (MSS)

Imagine that n parties wanted to share a secret message between *any* two complementary subgroups as they desire, i.e., between any subgroup of k parties ($k \leq n-1$) and the subgroup formed by the remaining parties. Suppose moreover that the shared secret is to be recovered by these subgroups *only when all parties* within each group collaborate (so that it is unnecessary to trust all parties within each group). A possibility to achieve this consists in: (i) the n parties share (many copies of) $|\mathrm{GHZ_n}\rangle$, (ii) each party randomly measures either the σ_x or the σ_y observable, (iii) the n parties are *randomly* separated into two groups and all parties assigned to the same group collaborate to compare their inputs and outputs, (iv) both *groups* announce their sum of inputs, (v) parties in the same group compute the product of their measurement outcome and deduce, using Eq. (7.2), the shared secret bit upon learning the sum of inputs of the other group, (vi) parties in one group use the shared secret keys to encrypt the message and send it to the other.

In the device-independent setting, security analysis is carried out by treating each physical subsystem together with their measurement device as a black box; conclusions are drawn directly from the measurement statistics. Indeed, the above protocol does not rely on the assumption of a GHZ state nor the particular measurements being performed, but rather the strong correlation present in Eq. (7.2) — for the right combination of inputs, the product of outputs are perfectly (anti) correlated.[3] Thus, the protocol essentially works by first distributing the correlated data needed to establish the secret keys, and performing the secret sharing [Sch07; GG97] between any two complementary subgroups of the n participating parties as they deem fit. Since the product of outcomes for each group is uniformly random, the protocol is secure against cheating by any dishonest parties within the group; no one can retrieve the shared key without collaborating with everyone else within the same group. What about eavesdropping by an external, post-quantum but non-signalling adversary Eve?

Since the GHZ correlations of Eq. (7.2) are biseparable, a naive attack by Eve may consist in preparing for the n parties the biseparable, non-signalling boxes that reproduces exactly Eq. (7.2). For instance, in the tripartite case, in accordance with the biseparable decomposition, she would prepare with equal probability 4 different versions of a deterministic box for one of the parties, and correspondingly 4 different versions of a PR box for the remaining two parties. If the decomposition that she chooses matches exactly the way the parties are separated into two groups, then after step (iv), she learns exactly the key and hence the message shared by these

[3] This happens in half the cases. In the other cases, the correlation is useless for key generation.

parties.[4] However, as the grouping is decided only after the measurement phase, she can guess the bipartition correctly only with a chance of $\frac{1}{3}$ in the tripartite case, and more generally $(2^{n-1}-1)^{-1}$ in the n-partite scenario. Evidently, this guessing probability rapidly approaches 0 as n increases, making it extremely difficult for Eve to succeed with this eavesdropping strategy for large n.

7.2.2 Application II: bipartite leakage-resilient QKD

Next, let us describe a quantum key distribution (QKD) protocol between two parties, A and B, which is as leakage-resilient [DP08; Sta+10; LRR14] as one could hope for. The protocol consists of: (i) preparation of many copies of $|\mathrm{GHZ_n}\rangle$, (ii) for each of these n-partite systems, a *randomly chosen subset*, say, k of the n subsystems are distributed to A, while the remaining $n-k$ subsystems are distributed to B, (iii) for each of these subsystems, A and B randomly measure σ_x or σ_y, (iv) both *parties* announce their sum of inputs, (v) for each n-partite system distributed from the source, A and B compute the product of their local measurement outcomes and deduce, using Eq. (7.2), the shared secret bit upon learning the sum of inputs of the other party.

As with the MSS protocol described above, the secret key is established through the perfect (anti) correlation present in the product of the outputs. Moreover, the gist of the protocol only relies on the correlation given by Eq. (7.2), rather than the actual state and measurement giving rise to this correlation, rendering the protocol ideal for device-independent analysis. However, in contrast with usual device-independent cryptography where leakage of information is not allowed, the above protocol is as leakage-resilient as one can hope for — the adversary Eve can certainly recover the secret key if all the output bits from either party leak to her, but if she misses merely one output bit from each party, the additional information that she gains from the leakage cannot improve her guess of the secret key. Now, if we *assume* that Eve has no control over how the subsystems are distributed in step (ii)[5] but otherwise only constrained by the non-signalling principle, then as with the MSS protocol, for n sufficiently large, her advantage of preparing some biseparable, non-signalling boxes for A & B is minimal.

[4] In this case, the product of outcomes for each group is a deterministic function (of the sum of inputs) known to Eve. The secret sharing protocol of Hillery *et al.* [HBB99] is thus insecure against this kind of attack by a non-signalling adversary.

[5] Instead of this assumption, A & B can employ *additional* measurement settings, cf. [AMP06], to certify that the overall correlations indeed exhibit genuine multipartite nonlocality and they are then again not susceptible to such an attack.

7.3 Discussion and conclusion

Let us now comment on some possible directions for future research. Clearly, we have only provided intuitions on why the protocols proposed above may be secure even in a device-independent setting. For odd $n \geq 3$, since the GHZ correlations violate the Mermin-Bell inequality maximally (see Appendix E.2), the result of Franz *et al.* [FFW11] implies that these correlations are necessarily monogamous with respect to any potential quantum eavesdropper. This strongly suggests that if we assume an independent-and-identically-distributed (i.i.d) scenario, a formal security proof of these protocols against a quantum adversary may be given even in the case with noisy correlations,[6] and in a device-independent setting. Evidently, a security proof without this assumption is even more desirable, and a possible path towards this is to prove that the protocols are even secure against an adversary that is only constrained by the non-signalling principle [PR94]. Our arguments on why the protocols are not immediately susceptible to a straightforward attack by such an eavesdropper, despite the fact that the correlations are biseparable, is an evidence pointing in this direction.

For leakage-resilient QKD, one could also imagine, instead of the above protocol, doing an existing QKD protocol many times in parallel and then using the XOR of the secret key bits to generate the final secret key. Although such a protocol requires many more qubits to establish the final secret key, it can clearly offer high level of leakage resilience. How would such a protocol perform compared with the above protocol based on $|\mathrm{GHZ_n}\rangle$? This certainly deserves some further investigation.

Coming back to ANL itself, let us note that the requirement of (1) nonlocality and (2) biseparability with respect to all bipartitions *may arguably not*, by themselves, imply that an outsider cannot attribute unambiguously the nonlocality to *any definite subset(s)* of the n parties. For instance, one may start with the tripartite GHZ correlation $P^3_{\mathrm{GHZ}}(\vec{a}|\vec{x})$, cf. Eq. (7.2), and trivially construct an example $P' = P^3_{\mathrm{GHZ}}(\vec{a}|\vec{x}) \prod_{i=4}^{n} P(a_i|x_i)$ for arbitrary n parties by introducing parties that are uncorrelated with the first three. While such an n-partite correlation P' indeed satisfies the two requirements stated above, one can unambiguously attribute the nonlocality present only to the three parties that give rise to $P^3_{\mathrm{GHZ}}(\vec{a}|\vec{x})$. Note, however, that such an identification is *incomplete* since the production of such a biseparable correlation only requires the nonlocal collaboration between two parties, and it is still impossible for an outsider to determine which two parties have collaborated nonlocally in producing the given correlation (Fig. 7.1 and Fig. 7.2). A

[6] Due to the noise robustness of the Mermin-Bell violation of $\vec{P}^n_{\mathrm{GHZ}}(\vec{a}|\vec{x})$, the ANL of $\vec{P}^n_{\mathrm{GHZ}}(\vec{a}|\vec{x})$ is also extremely robust to noise.

more precise definition of ANL may thus require also a specification of the extent (size) of the nonlocal resource needed in producing the given correlation, a task that shall be pursued elsewhere [Lia+14]. For our GHZ examples, except for the cases where n is even with $\frac{n}{2}$ odd, it can be shown (see Appendix E.4) using the result of Ref. [Ban+09] that the correlations of Eq. (7.2) are not triseparable, i.e., not producible by a partitioning of the parties into three groups (where only parties within the same group are allowed to collaborate nonlocally). Hence, the generation of these correlations indeed requires the nonlocal collaboration of at least $\lceil \frac{n}{2} \rceil$ parties in one group; an analogous statement for the remaining cases would be desirable.

Chapter 8

Overview and future perspectives

The objective of this thesis was to make steps forward in our understanding of: $i)$ how entanglement, nonlocality and other quantum features such as certified randomness relate to one another – both qualitatively and quantitatively; and $ii)$ the potentiality of entanglement and of nonlocal correlations as resources for device-independent information tasks.

With these objectives in mind, the contributions of this thesis are the following.

The nonlocal volume: a measure putting maximal entanglement and nonlocality in a quantitative equivalence.– In chapter 3, we got interested in whether "more" entanglement leads to "more" nonlocality and the concept of *anomalies*: so far, almost all measures of nonlocality put non maximally entangled states as maximally nonlocal. We were interested in understanding if these anomalies stem from a fundamental inequivalence, or rather as an artefact of the used measure of nonlocality. In this spirit, we studied a recently introduced measure of nonlocality defined as the probability that a state generates nonlocal correlations when random measurements are being performed on it – the *nonlocal volume*.

First, we proved that this measure satisfies basic properties as an operational measure of nonlocality. We have then provided both analytical and numerical results providing evidence that this measure puts maximal (pure state) entanglement and maximal nonlocality in a one-to-one correspondence. Our observations are to a large extent based on inclusion relations between the sets of measurements leading to nonlocal correlations when performed on different entangled systems. In particular, we have shown that correlation Bell inequalities (or XOR games) are monotones of entanglement for two-qubit systems: the more entanglement in a pure state, the larger the probability to violate these inequalities when random measurements are performed on it. Finally, we extended our results and observations to classes of multipartite systems.

Future perspectives: Our work represents the first analytical results using the nonlocal volume as a measure. The main reason why so little is know analytically about the measure is that it is typically difficult to tackle the problem directly as it involves solving complicated integrals. We circumvented the problem by studying the inclusion relations of the sets of measurements leading to a violation of correlation inequalities when made on different entangled systems. This opens a novel interesting direction of research: understand, more generally, what are the relations between the sets of measurements leading to nonlocal correlations when performed on different entangled systems.

Second, it would be interesting to explore specifically how our results and the inclusion relations of the sets of measurements generalise to scenarios with more outcomes. By generalising the notion of correlation inequalities[1], using Weyl operators for example, is it possible to extend the inclusion relations to set-ups with more outcomes?

Unbounded randomness certification using sequences of measurements.– We addressed the question of whether there exist fundamental bounds on the amount of randomness that can be generated from measurements on entangled systems. In the standard Bell scenario, each party performs a single measurement on its share of each copy of the system. In that scenario, only a finite amount of randomness of at most $4\log 2(d)$ bits can be certified from a pair of entangled particles of dimension d.

In chapter 4, we showed that this limitation can be overcome using sequences of measurements on the same system. More precisely, we proved that one can certify *any* amount of random bits from a pair of qubits in a pure state as the resource, even if it is arbitrarily weakly entangled. In addition, this certification is achieved by near-maximal violation of a particular Bell inequality for each measurement in the sequence. Our results show that entangled systems are unbounded sources of certified random numbers and of nonlocal correlations in a sequence.

Future perspectives:

The main objective of this work was to lift the limitations of the standard scenario for the certification of random numbers from measurements on quantum systems. As such, it should essentially be understood as a proof of principle. An important direction of future research is to explore its experimental feasibility. Indeed, our scheme can be adapted to one that is resistant to imperfections by generating only a finite amount of randomness. The first experiments implementing sequences of measurements on quantum systems have since then be performed. Nevertheless, these require a high level of trust and are not being performed in a DI manner, implying that no randomness can be certified from them. An experimental challenge is to come up with a true DI sequence of measurements. This should allow, in

[1] To be exact, one needs to generalise the Bell operator associated to the inequality, i.e. the operator acting on the state.

principle at least, for the implementation of a protocol generating random numbers in a sequence.

Second, it would be interesting to explore whether it is possible to certify randomness in a sequence as we do against a post-quantum adversary. Indeed, in our case the certification is built on the assumption that the adversary is bound by the laws of Quantum Theory. It would be interesting to explore how much randomness can be certified, for example, against a post-quantum but no-signalling adversary. One possibility is that Quantum Theory somehow is the only theory allowing for an unbounded amount of certified randomness in a sequence. A related problem is to achieve randomness amplification – and not only certification – from sequences of measurements.

Towards an equivalence between multipartite entanglement and multipartite nonlocality.– The equivalence between pure state entanglement and nonlocality has been established in the bipartite set-up and extended to the multipartite one: one can always find local measurements on such states such as to generate nonlocal correlations [Gis91; PR92; GG16]. Nevertheless, in the multipartite scenario the generated nonlocality has the caveat of being essentially bipartite. The equivalence between the genuine multipartite notions of entanglement and nonlocality is yet to be proven.

In chapter 5, we made steps towards showing the equivalence between genuine multipartite entanglement (GME) of pure states and genuine multipartite nonlocality (GMNL). Based on an operational understanding of multipartite entanglement, we developed a simple method to design Bell inequalities suited for the detection of multipartite nonlocal correlations generated from pure states. We first showed analytically that large classes of GME pure states violate our inequalites, even ones that are arbitrarily little entangled and for any number of observers. We also provided numerical evidence that all systems of three and four qubit in a GME pure state violate our inequalities. Our results, together with the very operational meaning of our inequalities, led us to conjecture that all GME pure states violate our inequalities for any number of observers.

Future perspectives: In our work, we have managed to show analytically that all GME pure states of three particles that are invariant under the permutation of two parties generate GMNL correlations. This was achieved using a single of our inequalities as witness. An important improvement would be to generalise our results to three-particle GME systems that have no symmetry, for which we have clear numerical evidence that the statement holds. A general proof of the equivalence between GME and GMNL for any number of parties seems difficult to tackle directly as no characterisation of GME pure states is know for more than three-qubit systems. One possibility would be to follow the lines of [PR92] and come up with a proof ad-absurdum.

Another interesting direction to explore is to understand the efficiency of our inequalities to witness multipartite nonlocal correlations generated from systems in a mixed state. One could also extend our numerical searches to larger number of parties in order to strengthen the evidences we already gathered. Finally, it would be interesting to try to implement an experiment for the violation of our inequalities for small numbers of parties but large classes of GME systems.

A framework for the study of correlations' depth.– It is in general harder to generate systems that are entangled between many parties rather than many systems entangled between fewer parties. A very natural way to quantify the complexity of multipartite nonlocal correlations is thus through the minimal size of the resource that is needed in order to generate them – the correlations' depth. Correlations that can be produced by distributing systems that are entangled between two parties only are then less complex than the ones that require entanglement between more parties. Naturally, the complexity of correlations also varies with the type of resources, as for example post-quantum but no-signalling ones, that are allowed. In chapter 6, we developed a framework for the study of the correlations' depth.

In addition, we provided a general recipe to construct Bell-like inequalities witnessing correlations' depth for any non-signalling resources, for any number of parties and any depth. Explicit examples of correlations where their MGS could be determined using this recipe and other numerical techniques were also provided.

Future perspectives: The first natural extension of our result was to obtain a simple family of inequalities – and not only ones that are build based on liftings of existing inequalities – witnessing $k-$depth of correlations. This was achieved in [Lia+15]. Further, in [Bac+18] the authors showed how to adapt technique based on semi-definite programming in order to quantify the depth of correlations. These results already provide useful tools for the detection of the depth of correlations. An interesting result would be to use this novel framework and tools in order to make the realisation of certain useful correlations "cheaper": these correlations would be generated by using entangled systems with lower depth than previously.

Additionally, it would be insightful to understand how and why the depth of certain nonlocal correlations varies in function of the nonlocal resources that is considered[2]. Is there an operational principle that would be violated if quantum correlations of a given depth were to be as powerful for the reproduction of nonlocal

[2] This is the case, for example, with the Mermin inequality[Mer90a]: the maximal (algebraic) bound of the inequality requires the use of GME entangled states, i.e. that are entangled between all parties. When using post-quantum but no-signalling resources, one only needs $\lceil \frac{n}{2} \rceil$ parties to be non-classically correlated [Lia+14].

correlations as post-quantum ones of the same depth?

Multipartite nonlocal correlations as resources for device-independent information tasks.– Multipartite set-ups are interesting at the fundamental level because richer notions of nonlocal correlations arise. Nevertheless, their potential use as resources in device-independent (DI) information tasks is less transparent. In chapter 7, we identified novel features characteristic of multipartite correlations and how these could be useful in DI tasks. A DI quantum key distribution (DIQKD) scheme that is resilient to leakage of information to the adversary and a secret sharing scheme between two groups of parties were proposed. A novel multipartite feature, anonymous nonlocality, allows parties to achieve an information task without revealing their identity, a potentially useful property in a cryptographic set-up.

Our work also hints at the fact that it is often not the multipartite extent of correlations that matters when designing information tasks. Rather, one should focus on other interesting properties – such as perfect correlations between parties – together with the fact that the correlations are nonlocal to any extent. From a resource-theoretic point of view, our work also sheds light on the potentiality of quantum resources as compared to post-quantum ones for the (re)production of nonlocal correlations. Indeed, we showed that the difference in the depth of certain correlations when using quantum resources as compared to no-signalling ones can be made arbitrarily large.

Future perspectives: It is desirable to understand whether there exist information tasks which require the generation of genuine multipartite nonlocal correlations (GMNL). Indeed, the characterisation of multipartite correlations and the quantification of their multipartite extent has seen some development lately, but are so far useful only for fundamental questions. In that spirit, it would be useful to understand if GMNL correlations also provide with true advantages in DI tasks.

Second, it would be interesting to compare the schemes we proposed, for example for DIQKD, with the ones where instead of using a multipartite entangled system one uses numerous bipartite systems. How multiple bipartite entangled systems compare to fewer multipartite ones in DI information tasks is an interesting question to investigate.

Appendix A

Appendices: Towards an equivalence between maximal entanglement and maximal nonlocality

A.1 Bell inequalities with single body correlators: violation with measurements on a partially entangled state only

Using linear programming, we obtained an example of particular local measurements that do not lead to nonlocality when made on the maximally entangled state, but do so on a partially entangled one. We checked that with our example, the inequality which is violated by the partially entangled state (3.1) with $\theta = \frac{3\pi}{16}$ contains single-body correlators, see Table A.2. Table A.1 presents Bloch vectors corresponding to Alice's and Bob's measurement settings, whereas Figure A.1 visualizes these vectors in the Bloch sphere.

TABLE A.1: Bloch vectors corresponding to measurement settings for A and B leading to the counterexample. Entanglement parameter $\theta = \frac{3\pi}{16}$.

Alice's measurements.

	$x = 0$	$x = 1$	$x = 2$
σ_x	0.0213	0.3539	0.8786
σ_y	0.9599	0.9320	−0.4772
σ_z	−0.2795	−0.0780	0.0176

Bob's measurements.

