Quantum codes and locally recoverable codes from evaluation codes

AUTHOR
Helena Martín Cruz

ADVISORS
Dr. Carlos Galindo Pastor
Dr. Fernando Javier Hernando Carrillo

PhD Thesis, June 2024

Programa de Doctorado en Ciencias
Escuela de Doctorado de la Universitat Jaume I

Quantum codes and locally recoverable codes from evaluation codes

---

Memoria presentada por Helena Martín Cruz para optar al grado de doctora por la Universitat Jaume I

DOCTORANDA
Helena Martín Cruz

DIRECTORES
Dr. Carlos Galindo Pastor
Dr. Fernando Javier Hernando Carrillo

Castelló de la Plana, Junio 2024

Funding and licence

Funding The author of this work has received financial support from the following sources:

- Research project **PGC2018-096446-B-C22**: Valoraciones, Foliaciones y Códigos Correctores de Errores Cuánticos.
  By MCIN/AEI/10.13039/501100011033 and by "ERDF A way of making Europe".
  From 01/01/2019 to 31/12/2022.

- Grant **PREDOC/2020/39**: Ayuda predoctoral para la formación de personal investigador.
  By Universitat Jaume I: Plan de Promoción de la Investigación de la UJI para el año 2020.
  From 01/05/2021 to 30/04/2025.

- Research project **UJI-B2021-02**: Valoraciones y positividad en la geometría algebraica. Aplicaciones a campos vectoriales y códigos correctores cuánticos.
  By Universitat Jaume I.
  From 01/01/2022 to 31/12/2024.

- Research project **TED2021-130358B-I00**: Teoría de Códigos y Tendencias Algebraicas para Criptografía, Almacenamiento de Datos Distribuidos, Aprendizaje Automático e Información Cuántica (secureCAT).
  By MCIN/AEI/10.13039/501100011033 and by "European Union NextGeneration EU/PRTR".
  From 01/12/2022 to 30/11/2024.

- Research project **GACUJIMA/2023/06**: Modalitat A: Ajudes de continuïtat de «Projectes de generació de coneixement» del Pla Estatal d'Investigació Científica i Tècnica i d'Innovació.
  By Universitat Jaume I.
  From 07/03/2023 to 31/12/2023.

- Grant **E-2022-12**: Beca para realizar estancias temporales en otros centros de investigación, para el personal docente e investigador de la Universidad, Acción 2 del Programa de movilidad del personal investigador.
  By Universitat Jaume I: Plan de Promoción de la Investigación de la UJI para el año 2022.
  From 30/03/2023 to 30/06/2023.

- Research project **PID2022-138906NB-C22**: Sistemas lineales y positividad. Foliaciones. Códigos cuánticos y localmente recuperables.
  By MCIN/AEI/10.13039/501100011033 and by "ERDF/UE".
  From 01/09/2023 to 31/08/2027.

- Research project **GACUJIMB/2023/03**: Modalitat B: Ajudes d'enfortiment de «Projectes de generació de coneixement» del Pla Estatal d'Investigació Científica i Tècnica i d'Innovació.
  By Universitat Jaume I.
  From 01/01/2024 to 31/12/2024.

"It is impossible to be a mathematician
without being a poet in soul"

— Sofia Kovalévskaya

Acknowledgments

I hope the non-Spanish-speaking reader will forgive me for my desire to express myself in my mother tongue.

Quisiera comenzar dedicando mis agradecimientos al proceso íntegro que he experimentado durante esta etapa, junto con todas las variables que han influido para que haya sucedido tal y como ha sido. Las enseñanzas que me ha aportado poseen un gran valor para mí.

Las primeras personas a las que siento que debo agradecer son mis directores, Carlos y Fernando, quienes han sido indispensables en todo el camino. Por el aprendizaje que me llevo de vosotros, impulsarme hacia aquello que creíais que era lo mejor para mí y haber respetado mis tiempos.

A todos los miembros del Departamento de Matemáticas de la Universitat Jaume I, por su disponibilidad y el buen ambiente en el que me he encontrado. En particular a quienes estuvieron más presentes amenizando los días: Julio, Alejandro, Vicent y Erik.

A mis compañeros convertidos en amigos: Elvira, Carlos Jesús, Alberto, Jordi, Mario, Luke y Aleix. Por eso simplemente, pero también por haber estado siempre disponibles para unas cervezas, escucharme y apoyarme cuando lo he necesitado y haberme integrado tan rápido en mi llegada a Castellón. A Sheldon, por todo lo anterior añadiendo horas de conversación y esfuerzo manteniendo nuestra amistad.

A todas las personas que me han recibido con afecto en mis visitas, en particular a Félix Delgado y Diego Ruano, y a los miembros del grupo SINGACOM, el proyecto SecureCAT y la red MatSI por su agradable compañía en los eventos a los que hemos asistido.

Thank you, Gary, for welcoming me most warmly during my stay at University College Dublin. A Bea, por tu compañía diaria e incluirme en los planes junto al resto de doctorandos de la UCD.

A la etapa vivida en Dublín por haberse producido en ese momento y por haberme puesto a prueba.

A los profesores del Grado y Máster en Matemáticas de la Universidad de Granada por la formación previa recibida, especialmente a aquellos que me impulsaron en mi decisión de iniciar este camino: Antonio y Pedro.

A mi lugar diario de (des)conexión y carga de dopamina y serotonina: Barbell Box. A cada una de las personas que he conocido aquí que, a diario o en las quedadas, me han aportado buenos momentos. A Lorena, Manu, Raki, Irene, Pebrereta y Davisín por todo

lo que habéis contribuido en mi felicidad y bienestar, haciendo que vuestra amistad me deje huella, y por haber estado ahí cuando más lo necesitaba. A Mike, porque avanzar hacia mi versión más fuerte ha sido más fácil con tu ayuda. Todo lo que lo anterior supone y pequeñas cosas como conversaciones, risas y gritos de ánimo me han aportado más que energía para afrontar esta etapa.

Al grupo de bailarines de Granada por lo que supuso en mis inicios de este trayecto y porque las (siempre insuficientes) veces que he compartido con vosotras en alguna visita he vuelto llena de emoción durante varios días. A Eibi, por haber dado lugar a que no solo mi danza, sino también mi persona, se haya nutrido de otro nivel de consciencia, conexión y otros estados positivos.

A mis amistades del pueblo. Volver a encontrarme con vosotros y sentir como si no hubiese pasado el tiempo me recargaba las pilas. A Jaime, por tu presencia y apoyo durante todo este tiempo. A María, por estar igual de predispuesta tanto para celebrar lo bueno como para preocuparte por mí. A Mar, por la ayuda que me has aportado con nuestras conversaciones, pero sobre todo por no dejar de estar.

A mi familia, por vuestro ejemplo, el apoyo constante y la confianza que siempre habéis depositado en mí. Por alegraros de mis logros más que yo, y porque simplemente veros o escucharos se ha sentido como medicina. Especialmente a ti, mamá, por estar a mi lado en la distancia sin fallar ni un solo día.

A la persona que he sido en cada etapa, porque aunque no era lo habitual en mí, agradecerme es uno de los aprendizajes personales más importantes que me llevo. Por cada una de mis acciones hasta hoy, y por la perseverancia y la aspiración de mejora que no han dejado de caracterizarme.

Al baile: mi imprescindible, siempre ahí, en todas sus y mis versiones. Por permitirme expresar lo que no se puede de otra forma. Por llenarme de vida, energía y paz.

A Andrea, por acompañarme en todo momento sin haber faltado tu cuidado. Y porque los aprendizajes más valiosos me los has enseñado tú.

Abstract

This PhD thesis addresses two current problems that belong to the fields of classical and quantum information theory. These are the repair problem in distributed and cloud storage systems and the construction of good quantum error-correcting codes. We mainly use tools coming from algebra and algebraic geometry.

The work is divided in four parts. The first part contains some preliminaries on classical (Chapter 1) and quantum (Chapter 2) error-correcting codes. Suitable classical error-correcting codes, particularly evaluation codes, are the main instrument to give a solution to the problems we address.

The second part is devoted to construct codes dealing the repair problem in the setting where simultaneous multiple device failures may happen. These codes are called (r, δ)-locally recoverable codes. Chapter 3 shows interesting advances by considering monomial-Cartesian codes as (r, δ)-locally recoverable codes. These codes come with a natural bound for their minimum distance and we determine those giving rise to (r, δ)-optimal locally recoverable codes for that minimum distance, which are in fact (r, δ)-optimal. We prove that a large subfamily of monomial-Cartesian codes admits subfield-subcodes with the same parameters of certain (r, δ)-optimal monomial-Cartesian codes but over smaller supporting fields. This fact allows us to determine infinitely many new (r, δ)-optimal locally recoverable codes.