$y = 0$	$y = 1$	$y = 2$	$y = 3$
0.8685	0.0095	−0.0025	0.6437
0.2420	0.6762	0.6456	0.0175
0.4326	0.7367	−0.7636	−0.7651

TABLE A.2: The violated Bell inequality in the counterexample case organized in the Collins-Gisin correlator table. Entanglement parameter $\theta = \frac{3\pi}{16}$.

	$\langle A_0 \rangle$	$\langle A_1 \rangle$	$\langle A_2 \rangle$
$\langle B_0 \rangle$	$\langle A_0 B_0 \rangle$	$\langle A_1 B_0 \rangle$	$\langle A_2 B_0 \rangle$
$\langle B_1 \rangle$	$\langle A_0 B_1 \rangle$	$\langle A_1 B_1 \rangle$	$\langle A_2 B_1 \rangle$
$\langle B_2 \rangle$	$\langle A_0 B_2 \rangle$	$\langle A_1 B_2 \rangle$	$\langle A_2 B_2 \rangle$
$\langle B_3 \rangle$	$\langle A_0 B_3 \rangle$	$\langle A_1 B_3 \rangle$	$\langle A_2 B_3 \rangle$

$=$

	-0.25	0	0.25
-0.13	0.25	-0.25	-0.25
-0.13	0.25	0.25	-0.25
-0.01	0	0	0
0	-0.25	0	0.25

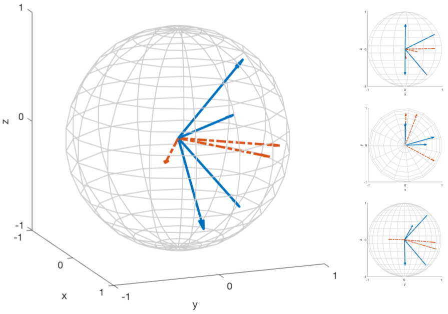

FIGURE A.1: Bloch vectors reproducing qubit counterexample measurement settings in the scenario $m_A = 3$, $m_B = 4$ for $\theta = \frac{3\pi}{16}$. Red solid vectors correspond to A's settings, blue dashed to B's. On the right projections to xz-plane, xy-plane and yz -plane are presented.

Appendix B

Appendices: Unbounded randomness certification using sequences of measurements

B.1 The guessing probability

We start our appendices with the following discussion, which is a summary of the work done in deriving the device-independent guessing probability (DIGP) [Pir+10; AMP12; NSPS14; Tor+15]. A conditional probability distribution that is the outcome distribution for some measurement on a quantum state is called a quantum distribution. For example, a distribution P with elements $p(ab|xy)$ is quantum if there exist at least one quantum state, i.e., a positive semi-definite hermitian unit trace matrix ρ and at least one set of measurements, i.e., a set of positive semi-definite hermitian matrices $M_{a|x}$, $M_{b|y}$ satisfying $\sum_a M_{a|x} = \sum_b M_{b|y} = 1$ such that $p(ab|xy) = Tr(M_{a|x} \otimes M_{b|y} \cdot \rho)$. We will often abuse notation and refer to a distribution by its elements $p(ab|xy)$ when there is no confusion in doing so.

The set $\mathcal{Q}$ of quantum distributions is convex and a distribution in $\mathcal{Q}$ that cannot be decomposed as a convex combination of other distributions is called *extremal* in $\mathcal{Q}$. For a non-extremal distribution $P(ab|xy)$ there is in general more than one possible convex decomposition.

A non-extremal distribution $p(ab|xy)$ with a convex decomposition $p(ab|xy) = \sum_\lambda q_\lambda p_\lambda(ab|xy)$ can be constructed by sampling the different distributions $p_\lambda(ab|xy)$ with probability q_λ. In this case knowledge about the convex decomposition chosen changes the ability of an eavesdropper to correctly guess the outcomes a and/or b.

Without knowledge of the decomposition, or for extremal distributions, the probability of correctly guessing the outcome of measurement y^0 is $\max_b p(b|y^0)$, the probability of the most likely outcome. With knowledge of the decomposition

$p(ab|xy) = \sum_\lambda q_\lambda p_\lambda(ab|xy)$, the probability is larger or equal to $\max_b p(b|y^0)$

$$\sum_\lambda q_\lambda \max_b p_\lambda(b|y^0) \geq \max_b \sum_\lambda q_\lambda p_\lambda(b|y^0) = \max_b p(b|y^0). \tag{B.1}$$

For a given observed non-extremal distribution P_{obs}, it is possible that it was produced by an agent Eve that has larger predictive power than an agent which only observes the outcomes.

We now want to consider the optimal probability for the agent Eve to correctly guess an outcome b of measurement y^0 given a distribution $p_{obs}(ab|xy)$ and control over its decomposition in extremal points. If the set of quantum distributions is closed there exist one or several optimal ways to decompose the given distribution that maximizes this probability. If the set is not closed but open or semi-open, there may not exist a maximum and the relevant quantity is instead the supremum value of Eves probability to correctly guess the outcome. Since $\max_b p(b|y^0)$ is a continuous function on the set of probability distributions it follows that the supremum value of $\sum_\lambda q_\lambda \max_b p_\lambda(b|y^0)$ as a function of all possible decompositions, indexed by λ, on an open or semi-open set of distributions is the same as the maximum value on the closure of the set. Therefore, in this case we can consider the closure of the set and express the probability as an optimization over the extremal points of this closed set.

With this disclaimer, the maximal probability for the agent Eve to correctly guess an outcome b of measurement y^0 given a distribution $p_{obs}(ab|xy)$ and control over the decomposition is the DIGP $G(y^0, P_{\mathrm{obs}})$

$$G(y^0, P_{\mathrm{obs}}) = \max_{q_\lambda, p_\lambda(ab|xy)} \sum_\lambda q_\lambda \max_b p_\lambda(b|y^0). \tag{B.2}$$

where λ is labelling the convex decompositions of $p_{\mathrm{obs}}(ab|xy)$ in terms of extremal distributions $p_\lambda(ab|xy)$. Note that if $\mathcal{Q}$ is not closed a given extremal point may not belong to the set but only to its closure. For any open interval of $\mathcal{Q}$ the function $G(y^0, P_{\mathrm{obs}})$ is a concave function [Pir+10]. Therefore this kind of maximization is called a *concave roof* construction.

The guessing probability can be approximated by a hierarchy of semidefinite programming (SDP) relaxations [NSPS14; BSS14]. We used Ncpol2sdpa [Wit15] to generate the relaxations for verifying some of the analytical results. We relied on the arbitrary-precision variant of the SDPA family of solvers [YFK03] for obtaining important numerical values, and the solver Mosek[1] in all other cases.

[1] `http://mosek.com/`

B.2 Continuity of the guessing probability in interior and extremal points of $\mathcal{Q}$

The guessing probability as a function on the space of probability distributions is not everywhere continuous. An example of this is that the family of Bell-inequalities of Ref. [AMP12] that certifies one bit of randomness for measurements on a state with arbitrarily little entanglement. The probability distribution corresponding to such a state and the measurements in Eq. 4.6 has $G(y^0, P_{obs}) = 1/2$ and is at the same time arbitrarily close to a distribution corresponding to measurements on a product state with $G(y^0, P_{obs}) = 1$, i.e., a distribution which can be prepared by a local deterministic procedure. There is thus a discontinuity where the guessing probability jumps from $1/2$ to 1. The key to understanding this discontinuity is that the local deterministic distribution is not extremal while the quantum distribution in the neighbouring point is extremal. As seen in Eq. B.1, the guessing probability is given by different functions depend ing on whether a distribution can be decomposed into other distributions or not, i.e., if it is extremal or not. This means discontinuities can appear at the boundary between extremal points and non-extremal points.

We will now show that discontinuities can *only* appear at such boundaries between extremal and non-extremal points in the boundary $\partial\mathcal{Q}$ of the quantum set $\mathcal{Q}$. To do this we use the property of the guessing probability described in Eq. B.1, together with some general properties of concave functions and in particular concave roof constructions.

We want to show that the following propositions are true:

Proposition 3. *The function $G(y^0, P_{obs})$ on the set of quantum distributions $\mathcal{Q}$ is continuous in the interior of $\mathcal{Q}$.*

Proposition 4. *The function $G(y^0, P_{obs})$ is continuous in any extremal point of $\mathcal{Q}$.*

Proposition 3 is trivial. The guessing probability $G(y^0, P_{\text{obs}})$ is concave by definition and any concave function is continuous on an open subset of its domain [Roc70]. In particular this means that $G(y^0, P_{\text{obs}})$ is continuous in the interior of $\mathcal{Q}$. Note that if $\mathcal{Q}$ is open, i.e. has no boundary, there can thus not exist any discontinuity.

To address proposition 4 we consider the restriction $G(y^0, P_{\text{obs}})^{\partial\mathcal{Q}}$ of $G(y^0, P_{\text{obs}})$ to the boundary $\partial\mathcal{Q}$ of the quantum set. First we note that the function $G(y^0, P_{\text{obs}})^{\partial\mathcal{Q}}$ by definition is continuous on any open set of extremal points since $\max_b p(b|y)$ is a continuous function. Next we observe that the boundary $\partial\mathcal{Q}$ can be decomposed into a collection of open sets of extremal points and a collection $\{S_i\}$ of closed connected possibly overlapping sets where each set is the closure of a maximal open connected subset. A maximal open connected subset M of the non-extremal points is an open set such that any other open connected set of non-extremal points which contains M is M itself. Therefore, each set S_i is the convex hull of the set of extremal points in its closure.

Any closed set S_i has a boundary ∂S_i with the rest of $\partial \mathcal{Q}$ which can be decomposed in the same way into open sets of extremal points and closed connected sets S_{ij} that are closures of maximal open connected sets of non-extremal points. The boundary ∂S_{ij} of S_{ij} with the rest of ∂S_i is in turn decomposable in the same way.

Continuing this successive decomposition of the boundary $\partial \mathcal{Q}$ we will eventually reach sets $S_{ijk...}$ that are one dimensional simplexes, or alternatively sets with only extremal points in the boundary. On sets of these two types $G(y^0, P_{\text{obs}})$ is a continuous function. To see this we introduce the following terminology, and use a theorem from Ref. [BL13].

A function for which all discontinuities are such that the function takes the higher value at a closed set and the lower value at an open set is called *upper semi-continuous*.

The function $G(y^0, P_{\text{obs}})^S$ defined on a closed convex set S can be viewed as an extension of $G(y^0, P_{\text{obs}})^{\partial S}$ to the interior of S. This extension is called the *concave roof extension*.

Theorem 14. *Let C be a compact set and $K = co(C)$ be the convex hull of C. If $F : C \to \mathbb{R}$ is bounded, upper semi-continuous, and concave on C, then the concave roof extension $\hat{F} : K \to \mathbb{R}$ of F to K is upper semi-continuous [BL13].*

The guessing probability is bounded and concave by definition. If the boundary of S has only extremal points it follows that $G(y^0, P_{\text{obs}})^{\partial S}$ is continuous in ∂S and by theorem 14 $G(y^0, P_{\text{obs}})^S$ is upper semi-continuous on S. Moreover, since $G(y^0, P_{\text{obs}})^S$ is concave it cannot have an upper semi-continuous discontinuity between the boundary and the interior. If S is a one-dimensional simplex we can, if necessary, restrict the domain of the guessing probability to a one dimensional subspace and make the same argument.

Next we consider discontinuities between S and an open set of extremal points.

Lemma 1. *Any discontinuity of $G(y^0, P_{obs})$ between a closed set and an open set of extremal points is upper semi-continuous.*

Proof. If the boundary point of the closed set is extremal the $G(y^0, P_{\text{obs}})$ is continuous since $\max_b p(b|y^0)$ is continuous. Next consider a non-extremal boundary point of the closed set. $G(y^0, P_{\text{obs}})$ in the non-extremal point is always greater or equal to $\max_b P(b|y^0)$ by Eq. B.1. Thus any discontinuity is upper semi-continuous. □

If there is a discontinuity of $G(y^0, P_{\text{obs}})$ on the boundary of S it is, by lemma 1 , upper semi-continuous and at a set of non-extremal points.

By repeated application of Theorem 14 and lemma 1 we can conclude that $G(y^0, P_{\mathrm{obs}})^{\partial\mathcal{Q}}$ is upper semi-continuous on $\partial\mathcal{Q}$ and that $G(y^0, P_{\mathrm{obs}})$ is upper semi-continuous on $\mathcal{Q}$. Since $G(y^0, P_{\mathrm{obs}})$ is concave there cannot be an upper semi-continuous discontinuity between the boundary $\partial\mathcal{Q}$ and the interior of $\mathcal{Q}$. Thus the only discontinuities are between non-extremal points in closed subsets of $\partial\mathcal{Q}$ and extremal points in open subsets of $\partial\mathcal{Q}$.

B.3 Bounds on the guessing probability as a function of a Bell inequality: Continuity at a unique point of maximal violation

We have described the guessing probability as a function on set of quantum distributions, but it is sometimes useful to consider it as a function of the violation of some given Bell inequality I. A Bell expression is a linear function on the space of distributions and the set of distributions for which it takes a given value t is a hyper-plane H_t. The different values of the Bell expression thus defines a family of parallel hyperplanes.

On each hyperplane H_t we can consider the restriction $G(y^0, P_{\mathrm{obs}})_t$ of $G(y^0, P_{\mathrm{obs}})$ to the intersection of H_t with $\mathcal{Q}$ and take its maximum $\max G(y^0, P_{\mathrm{obs}})_t$ on this intersection. This maximum is the highest probability for Eve to guess the outcome of y^0 for any distribution $P \in \mathcal{Q}$ such that $I(P) = t$. The function $\max G(y^0, P_{\mathrm{obs}})_t$ can have a discontinuity at $t = t_c$ only if H_{t_c} intersects with a point in $\mathcal{Q}$ at which $G(y^0, P_{\mathrm{obs}})$ is discontinuous.

Let us consider a Bell expression I and its maximal value t_{max} on $\mathcal{Q}$. If the intersection of $H_{t_{max}}$ and $\mathcal{Q}$ is a single extremal point it follows from Propositions 3 and 4 that there is a $t_c \neq t_{max}$ such that for the range $t_c \leq t \leq t_{max}$ for which $\max G(y^0, P_{\mathrm{obs}})_t$ is a continuous function of t.

If the intersection of $H_{t_{max}}$ and $\mathcal{Q}$ contains more than one extremal point it also contains a set of non-extremal points of $\partial\mathcal{Q}$ and $G(y^0, P_{\mathrm{obs}})$ could have a discontinuity between this set and an open set of extremal points. This discontinuity could lead to a discontinuity of the function $\max G(y^0, P_{\mathrm{obs}})_t$ at t_{max}.

B.4 Guessing probability for a sequence

So far, we have discussed the continuity properties of the guessing probability in the standard scenario, where one single measurement $M_{a|x}$ is made on Alice's side and $M_{b|y}$ on Bob's. The goal of this section is to extend these properties to the case where sequential measurements $M_{a_i|x_i}$ and $M_{b_i|y_i}$ are performed by each party, where i labels the position of a particular measurement in the sequence.

Let us consider a sequence of measurements $\hat{\sigma}(\xi_i)$ chosen by Bob and denote $(\xi_1, \xi_2, \ldots, \xi_n) \equiv \vec{\xi}$. The convex decomposition of the observed outcome distribution that gives Eve optimal probability to correctly guess the sequence of outcomes $\vec{b}_n$ of the measurements $(y_1^0, y_2^0, \ldots, y_n^0) \equiv \vec{y}_n^0$ is a function of $\vec{\xi}$. The guessing probability $G(\vec{y}_n^0, P_{\text{obs}})$ is thus given by

$$G(\vec{y}_n^0, P_{\text{obs}}) = \sum_{\lambda_{\vec{\xi}}} q_{\lambda_{\vec{\xi}}} \max_{\vec{b}_n} p_{\lambda_{\vec{\xi}}}(b_1|y_1^0) \cdot p_{\lambda_{\vec{\xi}}}(b_2|y_2^0, y_1^0, b_1) \ldots p_{\lambda_{\vec{\xi}}}(b_n|\vec{y}_n^0 \vec{b}_{n-1}). \tag{B.3}$$

where the extremal distributions $p_{\lambda_{\vec{\xi}}}(b_n|y_n \ldots)$ and weights $q_{\lambda_{\vec{\xi}}}$ of the optimal convex decomposition are functions of $\vec{\xi}$ as indicated by the index $\lambda_{\vec{\xi}}$. Let us assume that a term which appears in the convex combination is

$$q_{\lambda_{\vec{\xi}}} p_{\lambda_{\vec{\xi}}}(b_1|y_1^0) \ldots p_{\lambda_{\vec{\xi}}}(b_n|\vec{y}_n^0 \vec{b}_{n-1}). \tag{B.4}$$

Thus we assume that it corresponds to the most probable sequence of outcomes $\vec{b}_n$ for a specific distribution indexed by $\lambda_{\vec{\xi}}$.

Given that Eve has chosen the optimal convex decomposition for guessing the outcomes of $\vec{y}_n^0$ we consider her probability of correctly guessing the outcome of y_m^0 for $1 \leq m \leq n$ given a particular sequence of previous outcomes $\vec{b}_{m-1}$. It is given by

$$\sum_{\lambda_{\vec{\xi}}} k_{\lambda_{\vec{\xi}}} \max_{b_m} p_{\lambda_{\vec{\xi}}}(b_m|\vec{y}_m^0 \vec{b}_{m-1}), \tag{B.5}$$

where $k_{\lambda_{\vec{\xi}}}$ is the probability that the distribution indexed by $\lambda_{\vec{\xi}}$ will be sampled given the sequence of previous outcomes $\vec{b}_{m-1}$

$$k_{\lambda_{\vec{\xi}}} = \frac{q_{\lambda_{\vec{\xi}}} p_{\lambda_{\vec{\xi}}}(b_1|y_1^0) \ldots p_{\lambda_{\vec{\xi}}}(b_{m-1}|\vec{y}_{m-1}^0 \vec{b}_{m-2})}{\sum_{\lambda_{\vec{\xi}}} q_{\lambda_{\vec{\xi}}} p_{\lambda_{\vec{\xi}}}(b_1|y_1^0) \ldots p_{\lambda_{\vec{\xi}}}(b_{m-1}|\vec{y}_{m-1}^0 \vec{b}_{m-2})}. \tag{B.6}$$

The probability in Eq. B.5 is larger or equal to $1/d_m$, where d_m is the number of possible outputs b_m, but is lower or equal to $G(y_m^0, P_{\text{obs}})$, the maximal probability that Eve could guess the outcome of y_m^0 correctly given that she had chosen an optimal strategy for this and not the optimal strategy for guessing the outcomes of the sequence $\vec{y}_n^0$. Thus if $G(y_m^0, P_{\text{obs}})$ is close to $1/d_m$ so is the expression in Eq. B.5.

B.5 Arbitrarily close to n random bits for n measurements

We want to prove that $G(\vec{y}^0_n, P_{\text{obs}})$ can be made arbitrarily close to 2^{-n} by making $G(y^0_m, P_{\text{obs}})$ sufficiently close to 1/2 for each $1 \leq m \leq n$.

The proof relies on the fact that if a convex combination of a collection of numbers x_i equals a, i.e., $\sum_i k_i x_i = a$ where $\sum k_i = 1$, and if $x_i \geq a$ for each i, it follows that for every i either $k_i = 0$ or $x_i = a$.

From this follows that when $G(y^0_m, P_{\text{obs}})$ is very close to 1/2 either $\max_{b_m} p_{\lambda_{\vec{\xi}}}(b_m|\vec{y}^0_m \vec{b}_{m-1})$ in Eq. B.5 is very close to 1/2 or $k_{\lambda_{\vec{\xi}}}$ is very close to zero for each $\lambda_{\vec{\xi}}$. To see this more clearly we construct the following bound

$$\begin{aligned} k_{\lambda_{\vec{\xi}}} \max_{b_m} p_{\lambda_{\vec{\xi}}}(b_m|\vec{y}^0_m \vec{b}_{m-1}) &\leq G(y^0_m, P_{\text{obs}}) - \sum_{\lambda' \neq \lambda} k_{\lambda'_{\vec{\xi}}} \max_{b_m} p_{\lambda'_{\vec{\xi}}}(b_m|\vec{y}^0_m \vec{b}_{m-1}) \\ &\leq G(y^0_m, P_{\text{obs}}) - 1/2(1 - k_{\lambda_{\vec{\xi}}}) \end{aligned}$$

where we used $\max_{b_m} p_{\lambda'_{\vec{\xi}}}(b_m|\vec{y}^0_m \vec{b}_{m-1}) \geq 1/2$ for each $\lambda'_{\vec{\xi}}$ and $\sum_{\lambda' \neq \lambda} k_{\lambda'_{\vec{\xi}}} = 1 - k_{\lambda_{\vec{\xi}}}$. It follows that

$$G(y^0_m, P_{\text{obs}}) - 1/2 \geq k_{\lambda_{\vec{\xi}}} [\max_{b_m} p_{\lambda_{\vec{\xi}}}(b_m|\vec{y}^0_m \vec{b}_{m-1}) - 1/2],$$

and given Eq. (B.6) this implies

$$G(y^0_m, P_{\text{obs}}) - 1/2 \geq q_{\lambda_{\vec{\xi}}} p_{\lambda_{\vec{\xi}}}(b_1|y^0_1) \dots p_{\lambda_{\vec{\xi}}}(b_{m-1}|\vec{y}^0_{m-1} \vec{b}_{m-2}) [\max_{b_m} p_{\lambda_{\vec{\xi}}}(b_m|\vec{y}^0_n \vec{b}_{m-1}) - 1/2].$$

Thus for sufficiently small $G(y^0_m, P_{\text{obs}}) - 1/2$ either $\max_{b_m} p_{\lambda_{\vec{\xi}}}(b_m|\vec{y}^0_m \vec{b}_{m-1}) - 1/2$ can be made arbitrarily small, or the probability $q_{\lambda_{\vec{\xi}}} p_{\lambda_{\vec{\xi}}}(b_1|y^0_1) \dots p_{\lambda_{\vec{\xi}}}(b_{m-1}|\vec{y}^0_{m-1} \vec{b}_{m-2})$ that the distribution labelled by $\lambda_{\vec{\xi}}$ is sampled when y^0_m is measured is made arbitrarily small.

The argument can be made for any B_m. For B_1, it follows that either $p_{\lambda_{\vec{\xi}}}(b_1|y^0_1)$ is made arbitrarily close to $1/2$ or $q_{\lambda_{\vec{\xi}}}$ is made arbitrarily close to 0. For B_2, it follows that either $p_{\lambda_{\vec{\xi}}}(b_2|y^0_2 y^0_1 b_1)$ is made arbitrarily close to $1/2$ or $q_{\lambda_{\vec{\xi}}} p_{\lambda_{\vec{\xi}}}(b_1|y^0_1)$ is made arbitrarily close to zero. Given the second option and that $p_{\lambda_{\vec{\xi}}}(b_1|y^0_1)$ is made arbitrarily close to $1/2$ it is implied that that $q_{\lambda(\vec{\xi})}$ is made arbitrarily close to 0. If on the other hand $p_{\lambda_{\vec{\xi}}}(b_1|y^0_1)$ is not very close to $1/2$ it follows that $q_{\lambda_{\vec{\xi}}}$ is made arbitrarily close to zero by the preceding argument.

By induction it is clear that either the term in Eq. B.4 satisfies that $p_{\lambda_{\vec{\xi}}}(b_1|y_1^0)\dots p_{\lambda_{\vec{\xi}}}(b_n|\vec{y}_n^0\vec{b}_n$ can be made arbitrarily close to 2^{-n} or alternatively $q_{\lambda_{\vec{\xi}}}$ is made arbitrarily small. Since the same is true for every $\lambda_{\vec{\xi}}$ in Eq. B.3 it follows that $G(\vec{y}_n^0, P_{\text{obs}})$ can be made arbitrarily close to 2^{-n}.

Note that the above argument can be straightforwardly extended to the case where the number of outputs d_i for each B_i can be different from 2. Thus, in this case $G(\vec{y}_n^0, P_{\text{obs}})$ can be made arbitrarily close to $\prod_{i=1}^n d_i^{-1}$ by making $G(y_m^0, P_{\text{obs}})$ sufficiently close to $1/d_m$ for each $1 \leq m \leq n$.

B.6 Our programs to obtain lower bounds on the certified randomness

In this section of the appendices we give the tables of results for section 4.7. We remind the reader that the computational details – exposed in a pedagogical way – of our results can be found online at:

`https://github.com/peterwittek/ipython-notebooks/blob/master/Unbounded_randomness.ipynb`

TABLE B.1: $\theta = \frac{\pi}{4}$, the maximally entangled state

ξ	$\sharp$ random bits
0.000	1.000
0.013	0.962
0.027	0.925
0.040	0.890
0.053	0.855
0.067	0.822
0.080	0.790
0.093	0.759
0.106	0.729
0.120	0.700
0.133	0.673
0.146	0.647
0.160	0.622
0.173	0.598
0.186	0.575
0.200	0.554
0.213	0.533
0.226	0.514
0.240	0.494
0.253	0.473
0.266	0.452
0.280	0.430
0.293	0.409
0.306	0.387
0.319	0.365
0.333	0.342
0.346	0.320
0.359	0.298
0.373	0.276
0.386	0.254
0.399	0.233
0.413	0.211
0.426	0.190
0.439	0.170
0.453	0.150
0.466	0.130
0.479	0.111
0.493	0.093
0.506	0.075
0.519	0.058
0.532	0.042
0.546	0.027
0.559	0.012
0.572	0.000

TABLE B.2: $\theta = \frac{\pi}{8}$

ξ	$\sharp$ random bits
0.000	1.000
0.013	0.941
0.027	0.884
0.040	0.830
0.053	0.779
0.067	0.729
0.080	0.682
0.093	0.637
0.106	0.595
0.120	0.555
0.133	0.519
0.146	0.485
0.160	0.453
0.173	0.424
0.186	0.396
0.200	0.371
0.213	0.348
0.226	0.327
0.240	0.307
0.253	0.289
0.266	0.273
0.280	0.258
0.293	0.243
0.306	0.229
0.319	0.214
0.333	0.200
0.346	0.186
0.359	0.171
0.373	0.157
0.386	0.143
0.399	0.129
0.413	0.115
0.426	0.102
0.439	0.089
0.453	0.077
0.466	0.064
0.479	0.053
0.493	0.041
0.506	0.031
0.519	0.021
0.532	0.012
0.546	0.004
0.559	0.000
0.572	0.000

TABLE B.3: $\theta = \frac{\pi}{16}$

ξ	$\sharp$ random bits
0.000	1.000
0.013	0.896
0.027	0.800
0.040	0.714
0.053	0.641
0.067	0.577
0.080	0.521
0.093	0.473
0.106	0.429
0.120	0.391
0.133	0.356
0.146	0.325
0.160	0.297
0.173	0.271
0.186	0.248
0.200	0.227
0.213	0.207
0.226	0.190
0.240	0.174
0.253	0.159
0.266	0.146
0.280	0.134
0.293	0.122
0.306	0.112
0.319	0.103
0.333	0.095
0.346	0.087
0.359	0.078
0.373	0.070
0.386	0.062
0.399	0.055
0.413	0.047
0.426	0.040
0.439	0.034
0.453	0.027
0.466	0.021
0.479	0.016
0.493	0.011
0.506	0.007
0.519	0.003
0.532	0.000
0.546	0.000
0.559	0.000
0.572	0.000

TABLE B.4: $\theta = \frac{\pi}{32}$

ξ	$\sharp$ random bits
0.000	1.000
0.013	0.823
0.027	0.706
0.040	0.619
0.053	0.551
0.067	0.493
0.080	0.444
0.093	0.400
0.106	0.362
0.120	0.328
0.133	0.297
0.146	0.269
0.160	0.244
0.173	0.221
0.186	0.200
0.200	0.181
0.213	0.163
0.226	0.147
0.240	0.133
0.253	0.119
0.266	0.107
0.280	0.095
0.293	0.085
0.306	0.076
0.319	0.067
0.333	0.059
0.346	0.052
0.359	0.046
0.373	0.040
0.386	0.035
0.399	0.030
0.413	0.025
0.426	0.021
0.439	0.017
0.453	0.013
0.466	0.009
0.479	0.006
0.493	0.004
0.506	0.002
0.519	0.000
0.532	0.000
0.546	0.000
0.559	0.000
0.572	0.000

Appendix C

Appendices: A simple approach to genuine multipartite nonlocality of pure states

C.1 Lifting Bell inequalities to more observers

The technique of lifting a Bell inequality consists in taking an inequality designed for a specific Bell set-up – with a fixed number of observers, measurements and outcomes–, and extending it to a set-up with an increased number of any of these variables. Here we are interested in lifting a Bell inequality to more observers. We will briefly review its definition and prove one property of these inequalities, which is used in Theorems 5 and 7.

Consider a Bell inequality for two observers (**??**) that, without loss of generality, can be written as

$$\mathcal{I} = \sum_{a_1a_2x_1x_2} c^{x_1x_2}_{a_1a_2} P(a_1a_2|x_1x_2) \leq 0 \tag{C.1}$$

where observer A_i performs a measurement x_i and obtains an outcome a_i. The coefficients $c^{x_1x_2}_{a_1a_2}$ are real numbers and $P(a_1a_2|x_1x_2)$ represents the observed outcome distribution, for each measurement pair. A *lifting* of this Bell inequality to n observers consists in extending the expression (C.1) by choosing a fixed measurement and outcome for observers $A_3, \ldots, A_n$:

$$\mathcal{I}^{A_1A_2}_{\vec{0}|\vec{0}} = \sum_{a_1a_2x_1x_2} c^{x_1x_2}_{a_1a_2} P(a_1a_2\vec{0}|x_1x_2\vec{0}) \leq 0 \tag{C.2}$$

where, without loss of generality, the fixed $n-2$ measurements and outcomes are set to $\vec{0} = \{0, \ldots, 0\}$. Notice that $P(a_1a_2\vec{0}|x_1x_2\vec{0}) = P(a_1a_2|x_1x_2, \vec{0}, \vec{0})P(\vec{0}|\vec{0})$, where $P(\vec{0}|\vec{0})$ is independent of measurements x_1 and x_2 according to the no-signaling principle. This means that if the conditional distribution $P_{\vec{0},\vec{0}}(a_1a_2|x_1x_2) \equiv$

$P(a_1a_2|x_1x_2,\vec{0},\vec{0})$ violates the bipartite inequality (C.1), it implies that the full distribution $P(\vec{a}|\vec{x})$ violates the lifted inequality (C.2). Therefore, the nonlocality of the conditional distribution is a sufficient condition for the nonlocality of the full distribution.

We now want to show that any biseparable distribution (5.19) where parties A_1 and A_2 belong to different groups of parties, $A_1 \in g$ and $A_2 \in \bar{g}$, does not violate a lifted Bell inequality (C.2):

$$\mathcal{I}^{A_1A_2}_{\vec{0}|\vec{0}}(P^{g/\bar{g}}_{\text{bisep}}) \leq 0 \tag{C.3}$$

Since a Bell inequality is a linear function and $P^{g/\bar{g}}_{\text{bisep}}$ is convex, it is enough to show that the previous inequality holds for any pure biseparable distribution $P(\vec{a}_g|\vec{x}_g)P(\vec{a}_{\bar{g}}|\vec{x}_{\bar{g}})$. We have then

$$\begin{aligned} \mathcal{I}^{A_1A_2}_{\vec{0}|\vec{0}}(P(\vec{a}_g|\vec{x}_g)P(\vec{a}_{\bar{g}}|\vec{x}_{\bar{g}})) &= \sum_{a_1a_2x_1x_2} c^{x_1x_2}_{a_1a_2} P_g(a_1\vec{0}|x_1\vec{0})P_{\bar{g}}(a_2\vec{0}|x_2\vec{0}) \\ = \sum_{a_1a_2x_1x_2} c^{x_1x_2}_{a_1a_2} P_{A_1}(a_1|x_1,\vec{0},\vec{0})&P_{A_2}(a_2|x_2,\vec{0},\vec{0})P_{g\setminus A_1}(\vec{0}|\vec{0})P_{\bar{g}\setminus A_1}(\vec{0}|\vec{0}) \leq 0 \end{aligned} \tag{C.4}$$

where the size of the vector $\vec{0}$ should be clear by the context. Notice that we have again used the fact that the distributions are no-signaling and that $P_{A_i}(a_i|x_i,\vec{0},\vec{0})$ are well-defined local distributions.

C.2 Properties of our families of Bell inequalities

C.2.1 The family of Bell inequalities $I^{A_1A_2\ldots A_n}_{\text{sym}}$ (5.20) witnesses genuine multipartite nonlocality

In this section we want to give a more detailed proof of Theorem 7, which states that for any number $n \geq 3$ of observers, all biseparable distributions (5.19) satisfy our family of inequalities (5.20),

$$I^{A_1A_2\ldots A_n}_{\text{sym}} = \sum_{i=1}^{n-1}\sum_{j>i}^{n} I^{A_iA_j}_{\vec{0}|\vec{0}} - \binom{n-1}{2} P(\vec{0}|\vec{0}) \leq 0 \tag{C.5}$$

where $\binom{n-1}{2} = \frac{(n-1)(n-2)}{2}$ and thus $I^{A_1A_2\ldots A_n}$ witnesses GMNL in the distributions. The proof for the family of inequalities $I^{A_1\ldots A_n}_{①}$ (5.21) follows exactly the same lines.

Proof. Our Bell inequalities $I^{A_1A_2\ldots A_n}$ are invariant under permutations of the observers. Since a Bell inequality is a linear function of the probability terms $P(\vec{a}|\vec{x})$, and by the convexity of biseparable distributions (5.19), we can restrict the proof – without loss of generality – to pure biseparable distributions of the form

$$P_{m/(n-m)} \equiv P(a_1a_2\ldots a_m|x_1x_2\ldots x_m)P(a_{m+1}a_{m+2}\ldots a_n|x_{m+1}x_{m+2}\ldots x_n)\,, \tag{C.6}$$

where the first term includes the variables of the m first observers and the second the remaining $n-m$. Let us recall that, inside each group, observers are allowed to share any no-signaling nonlocal resources. Our proof consists in counting how many lifted inequalities $I^{A_iA_j}_{\vec{0}|\vec{0}}$ (5.22) can be violated by a pure biseparable distribution (C.6). We will see that this happens to *at most* $\binom{n-1}{2}$ lifted inequalities. Indeed, a term $I^{A_iA_j}_{\vec{0}|\vec{0}}$ can only be positive if observers A_i and A_j belong to the same group ($i,j \leq m$ or $i,j > m$), since otherwise there are only classically correlated (see Appendix C.1). Thus

$$\begin{aligned}
I^{A_1A_2\ldots A_n}_{\text{sym}}(P_{m/(n-m)}) &\leq \sum_{i=1}^{m-1}\sum_{j>i}^{m} I^{A_iA_j}_{\vec{0}|\vec{0}} + \sum_{k=m+1}^{n-1}\sum_{l>k}^{n} I^{A_kA_l}_{\vec{0}|\vec{0}} - \binom{n-1}{2}P(\vec{0}|\vec{0}) \\
&= \sum_{i=1}^{m-1}\sum_{j>i}^{m} I^{A_iA_j}_{\vec{0}|\vec{0}} - \binom{m}{2}P(\vec{0}|\vec{0}) + \sum_{k=m+1}^{n-1}\sum_{l>k}^{n} I^{A_kA_l}_{\vec{0}|\vec{0}} - \binom{n-m}{2}P(\vec{0}|\vec{0}) \\
&\qquad -(m-1)(n-m-1)P(\vec{0}|\vec{0}) \\
&= \sum_{i=1}^{m-1}\sum_{j>i}^{m} \bar{I}^{A_iA_j}_{\vec{0}|\vec{0}} + \sum_{k=m+1}^{n-1}\sum_{l>k}^{n} \bar{I}^{A_kA_l}_{\vec{0}|\vec{0}} - (m-1)(n-m-1)P(\vec{0}|\vec{0}) \\
&\leq -(m-1)(n-m-1)P(\vec{0}|\vec{0}) \leq 0
\end{aligned} \tag{C.7}$$

in which we have used the fact that $\sum_{i=1}^{m-1}\sum_{j>i}^{m} I^{A_iA_j}_{\vec{0}|\vec{0}}$ contains $\binom{m}{2}$ lifted terms and $\sum_{k=m+1}^{n-1}\sum_{l>k}^{n} I^{A_kA_l}_{\vec{0}|\vec{0}}$ contains $\binom{n-m}{2}$ of them. We have further used $\bar{I}^{A_iA_j}_{\vec{0}|\vec{0}} \equiv I^{A_iA_j}_{\vec{0}|\vec{0}} - P(\vec{0}|\vec{0}) \leq 0$, for any i,j (see equation (5.24)). Notice that the situation where most lifted terms $I^{A_iA_j}_{\vec{0}|\vec{0}}$ could be positive occurs for bipartitions of one versus $n-1$ observers, hence the $\binom{n-1}{2}$ factor in our Bell inequalities (C.5). □

C.2.2 A recursive formula for our inequalities

Our family of Bell inequalities $I_{\text{sym}}^{A_1A_2\ldots A_n}$ can also be written in a recursive form, which shows its rich multipartite structure and operational meaning:

$$I_{\text{sym}}^{A_1A_2\ldots A_n} = \frac{1}{n-2}\sum_{i=1}^{n} I_{0|0}^{\text{all}\setminus A_i} - P(\vec{0}|\vec{0}) \leq 0 \tag{C.8}$$

for $n \geq 3$, where $I_{0|0}^{\text{all}\setminus A_i}$ is the Bell inequality testing genuine nonlocality between $n-1$ parties lifted to n parties, with party A_i's input and outcome set to 0

$$I_{0|0}^{\text{all}\setminus A_i} = \frac{1}{n-3}\sum_{\substack{j=1\\ j\neq i}}^{n} I_{0|0}^{\text{all}\setminus A_iA_j} - P(\vec{0}|\vec{0})\,. \tag{C.9}$$

The seed of this recursive expression is the variant of the CHSH inequality (5.2).