Our constructions of new and good quantum-error correcting codes are given in the third part of this PhD thesis. Chapter 4 shows how to construct new stabilizer quantum error-correcting codes from generalized (or twisted) monomial-Cartesian codes. Our construction uses an explicitly defined twist vector, and we present formulae for the minimum distance and dimension. Generalized monomial-Cartesian codes arise from polynomials in m variables. When $m = 1$ our codes are quantum maximum distance separable, and when $m = 2$ and our lower bound for the minimum distance is 3, the obtained codes are at least Hermitian almost maximum distance separable. Continuing with the case $m = 2$ we prove that, for an infinite family of parameters, our codes beat the quantum Gilbert-Varshamov bound. Our construction gives rise to many codes whose parameters improve those appearing in the literature.

Quantum error-correcting codes with good parameters can also be constructed by evaluating polynomials at the roots of the trace polynomial. In Chapter 5, we propose to evaluate polynomials at the roots of what we call trace-depending polynomials. They are given by a nonzero constant plus the trace of a polynomial. We show that this

procedure gives rise to stabilizer quantum error-correcting codes with a new wide range of lengths and with excellent parameters. Namely, we are able to provide new binary records according to Markus Grassl tables and non-binary codes improving the ones available in the literature.

Some ideas on future research can be found in the brief fourth part which finishes this thesis.

Resumen

Esta tesis doctoral aborda dos problemas actuales que pertenecen a los campos de la teoría de la información clásica y cuántica. Estos son el problema de recuperación en sistemas de almacenamiento distribuido y en la nube y la construcción de buenos códigos cuánticos correctores de errores. Principalmente usamos herramientas provenientes del álgebra y la geometría algebraica.

El trabajo se divide en cuatro partes. La primera parte contiene algunos preliminares sobre los códigos clásicos (Capítulo 1) y cuánticos (Capítulo 2) correctores de errores. Ciertos códigos clásicos correctores de errores, en particular códigos de evaluación, son el principal instrumento para dar solución a los problemas que abordamos.

La segunda parte se dedica a construir códigos diseñados para tratar el problema de recuperación bajo la situación en la que se puedan producir fallos en varios nodos simultáneamente. Estos códigos se denominan códigos (r, δ)-localmente recuperables. El Capítulo 3 muestra avances interesantes considerando los códigos Cartesiano-monomiales como códigos (r, δ)-localmente recuperables. Estos códigos poseen una cota natural para su distancia mínima que nos permite determinar aquellos que dan lugar a códigos (r, δ)-óptimos localmente recuperables para esa distancia mínima, que de hecho son (r, δ)-óptimos. Probamos que una amplia subfamilia de códigos Cartesiano-monomiales admite subcódigos-subcuerpo con los mismos parámetros que ciertos códigos Cartesiano-monomiales (r, δ)-óptimos pero sobre cuerpos más pequeños. Este hecho nos permite determinar un número infinito de nuevos códigos (r, δ)-óptimos localmente recuperables.

Nuestras construcciones de nuevos y buenos códigos cuánticos correctores de errores se presentan en la tercera parte de esta tesis doctoral. El Capítulo 4 muestra cómo construir nuevos códigos cuánticos estabilizadores correctores de errores a partir de códigos Cartesiano-monomiales generalizados (o twisteados). Nuestra construcción usa un vector de twisteo definido explícitamente, y presentamos fórmulas para la distancia mínima y la dimensión. Los códigos Cartesiano-monomiales generalizados surgen a partir de polinomios en m variables. Cuando $m = 1$ nuestros códigos son cuánticos de máxima distancia de separación, y cuando $m = 2$ y nuestra cota inferior para la distancia mínima es 3, los códigos obtenidos son al menos Hermitianos de casi máxima distancia de separación. Continuando con el caso $m = 2$ probamos que, para una familia infinita de parámetros, nuestros códigos baten la cota Gilbert-Varshamov cuántica. Nuestra construcción da lugar a muchos códigos cuyos parámetros mejoran los existentes en la literatura.

También se pueden construir códigos cuánticos correctores de errores con buenos

parámetros evaluando polinomios en las raíces del polinomio traza. En el Capítulo 5, proponemos evaluar polinomios en las raíces de lo que llamamos polinomios dependientes de la traza. Estos vienen dados por una constante no nula más el polinomio traza cuyo argumento es otro polinomio. Demostramos que este procedimiento da lugar a códigos cuánticos estabilizadores correctores de errores con un nuevo rango de longitudes y con parámetros excelentes. En efecto, somos capaces de proporcionar nuevos récords binarios con respecto a las tablas de Markus Grassl y códigos no binarios que mejoran los existentes en la literatura.

Algunas ideas de trabajo futuro se pueden encontrar en la breve cuarta parte concluyendo esta memoria.

Contents

Acknowledgments vii

Abstract ix

Resumen xi

Introduction 1

I Preliminaries 17

1. Classical error-correcting codes 21

1.1. Encoding of information. Error-correcting codes . . . 21

1.2. Linear codes . . . 25

1.2.1. Decoding processes . . . 27

1.2.2. Singleton bound . . . 28

1.2.3. MDS codes . . . 28

1.3. Evaluation codes . . . 29

1.3.1. Monomial-Cartesian codes . . . 30

1.4. Locally recoverable codes . . . 34

1.5. Subfield-subcodes . . . 37

1.5.1. Subfield-subcodes of J-affine variety codes . . . 38

2. Quantum error-correcting codes 45

2.1. A basic introduction to quantum mechanics . . . 46

2.1.1. Postulates of quantum mechanics . . . 46

2.2. Quantum error-correcting codes . . . 50

2.2.1. Generalities . . . 50

2.2.2. A quantum error model . . . 54

2.3. Stabilizer codes . . . 56

2.3.1. Stabilizer codes from additive codes over $\mathbb{F}_Q$ . . . 59

2.3.2. Stabilizer codes from additive codes over $\mathbb{F}_{Q^2}$ . . . 59

2.3.3. Stabilizer codes from linear codes over $\mathbb{F}_{Q^2}$ . . . 60

2.3.4. Bounds on stabilizer codes . . . 60

II Locally recoverable codes from evaluation codes 63

3. Optimal (r,δ)-locally recoverable codes from monomial-Cartesian codes and their subfield subcodes 65
3.1. Locally recoverable monomial-Cartesian codes . . . 66
3.2. Optimal monomial-Cartesian codes . . . 68
3.2.1. The bivariate case $(m = 2)$ . . . 69
3.2.1.1. Proof of Remark 3.2.4 . . . 73
3.2.2. The multivariate case $(m \geq 3)$ . . . 85
3.3. Optimal subfield-subcodes . . . 88
3.3.1. Optimal (r,δ)-LRCs coming from subfield-subcodes of bivariate MCCs . . . 90
3.3.2. Optimal (r,δ)-LRCs coming from subfield-subcodes of multivariate MCCs . . . 103

III Quantum codes from evaluation codes 109

4. Stabilizer quantum codes from generalized monomial-Cartesian codes 111
4.1. Generalized monomial-Cartesian codes . . . 112
4.2. Constructions of stabilizer quantum codes from generalized monomial-Cartesian codes . . . 115
4.2.1. Self-orthogonality conditions . . . 116
4.2.2. Our general construction . . . 118
4.2.3. Our specific construction . . . 118
4.2.4. The dimension . . . 121
4.3. MDS and Hermitian almost MDS quantum codes . . . 122
4.4. Beating Gilbert-Varshamov bound . . . 123
4.4.1. The case $d = 3$ . . . 125
4.5. Examples . . . 126

5. Stabilizer quantum codes from evaluation codes at the roots of trace-depending polynomials 131
5.1. Evaluation codes and b-th trace-depending polynomials . . . 132
5.1.1. The b-th trace-depending polynomials . . . 132
5.1.2. Evaluation codes at the roots of trace-depending polynomials . . . 135
5.2. Subfield-subcodes of evaluation codes at the roots of trace-depending polynomials . . . 151
5.3. Examples . . . 155
5.3.1. Binary examples . . . 155
5.3.2. Non-binary examples . . . 156
5.4. Sporadic stabilizer quantum codes from trace-depending polynomials . . . 157

IV Further research. Some advances 159

Conclusions 163

Conclusiones 165

List of Figures 167

List of Tables 169

References 171

Introduction

In this thesis we deal with two problems that have gained importance in the last years and are quite prevalent nowadays: the repair problem in distributed and cloud storage systems and the search of quantum error-correcting codes with good parameters.