Proof. We prove that the recursive expression (C.8) is equivalent to the direct expression (C.5) for $I_{\text{sym}}^{A_1A_2\ldots A_n}$ through mathematical induction. First, we check that for $n=3$ the equivalence holds, which can easily be done by developing both expressions. Then, we show that if the equivalence is true for n, it implies that it is true also for $n+1$.

Suppose the equivalence holds for n:

$$\frac{1}{n-2}\sum_{i=1}^{n} I_{0|0}^{\text{all}\setminus A_i} - P(\vec{0}|\vec{0}) = \sum_{i=1}^{n-1}\sum_{j>i}^{n} I_{\vec{0}|\vec{0}}^{A_iA_j} - \binom{n-1}{2}P(\vec{0}|\vec{0})\,. \tag{C.10}$$

For $n+1$, we develop the recursive expression in (C.8), where $I_{0|0}^{\text{all}\setminus A_i}$ is now an n observer inequality for which the recurrence hypothesis (C.10) can be used:

$$\begin{aligned}
&\frac{1}{n-1}\sum_{i=1}^{n+1} I_{0|0}^{\text{all}\setminus A_i} - P(\vec{0}|\vec{0})\\
&\overset{(\text{C.10})}{=} \frac{1}{n-1}\sum_{i=1}^{n+1}\left(\sum_{\substack{j=1\\ j\neq i}}^{n}\sum_{\substack{k>j\\ k\neq i}}^{n+1} I_{\vec{0}|\vec{0}}^{A_jA_k} - \binom{n-1}{2}P(\vec{0}|\vec{0})\right) - P(\vec{0}|\vec{0})\\
&= \frac{1}{n-1}\sum_{i=1}^{n+1}\left(\sum_{\substack{j=1\\ j\neq i}}^{n}\sum_{\substack{k>j\\ k\neq i}}^{n+1} I_{\vec{0}|\vec{0}}^{A_jA_k}\right) - \left(\frac{n+1}{n-1}\binom{n-1}{2}+1\right)P(\vec{0}|\vec{0})
\end{aligned} \tag{C.11}$$

Note that the last expression can be simplified taking into account that the terms $I_{\vec{0}|\vec{0}}^{A_jA_k}$ are being counted multiple times. Since the inequalities are invariant under permutations of observers, we can restrict our attention to counting how many times the particular term $I^{A_1A_2}_{\vec{0}|\vec{0}}$ appears in (C.11). One can check that $\sum\limits_{\substack{j=1\\j\neq i}}^{n}\sum\limits_{\substack{k>j\\k\neq i}}^{n+1} I^{A_jA_k}_{\vec{0}|\vec{0}}$ gives one term $I^{A_1A_2}_{\vec{0}|\vec{0}}$ if $i \neq 1,2$. Suming over i, we get a total of $n-1$ terms, from which we obtain

$$\frac{1}{n-1}\sum_{i=1}^{n+1}\left(\sum_{\substack{j=1\\j\neq i}}^{n}\sum_{\substack{k>j\\k\neq i}}^{n+1} I^{A_jA_k}_{\vec{0}|\vec{0}}\right) - \left(\frac{n+1}{n-1}\binom{n-1}{2}+1\right)P(\vec{0}|\vec{0}) = \sum_{j=1}^{n}\sum_{k>j}^{n+1} I^{A_jA_k}_{\vec{0}|\vec{0}} - \binom{n}{2}P(\vec{0}|\vec{0}) \tag{C.12}$$

where we used $\frac{n+1}{n-1}\binom{n-1}{2}+1 = \binom{n}{2}$. Since the last expression coincides with the direct expression (C.5) for $n+1$ observers, we finish our proof. □

C.2.3 Fully local strategies that saturate the inequalities

Interestingly, one can check that the (fully) local strategy

$$P_{\text{L}}(a_1a_2...a_n|x_1x_2...x_n) = \begin{cases} 1 & \text{if} \quad a_i = 1 \;\; \forall i \text{ and } \forall x_i \\ 0 & \text{else} \end{cases} \tag{C.13}$$

saturates our families of inequalities (5.20) and (5.21) since there is no term in the inequalities where all outcomes have value 1. Nonlocal resources shared between a subset of the observers are thus useless to reach better bounds on our family, only nonlocal resources shared between *all* observers are relevant. Remark that these observation generalise to all the families of inequalities that have the CHSH inequality $I^{A_1A_2}$ (5.2) as seed.

C.2.4 Post-quantum no-signaling resources that violate the inequalites

Consider a genuine multipartite generalisation of the (no-signaling) PR-box [PR94]:

$$P_{\text{NS}}(\vec{a}|\vec{x}) = \begin{cases} \frac{1}{2^{n-1}} & \text{if} \quad \oplus_{i=1}^{n} a_i = \oplus_{i=1}^{n-1} \oplus_{j>i}^{n} x_i x_j \\ 0 & \text{else} \end{cases} \tag{C.14}$$

where the marginal distributions are completely random, i.e. $P_{\text{NS}}(a_i|x_i) = \frac{1}{2}, \forall i$. It is interesting to see that this post-quantum no-signaling distribution violates our Bell inequalities $I^{A_1A_2...A_n}$, for all $n \geq 2$,

$$I^{A_1A_2...A_n}_{\text{sym}}(P_{\text{NS}}) = \frac{n-1}{2^{n-1}} > 0\,. \tag{C.15}$$

Proof. The proof follows from direct evaluation of our inequalities (C.5) with the no-signaling box (C.14). First, we get that $I^{A_iA_j}_{\vec{0}|\vec{0}}(P_{\text{NS}}) \overset{(5.22)}{=} P_{\text{NS}}(\vec{0}|\vec{0}) \quad \forall i,j$ because $P_{\text{NS}}(\vec{0}|\vec{0})$ is the only non-vanishing term. Then

$$\begin{aligned} I^{A_1A_2\ldots A_n}_{\text{sym}}(P_{\text{NS}}) &= \sum_{i=1}^{n-1}\sum_{j>i}^{n} P_{\text{NS}}(\vec{0}|\vec{0}) - \binom{n-1}{2} P_{\text{NS}}(\vec{0}|\vec{0}) \\ &= \frac{1}{2^{n-1}}\left[\binom{n}{2} - \binom{n-1}{2}\right] = \frac{n-1}{2^{n-1}} > 0, \quad \forall n \geq 2 \end{aligned} \tag{C.16}$$

which finishes our proof. □

A similar proof can be made for the inequalities in the family $I^{A_1\ldots A_n}_{①}$ (5.21).

C.3 All pure GME states of the family $|GHZ^n\rangle_\theta = \cos\theta|0\rangle^{\otimes n} - \sin\theta|1\rangle^{\otimes n}$ generate GMNL correlations

Here we prove Theorem 8 in detail.

Proof. Our proof is constructive as we will provide, for all states

$$|GHZ^n\rangle_\theta = \cos\theta|0\rangle^{\otimes n} - \sin\theta|1\rangle^{\otimes n} \tag{C.17}$$

with $\theta \in]0, \frac{\pi}{4}[$, local measurements that lead to explicit distributions $P_{GHZ^n_\theta}(\vec{a}|\vec{x})$ violating our family of inequalities $I^{A_1\ldots A_n}_{\text{sym}}$(5.20).

In order to provide symmetry to the problem, and significantly reduce the degrees of freedom, all the observers use the same projective measurements $m_{a_i|x_i} = m_{a|x}$:

$$\begin{aligned} m_{0|x} &= \cos\alpha_x\langle 0| + \sin\alpha_x\langle 1| \\ m_{1|x} &= \sin(\alpha_x\langle 0| - \cos\alpha_x\langle 1|\,. \end{aligned} \tag{C.18}$$

Since both the state (C.17) and measurements (C.18) are invariant under permutations of the observers, the generated distribution $P_{GHZ^n_\theta}(\vec{a}|\vec{x})$ also has this symmetry. For three observers for example, we get that $P(100|100) = P(010|010) = P(001|001)$ or $P(000|011) = P(000|101) = P(000|110)$ or that the lifted inequalities are all equal $I^{A_1A_2}_{\vec{0}|\vec{0}} = I^{A_1A_3}_{\vec{0}|\vec{0}} = I^{A_2A_3}_{\vec{0}|\vec{0}}$. This implies that inequalities $I^{A_1\ldots A_n}$

(5.21), when evaluated on the generated distributions, simplify to

$$\begin{aligned} I_{\text{sym}}^{A_1A_2\ldots A_n}(P_{GHZ_\theta^n}) &= \binom{n}{2} I_{\vec{0}|\vec{0}}^{A_1A_2} - \binom{n-1}{2} P(\vec{0}|\vec{0}) \\ = (n-1)P(00\vec{0}|00\vec{0}) &- 2\binom{n}{2} P(10\vec{0}|10\vec{0}) - \binom{n}{2} P(00\vec{0}|11\vec{0}) \end{aligned} \tag{C.19}$$

where we have used that $\binom{n}{2} - \binom{n-1}{2} = n-1$. Using measurements (C.18) on the state (C.17) we obtain all the terms of (C.19)

$$\begin{aligned} P(00\vec{0}|00\vec{0}) &= \big(\cos^n(\alpha_0)\cos(\theta) - \sin^n(\alpha_0)\sin(\theta)\big)^2 \\ P(10\vec{0}|10\vec{0}) &= \big(\cos^{n-1}(\alpha_0)\sin(\alpha_1)\cos(\theta) + \sin^{n-1}(\alpha_0)\cos(\alpha_1)\sin(\theta)\big)^2 \\ P(00\vec{0}|11\vec{0}) &= \big(\cos^{n-2}(\alpha_0)\cos^2(\alpha_1)\cos(\theta) - \sin^{n-2}(\alpha_0)\sin^2(\alpha_1)\sin(\theta)\big)^2 \end{aligned} \tag{C.20}$$

We want now to find angles α_x of the local measurements (C.18) such that the quantity (C.19) is always positive. A particular solution is

$$\begin{cases} P(00\vec{0}|00\vec{0}) > 0 \\ P(10\vec{0}|10\vec{0}) = P(00\vec{0}|11\vec{0}) = 0 \end{cases} . \tag{C.21}$$

which holds true for angles

$$\begin{aligned} \alpha_0 &= \arctan(\tan^{\frac{-3}{3n-4}}\theta) \\ \alpha_1 &= -\arctan(\tan^{\frac{-1}{3n-4}}\theta) \end{aligned} \tag{C.22}$$

when $\theta \in]0, \frac{\pi}{4}[$. The value of the inequalities at these angles is

$$\begin{aligned} I_{\text{sym}}^{A_1A_2\ldots A_n}(P_{GHZ}(\vec{a}|\vec{x})) &= (n-1)P(00\vec{0}|00\vec{0}) \\ = (n-1)\big(\cos^n(\arctan(\tan^{\frac{-3}{3n-4}}\theta))\cos(\theta) &- \sin^n\left(\arctan(\tan^{\frac{-3}{3n-4}}\theta)\right)\sin(\theta)\big)^2 \end{aligned} \tag{C.23}$$

which is positive for $\theta \in]0, \pi/4[$, as promised. □

For the maximally entangled state ($\theta = \pi/4$) we have $P(\vec{0}|\vec{0}) = 0$, which means that our construction breaks. However, this state is already known to be genuine multipartite nonlocal for all number of observers [Ban+09], and moreover we numerically found several sets of measurements on it that lead to a violation of our inequalities.

C.4 Proof of theorem 6

We here provide a formal proof of theorem 6. Let us start with an observation that will be used in the upcoming proof.

Observation.– On any pure, non maximally entangled, two qubit state

$$|\phi_\theta\rangle = cos(\theta)|00\rangle + sin(\theta)|11\rangle \tag{C.24}$$

i.e. for $\theta \in]0, \frac{\pi}{4}[$, the measurements

$$\begin{aligned} M_{0|0} &= cos(\alpha)\langle 0| + e^{i\delta} sin(\alpha)\langle 1| \\ M_{0|1} &\propto cos^2(\theta)cos(\alpha)\langle 0| + e^{i\delta} sin^2(\theta)sin(\alpha)\langle 1| \\ \\ N_{0|0} &\propto sin^3(\theta)e^{i\delta} sin(\alpha)\langle 0| - cos^3(\theta)cos(\alpha)\langle 1| \\ N_{0|1} &\propto sin(\theta)sin(\alpha)e^{i\delta}\langle 0| - cos(\theta)cos(\alpha)\langle 1| \end{aligned} \tag{C.25}$$

lead to correlations $P_\theta(ab|xy) = \langle\phi_\theta|\big(M_{a|x} \otimes N_{b|y}\big)|\phi_\theta\rangle$ that violate inequality (5.2) $I^{A_1A_2}(P_\theta(ab|xy)) > 0$ with the free parameters α and δ such that $\alpha \neq 0, \pi/2$ for any $\theta \neq 0, \pi/4$. More precisely, they lead to the particular violation of the inequality (5.2)

$$I^{A_1A_2}(P_\theta(ab|xy)) = P_\theta(00|00) > 0 \tag{C.26}$$

and thus $P_\theta(01|01) = P_\theta(10|10) = P_\theta(00|11) = 0$, i.e. a realisation of the bipartite Hardy paradox [Har93]. A proof of this observations can be found further in the appendices C.5.

Since we are interested in a violation up to any extent of our inequality

$$I^{A_1A_2}(P_\theta(ab|xy)) > 0 \tag{C.27}$$

whose bound is zero, we have taken the freedom not to normalise some of the measurements in (C.25). In other words, the observation (C.4) implies that for any non-maximally entangled pure two qubit state $|\phi_\theta\rangle$ (C.24), one can chose one of the measurement of one of the parties for free (as expressed by the free parameters α and δ such that $\alpha \neq 0, \pi/2$) and still find three other measurements such that the generated correlations violated the inequality.

Now we want to show that a large class of three qubit GME states violate inequality$I^{A_1A_2A_3}_{\mu=0}$ (5.5). In [Ací+00], it was shown that all three qubits in a pure state could be written as

$$|\Psi_3\rangle = h_0|000\rangle + h_1 e^{i\phi}|100\rangle + h_2|101\rangle + h_3|110\rangle + h_4|111\rangle \tag{C.28}$$

where $h_i \geq 0$, $\sum_i h_i^2 = 1$ and $\phi \in [0, \pi]$. On these states, we impose the additional constrain that $h_2 = h_3$, i.e. we consider only the states (C.28) which are symmetrical with respect to the permutations of the parties $A_2 \leftrightarrow A_3$. By relabelling the parties' index, however, any state which is symmetrical with respect to the permutation of two out of the three parties can be transformed to one where the symmetry is between parties A_2 and A_3, which we chose without loss of generality. Now, party A_2 and A_3 both make the same projective measurement $\langle m_{a_i|x_i}|$ for their input choice $x_2 = x_3 = 0$

$$\langle m_{0|x_i=0}| = \cos(\alpha)\langle 0| + \sin(\alpha)\langle 1| \tag{C.29}$$

for some (yet) free angle α[1]. The state that is prepared between parties A_1A_3 (resp. A_1A_2) from party A_2 (A_3) by performing measurement $\langle m_{0|x_i=0}|$ (C.29) on the state $|\Psi_3\rangle$ (C.28) conditioned on obtaining the outcome $a_2 = 0$ ($a_3 = 0$) is

$$\begin{aligned} |\psi_{0|0}^{A_1A_2}\rangle = |\psi_{0|0}^{A_1A_3}\rangle \propto \cos(\alpha)h_0|00\rangle + \big(\cos(\alpha)h_1 + \sin(\alpha)h_2\big)|10\rangle \\ +\big(\cos(\alpha)h_2 + \sin(\alpha)h_4\big)|11\rangle \end{aligned} \tag{C.30}$$

since $h_2 = h_3$ and that both the state $|\Psi_3\rangle$ (C.28) and measurements $\langle m_{0|x_i}|$ are symmetrical with respect to permutation $A_2 \leftrightarrow A_3$. Using the concurrence, the state $|\psi_{0|0}^{A_1A_2}\rangle$ (C.30) is entangled if and only if

$$\begin{aligned} \det\begin{pmatrix} \cos(\alpha)h_0 & 0 \\ \cos(\alpha)h_1 + \sin(\alpha)h_2 & \cos(\alpha)h_2 + \sin(\alpha)h_4 \end{pmatrix} \neq 0 \\ \Leftrightarrow \cos(\alpha)h_0\big(\cos(\alpha)h_2 + \sin(\alpha)h_4\big) \neq 0 \end{aligned} \tag{C.31}$$

leading to the four conditions

$$\alpha \neq \frac{\pi}{2} \tag{C.32}$$

$$\tan(\alpha) \neq -\frac{h_2}{h_4} \tag{C.33}$$

$$h_0 \neq 0 \tag{C.34}$$

$$h_2 \neq 0 \neq h_4 \tag{C.35}$$

[1] Remark additionally that we do not make use of a potential second degree of freedom (the phase).