They are framed within *information theory*, a scientific area shared between mathematics and computer science. This discipline was born in 1948 with the work of C. E. Shannon, when for the first time the information was treated as a mathematical object by considering digital information. Since then, this theory, its techniques and their efficiency have experienced an exponential growth. These advances together with those in telecommunications are, nowadays, crucial for the industrial and financial sectors.

Information theory has different branches, one of them to which our research belongs is the *theory of error-correcting codes*. It arises from the need of avoiding the corruption of the transmitted information. Others branches intend to use the codes for other applications, such as data compression, cryptography and networking. All of them belong to *coding theory*, which mainly uses algebraic techniques involving mathematical areas as Galois theory, group theory or polynomial algebra.

Companies such as Google, Meta or Microsoft manage systems where digital data are stored in several nodes. Due to the huge amount of stored information, the problem of loss of data due to node failures has acquired a lot of significance. A reliable storage is required, in such way that information from any (failed) node can be recovered from that contained in other few nodes. The repair problem mentioned at the beginning of this introduction looks for a solution. Despite the fact that error-correcting codes are originally designed to make computing devices be resilient against errors, some of them, named *locally recoverable* (or *repairable*) *codes* (LRCs), can also be used for this end, protecting stored data using their potential of detection and recovery from errors.

The importance of quantum computing is beyond doubt. Shor's polynomial time algorithms for prime factorization and discrete logarithms on quantum computers [114, 113] are an illustrating example, because they give a solution to hitherto intractable problems. Quantum computers are governed by the rules of quantum mechanics, since they use subatomic particles to hold memory. Important obstacles for their reliability are the loss of coherence and the fact that they have higher error rates than the classical computers. These obstacles can be treated with quantum error-correcting codes [112, 119]. Thus, quantum error-correction is a key tool in quantum computing, which works despite quantum information cannot be cloned [34, 128]. This explains why many researchers

are looking for good *quantum error-correcting codes* (QECCs). Note that researchers and companies are actively engaged in constructing quantum computers with many qubits [26, 18].

Classical error-correcting codes and QECCs are very related, in fact, a certain type of QECCs can be constructed from classical ones. Those we consider are linear codes over finite fields $\mathbb{F}_Q$ (of cardinality a prime power Q). Linear codes are simply $\mathbb{F}_Q$-vector subspaces of $\mathbb{F}_Q^n$. The parameters of a linear code are usually expressed as $[n,k,d]_Q$, where n is the length, k the dimension and d the minimum distance. The cardinality Q of the field $\mathbb{F}_Q$ refers to the number of digits used to represent information, the dimension is related to the information that can be encoded; and the minimum distance measures the capability to detect and correct errors.

Parameters of a linear code are constrainted by the Singleton bound: $k+d \leq n+1$, and codes reaching equality are called *maximum distance separable* (*MDS*) codes. It establishes a limit on the parameters independently of Q, and MDS codes are desirable in the sense that they achieve the best relation on them. However, the length of an MDS code seems to be bounded above by $Q+1$ (or $Q+2$ in some exceptional case) according to the MDS conjecture, posed by Segre in 1955 and only proved in some cases. We state it in Conjecture 1.2.12. Notice that with a high value of k we can encode more information, and $k \leq n$, so it could be desirable to have long codes. Taking into account that a big Q takes us to a bigger cost on the computations, in many occasions it is also interesting to construct long codes over small fields even though they are not MDS.

We are able to do that in two ways. One is by considering *subfield-subcodes* of long codes over big fields. Given a code $\mathcal{C} \subseteq \mathbb{F}_Q^n$ and a subfield $\mathbb{F}_{Q'}$ of $\mathbb{F}_Q$, the code $\mathcal{C}' = \mathcal{C} \cap \mathbb{F}_{Q'}^n$ is named the *subfield-subcode* of $\mathcal{C}$ over $\mathbb{F}_{Q'}$. This procedure turns to be a key tool to construct good codes.

The other way we mentioned comes from the use of *evaluation codes*. They are linear codes of the form $\mathcal{C}_V^P = \mathrm{ev}_P(V) \subseteq \mathbb{F}_Q^n$ defined as the image of a linear map

$$\mathrm{ev}_P : V \to \mathbb{F}_Q^n, \quad \mathrm{ev}_P(f) = (f(\alpha_1), \ldots, f(\alpha_n)),$$

called *evaluation map*, where $P = \{\alpha_1, \ldots, \alpha_n\}$ is a set of n distinct points of some set $\mathcal{X}$ and $V = \{f : \mathcal{X} \to \mathbb{F}_Q\}$ is a vector space of functions from $\mathcal{X}$ to the finite field $\mathbb{F}_Q$. Evaluation codes with a big set P and small Q provide long codes over small fields. Notice that both ways described in the last two paragraphs can also be applied in combination.

Monomial-Cartesian codes (MCCs) are a class of evaluation codes which constitutes our main tool in Chapters 3 and 4 of this work. Chapter 5 is also supported on a different class of evaluation codes.

MCCs were first introduced in [54] and, later in [93], they were named MCCs. In [93] the authors only use algebraic tools (see also [95]) but we prefer a more geometrical definition where we regard these codes as affine variety codes. *Affine variety codes* were introduced by Fitzgerald and Lax in [40] by evaluating elements in $\mathbb{F}_Q[X_1, \ldots, X_m]/I$, where I is an ideal of $\mathbb{F}_Q[X_1, \ldots, X_m]$, the ring of polynomials in m variables over $\mathbb{F}_Q$.

Then, in Definition 1.3.3 we introduce MCCs as evaluation codes obtained as the image of maps

$$\mathrm{ev}_P : V_\Delta \subset \mathbb{F}_Q[X_1, \dots, X_m] / I \to \mathbb{F}_Q^n, \quad \mathrm{ev}_P(f) = (f(\boldsymbol{\alpha}_1), \dots, f(\boldsymbol{\alpha}_n)),$$

where $m \geq 1$ is a positive integer, $P = P_1 \times \cdots \times P_m = \{\boldsymbol{\alpha}_1, \dots, \boldsymbol{\alpha}_n\}$ a Cartesian product of sets $P_j \subseteq \mathbb{F}_Q$, $1 \leq j \leq m$, I the vanishing ideal at P of $\mathbb{F}_Q[X_1, \dots, X_m]$ and

$$V_\Delta = \left\langle X_1^{e_1} \cdots X_m^{e_m} \mid (e_1, \dots, e_m) \in \Delta \right\rangle_{\mathbb{F}_Q}$$

the $\mathbb{F}_Q$-linear space generated by the classes of monomials with exponents in some subset Δ of tuples of exponents of monomials reduced modulo I.

Many evaluation codes evaluate univariate polynomials in some subset of $\mathbb{F}_Q$, for example Reed-Solomon codes, which requires a big field for having long codes. MCCs allow us to obtain codes as long as desired without increasing the cardinality Q of the field $\mathbb{F}_Q$, but only by increasing the number m of variables. MCCs have been considered for different applications, such as quantum codes, LRCs with availability and polar codes [93, 22]. Moreover the above evaluation map is also used in [25] to define codes with variable locality and availability.

The family of MCCs extends that of *J-affine variety codes*, previously introduced in [49]. Although the authors used that denomination, one must not confuse these codes with those satisfying the more general definition of affine variety code. J-affine variety codes are MCCs where the evaluation set P is a Cartesian product of multiplicative subgroups of $\mathbb{F}_Q$ to which we could also add the element $0 \in \mathbb{F}_Q$. The notation J refers to a subset $J \subseteq \{1, \dots, m\}$ used to detect the variables where $0 \in \mathbb{F}_Q$ is not evaluated. That is, denoting by $U_t \subseteq \mathbb{F}_Q$ the set of t-th roots of unity for some $t \mid Q-1$, $P_j = U_{n_j}$, for some $n_j \mid Q-1$, when $j \in J$, and $P_j = U_{n_j - 1} \cup \{0\}$, for some $n_j - 1 \mid Q - 1$, otherwise. J-affine variety codes can be thought as a generalization of cyclic codes to several variables. The possibility of introducing 0 increases the range of lengths, and the mentioned multiplicative structure eases the control of these codes. We will consider J-affine variety codes when applying techniques of subfield-subcodes since their structure is useful for that purpose.