First, remark that both conditions (C.34) and (C.35) only mean that the state $|\Psi_3\rangle$ (C.28) needs to be GME (as well as symmetrical $h_2 = h_3$). Now, since the parameter α is free, we choose to avoid the two values $\alpha = \frac{\pi}{2}$ and $\alpha = -\arctan\left(\frac{h_2}{h_4}\right) \neq 0$. In the end, one can tune continuously the parameter α (up to the forbidden values (C.32) and (C.33)) so that the prepared states $|\psi_{0|0}^{A_1A_2}\rangle = |\psi_{0|0}^{A_1A_3}\rangle$ are not maximally entangled. One can then use observation C.4, as well as the symmetries $A_2 \leftrightarrow A_3$ that was imposed on both state and measurements, to obtain

$$\begin{aligned} I_{\mu=0}^{A_1A_2A_3} &= I_{0|0}^{A_1A_2} + I_{0|0}^{A_1A_3} - P(000|000) = 2I_{0|0}^{A_1A_2} - P(000|000) \\ &= P(000|000) - 2P(100|100) - 2P(010|010) - 2P(000|110) > 0 \end{aligned} \tag{C.36}$$

by choosing A_1's measurements as in (C.25) for the prepared (non maximally entangled) state $|\psi_{0|0}^{A_1A_2}\rangle$ (C.30), i.e. realising

$$\begin{aligned} P(000|000) &> 0 \\ P(010|010) &= 0 \\ P(100|100) &= 0 \\ P(000|110) &= 0 \end{aligned} \tag{C.37}$$

C.5 Hardy's measurements for $n = 2$

From the realisation (C.26), we have four conditions

$$\begin{aligned} P(00|00) &> 0 \\ P(01|01) &= 0 \\ P(10|10) &= 0 \\ P(00|11) &= 0 \end{aligned} \tag{C.38}$$

to be satisfied by the measurement $M_{a|x}$ and $N_{b|y}$ made on the state $|\phi_\theta\rangle = cos(\theta)|00\rangle + sin(\theta)|11\rangle$ written in it's Schmidt basis by A and B respectively. We start by choosing $M_{0|0} = cos\alpha\langle 0| + sin\alpha e^{i\delta}\langle 1|$ freely and then try to satisfy these four conditions. From $P(01|01) = 0$ we get that

$$\begin{aligned} (cos\alpha\langle 0| + sin\alpha e^{i\delta}\langle 1|) \otimes N_{0|1} \cdot (cos(\theta)|00\rangle + sin(\theta)|11\rangle) &= 0 \\ \Leftrightarrow N_{0|1}(cos\alpha cos\theta|0\rangle + e^{i\delta} sin\alpha sin\theta|1\rangle) &= 0 \\ \Leftrightarrow N_{0|1} \propto e^{i\delta} sin\alpha sin\theta\langle 0| - cos\alpha cos\theta\langle 1| & \end{aligned} \tag{C.39}$$

where we use non normalized measurements, which, again, does not make a difference when interested in conditions of the form $P(a_1a_2|x_1x_2) = 0$ or $P(a_1a_2|x_1x_2) > 0$. Considering projective two-outcome measurements:

$$N_{1|1} \propto cos\alpha cos\theta\langle 0| + e^{-i\delta} sin\alpha sin\theta \langle 1| \tag{C.40}$$

Then, with condition $P(00|11) = 0$

$$\begin{aligned}
M_{1|1} \otimes N_{1|1}(cos(\theta)|00\rangle + sin(\theta)|11\rangle) &= 0 \\
\Leftrightarrow M_{1|1}(cos\alpha cos^2\theta|0\rangle + e^{-i\delta} sin\alpha sin^2\theta|1\rangle) &= 0 \\
\Rightarrow M_{1|1} \propto e^{-i\delta} sin\alpha sin^2\theta\langle 0| - cos\alpha cos^2\theta\langle 1| & \qquad (C.41) \\
\Rightarrow M_{0|1} \propto cos\alpha cos^2\theta\langle 0| + e^{i\delta} sin\alpha sin^2\theta\langle 1| & \qquad (C.42)
\end{aligned}$$

Finally, from condition $P(10|10) = 0$

$$\begin{aligned}
M_{0|1} \otimes N_{0|0}(cos(\theta)|00\rangle + sin(\theta)|11\rangle) &= 0 \\
\Rightarrow N_{0|0} \propto e^{i\delta} sin\alpha sin^3\theta\langle 0| - cos\alpha cos^3\theta\langle 1| & \qquad (C.43) \\
\Rightarrow N_{1|0} \propto cos\alpha cos^3\theta\langle 0| + e^{-i\delta} sin\alpha sin^3\theta\langle 1| & \qquad (C.44)
\end{aligned}$$

Now one can check that with these measurements on the state $cos(\theta)|00\rangle + sin(\theta)|11\rangle$ gives:

$$M_{0|0} \otimes N_{0|0}(cos(\theta)|00\rangle + sin(\theta)|11\rangle) \propto ... = -\frac{e^{i\delta}}{8} sin2\alpha sin4\theta \tag{C.45}$$

That is equal to zero – i.e. $P(00|00) = 0$ – if and only if $\alpha = 0, \pi/2$ or $\theta = 0, \pi/4$. In the end, the conditions (C.38) are satisfied for these measurements for all non-maximally entangled states with any set of measurements of the form

$$\begin{aligned} M_{0|0} &= cos(\alpha)\langle 0| + e^{i\delta} sin(\alpha)\langle 1| \\ M_{0|1} &\propto cos^2(\theta)cos(\alpha)\langle 0| + e^{i\delta} sin^2(\theta)sin(\alpha)\langle 1| \\ \\ N_{0|0} &\propto sin^3(\theta)e^{i\delta} sin(\alpha)\langle 0| - cos^3(\theta)cos(\alpha)\langle 1| \\ N_{0|1} &\propto sin(\theta)sin(\alpha)e^{i\delta}\langle 0| - cos(\theta)cos(\alpha)\langle 1| \end{aligned} \tag{C.46}$$

except for the forbidden values of $\alpha = 0, \pi/2$.

Appendix D

Appendices: Quantifying multipartite nonlocality via the size of the resource

D.1 Proof that all full-correlation functions are attainable using a non-signaling resource

Our goal here is to give a proof that when restricted to the $(\ell-1)\,m^n$-dimensional space of full-correlation functions defined by Eq. (6.9), the set of legitimate correlations coincide with that achievable by a non-signaling resource $\mathcal{NS}_n$. To this end, it is worth reminding that the set of normalized correlations in this space is precisely the set of correlations achievable by the Svetlichny resource $\mathcal{S}_n$. To prove the desired result, it is then sufficient to show that all extreme points of $\mathcal{S}_n$ in this space are also achievable using $\mathcal{NS}_n$.

Proof. Firstly, let us note that all extremal strategies of these full-correlation functions are deterministic function of the joint inputs $\vec{x}$, i.e., they are defined by specifying for each given $\vec{x}$, the corresponding sum of outputs modulo ℓ. In other words, for each of these extremal strategies and for each given $\vec{x}$, we have that

$$P([\mathbf{a}_{\vec{x}}]_k = r) = \delta_{r,f(\vec{x})}, \tag{D.1}$$

where $f(\vec{x})$ is some deterministic, r-value function of $\vec{x}$. Different extremal strategies of $\mathcal{S}_n$ in this space then corresponds to different choices of $f(\vec{x})$. To prove Theorem 12, it is then sufficient to find a non-signaling strategy that gives Eq. (D.1) for an arbitrary choice of $f(\vec{x})$.

Let us first illustrate how this works in the scenario of $n=2$. Consider the following normalized probability distribution

$$P(a_1a_2|x_1x_2) = \frac{1}{\ell}\delta_{a_1+a_2 \bmod \ell,\, f(x_1,x_2)}. \tag{D.2}$$

Note that (regardless of x_1 and x_2) for each a_1 — due to the Kronecker delta — there is one, and only one value of a_2 such that the right-hand-side of Eq. (D.2) is non-vanishing; likewise for a_2. As a result, the corresponding marginal distributions are given by:

$$\begin{aligned} P(a_1|x_1x_2) &= \sum_{a_2} \frac{1}{\ell}\delta_{a_1+a_2 \bmod \ell, f(x_1,x_2)} = \frac{1}{\ell}, \\ P(a_2|x_1x_2) &= \sum_{a_1} \frac{1}{\ell}\delta_{a_1+a_2 \bmod \ell, f(x_1,x_2)} = \frac{1}{\ell}. \end{aligned} \tag{D.3}$$

Both these marginal distributions are independent of the input of the other party and hence the distribution given in Eq. (D.2) satisfies the non-signaling constraints. From these observations and Eq. (6.9b), it is also easy to see that the non-signaling distribution given in Eq. (D.2) satisfies Eq. (D.1). We have thus shown that in the above-mentioned subspace of full-correlation functions, the extremal strategy of $\mathcal{S}_2$ can also be achieved by a non-signaling correlation. More generally, for arbitrary $n \geq 2$, it is easy to verify that the following distribution:

$$P(\vec{a}|\vec{x}) = \frac{1}{\ell^{n-1}}\delta_{\sum_i a_i \bmod \ell, f(\vec{x})} \tag{D.4}$$

is non-signaling, giving a uniform n''-partite marginal distribution of $\ell^{-n''}$, and satisfies Eq. (D.1). In other words, we have proved that the extremal strategy of $\mathcal{S}_n$ in the subspace of full-correlation functions can always be achieved using a non-signaling strategy. □

D.2 Proof of Corollary 1

Here, we give a proof of Corollary 1. For concreteness, we shall provide a proof for $\mathcal{R} = \mathcal{S}$. The case for $\mathcal{R} = \mathcal{T}$ follows from the inclusion relations given in Eq. (6.3).

Proof. Given inequality (6.10), the inclusion relations of Eq. (6.3) immediately imply that inequality (6.11) holds true for all $\mathcal{P}(\vec{a}|\vec{x}) \in \mathcal{NS}_{n,k}$. It thus remains to show that there also exists $P(\vec{a}|\vec{x}) = P_0^{\mathcal{NS}}(\vec{a}|\vec{x}) \in \mathcal{NS}_{n,k}$ such that the inequality (6.11) is saturated, i.e.,

$$\sum_{\vec{x}} \sum_{r=0}^{\ell-1} \beta_{\vec{x}}^r P_0^{\mathcal{NS}}([\mathbf{a}_{\vec{x}}]_\ell = r) = B_{n,k}^{\mathcal{S}}. \tag{D.5}$$

By assumption, there exists extremal $P(\vec{a}|\vec{x}) = P^{\mathcal{S}}(\vec{a}|\vec{x}) \in \mathcal{S}_{n,k}$ such that inequality (6.10) is saturated, i.e.,

$$\sum_{\vec{x}} \sum_{r=0}^{\ell-1} \beta^r_{\vec{x}} P^{\mathcal{S}}([\mathbf{a}_{\vec{x}}]_\ell = r) = B^{\mathcal{S}}_{n,k}. \tag{D.6}$$

From the definition of the full-correlation function, Eq. (6.9b), and the assumed k-producibility of the correlation, we have

$$\begin{aligned} P^{\mathcal{S}}([\mathbf{a}_{\vec{x}}]_\ell = r) &= \sum_{\vec{a}} P^{\mathcal{S}}(\vec{a}|\vec{x})\, \delta_{[\mathbf{a}_{\vec{x}}]_\ell, r} \\ &= \sum_{\vec{a}} \prod_{i=1}^{G} P^{\mathcal{S}}(\vec{a}^{[i]}|\vec{x}^{[i]})\, \delta_{[\mathbf{a}_{\vec{x}}]_\ell, r}, \end{aligned} \tag{D.7a}$$

where $P^{\mathcal{S}}(\vec{a}^{[i]}|\vec{x}^{[i]})$ refers to the i-th constituent distribution, which is at most k-partite. Denote the sum of the outputs in the j-th group by $\mathbf{a}_{\vec{x}^{[j]}}$, we can then further rewrite $P^{\mathcal{S}}([\mathbf{a}_{\vec{x}}]_\ell = r)$ as:

$$\begin{aligned} &\prod_{i=1}^{G} \sum_{\vec{a}^{[i]}} P^{\mathcal{S}}(\vec{a}^{[i]}|\vec{x}^{[i]})\, \delta_{\left[\sum_j \left[\mathbf{a}_{\vec{x}^{[j]}}\right]_\ell\right]_\ell, r} \\ =&\prod_{i=1}^{G} \sum_{\vec{a}^{[i]}} \sum_{r^{[i]}=0}^{\ell-1} P^{\mathcal{S}}(\vec{a}^{[i]}|\vec{x}^{[i]}) \delta_{\left[\mathbf{a}_{\vec{x}^{[i]}}\right]_\ell, r^{[i]}}\, \delta_{\left[\sum_j \left[\mathbf{a}_{\vec{x}^{[j]}}\right]_\ell\right]_\ell, r}. \end{aligned} \tag{D.7b}$$

Note that for each $\vec{x}^{[i]}$, due to the Kronecker delta $\delta_{\left[\mathbf{a}_{\vec{x}^{[i]}}\right]_\ell, r^{[i]}}$, there is only one term in the sum over $r^{[i]}$ that contributes non-trivially. Swapping the order of the sums gives:

$$\begin{aligned} &\prod_{i=1}^{G} \sum_{r^{[i]}=0}^{\ell-1} \sum_{\vec{a}^{[i]}} P^{\mathcal{S}}(\vec{a}^{[i]}|\vec{x}^{[i]}) \delta_{\left[\mathbf{a}_{\vec{x}^{[i]}}\right]_\ell, r^{[i]}}\, \delta_{\left[\sum_j \left[\mathbf{a}_{\vec{x}^{[j]}}\right]_\ell\right]_\ell, r} \\ =&\prod_{i=1}^{G} \sum_{r^{[i]}=0}^{\ell-1} \sum_{\vec{a}^{[i]}} P^{\mathcal{S}}(\vec{a}^{[i]}|\vec{x}^{[i]}) \delta_{\left[\mathbf{a}_{\vec{x}^{[i]}}\right]_\ell, r^{[i]}}\, \delta_{\left[\sum_j r^{[j]}\right]_\ell, r} \\ =&\prod_{i=1}^{G} \sum_{r^{[i]}=0}^{\ell-1} P^{\mathcal{S}}(\left[\mathbf{a}_{\vec{x}^{[i]}}\right]_\ell = r^{[i]})\, \delta_{\left[\sum_j r^{[j]}\right]_\ell, r} \end{aligned} \tag{D.7c}$$

which means that $P^{\mathcal{S}}([\mathbf{a}_{\vec{x}}]_\ell = r)$ factorizes into a (linear combination of) product of *full-correlation functions* for each group $P^{\mathcal{S}}(\left[\mathbf{a}_{\vec{x}^{[i]}}\right]_\ell = r^{[i]})$. By Theorem 12, there is no loss of generality in replacing the constituent distribution from the i-th group $P^{\mathcal{S}}(\vec{a}^{[i]}|\vec{x}^{[i]})$ by some non-signaling distributions $P_0^{\mathcal{NS}}(\vec{a}^{[i]}|\vec{x}^{[i]})$ such that they agree at the level of the full-correlation functions, i.e.,

$$P^{\mathcal{S}}([\mathbf{a}_{\vec{x}^{[i]}}]_\ell = r^{[i]}) = P_0^{\mathcal{NS}}([\mathbf{a}_{\vec{x}^{[i]}}]_\ell = r^{[i]}) \quad \forall\, i, r^{[i]} \tag{D.8}$$

Substituting this back into Eq. (D.7) and then Eq. (D.6), we thus obtain Eq. (D.5) by identifying

$$P_0^{\mathcal{NS}}([\mathbf{a}_{\vec{x}^{[i]}}]_\ell = r^{[i]}) = \sum_{\vec{a}} \prod_{i=1}^{G} P^{\mathcal{NS}}(\vec{a}^{[i]}|\vec{x}^{[i]})\, \delta_{[\mathbf{a}_{\vec{x}}]_\ell, r}. \tag{D.9}$$

□

An immediate consequence of the above Corollary is that any full-correlation Bell-like inequality for $\mathcal{S}_{n,k}$, such as those derived in Refs. [Ban+12; Sve87; Col+02b; JLM05; Ban+11; Che+11], is also valid and tight for $\mathcal{NS}_{n,k}$.

D.3 Proof of Theorem 13

We now provide a proof of Theorem 13.

Proof. By assumption, the following expression holds true

$$I_n = \sum_{\vec{a},\vec{x}} \beta_{\vec{x}}^{\vec{a}} P(\vec{a}|\vec{x}) \leq 0 \tag{D.10}$$

for all $P(\vec{a}|\vec{x}) \in \mathcal{R}_{n,k}$, and our goal is to show that

$$I_{n+h} = \sum_{\vec{a},\vec{x}} \beta_{\vec{x}}^{\vec{a}} P(\vec{a},\vec{o}|\vec{x},\vec{s}) \overset{\mathcal{R}_{n+h,k}}{\leq} 0, \tag{D.11}$$

for arbitrary $h \geq 1$ and *all fixed* choices of $\vec{o}$ and $\vec{s}$. We will show that this is the case by *reductio ad impossibilem*.

Suppose the converse, namely, that there exists some choice of $\vec{o}$, $\vec{s}$ and h such that for some $P(\vec{a},\vec{o}|\vec{x},\vec{s}) \in \mathcal{R}_{n+h,k}$,

$$\sum_{\vec{a},\vec{x}} \beta_{\vec{x}}^{\vec{a}} P(\vec{a},\vec{o}|\vec{x},\vec{s}) > 0. \tag{D.12}$$

By linearity of the expression and the requirement that $P(\vec{a},\vec{o}|\vec{x},\vec{s}) \in \mathcal{R}_{n+h,k}$, the above inequality implies that there exists some correlation

$$P(\vec{a},\vec{o}|\vec{x},\vec{s}) = \prod_{i=1}^{G} P^{\mathcal{R}}(\vec{a}^{[i]},\vec{o}^{[i]}|\vec{x}^{[i]},\vec{s}^{[i]}) \tag{D.13}$$

such that

$$\sum_{\vec{a},\vec{x}} \beta^{\vec{a}}_{\vec{x}} \prod_{i=1}^{G} P^{\mathcal{R}}(\vec{a}^{[i]},\vec{o}^{[i]}|\vec{x}^{[i]},\vec{s}^{[i]}) > 0, \tag{D.14}$$

where $P^{\mathcal{R}}(\vec{a}^{[i]},\vec{o}^{[i]}|\vec{x}^{[i]},\vec{s}^{[i]})$ refers to the i-th constituent distribution (from the i-th group), and as with $P(\vec{a},\vec{o}|\vec{x},\vec{s})$, we have used $\vec{o}^{[i]}$ and $\vec{s}^{[i]}$ to indicate, respectively, the (possibly empty) outcome and setting string that are *fixed* in $P^{\mathcal{R}}(\vec{a}^{[i]},\vec{o}^{[i]}|\vec{x}^{[i]},\vec{s}^{[i]})$. Note that the assumption of $P(\vec{a},\vec{o}|\vec{x},\vec{s}) \in \mathcal{R}_{n+h,k}$ implies that each constituent distribution is at most k-partite and their respective size n_i sum up to $n+h$, i.e., $\sum_{i=1}^{G} n_i = n+h$.