The contents in this PhD thesis are distributed in six chapters which are gathered in four parts. Preliminaries constitute Part I, and are divided in two chapters, devoted to classical (Chapter 1) and quantum (Chapter 2) error-correcting codes. Because of the fact that an important family of QECCs can be constructed from classical codes, Chapter 1 contains most of the preliminar knowledge we need. In particular, it introduces evaluation codes, MCCs, LRCs and subfield-subcodes. Chapter 2 recalls the rules of quantum mechanics and the differences between quantum and classical codes. Parts II and III contain new constructions of LRCs (Chapter 3) and QECCs (Chapters 4 and 5), respectively. Finally we devote a last part (Part IV) to explain some ideas for future work.

The contents of the following papers (carried out with my advisors, B. Barbero-Lucas, G. McGuire and D. Ruano) are included, respectively, in Chapters 3 to 5 of this thesis. The notation has been adapted in order to facilitate understanding of the text, for example to homogenize it across different chapters. We have only added to these chapters Remark 3.2.4 and its proof in Chapter 3 and Example 4.2.8 in Chapter 4 for completeness.

[45] C. Galindo, F. Hernando, and H. Martín-Cruz. Optimal (r,δ)-LRCs from monomial-Cartesian codes and their subfield-subcodes. *Des. Codes Cryptogr.*, 2024. DOI 10.1007/s10623-024-01403-z.

[11] B. Barbero-Lucas, F. Hernando, H. Martín-Cruz, and G. McGuire. MDS, Hermitian almost MDS, and Gilbert–Varshamov quantum codes from generalized monomial-Cartesian codes. *Quantum Inf. Process.*, 23(86), 2024.

[46] C. Galindo, F. Hernando, H. Martín-Cruz, and D. Ruano. Stabilizer quantum codes defined by trace-depending polynomials. *Finite Fields Appl.*, 87:102138, 2023.

Next, we explain the context and the advances we have obtained with respect to the two problems addressed in this PhD thesis.

Locally recoverable codes were introduced in [55]. Specifically, an error-correcting code $\mathcal{C}$ is named an LRC *with locality* r whenever any coordinate c_i of any element $\boldsymbol{c} = (c_1,\ldots,c_n)$ in $\mathcal{C}$ can be recovered by accessing at most r other coordinates, whose positions constitute the so-called *recovery set*. The literature contains a good number of papers on this class of codes, some of them are [133, 86, 99, 92, 72, 87, 110]. A variation of Reed-Solomon codes was introduced in [122] for recovering purposes. In [13] these codes were extended to LRCs over algebraic curves. Among the different classes of codes considered as good candidates for local recovering, cyclic codes and subfield-subcodes of cyclic codes play an important role, this is because the cyclic shifts of a recovery set again provide recovery sets [29, 56, 68, 123]. In [100] the author introduces a model of locally recoverable code that also includes local error detection, increasing the security of the recovery system.

There is a Singleton-like bound for LRCs with locality r [55]. Denoting $[n,k,d]$ the parameters of an LRC, this inequality is $k+d+\left\lceil \frac{k}{r} \right\rceil \leq n+2$. Codes attaining this bound are named optimal r-LRCs and interesting constructions of this class of codes can be found in [122] and [124] (see also [12, 13, 102, 103, 110]). When considering codes over the finite field $\mathbb{F}_Q$, optimal r-LRCs can be obtained for all lengths $n \leq Q$ [130] and a challenging question is to study how long these codes can be [64].

The fact that simultaneous multiple device failures may happen leads us to the concept of LRC *with locality* (r,δ) (or (r,δ)-LRC), with r and $\delta \geq 2$ positive integers, meaning that any coordinate can be recovered from at most other $r+\delta-2$ coordinates but allowing that $\delta-2$ of them can also fail. This class of codes were introduced in [106],

see Definition 1.4.4, and they also admit a Singleton-like bound [106]:

$$k + d + \left(\left\lceil \frac{k}{r} \right\rceil - 1\right)(\delta - 1) \leq n + 1.$$

Codes attaining this bound are named *optimal* (r, δ)-LRCs. In this work and in this context, we call them simply *optimal* codes.

Optimal codes have been studied in [29, 81, 92, 121, 72, 27, 36, 108], mainly coming from cyclic and constacyclic codes. A somewhat different way for obtaining LRCs with locality (r, δ) was started in [47], where the supporting codes are J-affine variety codes. We are interested in optimal codes and the recent literature presents a number of results giving parameters of codes of this type [29, 121, 27, 129, 28, 36, 131, 132, 31, 90, 79]. The length of most of these codes is a multiple of $r + \delta - 1 \leq Q$ and, in this case, and for unbounded length and small size fields, their distances have restrictions being at most 3δ. Larger distances can be obtained when $Q^2 + Q$ is a bound for the length. One must use different constructions to get these optimal codes, and a large size of the supporting field seems to make easier to find optimal codes [117].

The goal of *Chapter 3 in this PhD thesis* is to obtain many *new optimal LRCs coming from MCCs*. As introduced above, they are vector subspaces generated by evaluating monomials in several variables, $\left\langle \mathrm{ev}_P(X_1^{e_1} \cdots X_m^{e_m}) \mid (e_1, \ldots, e_m) \in \Delta \right\rangle$, and the set Δ of exponents of their generators determines the dimension and a natural bound d_0 for the minimum distance (see Proposition 1.3.7 and Corollary 1.3.10). This bound is deduced of the so-called *footprint bound* [52, 51] which can be proved with techniques of the Gröbner basis theory [32].

The bound d_0 depends on the elements in Δ and we represent Δ in a grid because it helps us to compute d_0. The reader can see an example of this representation (in the bivariate case –$m = 2$–) in Figure 1.5. These representations are crucial in our searching for optimal codes. Codes which are optimal when using the bound d_0 for the minimum distance are named *d_0-optimal codes*. These codes are those attaining equality in both inequalities below:

$$k + d_0 + \left(\left\lceil \frac{k}{r} \right\rceil - 1\right)(\delta - 1) \leq k + d + \left(\left\lceil \frac{k}{r} \right\rceil - 1\right)(\delta - 1) \leq n + 1.$$

In our work, we introduce a recovery procedure based on interpolation which makes easy to obtain the values r and δ of some MCCs regarded as LRCs (Proposition 3.1.1). Supported on these facts, we provide a large family of optimal MCCs. Subsection 3.2.1 of this thesis studies bivariate codes and Subsection 3.2.2 multivariate ($m \geq 3$) codes. In fact, *codes given in Propositions 3.2.1, 3.2.2 and 3.2.3, 3.2.13 and 3.2.14 give the d_0-optimal LRCs one can get with this type of codes*. We remark that the lengths n of these optimal (r, δ)-LRCs are unbounded and divisible by $r + \delta - 1 \leq Q$.

The above five propositions *determine all the parameters of the d_0-optimal LRCs given by MCCs*, see Remarks 3.2.4 and 3.2.15. These parameters are grouped in Corollary 3.2.12 for the bivariate case and in Corollary 3.2.17 for the multivariate case. Thus,

one gets a *large family of optimal LRCs that can be constructed by a unique and simple procedure*. This family provides, on the one hand, the parameters of those LRCs over $\mathbb{F}_Q$ given in [28] whose lengths are of the form $N(r+\delta-1)$ where N can be written as a product of integers less than or equal to Q and, on the other hand, the parameters of those LRCs in [90] with length less than or equal to Q^2+Q. In addition, MCCs are related with and include the family of codes introduced in [3] whose evaluation map is the same as MCCs but their evaluation sets V_Δ are only a subset of ours. This makes that the sets Δ in [3] have specific shapes while ours can have arbitrary shapes and therefore we obtain many more optimal (r,δ)-LRCs (see Remark 3.2.19 for details).

The above codes do not give new parameters but subfield-subcodes of many subfamilies of them *do give*. Thus, *providing new families of optimal LRCs is our main goal in this chapter*. Indeed, in Section 3.3 we prove that, considering subfield-subcodes of suitable J-affine variety codes over subfields $\mathbb{F}_{Q'}$ of $\mathbb{F}_Q$, we get LRCs over $\mathbb{F}_{Q'}$ with the same parameters of certain MCCs over $\mathbb{F}_Q$ considered in Section 3.2, being then optimal. That way we obtain *optimal LRCs over smaller supporting fields which behave as MCCs and are new* because there is no code in the literature with the same parameters and locality. We have seen that our codes are new by comparing with the codes given in the references [29, 81, 92, 121, 72, 27, 129, 28, 36, 131, 132, 108, 31, 90, 79], which group the known optimal (r,δ)-LRCs whose lengths n are divisible by $r+\delta-1$. Moreover, our codes are Q'-ary such that $r+\delta-1$ equals either $Q'+1$ or $Q'+2$ and their length is a multiple of some of these values, so $r+\delta-1>Q'$.

Our results are quite technical, and at the beginning of Section 3.3, before Subsection 3.3.1, a more detailed explanation of these facts is given. Our choice of the above mentioned suitable J-affine variety codes is supported on the ideas exposed in such an explanation. *Propositions 3.3.4 and 3.3.6 for the bivariate case, and Propositions 3.3.11 and 3.3.12 for the multivariate case explain how to construct new optimal (r,δ)-LRCs following our strategy*. We give two results in each case because we construct two families of codes, the first one is for codes over any field and the second one is for characteristic two codes only. Lemmas 3.3.3 and 3.3.5 are important results in order to get the explicit values of r and δ from our recovery procedure (Proposition 3.1.1).

In sum, *the main results of Chapter 3 are Theorems 3.3.9, 3.3.10, 3.3.14 and 3.3.15*, that we state below as Theorems A, B, C and D, respectively. *Theorem 3.3.9 (respectively, 3.3.14) gives parameters of new optimal LRCs over any field coming from the bivariate (respectively, multivariate) case. Theorems 3.3.10 and 3.3.15 do their own but only for characteristic two fields*. Remarks 3.3.7 and 3.3.13 justify the novelty of our codes. Finally, in Examples 3.3.8 and Tables 3.1 and 3.2, one can find some numerical examples of new optimal LRCs over small fields.

Theorem A. *Let $\mathbb{F}_{p^l}$ be a finite field, p being a prime number and l a positive integer. Consider another positive integer h such that h divides l, $p^h \geq 4$ if $p=2$ ($p^h \geq 5$, otherwise) and assume $p^h+1 \mid p^l-1$. Consider also nonnegative integers z and t satisfying $0 \leq t < z \leq \left\lfloor \frac{p^h}{2} \right\rfloor - 1$, $2t \geq \max\{0, 4z-p^h-1\}$. Regard $\mathbb{F}_{p^h}$ as a subfield of $\mathbb{F}_{p^l}$.*

Then, there exists an optimal (r,δ)-LRC over $\mathbb{F}_{p^h}$ with the following parameters depending on two integer variables n' and a:

$$[n,k,d]_{p^h} = \left[(p^h+1)n', (n'-1)(2z+1)+2a+1, p^h+1-2a\right]_{p^h}$$

and

$$(r,\delta) = (2z+1, p^h-2z+1),$$

whenever some of the following conditions hold:

(1) $n' \mid p^l-1$ *and* $a=z$.

(2) $n'-1 \mid p^l-1$ *and* $a=z$.

(3) $n'-1 \mid p^l-1$, $a=t$ *and, if p is odd, either* $\gcd(n',p^h) \neq 1$ *or* $\gcd(n',p^h+1) \neq 1$.

Assume now that $p=2$ and consider a nonnegative integer u and, if $u \geq 1$, a nonnegative integer v, satisfying $0 \leq u \leq \frac{p^h}{2}-2$, $0 \leq v < u$ and $2v+1 \geq \max\{0, 4u+1-p^h\}$.

Then, there exists an optimal (r,δ)-LRC over $\mathbb{F}_{p^h}$ with the following parameters depending on two integer variables n' and a:

$$[n,k,d]_{p^h} = \left[(p^h+1)n', (n'-1)(2u+2)+2a+2, p^h-2a\right]_{p^h}$$

and

$$(r,\delta) = (2u+2, p^h-2u),$$

whenever some of the following conditions hold:

(1) $n' \mid p^l-1$ *and* $a=u$.

(2) $n'-1 \mid p^l-1$ *and* $a=u$.

(3) $n'-1 \mid p^l-1$ *and* $a=v$.

Theorem B. *Let $\mathbb{F}_{2^l}$ be a finite field, $l \geq 4$ being an even positive integer and $h=\frac{l}{2}$. Consider also a positive integer z satisfying $2 \leq z \leq 3$, $2^h-2z+1 \geq \max\{0, 2^h-6\}$. Regard $\mathbb{F}_{2^h}$ as a subfield of $\mathbb{F}_{2^l}$.*

Then, there exists an optimal (r,δ)-LRC over $\mathbb{F}_{2^h}$ with the following parameters depending on the integer variables n', a, b and c:

$$[n,k,d]_{2^h} = \left[(2^h+2)n', a(n'-1)+b, 2h+3-b\right]_{2^h}$$

and

$$(r,\delta) = (a,c),$$

whenever some of the following conditions hold:

(1) $n' \mid 2^l-1$ *and* $(a,b,c) = (3,3,2^h)$.

(2) $n'-1 \mid 2^l-1$ *and* $(a,b,c) = (3,3,2^h)$.

(3) $n' \mid 2^l - 1$ *and* $(a,b,c) = (2^h - 1, 2^h - 1, 4)$.

(4) $n' - 1 \mid 2^l - 1$ *and* $(a,b,c) = (2^h - 1, 2^h - 1, 4)$.

(5) $n' - 1 \mid 2^l - 1$ *and* $(a,b,c) = (2^h - 1, 2^h - 2z + 2, 4)$.

Finally, consider n' *and* j *positive integers such that* $j \leq n' - 1$ *and they satisfy some of the following conditions:*

(1) $n' \mid 2^h - 1$ *and* $j \geq \max\{1, n' - 2^{h-1}\}$.

(2) $n' - 1 \mid 2^h - 1$ *and* $\max\{1, n' - 2^{h-1}\} \leq j < n' - 1$.

(3) $n' - 1 \mid 2^l - 1$ *and* $j = n' - 1$.

Then, there exists an optimal (r,δ)*-LRC over* $\mathbb{F}_{2^h}$ *with parameters*

$$[n,k,d]_{2^h} = \left[(2^h+2)n', 3j+1, (2^h+2)(n'-j)\right]_{2^h}$$

and

$$(r,\delta) = (3, 2^h).$$

Theorem C. *Keep the same notation as in Theorem A. Consider also subsets* S_1, $S_2 \subseteq \{1, \ldots, m-1\}$ *such that* $S_1 \cup S_2 = \{1, \ldots, m-1\}$ *and* $S_1 \cap S_2 = \varnothing$.

Then, on the one hand, there exists an optimal (r,δ)*-LRC over* $\mathbb{F}_{p^h}$ *with the following parameters depending on the integer variables* $n_1, \ldots, n_{m-1}$ *and* a*:*

$$[n,k,d]_{p^h} = \left[(p^h+1)n_1 \cdots n_{m-1}, (2z+1)n_1 \cdots n_{m-1} - a, p^h + 1 - 2z + a\right]_{p^h}$$

and

$$(r,\delta) = (2z+1, p^h - 2z + 1),$$

whenever some of the following conditions hold:

(1) $n_j \mid p^l - 1$ *for all* $j \in S_1$, $n_j - 1 \mid p^l - 1$ *for all* $j \in S_2$ *and* $a = 0$.

(2) $S_1 = \varnothing$, $n_j - 1 \mid p^l - 1$ *for all* $j \in S_2$, $a = 2(z-t)$ *and, if* p *is odd, either* $\gcd\left(n_1 \cdots n_{m-1}, p^h\right) \neq 1$ *or* $\gcd\left(n_1 \cdots n_{m-1}, p^h + 1\right) \neq 1$.

On the other hand, there exists an optimal (r,δ)*-LRC over* $\mathbb{F}_{p^h}$ *with parameters*

$$[n,k,d]_{p^h} = \left[(p^h+1)n_1 \cdots n_{m-1}, (2u+2)n_1 \cdots n_{m-1} - a, p^h - 2u + a\right]_{p^h}$$

and

$$(r,\delta) = (2u+2, p^h - 2u),$$

whenever some of the following conditions hold:

(1) $n_j \mid p^l - 1$ *for all* $j \in S_1$, $n_j - 1 \mid p^l - 1$ *for all* $j \in S_2$ *and* $a = 0$.

(2) $S_1 = \varnothing$, $n_j - 1 \mid p^l - 1$ *for all* $j \in S_2$ *and* $a = 2(u-v)$.