Evidently, since inequality (D.14) is *strict* and that $P^{\mathcal{R}}(\vec{a}^{[i]},\vec{o}^{[i]}|\vec{x}^{[i]},\vec{s}^{[i]}) \geq 0$ for all $\vec{a}^{[i]}$ and $\vec{x}^{[i]}$, it must be the case that

$$\sum_{\vec{a}^{[i]}} P^{\mathcal{R}}(\vec{a}^{[i]},\vec{o}^{[i]}|\vec{x}^{[i]},\vec{s}^{[i]}) > 0 \tag{D.15}$$

for all $\vec{x}^{[i]}$ that contribute nontrivially in the left-hand-side of Eq. (D.14). In fact, since the left-hand-side of inequality (D.15) can also be obtained by performing the appropriate sums of Eq. (D.13)

$$\begin{aligned}\sum_{\vec{a},\vec{o}^{[j]}|j\neq i} P(\vec{a},\vec{o}|\vec{x},\vec{s}) &= \sum_{\vec{a},\vec{o}^{[j]}|j\neq i} \prod_{\ell=1}^{G} P^{\mathcal{R}}(\vec{a}^{[\ell]},\vec{o}^{[\ell]}|\vec{x}^{[\ell]},\vec{s}^{[\ell]}) \\ &= \sum_{\vec{a}^{[i]}} P^{\mathcal{R}}(\vec{a}^{[i]},\vec{o}^{[i]}|\vec{x}^{[i]},\vec{s}^{[i]}),\end{aligned} \tag{D.16}$$

we see that by the non-signaling nature of $P(\vec{a},\vec{o}|\vec{x},\vec{s})$, the very last expression of Eq. (D.16) must also be independent of $\vec{x}^{[i]}$. Hereafter, we shall simply write these marginal distributions as:

$$P^{\mathcal{R}}(\vec{o}^{[i]}|\vec{s}^{[i]}) = \sum_{\vec{a}^{[i]}} P^{\mathcal{R}}(\vec{a}^{[i]},\vec{o}^{[i]}|\vec{x}^{[i]},\vec{s}^{[i]}). \tag{D.17}$$

Hence, from inequality (D.15), we see that the conditional distributions

$$\tilde{P}^{|\vec{o}^{[i]},\vec{s}^{[i]}}(\vec{a}^{[i]}|\vec{x}^{[i]}) = \frac{P^{\mathcal{R}}(\vec{a}^{[i]},\vec{o}^{[i]}|\vec{x}^{[i]},\vec{s}^{[i]})}{P^{\mathcal{R}}(\vec{o}^{[i]}|\vec{s}^{[i]})} \tag{D.18}$$

are well-defined for all $\vec{x}^{[i]}$ and satisfy the normalization condition $\sum_{\vec{a}^{[i]}} \tilde{P}^{|\vec{o}^{[i]},\vec{s}^{[i]}}(\vec{a}^{[i]}|\vec{x}^{[i]}) = 1$. With some thought, one can also see that the conditional distribution defined in Eq. (D.18) also inherits the property of the defining distribution, i.e., satisfying the constraint defined by $\mathcal{R}$. For instance, if $P^{\mathcal{R}}(\vec{a}^{[i]},\vec{o}^{[i]}|\vec{x}^{[i]},\vec{s}^{[i]})$ admits a quantum representation, so does $\tilde{P}^{|\vec{o}^{[i]},\vec{s}^{[i]}}(\vec{a}^{[i]}|\vec{x}^{[i]})$.

Dividing inequality (D.14) by $\prod_i P^{\mathcal{R}}(\vec{o}^{[i]}|\vec{s}^{[i]})$ and using Eq. (D.18), we obtain

$$\sum_{\vec{a},\vec{x}} \beta^{\vec{a}}_{\vec{x}} \prod_{i=1}^{G} \tilde{P}^{|\vec{o}^{[i]},\vec{s}^{[i]}}(\vec{a}^{[i]}|\vec{x}^{[i]}) > 0. \tag{D.19}$$

As mentioned above, for all i, the conditional distribution $\tilde{P}^{|\vec{o}^{[i]},\vec{s}^{[i]}}(\vec{a}^{[i]}|\vec{x}^{[i]})$ is a legitimate distribution with respect to the resource $\mathcal{R}$ and cannot be more than k-partite, i.e, $\prod_{i=1}^{G} \tilde{P}^{|\vec{o}^{[i]},\vec{s}^{[i]}}(\vec{a}^{[i]}|\vec{x}^{[i]}) \in \mathcal{R}_{n,k}$. Hence, inequality (D.19) implies that the original inequality I_n can be violated by correlation in $\mathcal{R}_{n,k}$, which contradicts our very first assumption that I_n is a legitimate Bell-like inequality for $\mathcal{R}_{n,k}$.

□

Appendix E

Appendices: Anonymous Quantum Nonlocality

E.1 An explicit biseparable decomposition of the n-partite GHZ correlations

For the n-partite GHZ state and the situation where all parties measure either the 0th-observable σ_x or the 1st observable σ_y, the resulting correlation of Eq. (7.2) can be rewritten in terms of the *correlator*, i.e., the expectation value of the product of outcomes:[1]

$$E(\vec{x}) = \sum_{a'_1, a'_2, \ldots, a'_n = 0,1} (-1)^{\sum_i a'_i} P(\vec{a}'|\vec{x}) = \cos\left(\mathbf{x}\frac{\pi}{2}\right) \tag{7.2}$$

where for conciseness of subsequent presentation we have used, instead, $a'_i = \frac{a_i+1}{2} = 0, 1$ to denote the output and as before, $\mathbf{x} = \sum_i x_i$ to denote the sum of inputs. Note that all the full n-partite correlators depend only on the parity of $\mathbf{x}$ and $\mathbf{x}/2$ whereas all the marginal correlators vanish.

Here we give a proof that the above correlation is biseparable with respect to *all* bipartitions whenever parties in each group are allowed to share arbitrary post-quantum but non-signaling (NS) resources, while parties in different groups can only be correlated through shared randomness. Note that the biseparability of Eq. (7.2) under the NS constraint implies that if parties in the same group are allowed to share a stronger resource, such as a Svetlichny resource [Sve87], or some other one-way signaling resource discussed in Refs. [Gal+12; Ban+13], the correlation must remain biseparable.

[1] To arrive at this n-partite correlator, see, eg., Eq. (23) of [WLB11].

Let us define the four families of n-partite NS boxes, labeled by μ_1, μ_2, μ_3 and μ_4:

$$\begin{aligned}
P^n_{\mu_1}(\vec{a}'|\vec{x}) &= \frac{1}{2^{n-1}}\delta_{\sum_{i=1}^n a'_i - H^n_0(\vec{x}) - H^n_3(\vec{x}) \bmod 2},\\
P^n_{\mu_2}(\vec{a}'|\vec{x}) &= \frac{1}{2^{n-1}}\delta_{\sum_{i=1}^n a'_i - H^n_0(\vec{x}) - H^n_1(\vec{x}) \bmod 2},\\
P^n_{\mu_3}(\vec{a}'|\vec{x}) &= \frac{1}{2^{n-1}}\delta_{\sum_{i=1}^n a'_i - H^n_1(\vec{x}) - H^n_2(\vec{x}) \bmod 2},\\
P^n_{\mu_4}(\vec{a}'|\vec{x}) &= \frac{1}{2^{n-1}}\delta_{\sum_{i=1}^n a'_i - H^n_2(\vec{x}) - H^n_3(\vec{x}) \bmod 2},
\end{aligned} \tag{E.1}$$

where $H^n_\ell(\vec{x}) = \sum_{j=0}^{\lfloor \frac{n-\ell}{4} \rfloor} F(4j+\ell, \vec{x})$,

$$F(k,\vec{x}) = \sum_G \prod_{i\in G} x_i \prod_{j\in G'} (x_j + 1) \tag{E.2}$$

and the sum $\sum_G$ is over all $G \subseteq [n] = \{1, 2, \ldots, n\}$ with group size $|G| = k$, and G' is the complement of G in $[n]$. Essentially, each term involved in the summand in $F(k,\vec{x})$, and hence $H^n_\ell(\vec{x})$ defines a distinct combination of inputs $\vec{x} = \vec{x}'$ such that $H^n_\ell(\vec{x}') = 1 \bmod 2$, and hence making the outputs anti-correlated. For instance, $F(0,\vec{x})$ only makes a nontrivial combination to $H^n_0(\vec{x})$ if all the inputs x_i are 0.

From Eq. (E.1), it is easy to verify that for all $1 \le k \le n-1$, the k-partite marginals of $P^n_j(\vec{a}'|\vec{x})$ are $1/2^k$ and these correlations indeed define NS probability distributions. Moreover, from Eq. (E.1) and these marginal distributions, one can show that these NS boxes give rise to vanishing marginal correlators and the following full n-partite correlators:

$$\begin{aligned}
E(\vec{x})_{\mu_1} &= (-1)^{H^n_0(\vec{x}) \oplus H^n_3(\vec{x})} = -E(\vec{x})_{\mu_3},\\
E(\vec{x})_{\mu_2} &= (-1)^{H^n_0(\vec{x}) \oplus H^n_1(\vec{x})} = -E(\vec{x})_{\mu_4},
\end{aligned} \tag{E.3}$$

where in Eq. (E.3), $\oplus$ denotes sum modulo 2 and in arriving at the second equality in each line, we have employed the identity $\sum_{j=0}^n F(j) = 1$ that holds for all n-bit strings $\vec{x}$.[2] To gain some intuition on these NS boxes, we note that for $n = 1$, the $\mu_{1/3}$ boxes correspond to the deterministic strategies $a' = x \oplus 1$ and $a' = x$ whereas the $\mu_{2/4}$ boxes correspond to the deterministic strategies $a' = 1$ and $a' = 0$. Similarly, for $n = 2$, the $\mu_{1/3}$ boxes correspond to the PR boxes defined by $a'_1 + a'_2 = (x_1+1)(x_2+1)$ and $a'_1 + a'_2 = (x_1+1)(x_2+1) \oplus 1$ whereas the $\mu_{2/4}$ boxes correspond to the PR boxes defined by $a'_1 + a'_2 = x_1 x_2 \oplus 1$ and

[2] This last sum involves all possible combinations of inputs and thus for all input bit strings $\vec{x}$, there is exactly one term in the expression that does not vanish, therefore giving the identity.

$a'_1 + a'_2 = x_1 x_2$. For $n = 3$, all these NS boxes correspond to some version of NS box 46 described in Ref. [PBS11]. It is conceivable that these boxes are extremal NS distributions for all n.

To reproduce the correlations given in Eq. (7.2) using biseparable $\mathcal{NS}$ resources with k parties in one group and the remaining $(n-k)$ parties in the other group, it suffices to consider an equal-weight mixture of the following four strategies:

1. The group of k parties share the k-partite version of the μ_1 box and the remaining parties share the $(n-k)$-partite version of the μ_2 box.

2. The group of k parties share the k-partite version of the μ_3 box and the remaining parties share the $(n-k)$-partite version of the μ_4 box.

3. The group of k parties share the k-partite version of the μ_2 box and the remaining parties share the $(n-k)$-partite version of the μ_1 box.

4. The group of k parties share the k-partite version of the μ_4 box and the remaining parties share the $(n-k)$-partite version of the μ_3 box.

For $n = 3$, the above strategy corresponds to a mixture of 4 different versions of the NS box 2 in Ref. [PBS11]. In general, to verify that the above strategy indeed gives rise to Eq. (7.2), we first remark that each of these strategies also reproduces Eq. (7.2) for the case when $\sum_i x_i$ is even. To see this, we use the fact that NS box μ_1 gives anti-correlation (i.e., expectation value -1) only if either $\sum_i x_i/2$ or $(1+\sum_i x_i)/2$ is even; NS box μ_2 gives anti-correlation only if $\sum_i x_i/2$ is even or $(1+\sum_i x_i)/2$ is odd; NS box μ_3 gives anti-correlation only if either $\sum_i x_i/2$ or $(1+\sum_i x_i)/2$ is odd; NS box μ_4 gives anti-correlation only if $\sum_i x_i/2$ is odd or $(1+\sum_i x_i)/2$ is even. Moreover, since strategy 1 and 3 are such that the correlation produced by parties in the same group are exactly opposite (likewise for strategy 2 and 4), we see that all the less-than-n-partite correlators, as well as the full n-partite correlator when $\sum_{i=1}^n x_i$ is odd, indeed vanishes as claimed.

E.2 Mermin-Bell violation of the GHZ correlations

Here, we compute the quantum expectation value of the GHZ correlations for the Mermin Bell inequality [Mer90a; Ard92; RS91; Belb; GBP98] (here written in the form derived in [WLB11])[3]

$$|\mathcal{B}^n_\pm| = 2^{\frac{1-n}{2}} \left| \sum_{\vec{x}\in\{0,1\}^n} \cos\left\{\frac{\pi}{4}\left[1 \pm (n - 2\mathbf{x})\right]\right\} E\left(\vec{x}\right)\right| \leq 1. \tag{E.4}$$

[3] $\mathcal{B}^n_+$ is the same Bell expression as the usual one obtained through the recursive formula [RS91; Belb; GBP98]; it can also be obtained by flipping all the inputs in $\mathcal{B}^n_-$.

The above Bell expression can be rewritten as:

$$\begin{aligned}2^{\frac{n-1}{2}}\,|\mathcal{B}^n_\pm| =& \Big|\sum_{\vec{x}\in\{0,1\}^n} \cos\left\{\frac{\pi}{4}\left[1 \pm (n-2\mathbf{x})\right]\right\} E(\vec{x})\Big|,\\ =& \Big|\sum_{\vec{x}\in\{0,1\}^n} \cos\left[\frac{\pi}{4}(1\pm n)\right] \cos\left(\mathbf{x}\frac{\pi}{2}\right) E(\vec{x})\\ &\pm \sum_{\vec{x}\in\{0,1\}^n} \sin\left[\frac{\pi}{4}(1\pm n)\right] \sin\left(\mathbf{x}\frac{\pi}{2}\right) E(\vec{x})\Big|.\end{aligned}$$

For the GHZ correlation of Eq. (7.2), this simplifies to

$$\begin{aligned}|\mathcal{B}^n_\pm| =& 2^{\frac{1-n}{2}}\Big|\sum_{\vec{x}\in\{0,1\}^n,\,\mathbf{x}\,\text{even}} \cos\left[\frac{\pi}{4}(1\pm n)\right]\cos^2\left(\mathbf{x}\frac{\pi}{2}\right)\Big|,\\ =& 2^{\frac{n-1}{2}}\left|\cos\left[\frac{\pi}{4}(1\pm n)\right]\right|,\end{aligned}$$

giving

$$\max_\pm |\mathcal{B}^n_\pm| = \begin{cases} 2^{\frac{n-1}{2}} & : n\,\text{odd} \\ 2^{\frac{n-2}{2}} & : n\,\text{even}\end{cases}, \tag{E.5}$$

i.e., achieving maximal [WW00] possible quantum value of $|\mathcal{B}^n_\pm|$ for odd n.

E.3 Quantum biseparable bound of the n-partite Mermin-Bell expression

For arbitrary odd $n \geq 3$, the Mermin-Bell expression $\mathcal{B}^n_+$ given on the left-hand-side of Eq. (E.4) is equivalent to a special case of a general family of permutationally invariant Bell expression described in Eq. (22) of [Ban+12],

$$\Omega_{n,2,2;\delta_{\mathbf{x},0}\cdot r} = 2^{n-2} - 2^{\frac{n-3}{2}}\mathcal{B}^n_+ \tag{E.6}$$

From Eq. (23) of Ref. [Ban+12], it can be shown that the above expression admits the following upper bound on the quantum biseparable bound:

$$\Omega_{n,2,2;\delta_{\mathbf{x},0}\cdot r} \geq 2^{n-3}(2-\sqrt{2}). \tag{E.7}$$

Combining these two equations and after some straightforward computations, we get the following upper bound on the quantum biseparable bound for the Mermin-Bell expression:

$$\mathcal{B}^n_+ \leq 2^{\frac{n}{2}-1}. \tag{E.8}$$

For arbitrary even $n \geq 2$, the Mermin-Bell expression $\mathcal{B}_{+}^{n}$ given on the left-hand-side of Eq. (E.4) is equivalent to the following Bell expression described in Eq. (1) of Ref. [Ban+12],

$$\mathcal{I}_{n,2,2} = 2^{n-1} - 2^{\frac{n-2}{2}}\mathcal{B}_{+}^{n} \tag{E.9}$$

From Eq. (25) of Ref. [Ban+12], we know that the above expression admits the following upper bound on the quantum biseparable bound:

$$\mathcal{I}_{n,2,2} \geq 2^{n-2}. \tag{E.10}$$

Combining these two equations, we arrive, again, at Eq. (E.8).

To see that the biseparable bound of Eq. (E.8) is tight, it suffices to note that the biseparable quantum state

$$|\psi\rangle = |\text{GHZ}_{n-1}\rangle \otimes |0\rangle \tag{E.11}$$

and the local observables

$$\begin{aligned} A_{x_i} &= \cos\alpha_{x_i}\sigma_x + \sin\alpha_{x_i}\sigma_y \quad \forall\ i = 1,\ldots,n-1, \\ A_{x_i} &= \beta_{x_i}\mathbb{1} \quad \text{for} \quad i = n. \end{aligned} \tag{E.12}$$

with $\alpha_0 = -\frac{\pi}{4(n-1)}$, $\alpha_1 = -\frac{\pi}{2} - \frac{\pi}{4(n-1)}$, $\beta_0 = -\sqrt{2}\sin\frac{n\pi}{4}$, and $\beta_1 = \sqrt{2}\cos\frac{n\pi}{4}$ indeed give rise to a quantum value of $\mathcal{B}_{+}^{n}$ of $2^{\frac{n}{2}-1}$. Since $\mathcal{B}_{-}^{n}$ can be obtained from $\mathcal{B}_{+}^{n}$ by flipping all the inputs, the same quantum biseparable bound holds for $\mathcal{B}_{-}^{n}$.

Since the GHZ correlations of Eq. (7.2) give Eq. (E.5), we see that for odd n, the generation of these correlations necessarily requires a genuinely n-partite entangled state, independent of the underlying Hilbert space dimension.

E.4 m-separability and multipartite nonlocality underlying the n-partite GHZ correlations

For odd n, we know from the main theorem of [Ban+09] that a quantum violation of $|\mathcal{B}_{\pm}^{n}| = 2^{\frac{n-1}{2}}$ implies that it is impossible to reproduce these GHZ correlations using any 3-separable resource (i.e., a partitioning of the parties into three groups, and where the parties within each group can share even arbitrary nonlocal resource).

For even n, let us evaluate the the quantum value of the following Bell expression [Ban+09]:

$$\begin{aligned}
|\mathcal{B}^n_\Sigma| =& \frac{1}{\sqrt{2}}\,|\mathcal{B}^n_+ + \mathcal{B}^n_-|\,, \\
=& \frac{1}{\sqrt{2}}\Big|\sum_{\vec{x}\in\{0,1\}^n}\sum_{s=0,1}\cos\frac{\pi}{4}[1+(-1)^s(n-2\mathbf{x})]\,E(\vec{x})\Big|, \\
=& \frac{1}{\sqrt{2}}\Big|\sum_{\vec{x}\in\{0,1\}^n} 2\cos\frac{\pi}{4}\cos\left[\frac{\pi}{4}(n-2\mathbf{x})\right]E(\vec{x})\Big|, \\
=& \Big|\sum_{\vec{x}\in\{0,1\}^n}\cos\left[\frac{\pi}{4}(n-2\mathbf{x})\right]E(\vec{x})\Big|.
\end{aligned} \tag{E.13}$$

For even n and $E(\vec{x})$ of Eq. (7.2), this becomes

$$\Big|\sum_{\vec{x}\in\{0,1\}^n,\,\mathbf{x}\,\text{even}}\cos\frac{n\pi}{4}\cos^2\mathbf{x}\frac{\pi}{2}\Big| = 2^{n-1}\left|\cos\frac{n\pi}{4}\right|,$$

giving a value of 2^{n-1} for even $\frac{n}{2}$ and 0 for odd $\frac{n}{2}$.