Theorem D. *Keep the same notation as in Theorem B. Consider also subsets* S_1, $S_2 \subseteq \{1,\dots,m-1\}$ *such that* $S_1 \cup S_2 = \{1,\dots,m-1\}$ *and* $S_1 \cap S_2 = \varnothing$.

Then, there exists an optimal (r,δ)*-LRC over* $\mathbb{F}_{2^h}$ *with the following parameters depending on the integer variables* $n_1,\dots,n_{m-1}$, a, b *and* c:

$$[n,k,d]_{2^h} = \left[(2^h+2)n_1\cdots n_{m-1}, an_1\cdots n_{m-1} - b, c+b\right]_{2^h}$$

and

$$(r,\delta) = (a,c),$$

whenever some of the following conditions hold:

(1) $n_j \mid 2^l - 1$ *for all* $j \in S_1$, $n_j - 1 \mid 2^l - 1$ *for all* $j \in S_2$ *and* $(a,b,c) = (3,0,2^h)$.

(2) $n_j \mid 2^l - 1$ *for all* $j \in S_1$, $n_j - 1 \mid 2^l - 1$ *for all* $j \in S_2$ *and* $(a,b,c) = (2^h-1,0,4)$.

(3) $S_1 = \varnothing$, $n_j - 1 \mid 2^l - 1$ *for all* $j \in S_2$ *and* $(a,b,c) = (3,2,2^h)$.

(4) $S_1 = \varnothing$, $n_j - 1 \mid 2^l - 1$ *for all* $j \in S_2$ *and* $(a,b,c) = (2^h-1,2z-3,4)$.

At the beginning of this introduction, we said that this PhD thesis is concerned with two problems. We have explained our achievements in the field of LRCs. *Chapters 4 and 5* deal with our second problem which is the construction of good QECCs. In the quantum setting, unlike the classical one, a unit of information can be simultaneously in several different states. For example, in the classical binary case a bit is either in state 0 or 1, but in the quantum case the *qubit* can be in a superposition of those states, a linear combination of 0 and 1 with complex coefficients. Specifically, a qubit is represented as a unit vector in the Hilbert space $\mathbb{C}^2$, where $\mathbb{C}$ denotes the complex field, for which we consider an orthonormal basis given by the vectors representing 0 and 1. Overall, we require to normalize the linear combination providing the qubits in order to set the probability of being in each state. In the general case, units of quantum information (*qudits*) are represented by unit vectors in r-dimensional Hilbert spaces $\mathbb{C}^r$.

Denoting again by Q a prime power and n a positive integer, a QECC of length n is a linear subspace $\mathcal{Q}$ of $\mathbb{C}^{Q^n} = \mathbb{C}^Q \otimes \overset{n)}{\cdots} \otimes \mathbb{C}^Q$, where $\otimes$ denotes the tensor product. Here $r = Q$ to take advantage of the structure of finite fields, so that elements in $\mathbb{F}_Q$ represent a basis of $\mathbb{C}^Q$. QECCs work focusing more on the errors that may occur than on the proper state vectors. It is convenient to perform this procedure because of the delicate nature of qudits. The set of errors is denoted by $\mathcal{G}_n$ and they are described by endomorphisms of the Hilbert space $\mathbb{C}^{Q^n}$. They have group structure generated by a finite set which is a so-called *nice error basis*. *Chapter 2* gives a quick introduction to QECCs and their relation to classical error-correcting codes.

In this thesis we consider Q^k-dimensional QECCs and their parameters are written $[[n,k,d]]_Q$. Their minimum distance d, as in the classical setting, measures the capability to detect and correct errors. Seminal papers on quantum error-correcting codes studied binary codes [19, 20, 57] (see also [4, 5, 63]). Later non-binary codes were also considered

[6, 73]; these last codes are particularly interesting in fault-tolerant computation [115, 76, 107, 59, 120, 21, 91]. The literature on quantum error-correcting codes is very extensive (some references are [16, 98, 80, 41, 23, 116]). Many of the known quantum error-correcting codes are *stabilizer* quantum codes, defined by Gottesman [57]. They are constructed thinking on the errors that are more likely. Thus the code contains those inaltered elements under the action of these errors. This makes sense because in the quantum setting there exist nontrivial errors that may have no effect on an encoded state. More concretely, a stabilizer code $\mathcal{Q} \neq \{0\}$ is an intersection of eigenspaces of the space $\mathbb{C}^{Q^n}$ (with respect to the eigenvalue 1) running over the elements of an abelian subgroup of the error group $\mathcal{G}_n$, see Definition 2.3.1.

Stabilizer quantum error-correcting codes have as a main advantage that they can be constructed from (classical) additive codes included in $\mathbb{F}_Q^{2n}$ which are self-orthogonal with respect to a trace symplectic form. This follows from the structure of the nice error basis. It is related with two types of errors, so that errors in $\mathcal{G}_n$ may be represented as vectors in $\mathbb{F}_Q^{2n}$ up to a scalar complex. These vectors have an even number of coordinates and can be divided into two halves each of them corresponding to a type of the mentioned errors, see Subsections 2.2.2 and 2.3.1 for details. As a particular case of the above construction, stabilizer codes can be obtained from Hermitian self-orthogonal linear codes over $\mathbb{F}_{Q^2}$, see Subsection 2.3.3. In this work, we mainly utilize this construction that will be stated in our forthcoming Corollary 2.3.8. For convenience, the next Corollary A recalls it.

Corollary A. Let $\mathcal{C}$ be an $[n,k]$ linear code over $\mathbb{F}_{Q^2}$ such that $\mathcal{C} \subseteq \mathcal{C}^{\perp_h}$, $\mathcal{C}^{\perp_h}$ denoting the Hermitian dual code of $\mathcal{C}$. Denote by $d^{\perp_h}$ the minimum distance of $\mathcal{C}^{\perp_h}$. Then, there exists an $[[n, n-2k, \geq d^{\perp_h}]]_Q$ stabilizer code.

There is a quantum version of the Singleton bound. Being $[[n,k,d]]_Q$ the parameters of a QECC, the quantum Singleton bound is:

$$n \geq k + 2(d-1).$$

Similarly to the classical setting, QECCs that achieve the above bound are named *quantum MDS* codes. One can find many papers on this class of codes (see [35, 9, 85] to cite only some articles from the last years). By applying the classical MDS conjecture to the classical codes over $\mathbb{F}_{Q^2}$ giving rise to stabilizer codes, the *quantum MDS conjecture* says, in this context, that the length of a Q-ary quantum MDS *stabilizer* code is at most Q^2+1 (or Q^2+2 in some exceptional case). We state it in Conjecture 2.3.10. Again as explained in the classical setting, it is interesting to obtain long Q-ary stabilizer codes with good parameters. J-affine variety codes have a good behavior for this purpose [43, 49, 41].

Chapters 4 and 5 in this thesis offer advances both in the search of MDS or almost MDS quantum codes and of good long quantum codes.

Chapter 4 uses Q^2-ary MCCs but makes a "twist" to the evaluation map ev_P, i.e. it multiplies each coordinate of $\mathrm{ev}_P(f)$ by some nonzero element in $\mathbb{F}_{Q^2}$, arising the so-called *twist vector* $\boldsymbol{v} = (v_1, \ldots, v_n) \in (\mathbb{F}_{Q^2}^*)^n$ and the resulting evaluation map:

$$\mathrm{ev}_{\boldsymbol{v},P}: V_\Delta \subset \mathbb{F}_{Q^2}[X_1, \ldots, X_m] \big/ I \to \mathbb{F}_{Q^2}^n, \qquad \mathrm{ev}_{\boldsymbol{v},P}(f) = (v_1 f(\boldsymbol{\alpha}_1), \ldots, v_n f(\boldsymbol{\alpha}_n)).$$

In the literature, constructions of this type are usually said to be *twisted* or *generalized*. Constructions of quantum codes from generalized Reed-Solomon codes are very common because some twists allow us to obtain a wider range of dimensions for Hermitian self-orthogonal codes than in the case of ordinary Reed-Solomon codes. Our twisted constructions of MCCs pursue the same goal and we find *QECCs with wider range of dimensions than those previously obtained with J-affine variety codes*. They also achieve our goal of obtaining long codes. However, an arbitrary set P cannot be considered, but P_1 must be the set of $\lambda(Q+1)$-th roots of unity $U_{\lambda(Q+1)}$, where $\lambda \mid Q-1$, and $P_2, \ldots, P_m \subseteq \mathbb{F}_{Q^2}^*$, see Definition 4.1.1. With this structure, although our definition is slightly different, we introduce what we name *generalized monomial-Cartesian codes*, which are obtained as the image of the above map $\mathrm{ev}_{\boldsymbol{v},P}$, see Definition 4.1.1 and Remark 4.1.2. Notice that they are a type of generalized affine variety code.

We use generalized monomial-Cartesian codes to construct Hermitian self-orthogonal classical linear codes, and thereby to get stabilizer quantum codes. Comparing our codes with codes in [30, 48, 88, 77, 23, 127, 15, 78, 126], we present evidence which shows their good quality as quantum codes. Previous works using twisted codes, [126] for example, have proved the existence of a twist vector with the required properties for the code to be self-orthogonal, whereas an interesting feature of our construction is that we define the twist vector *explicitly*, see Equation (4.2.1). Moreover in Remark 4.2.2 we show that our construction gives rise to some Hermitian self-orthogonal twisted J-affine variety codes that would not be self-orthogonal without making the twist. In addition, contrary to usual, our twist makes the evaluation of any monomial to be orthogonal to all but one evaluation of another monomial, what allows the self-orthogonality conditions and control of the dimension to be more manageable.

Our construction is presented in Section 4.2 and it follows from the Hermitian self-orthogonality conditions stated in Proposition 4.2.1. Its proof shows that the choice of our twist vector is essential for our development and fundamentally depends on the first variable.

Firstly we present *a general construction (Theorem 4.2.4)*, stated for convenience of the reader in the below Theorem E. This construction does not give an explicit bound for the minimum distance of the obtained stabilizer code, but it ensures the minimum distance is bounded below by that of the Euclidean dual code of the corresponding MCC considered (not twisted). Thus, we can provide a bound from our above bound for MCCs.

Theorem E. *Let Q be an odd prime power and let $m \geq 1$, $\lambda \mid Q-1$, $n_1 := \lambda(Q+1)$ and $2 \leq n_j \leq Q^2-1$, $j = 2, \ldots, m$, be positive integers. Let $n := n_1 \cdots n_m$. Consider the twist vector $\boldsymbol{v}$ defined in Equality (4.2.1) and the set E_0 introduced in Definition 4.2.3. Let Δ be a subset of E_0. Then, the code $\mathcal{C}_{\boldsymbol{v},\Delta} = \mathrm{ev}_{\boldsymbol{v},P}(V_\Delta)$ satisfies*

$$\mathcal{C}_{\boldsymbol{v},\Delta} \subseteq (\mathcal{C}_{\boldsymbol{v},\Delta})^{\perp_h}.$$

Therefore, there exists a stabilizer quantum code with parameters

$$[[n, n-2\#\Delta, \geq d]]_Q$$

where # means cardinality and d denotes the minimum distance of the Euclidean dual code $(\mathcal{C}_{\mathbf{1},\Delta})^{\perp_e}$ *of* $\mathcal{C}_{\mathbf{1},\Delta}$*, being* $\mathbf{1} = (1,\dots,1) \in \mathbb{F}_{Q^2}^n$.

Then, we present *a more specific construction* based on hyperbolic codes [53]. It *allows us to control the minimum distance and maximize the dimension of the resulting quantum code (Theorem 4.2.7).* It is also stated in Theorem F below. Example 4.2.8 illustrates an intuitive strategy to obtain the statement of Theorem 4.2.7.

Theorem F. *Keep the same notation as in Theorem E. Let* t *be a positive integer such that*

$$2 \le t \le \frac{Q+3}{2}$$

and consider the set Δ_t *introduced in Definition 4.2.5. Then,* $\mathcal{C}_{\boldsymbol{v},\Delta_t} \subseteq (\mathcal{C}_{\boldsymbol{v},\Delta_t})^{\perp_h}$ *and therefore there exists a stabilizer quantum code with parameters*

$$[[n, n - 2\#\Delta_t, \ge t]]_Q.$$

A remarkable fact is that our construction with $m = 1$ gives *quantum MDS codes*, we show it in Section 4.3. We also prove that when $m = 2$ and our lower bound for the minimum distance is 3, the codes are *at least Hermitian almost MDS*. This concept means that the parameters do not reach the quantum Singleton bound but are the closest we can get with Hermitian duality to this bound. Section 4.4 gives a new evidence that *many of our codes are good*, since we prove that infinitely many of them –in the case $m = 2$– beat the quantum Gilbert-Varshamov bound [39], this last bound is recalled in Theorem 2.3.11. Finally, Tables 4.3 to 4.7 of Chapter 4 present some examples with small parameters that *beat the best known codes in the literature*.

Long Q-ary stabilizer codes with good parameters can also be obtained from evaluation codes and their subfield-subcodes [49, 41, 50]. The previous references consider large fields, $\mathbb{F}_{Q^{2\mu}}$, μ a positive integer, and evaluate adequate vector spaces of polynomials with coefficients in $\mathbb{F}_{Q^{2\mu}}$ at suitable roots of the unity where, in addition, one may or may not evaluate at zero, that is, those references use J-affine variety codes. However, in [50], the authors discovered that evaluating at the set formed by the roots (and also, at the set of non-roots) of the *trace polynomial* $\mathrm{tr}_{2\mu}(X) = X + X^Q + \cdots + X^{Q^{2\mu-1}}$, one gets excellent Q-ary quantum codes, both binary and non-binary.

Motivated by the fact that evaluating at the zeros of the trace polynomial produces codes with good behavior, in Chapter 5 we consider trace-depending polynomials, instead of $\mathrm{tr}_{2\mu}(X)$. Our goal is to get stabilizer quantum codes with new lengths and good parameters. For us, a trace-depending polynomial is a polynomial of the form $\gamma + \mathrm{tr}_{2\mu}(h(X))$, where $\gamma \in \mathbb{F}_{Q^{2\mu}}$ and $h(X) \in \mathbb{F}_{Q^{2\mu}}[X]$. The benefits of this new procedure are showed at the end of the chapter, in Section 5.4, where *we introduce several trace-depending polynomials* such that evaluating at their roots gives rise to *a considerable number of binary quantum records according to* [62], see Table 5.13. For us, a (code) record means a binary quantum code such that either its parameters are better than those of a code in [62] or match with a missing entry in [62]. These codes are

stabilizer and we are able to determine their dimensions and minimum distances, but we need to use the computational algebra system Magma [17] for checking the Hermitian self-orthogonality of the involved linear codes.

As a consequence, it is undoubtedly interesting to do a theoretical analysis of the family of quantum codes obtained by evaluating at the zeros of trace-depending polynomials. That is, to give conditions guaranteeing self-orthogonality for the constituent linear codes and compute their parameters. Notice that the length of the codes given in [50] is $Q^{2\mu-1}$ since $\mathrm{tr}_{2\mu}(X)$ completely factorizes in the field $\mathbb{F}_{Q^{2\mu}}$, but these new quantum codes have a wider range of lengths. A global study seems untractable because the behavior of the trace-depending polynomials is unknown.

In Chapter 5, *we restrict ourselves to a specific family of trace-depending polynomials and perform a complete study of the stabilizer quantum codes supported on that family.* This family is formed by the so-called b-th trace-depending polynomials, $\mathrm{Tr}_b(X)$, where $b = b(t) = 1 + Q^t$, $0 < t \leq \mu$ (see Definition 5.1.1). We define the polynomial $\mathrm{Tr}_b(X)$ as the representative with minimum degree of the class of the following polynomial $P_b(X)$ in the quotient ring $\mathbb{F}_{Q^{2\mu}}[X]/\langle X^{Q^{2\mu}-1} - 1\rangle$:

$$P_b(X) := \begin{cases} 1 + \mathrm{tr}_{2\mu}(X^b) & \text{if } 0 < t < \mu, \\ 1 + \mathrm{tr}_{\mu}(X^b) & \text{otherwise } (t = \mu), \end{cases}$$

being $\mathrm{tr}_\mu(X) := X + X^Q + X^{Q^2} + \cdots + X^{Q^{\mu-1}}$. Then, the linear codes we look for being Hermitian self-orthogonal are $\mathbb{F}_{Q^{2\mu}}$-ary evaluation codes where P is the set of roots of $\mathrm{Tr}_b(X)$ in $\mathbb{F}_{Q^{2\mu}}$ and $V = \langle X^e \mid e \in \Delta\rangle$ for some set $\Delta \subseteq \{0, 1, \ldots, n-1\}$, being n the cardinality of P. Note that, in order to apply our forthcoming Lemma 5.1.8, we consider only polynomials $\mathrm{Tr}_b(X)$ which completely factorize in $\mathbb{F}_{Q^{2\mu}}$. Proposition 5.1.6 gives a full description of the polynomials $\mathrm{Tr}_b(X)$, and Theorem 5.1.9 determines when the sum of the i-th powers, $1 \leq i \leq \deg \mathrm{Tr}_b(X)$, of the roots of $\mathrm{Tr}_b(X)$ vanishes, which is a crucial fact for determining the self-orthogonality of the constituent linear codes. This last property is studied in *Theorem 5.1.14 giving rise to Q^μ-ary stabilizer quantum codes* (see Corollary 5.1.15, also stated in the next Corollary B). All these results are presented in Section 5.1.