Again, note from the main theorem of Ref. [Ban+09] that for even n, any correlation producible by a partition of the n parties into 3 groups (each sharing some Svetlichny resource $\mathcal{S}$ [Sve87; Gal+12; Ban+13]) can at most give a value of $\mathcal{B}^n_\Sigma = 2^{n-2}$. This means that, as with odd n, the n-partite GHZ correlation for even n with even $\frac{n}{2}$ is not producible by any partition of the parties into 3 groups, even if parties in each group are allowed to share whatever nonlocal resource.

Together with the biseparable decomposition obtained for these correlations, the above results on m-separability imply that for (1) odd n and (2) even n with even $\frac{n}{2}$, generation of the GHZ correlations of Eq. (7.2) requires the nonlocal collaboration of at least $\lceil\frac{n}{2}\rceil$ parties in one group.

Bibliography

[Aci+01] A Acin, A Andrianov, E Jané, and Rolf Tarrach. “Three-qubit pure-state canonical forms”. In: *Journal of Physics A: Mathematical and General* 34.35 (2001), p. 6725.

[Aci+02] Antonio Acin, Thomas Durt, Nicolas Gisin, and José Ignacio Latorre. “Quantum nonlocality in two three-level systems”. In: *Physical Review A* 65.5 (2002), p. 052325.

[Ací+00] Antonio Acín, A Andrianov, L Costa, E Jané, JI Latorre, and Rolf Tarrach. “Generalized Schmidt decomposition and classification of three-quantum-bit states”. In: *Physical Review Letters* 85.7 (2000), p. 1560.

[Ací+07] Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani. “Device-independent security of quantum cryptography against collective attacks”. In: *Physical Review Letters* 98.23 (2007), p. 230501.

[Ací+16] Antonio Acín, Stefano Pironio, Tamás Vértesi, and Peter Wittek. “Optimal randomness certification from one entangled bit”. In: *Phys. Rev. A* 93.4 (2016), p. 040102. DOI: 10.1103/PhysRevA.93.040102.

[ADR82] Alain Aspect, Jean Dalibard, and Gérard Roger. “Experimental test of Bell’s inequalities using time-varying analyzers”. In: *Physical review letters* 49.25 (1982), p. 1804.

[AF+18] Rotem Arnon-Friedman, Frédéric Dupuis, Omar Fawzi, Renato Renner, and Thomas Vidick. “Practical device-independent quantum cryptography via entropy accumulation”. In: *Nature communications* 9.1 (2018), p. 459.

[AGG05] Antonio Acín, Richard Gill, and Nicolas Gisin. “Optimal Bell tests do not require maximally entangled states”. In: *Physical review letters* 95.21 (2005), p. 210402.

[AGM06] Antonio Acin, Nicolas Gisin, and Lluis Masanes. “From Bell’s theorem to secure quantum key distribution”. In: *Physical review letters* 97.12 (2006), p. 120405.

[AM16] Antonio Acín and Lluis Masanes. “Certified randomness in quantum physics”. In: *Nature* 540.7632 (2016), p. 213.

[AMP06] Antonio Acín, Serge Massar, and Stefano Pironio. “Efficient quantum key distribution secure against no-signalling eavesdroppers”. In: *New Journal of Physics* 8.8 (2006), p. 126.

[AMP12] Antonio Acín, Serge Massar, and Stefano Pironio. “Randomness versus Nonlocality and Entanglement”. In: *Phys. Rev. Lett.* 108 (10 2012), p. 100402. DOI: 10.1103/PhysRevLett.108.100402.

[Aol+12] Leandro Aolita, Rodrigo Gallego, Adán Cabello, and Antonio Acín. “Fully nonlocal, monogamous, and random genuinely multipartite quantum correlations”. In: *Physical review letters* 108.10 (2012), p. 100401.

[Ard92] Mohammad Ardehali. “Bell inequalities with a magnitude of violation that grows exponentially with the number of particles”. In: *Physical Review A* 46.9 (1992), p. 5375.

[Aug+15] R Augusiak, Maciej Demianowicz, J Tura, and Antonio Acín. “Entanglement and nonlocality are inequivalent for any number of parties”. In: *Physical review letters* 115.3 (2015), p. 030404.

[AVC03] Antonio Acin, Guifre Vidal, and J Ignacio Cirac. “On the structure of a reversible entanglement generating set for tripartite states”. In: *Quantum Information & Computation* 3.1 (2003), pp. 55–63.

[Bac+18] Flavio Baccari, Jordi Tura, Matteo Fadel, Albert Aloy, Jean-Daniel Bancal, Nicolas Sangouard, Maciej Lewenstein, Antonio Acín, and Remigiusz Augusiak. “Bell correlations depth in many-body systems”. In: *arXiv preprint arXiv:1802.09516* (2018).

[Ban] In:

[Ban+09] Jean-Daniel Bancal, Cyril Branciard, Nicolas Gisin, and Stefano Pironio. “Quantifying multipartite nonlocality”. In: *Physical Review Letters* 103.9 (2009), p. 090503.

[Ban+11] Jean-Daniel Bancal, Nicolas Brunner, Nicolas Gisin, and Yeong-Cherng Liang. “Detecting genuine multipartite quantum nonlocality: a simple approach and generalization to arbitrary dimensions”. In: *Physical review letters* 106.2 (2011), p. 020405.

[Ban+12] Jean-Daniel Bancal, Cyril Branciard, Nicolas Brunner, Nicolas Gisin, and Yeong-Cherng Liang. “A framework for the study of symmetric full-correlation Bell-like inequalities”. In: *Journal of Physics A: Mathematical and Theoretical* 45.12 (2012), p. 125301.

[Ban+13] Jean-Daniel Bancal, Jonathan Barrett, Nicolas Gisin, and Stefano Pironio. “Definitions of multipartite nonlocality”. In: *Physical Review A* 88.1 (2013), p. 014102.

[Ban11] JD Bancal. “J.-D. Bancal, N. Gisin, Y.-C. Liang, and S. Pironio, Phys. Rev. Lett. 106, 250404 (2011).” In: *Phys. Rev. Lett.* 106 (2011), p. 250404.

[Ban13] Jean-Daniel Bancal. *On the device-independent approach to quantum physics: advances in quantum nonlocality and multipartite entanglement detection*. Springer Science & Business Media, 2013.

[Ban14a] Jean-Daniel Bancal. “Device-independent witnesses of genuine multipartite entanglement”. In: *On the Device-Independent Approach to Quantum Physics*. Springer, 2014, pp. 73–80.

[Ban14b] Jean-Daniel Bancal. “Quantum non-locality based on finite-speed causal influences leads to superluminal signalling”. In: *On the Device-Independent Approach to Quantum Physics*. Springer, 2014, pp. 97–105.

[Bar+05] Jonathan Barrett, Noah Linden, Serge Massar, Stefano Pironio, Sandu Popescu, and David Roberts. “Nonlocal correlations as an information-theoretic resource”. In: *Physical Review A* 71.2 (2005), p. 022101.

[Bar+13] Tomer Jack Barnea, Jean-Daniel Bancal, Yeong-Cherng Liang, and Nicolas Gisin. “Tripartite quantum state violating the hidden-influence constraints”. In: *Physical Review A* 88.2 (2013), p. 022123.

[Bar02] Jonathan Barrett. “Nonsequential positive-operator-valued measurements on entangled mixed states do not always violate a Bell inequality”. In: *Physical Review A* 65.4 (2002), p. 042302.

[BB84] Charles Bennett and Gilles Brassard. “Quantum cryptography: public key distribution and coin tossing Int”. In: *Conf. on Computers, Systems and Signal Processing (Bangalore, India, Dec. 1984)*. 1984, pp. 175–9.

[Bela] In: ().

[Belb] Belinskiĭ. “Interference of light and Bell’s theorem”. In: ().

[Bel01] John S Bell. “On the Einstein Podolsky Rosen paradox”. In: *John S Bell On The Foundations Of Quantum Mechanics*. World Scientific, 2001, pp. 7–12.

[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: *Physical review letters* 70.13 (1993), p. 1895.

[Ben+99] Charles H Bennett, David P DiVincenzo, Tal Mor, Peter W Shor, John A Smolin, and Barbara M Terhal. “Unextendible product bases and bound entanglement”. In: *Physical Review Letters* 82.26 (1999), p. 5385.

[BGS05] Nicolas Brunner, Nicolas Gisin, and Valerio Scarani. “Entanglement and non-locality are different resources”. In: *New Journal of Physics* 7.1 (2005), p. 88.

[BHK05] Jonathan Barrett, Lucien Hardy, and Adrian Kent. “No signaling and quantum key distribution”. In: *Physical review letters* 95.1 (2005), p. 010503.

[BL13] Orest Bucicovschi and Jiří Lebl. “On the Continuity and Regularity of Convex Extensions”. In: *J. Convex Anal.* 20.4 (2013), pp. 1113–1126.

[Bou+14] Jan Bouda, Marcin Pawłowski, Matej Pivoluska, and Martin Plesch. “Device-independent randomness extraction from an arbitrarily weak min-entropy source”. In: *Physical Review A* 90.3 (2014), p. 032313.

[Bow+16] Joseph Bowles, Jérémie Francfort, Mathieu Fillettaz, Flavien Hirsch, and Nicolas Brunner. “Genuinely multipartite entangled quantum states with fully local hidden variable models and hidden multipartite nonlocality”. In: *Physical review letters* 116.13 (2016), p. 130401.

[BP05] Jonathan Barrett and Stefano Pironio. “Popescu-Rohrlich correlations as a unit of nonlocality”. In: *Physical review letters* 95.14 (2005), p. 140401.

[Bra+13] Cyril Branciard, Denis Rosset, Yeong-Cherng Liang, and Nicolas Gisin. “Measurement-device-independent entanglement witnesses for all entangled quantum states”. In: *Physical review letters* 110.6 (2013), p. 060405.

[Bru+14] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner. “Bell nonlocality”. In: *Reviews of Modern Physics* 86.2 (2014), p. 419.

[BSS14] Jean-Daniel Bancal, Lana Sheridan, and Valerio Scarani. “More Randomness from the Same Data”. In: *New J. Phys.* 16.3 (2014), p. 033011. DOI: 10.1088/1367-2630/16/3/033011.

[Buh+10] Harry Buhrman, Richard Cleve, Serge Massar, and Ronald De Wolf. “Nonlocality and communication complexity”. In: *Reviews of modern physics* 82.1 (2010), p. 665.

[BV04] Stephen Boyd and Lieven Vandenberghe. *Convex optimization*. Cambridge university press, 2004.

[BV13] Jop Briët and Thomas Vidick. “Explicit lower and upper bounds on the entangled value of multiplayer XOR games”. In: *Communications in Mathematical Physics* 321.1 (2013), pp. 181–207.

[BW92] Charles H Bennett and Stephen J Wiesner. “Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states”. In: *Physical review letters* 69.20 (1992), p. 2881.

[CAA18] Florian J. Curchod, Mafalda L. Almeida, and Antonio Acín. “A simple approach to genuine multipartite nonlocality of pure states”. In: *To appear* (2018).

[Cav+11] Daniel Cavalcanti, Mafalda L. Almeida, Valerio Scarani, and Antonio Acín. “Quantum networks reveal quantum nonlocality”. In: *Nature communications* 2 (2011), p. 184.

[Cer+05] Nicolas J Cerf, Nicolas Gisin, Serge Massar, and Sandu Popescu. “Simulating maximal quantum entanglement without communication”. In: *Physical Review Letters* 94.22 (2005), p. 220403.

[Cer02] José L Cereceda. “Three-particle entanglement versus three-particle nonlocality”. In: *Physical Review A* 66.2 (2002), p. 024102.

[CGL15] Florian J. Curchod, Nicolas Gisin, and Yeong-Cherng Liang. “Quantifying multipartite nonlocality via the size of the resource”. In: *Physical Review A* 91.1 (2015), p. 012121.

[Che+04] Jing-Ling Chen, Chunfeng Wu, Leong Chuan Kwek, and Choo Hiap Oh. “Gisin’s theorem for three qubits”. In: *Physical review letters* 93.14 (2004), p. 140407.

[Che+11] Jing-Ling Chen, Dong-Ling Deng, Hong-Yi Su, Chunfeng Wu, and CH Oh. “Detecting full N-particle entanglement in arbitrarily-high-dimensional systems with Bell-type inequalities”. In: *Physical Review A* 83.2 (2011), p. 022316.

[Che+14] Qing Chen, Sixia Yu, Chengjie Zhang, CH Lai, and CH Oh. “Test of genuine multipartite nonlocality without inequalities”. In: *Physical review letters* 112.14 (2014), p. 140404.

[Chs] In: ().

[Cir80] Boris S Cirel’son. “Quantum generalizations of Bell’s inequality”. In: *Letters in Mathematical Physics* 4.2 (1980), pp. 93–100.

[CK11] Roger Colbeck and Adrian Kent. “Private randomness expansion with untrusted devices”. In: *Journal of Physics A: Mathematical and Theoretical* 44.9 (2011), p. 095305.

[Cla+69] John F Clauser, Michael A Horne, Abner Shimony, and Richard A Holt. “Proposed experiment to test local hidden-variable theories”. In: *Physical review letters* 23.15 (1969), p. 880.

[Cle+04] Richard Cleve, Peter Hoyer, Benjamin Toner, and John Watrous. “Consequences and limits of nonlocal strategies”. In: *Computational Complexity, 2004. Proceedings. 19th IEEE Annual Conference on*. IEEE. 2004, pp. 236–249.

[CLG14] Florian J. Curchod, Yeong-Cherng Liang, and Nicolas Gisin. “Multipartite nonlocality as a resource and quantum correlations having indefinite causal order”. In: *Journal of Physics A: Mathematical and Theoretical* 47.42 (2014), p. 424014.

[Col+02a] Daniel Collins, Nicolas Gisin, Noah Linden, Serge Massar, and Sandu Popescu. “Bell inequalities for arbitrarily high-dimensional systems”. In: *Physical review letters* 88.4 (2002), p. 040404.

[Col+02b] Daniel Collins, Nicolas Gisin, Sandu Popescu, David Roberts, and Valerio Scarani. “Bell-type inequalities to detect true n-body nonseparability”. In: *Physical review letters* 88.17 (2002), p. 170405.

[CR12] Roger Colbeck and Renato Renner. “Free randomness can be amplified”. In: *Nature Physics* 8.6 (2012), p. 450.

[CS16] Daniel Cavalcanti and Paul Skrzypczyk. “Quantitative relations between measurement incompatibility, quantum steering, and nonlocality”. In: *Physical Review A* 93.5 (2016), p. 052112.

[Cur+17] Florian J. Curchod, Markus Johansson, Remigiusz Augusiak, Matthew J. Hoban, Peter Wittek, and Antonio Acín. “Unbounded randomness certification using sequences of measurements”. In: *Physical Review A* 95.2 (2017), p. 020102.

[Cur+18] Florian J. Curchod, Markus Johansson, Remigiusz Augusiak, Matty J. Hoban, Peter Wittek, and Antonio Acín. “Entangled systems are unbounded sources of nonlocal correlations and of certified random numbers”. In: *LIPIcs-Leibniz International Proceedings in Informatics*. Vol. 73. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik. 2018.

[Cur13] F. J. Curchod. “Master Thesis”. In: *University of Geneva* (2013).

[Dam99] Wim van Dam. “Nonlocality and communication complexity”. PhD thesis. University of Oxford, 1999.

[DC00] W Dür and JI Cirac. “Classification of multiqubit mixed states: Separability and distillability properties”. In: *Physical Review A* 61.4 (2000), p. 042314.

[DiV+03] David P DiVincenzo, Tal Mor, Peter W Shor, John A Smolin, and Barbara M Terhal. “Unextendible product bases, uncompletable product bases and bound entanglement”. In: *Communications in Mathematical Physics* 238.3 (2003), pp. 379–410.

[DP08] Stefan Dziembowski and Krzysztof Pietrzak. “Leakage-resilient cryptography”. In: *Foundations of Computer Science, 2008. FOCS’08. IEEE 49th Annual IEEE Symposium on*. IEEE. 2008, pp. 293–302.

[DPP05] Giacomo Mauro D'Ariano, Paoloplacido Lo Presti, and Paolo Perinotti. "Classical randomness in quantum measurements". In: *J. Phys. A: Math. Gen.* 38.26 (2005), p. 5979. DOI: 10.1088/0305-4470/38/26/010.

[Ebe93] Philippe H Eberhard. "Background level and counter efficiencies required for a loophole-free Einstein-Podolsky-Rosen experiment". In: *Physical Review A* 47.2 (1993), R747.

[Eke91] Artur K Ekert. "Quantum cryptography based on Bell's theorem". In: *Physical review letters* 67.6 (1991), p. 661.

[EPR35] Albert Einstein, Boris Podolsky, and Nathan Rosen. "Can quantum-mechanical description of physical reality be considered complete?" In: *Physical review* 47.10 (1935), p. 777.

[FC72] Stuart J. Freedman and John F. Clauser. "Experimental test of local hidden-variable theories". In: *Physical Review Letters* 28.14 (1972), p. 938.

[FFW11] Torsten Franz, Fabian Furrer, and RF Werner. "Extremal quantum correlations and cryptographic security". In: *Physical review letters* 106.25 (2011), p. 250502.

[Fin82] Arthur Fine. "Hidden variables, joint probability, and the Bell inequalities". In: *Physical Review Letters* 48.5 (1982), p. 291.

[FP15] EA Fonseca and Fernando Parisio. "Measure of nonlocality which is maximal for maximally entangled qutrits". In: *Physical Review A* 92.3 (2015), p. 030101.

[Fri+13] Tobias Fritz, Ana Belén Sainz, Remigiusz Augusiak, J Bohr Brask, Rafael Chaves, Anthony Leverrier, and Antonio Acín. "Local orthogonality as a multipartite principle for quantum correlations". In: *Nature communications* 4 (2013), p. 2263.

[Fro81] Marcel Froissart. "Constructive generalization of Bell's inequalities". In: *Il Nuovo Cimento B (1971-1996)* 64.2 (1981), pp. 241–251.

[Gal+12] Rodrigo Gallego, Lars Erik Würflinger, Antonio Acín, and Miguel Navascués. "Operational framework for nonlocality". In: *Physical review letters* 109.7 (2012), p. 070401.

[Gal+13] Rodrigo Gallego, Lluis Masanes, Gonzalo De La Torre, Chirag Dhara, Leandro Aolita, and Antonio Acín. "Full randomness from arbitrarily deterministic events". In: *Nature communications* 4 (2013), p. 2654.

[Gal+14] Rodrigo Gallego, Lars Erik Würflinger, Rafael Chaves, Antonio Acín, and Miguel Navascués. “Nonlocality in Sequential Correlation Scenarios”. In: *New J. Phys.* 16.3 (2014), p. 033037. DOI: 10.1088/1367-2630/16/3/033037.

[GBP98] Nicolas Gisin and Helle Bechmann-Pasquinucci. “Bell inequality, Bell states and maximally entangled states for n qubits”. In: *Physics Letters A* 246.1-2 (1998), pp. 1–6.

[GG16] Mariami Gachechiladze and Otfried Gühne. “Addendum to" Generic quantum nonlocality"[Phys. Lett. A 166, 293 (1992)]”. In: *arXiv preprint arXiv:1607.02948* (2016).

[GG97] Jozef Gruska and J Gruska. *Foundations of computing*. International Thomson Computer Press Boston, MA, USA, 1997.

[GHZ89] Daniel M Greenberger, Michael A Horne, and Anton Zeilinger. “Going beyond Bell’s theorem”. In: *Bell’s theorem, quantum theory and conceptions of the universe*. Springer, 1989, pp. 69–72.

[Gis91] Nicolas Gisin. “Bell’s inequality holds for all non-product states”. In: *Physics Letters A* 154.5-6 (1991), pp. 201–202.

[Giu+15] Marissa Giustina, Marijn AM Versteegh, Sören Wengerowsky, Johannes Handsteiner, Armin Hochrainer, Kevin Phelan, Fabian Steinlechner, Johannes Kofler, Jan-Åke Larsson, Carlos Abellán, et al. “Significant-loophole-free test of Bell?s theorem with entangled photons”. In: *Physical review letters* 115.25 (2015), p. 250401.

[Grü+67] Branko Grünbaum, Victor Klee, Micha A Perles, and Geoffrey Colin Shephard. *Convex polytopes*. Vol. 16. Springer, 1967.

[GTB05] Otfried Gühne, Géza Tóth, and Hans J Briegel. “Multipartite entanglement in spin chains”. In: *New Journal of Physics* 7.1 (2005), p. 229.

[Gur04] Leonid Gurvits. “Classical complexity and quantum entanglement”. In: *Journal of Computer and System Sciences* 69.3 (2004), pp. 448–484.

[Har93] Lucien Hardy. “Nonlocality for two particles without inequalities for almost all entangled states”. In: *Physical Review Letters* 71.11 (1993), p. 1665.

[HBB99] Mark Hillery, Vladimír Bužek, and André Berthiaume. “Quantum secret sharing”. In: *Physical Review A* 59.3 (1999), p. 1829.

[Hen+15] Bas Hensen, Hannes Bernien, Anaïs E. Dréau, Andreas Reiserer, Norbert Kalb, Machiel S. Blok, Just Ruitenberg, Raymond FL. Vermeulen, Raymond N. Schouten, Carlos Abellán, et al. "Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres". In: *Nature* 526.7575 (2015), pp. 682–686.

[HHH95] Ryszard Horodecki, Pawel Horodecki, and Michal Horodecki. "Violating Bell inequality by mixed spin-12 states: necessary and sufficient condition". In: *Physics Letters A* 200.5 (1995), pp. 340–344.

[HHH98] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki. "Mixed-state entanglement and distillation: is there a ?bound? entanglement in nature?" In: *Physical Review Letters* 80.24 (1998), p. 5239.

[Hir+13] Flavien Hirsch, Marco Túlio Quintino, Joseph Bowles, and Nicolas Brunner. "Genuine hidden quantum nonlocality". In: *Physical review letters* 111.16 (2013), p. 160402.

[Hol73] Alexander Semenovich Holevo. "Bounds for the quantity of information transmitted by a quantum communication channel". In: *Problemy Peredachi Informatsii* 9.3 (1973), pp. 3–11.

[Hor+09] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki. "Quantum entanglement". In: *Reviews of modern physics* 81.2 (2009), p. 865.

[Hu+16] Meng-Jun Hu, Zhi-Yuan Zhou, Xiao-Min Hu, Chuan-Feng Li, Guang-Can Guo, and Yong-Sheng Zhang. "Experimental Sharing of Nonlocality among Multiple Observers with One Entangled Pair via Optimal Weak Measurements". In: *arXiv:1609.01863* (2016). eprint: 1609.01863.

[JLM05] Nick S Jones, Noah Linden, and Serge Massar. "Extent of multiparticle quantum nonlocality". In: *Physical Review A* 71.4 (2005), p. 042329.

[Lia+10] Yeong-Cherng Liang, Nicholas Harrigan, Stephen D Bartlett, and Terry Rudolph. "Nonclassical correlations from randomly chosen local measurements". In: *Physical review letters* 104.5 (2010), p. 050401.

[Lia+14] Yeong-Cherng Liang, Florian J. Curchod, Joseph Bowles, and Nicolas Gisin. "Anonymous Quantum Nonlocality". In: *Physical review letters* 113.13 (2014), p. 130401.

[Lia+15] Yeong-Cherng Liang, Denis Rosset, Jean-Daniel Bancal, Gilles Pütz, Tomer Jack Barnea, and Nicolas Gisin. "Family of bell-like inequalities as device-independent witnesses for entanglement depth". In: *Physical review letters* 114.19 (2015), p. 190401.

[Lip+18] Victoria Lipinska, Florian J. Curchod, Alejandro Máttar, and Antonio Acín. “Towards an equivalence between maximal entanglement and maximal quantum nonlocality”. In: *New Journal of Physics* (2018).

[LRR14] Felipe G Lacerda, Joseph M Renes, and Renato Renner. “Classical leakage resilience from fault-tolerant quantum computation”. In: *arXiv preprint arXiv:1404.7516* (2014).

[LVB11] Yeong-Cherng Liang, Tamás Vértesi, and Nicolas Brunner. “Semi-device-independent bounds on entanglement”. In: *Physical Review A* 83.2 (2011), p. 022108.

[Mer90a] N David Mermin. “Extreme quantum entanglement in a superposition of macroscopically distinct states”. In: *Physical Review Letters* 65.15 (1990), p. 1838.

[Mer90b] N David Mermin. “Simple unified form for the major no-hidden-variables theorems”. In: *Physical Review Letters* 65.27 (1990), p. 3373.

[MLD08] Lluís Masanes, Yeong-Cherng Liang, and Andrew C. Doherty. “All bipartite entangled states display some hidden nonlocality”. In: *Physical review letters* 100.9 (2008), p. 090403.

[Mor+13] Tobias Moroder, Jean-Daniel Bancal, Yeong-Cherng Liang, Martin Hofmann, and Otfried Gühne. “Device-independent entanglement quantification and related applications”. In: *Physical review letters* 111.3 (2013), p. 030501.

[MPA11] Lluís Masanes, Stefano Pironio, and Antonio Acín. “Secure device-independent quantum key distribution with causally independent measurement devices”. In: *Nature communications* 2 (2011), p. 238.

[MPR04] Peter Mitchell, Sandu Popescu, and David Roberts. “Conditions for the confirmation of three-particle nonlocality”. In: *Physical Review A* 70.6 (2004), p. 060101.

[MS06] André Allan Méthot and Valerio Scarani. “An anomaly of non-locality”. In: *arXiv preprint quant-ph/0601210* (2006).

[MS16] Carl A Miller and Yaoyun Shi. “Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices”. In: *Journal of the ACM (JACM)* 63.4 (2016), p. 33.

[MY98] Dominic Mayers and Andrew Yao. “Quantum cryptography with imperfect apparatus”. In: *Foundations of Computer Science, 1998. Proceedings. 39th Annual Symposium on*. IEEE. 1998, pp. 503–509.

[Nie99] Michael A Nielsen. “Conditions for a class of entanglement transformations”. In: *Physical Review Letters* 83.2 (1999), p. 436.

[NKI02] Koji Nagata, Masato Koashi, and Nobuyuki Imoto. "Configuration of separability and tests for multipartite entanglement in Bell-type experiments". In: *Physical review letters* 89.26 (2002), p. 260401.

[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), p. 073013.

[NSPS14] Olmo Nieto-Silleras, Stefano Pironio, and Jonathan Silman. "Using complete measurement statistics for optimal device-independent randomness evaluation". In: *New J. Phys.* 16.1 (2014), p. 013035. DOI: 10.1088/1367-2630/16/1/013035.

[Pal12] Carlos Palazuelos. "Superactivation of quantum nonlocality". In: *Physical review letters* 109.19 (2012), p. 190401.

[PBS11] Stefano Pironio, Jean-Daniel Bancal, and Valerio Scarani. "Extremal correlations of the tripartite no-signaling polytope". In: *Journal of Physics A: Mathematical and Theoretical* 44.6 (2011), p. 065303.

[Per96] Asher Peres. "Separability criterion for density matrices". In: *Physical Review Letters* 77.8 (1996), p. 1413.

[Pir+10] Stefano Pironio, Antonio Acín, Serge Massar, A Boyer de La Giroday, Dzimitry N Matsukevich, Peter Maunz, Steven Olmschenk, David Hayes, Le Luo, T Andrew Manning, and C. Monroe. "Random Numbers Certified by Bell's Theorem". In: *Nature* 464.7291 (2010), pp. 1021–1024. DOI: 10.1038/nature09008.

[Pir05] Stefano Pironio. "Lifting bell inequalities". In: *Journal of mathematical physics* 46.6 (2005), p. 062112.

[Pir14] Stefano Pironio. "All Clauser–Horne–Shimony–Holt polytopes". In: *Journal of Physics A: Mathematical and Theoretical* 47.42 (2014), p. 424020.

[Pop95] Sandu Popescu. "Bell's Inequalities and Density Matrices: Revealing "Hidden" Nonlocality". In: *Phys. Rev. Lett.* 74.14 (1995), pp. 2619–2622. ISSN: 1079-7114. DOI: 10.1103/physrevlett.74.2619.

[Pr] In: ().

[PR92] Sandu Popescu and Daniel Rohrlich. "Generic quantum nonlocality". In: *Physics Letters A* 166.5-6 (1992), pp. 293–297.

[PR94] Sandu Popescu and Daniel Rohrlich. "Quantum nonlocality as an axiom". In: *Foundations of Physics* 24.3 (1994), pp. 379–385.

[PR97] Sandu Popescu and Daniel Rohrlich. "Thermodynamics and the measure of entanglement". In: *Physical Review A* 56.5 (1997), R3319.

[PV11] Károly F Pál and Tamás Vértesi. “Multisetting Bell-type inequalities for detecting genuine multipartite entanglement”. In: *Physical Review A* 83.6 (2011), p. 062123.

[Qui12] M. T. Quintino. “Master Thesis”. In: *Universidade Federal de Minas Gerais* (2012).

[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), p. 424022.

[Roc70] Tyrrell Rockafellar. *Convex Analysis*. Princeton Press, 1970.

[Ros+12] Denis Rosset, Raphael Ferretti-Schöbitz, Jean-Daniel Bancal, Nicolas Gisin, and Yeong-Cherng Liang. “Imperfect measurement settings: Implications for quantum state tomography and entanglement witnesses”. In: *Physical Review A* 86.6 (2012), p. 062325.

[Ros+17] Anna de Rosier, Jacek Gruca, Fernando Parisio, Tamás Vértesi, and Wiesław Laskowski. “Multipartite nonlocality and random measurements”. In: *Physical Review A* 96.1 (2017), p. 012101.

[RS91] SM Roy and Virendra Singh. “Tests of signal locality and Einstein-Bell locality for multiparticle systems”. In: *Physical review letters* 67.20 (1991), p. 2761.

[RT09] Oded Regev and Ben Toner. “Simulating quantum correlations with finite communication”. In: *SIAM Journal on Computing* 39.4 (2009), pp. 1562–1580.

[Sal+17] Alexia Salavrakos, Remigiusz Augusiak, Jordi Tura, Peter Wittek, Antonio Acín, and Stefano Pironio. “Bell Inequalities Tailored to Maximally Entangled States”. In: *Physical review letters* 119.4 (2017), p. 040402.

[Sch+17] Matteo Schiavon, Luca Calderaro, Mirko Pittaluga, Giuseppe Vallone, and Paolo Villoresi. “Three-observer Bell inequality violation on a two-qubit entangled state”. In: *Quantum Science and Technology* 2.1 (2017), p. 015010. DOI: 10.1088/2058-9565/aa62be.

[Sch07] Bruce Schneier. *Applied cryptography: protocols, algorithms, and source code in C*. john wiley & sons, 2007.

[Sch35] Erwin Schrödinger. “Discussion of probability relations between separated systems”. In: *Mathematical Proceedings of the Cambridge Philosophical Society*. Vol. 31. 4. Cambridge University Press. 1935, pp. 555–563.

[Sha+12] Peter Shadbolt, Tamás Vértesi, Yeong-Cherng Liang, Cyril Branciard, Nicolas Brunner, and Jeremy L O'brien. "Guaranteed violation of a Bell inequality without aligned reference frames or calibrated devices". In: *Scientific reports* 2 (2012), p. 470.

[Sha+15] Lynden K. Shalm, Evan Meyer-Scott, Bradley G. Christensen, Peter Bierhorst, Michael A. Wayne, Martin J. Stevens, Thomas Gerrits, Scott Glancy, Deny R. Hamel, Michael S. Allman, et al. "Strong loophole-free test of local realism". In: *Physical review letters* 115.25 (2015), p. 250402.

[Sil+15] Ralph Silva, Nicolas Gisin, Yelena Guryanova, and Sandu Popescu. "Multiple Observers Can Share the Nonlocality of Half of an Entangled Pair by Using Optimal Weak Measurements". In: *Phys. Rev. Lett.* 114.25 (2015), p. 250401. DOI: 10.1103/physrevlett.114.250401.

[SNC14] Paul Skrzypczyk, Miguel Navascués, and Daniel Cavalcanti. "Quantifying einstein-podolsky-rosen steering". In: *Physical review letters* 112.18 (2014), p. 180404.

[SS02] Michael Seevinck and George Svetlichny. "Bell-type inequalities for partial separability in N-particle systems and quantum mechanical violations". In: *Physical review letters* 89.6 (2002), p. 060401.

[Sta+10] François-Xavier Standaert, Olivier Pereira, Yu Yu, Jean-Jacques Quisquater, Moti Yung, and Elisabeth Oswald. "Leakage resilient cryptography in practice". In: *Towards Hardware-Intrinsic Security*. Springer, 2010, pp. 99–134.

[Sve87] George Svetlichny. "Distinguishing three-body from two-body nonseparability by a Bell-type inequality". In: *Physical Review D* 35.10 (1987), p. 3066.

[SW97] Benjamin Schumacher and Michael D Westmoreland. "Sending classical information via noisy quantum channels". In: *Physical Review A* 56.1 (1997), p. 131.

[TB03] Ben F Toner and Dave Bacon. "Communication cost of simulating Bell correlations". In: *Physical Review Letters* 91.18 (2003), p. 187904.

[Ter00] Barbara M. Terhal. "Bell inequalities and the separability criterion". In: *Physics Letters A* 271.5-6 (2000), pp. 319–326.

[Tor+15] Gonzalo de la Torre, Matty J. Hoban, Chirag Dhara, Giuseppe Prettico, and Antonio Acín. "Maximally Nonlocal Theories Cannot Be Maximally Random". In: *Phys. Rev. Lett.* 114.16 (2015), p. 160502. DOI: 10.1103/physrevlett.114.160502.

[Tsi93] Boris S Tsirelson. "Some results and problems on quantum Bell-type inequalities". In: *Hadronic Journal Supplement* 8.4 (1993), pp. 329–345.

[Tur+14] Jordi Tura, Remigiusz Augusiak, Ana Belén Sainz, Tamas Vértesi, Maciej Lewenstein, and Antonio Acín. "Detecting nonlocality in many-body quantum states". In: *Science* 344.6189 (2014), pp. 1256–1258.

[VB10] T Vértesi and E Bene. "Two-qubit Bell inequality for which positive operator-valued measurements are relevant". In: *Physical Review A* 82.6 (2010), p. 062115.

[VB12] Tamás Vértesi and Nicolas Brunner. "Quantum nonlocality does not imply entanglement distillability". In: *Physical review letters* 108.3 (2012), p. 030403.

[VP08] T Vértesi and KF Pál. "Generalized Clauser-Horne-Shimony-Holt inequalities maximally violated by higher-dimensional systems". In: *Physical Review A* 77.4 (2008), p. 042106.

[VV14] Umesh Vazirani and Thomas Vidick. "Fully device-independent quantum key distribution". In: *Physical review letters* 113.14 (2014), p. 140501.

[VW11] Thomas Vidick and Stephanie Wehner. "More nonlocality with less entanglement". In: *Physical Review A* 83.5 (2011), p. 052310.

[Wer89] Reinhard F Werner. "Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model". In: *Physical Review A* 40.8 (1989), p. 4277.

[Wit15] Peter Wittek. "Algorithm 950: Ncpol2sdpa—Sparse Semidefinite Programming Relaxations for Polynomial Optimization Problems of Noncommuting Variables". In: *ACM Trans. Math. Software* 41.3 (2015), p. 21. DOI: 10.1145/2699464.

[WJD07] Howard M Wiseman, Steve James Jones, and Andrew C Doherty. "Steering, entanglement, nonlocality, and the Einstein-Podolsky-Rosen paradox". In: *Physical review letters* 98.14 (2007), p. 140402.

[WLB11] Joel J Wallman, Yeong-Cherng Liang, and Stephen D Bartlett. "Generating nonclassical correlations without fully aligning measurements". In: *Physical Review A* 83.2 (2011), p. 022110.

[Woo98] William K Wootters. "Entanglement of formation of an arbitrary state of two qubits". In: *Physical Review Letters* 80.10 (1998), p. 2245.

[WW00] Reinhard F Werner and Michael M Wolf. "Bell's inequalities for states with positive partial transpose". In: *Physical Review A* 61.6 (2000), p. 062102.

[WW01a] Reinhard F Werner and Michael M Wolf. "All-multipartite Bell-correlation inequalities for two dichotomic observables per site". In: *Physical Review A* 64.3 (2001), p. 032112.

[WW01b] Reinhard F Werner and Michael M Wolf. "Bell inequalities and entanglement". In: *arXiv preprint quant-ph/0107093* (2001).

[WZ82] William K Wootters and Wojciech H Zurek. "A single quantum cannot be cloned". In: *Nature* 299.5886 (1982), pp. 802–803.

[YFK03] Makoto Yamashita, Katsuki Fujisawa, and Masakazu Kojima. "Implementation and evaluation of SDPA 6.0 (semidefinite programming algorithm 6.0)". In: *Optim. Method. Softw.* 18.4 (2003), pp. 491–505. DOI: 10.1080/1055678031000118482.

[YO13] Sixia Yu and CH Oh. "Tripartite entangled pure states are tripartite nonlocal". In: *arXiv preprint arXiv:1306.5330* (2013).

[ZG08] Stefan Zohren and Richard D Gill. "Maximal violation of the Collins-Gisin-Linden-Massar-Popescu inequality for infinite dimensional states". In: *Physical review letters* 100.12 (2008), p. 120406.

[Śli03] Cezary Śliwa. "Symmetries of the Bell correlation inequalities". In: *Physics Letters A* 317.3-4 (2003), pp. 165–168.