Corollary B. *Keep the above notation and assume that (Q, μ, b) is a triple such that the polynomial $\mathrm{Tr}_b(X)$ completely factorizes in $\mathbb{F}_{Q^{2\mu}}$. Then there exists an integer $A(Q,t)$ (defined in the statement of Theorem 5.1.14) such that for each non-negative integer $\tau \leq A(Q,t)$, there is a stabilizer quantum code with parameters*

$$[[Q^{2\mu-1-t} + Q^{2\mu-1}, Q^{2\mu-1-t} + Q^{2\mu-1} - 2\tau - 2, \geq \tau + 2]]_{Q^\mu}.$$

With the above ingredients and using subfield-subcodes, in Section 5.2 we *determine parameters of $Q^{\mu'}$-ary stabilizer quantum error-correcting codes, where μ' divides μ* (see *Theorem 5.2.3*). We also state this theorem in the below Theorem G. One can also obtain quantum codes by successively using Theorem 5.1.14 and *Theorem 5.3.1* or Theorems 5.2.3 and 5.3.1. In this way, we get many new good codes. These codes enlarge the

constellation of lengths of the quantum error-correcting codes obtained by evaluating at the zeros of the trace polynomial [50].

Theorem G. *Keep the above notation and assume that* $(Q,\mu,b) \neq (2,2,3)$ *is a triple such that the polynomial* $\mathrm{Tr}_b(X)$ *completely factorizes in* $\mathbb{F}_{Q^{2\mu}}$. *Fix a positive integer* $\mu' < \mu$ *such that* μ' *divides* μ *and regard* $\mathbb{F}_{Q^{2\mu'}}$ *as a subfield of* $\mathbb{F}_{Q^{2\mu}}$. *Consider the set* $\mathcal{A} := \{a_0 < a_1 < \cdots < a_\nu\}$ *introduced at the beginning of Section 5.2 and the values* $A(Q,t)$, $B(Q,t)$, $B^1(Q,t)$ *and* $C(Q,t)$ *introduced in Theorems 5.1.14 and 5.2.3. Define* $D(Q,t)$ *as follows:*

- *When* $t > 1$,
  - $D(Q,t) := A(Q,t)$, *whenever* $\mu' \neq 1$.
  - *Otherwise* ($\mu' = 1$)*:*

$$D(Q,t) := \begin{cases} B(Q,t) & \text{if } \mu \text{ is even,} \\ \min\{A(Q,t), B(Q,t)\} & \text{otherwise.} \end{cases}$$

- *When* $t = 1$ *and* $\mu \neq 2$,
  - $D(Q,t) := A(Q,t)$, *whenever* $\mu' > 2$,
  - $D(Q,t) := C(Q,t)$, *whenever* $\mu' = 2$,
  - $D(Q,t) := B^1(Q,t)$, *otherwise* ($\mu' = 1$).
- *When* $t = 1$ *and* $\mu = 2$, $D(Q,t) := Q - 2$.

Then, for each element $a_\tau \in \mathcal{A}$ *such that* $a_\tau \leq D(Q,t)$, *there exists an Hermitian self-orthogonal code over* $\mathbb{F}_{Q^{2\mu'}}$ *whose dimension is bounded above by the value* $\sum_{\ell=0}^{\tau} \#\Lambda_{a_\ell}$ *(see the beginning of Section 5.2 and Proposition 5.2.2 for details). As a consequence, there exists a stabilizer quantum code with parameters*

$$\left[\left[Q^{2\mu-1-t} + Q^{2\mu-1}, \geq Q^{2\mu-1-t} + Q^{2\mu-1} - 2\sum_{\ell=0}^{\tau} \#\Lambda_{a_\ell}, \geq a_{\tau+1} + 1 \right]\right]_{Q^{\mu'}}.$$

Subsections 5.3.1 and 5.3.2 supply quantum codes constructed with our theoretical results, some good examples are either along the text or in Tables 5.9 to 5.12. In Subsection 5.3.1, we prove that *our development gives rise to new and good binary quantum codes, some of them being records according to* [62]. In Subsection 5.3.2 we provide *new non-binary quantum error-correcting codes, some of them improving the parameters of the codes available in the literature.* All the given codes have parameters exceeding the quantum Gilbert-Varshamov bound.

To conclude, Part IV provides some ideas for future research. We give a construction and a brief explanation of our ideas to obtain *new* stabilizer quantum codes from Hermitian self-orthogonal linear codes and the techniques to get subfield-subcodes. We aim for the lengths of the Hermitian self-orthogonal linear codes we construct not to be

obtainable with univariate {1}-affine variety codes (BCH codes). These last codes are used in [41] with the same objective. Thus, we want to enlarge the range of dimensions of the Hermitian self-orthogonal {1}-affine variety codes given in [41]. Our computations show substantial advances in this sense and the expected quantum codes will have very good parameters.

We end this introduction by noticing that we consider the unusual notation Q for a prime power here and in Part I, setting the symbol q to be used in every particular construction. Indeed, in each chapter of Parts II and III such a Q corresponds to some power of another prime power q.

Part I

Preliminaries

The first part of this PhD thesis introduces the basic objects and some results that we will use later. It is divided into two chapters devoted to classical (Chapter 1) and quantum (Chapter 2) error-correcting codes. All quantum error-correcting codes we provide in Part III are constructed from classical error-correcting codes. Thus, in Chapter 1, we fix notation, present the framework and provide the basic tools of this work. Only a few results are essential for constructing quantum error-correcting codes from classical codes. However, for the sake of completeness, we give an introduction to quantum error-correcting codes. We hope it will help the reader understand better the difference between classical and quantum codes.

Let us give some basic notation: $\#S$ denotes the cardinality of some set S. When S lives in a commutative ring (respectively, vector space), $\langle S \rangle$ means ideal (respectively, vector subspace) generated by S. For vector spaces, sometimes we also write a subindex to specify the scalar field. The dimension of a vector space V is denoted $\dim(V)$. The kernel and the image of a linear map f are denoted, respectively, $\mathrm{Ker}(f)$ and $\mathrm{Im}(f)$. Let $\mathbb{N}$, $\mathbb{N}_0$, $\mathbb{Z}$, $\mathbb{C}$ stand, respectively, for the set of positive integers, the set of nonnegative integers, the ring of integers and the complex field. Let $n > 1$ be a positive integer and $(G, \cdot)$ be a grupoid. The $*$-product in G^n is defined as

$$* : G^n \times G^n \to G^n, \quad (a_1, \ldots, a_n) * (b_1, \ldots, b_n) = (a_1 \cdot b_1, \ldots, a_n \cdot b_n).$$

Given integers e, e', n, the fact that e is congruent with e' modulo n is denoted $e \equiv e' \mod n$. Lastly, $\deg(f)$ stands for the degree of a univariate polynomial f.

Chapter 1

Classical error-correcting codes

In this first chapter, we take a brief tour of some topics on error-correcting codes. We focus on concepts and results we will use along this thesis. Section 1.1 succinctly introduces error-correcting codes. The essentials on linear codes are explained in Section 1.2, while Section 1.3 defines evaluation codes and introduces an interesting subfamily, called monomial-Cartesian codes, which we will use in this thesis. Locally recoverable codes are defined in Section 1.4. Here, we give some results that will be needed in Part II where monomial-Cartesian codes are used to get good locally recoverable codes. Finally, in Section 1.5 subfield-subcodes of a code are recalled. They allow us to obtain good codes from other codes by reducing their supporting field. Useful results can be obtained from subfield-subcodes of J-affine variety codes, a class of monomial-Cartesian codes whose structure eases their management.

The main references for Sections 1.1 and 1.2 are [96, 71, 70, 101], [101, 49, 93, 51, 41, 22] for Section 1.3, [55, 106, 47] for Section 1.4 and [71, 33, 49, 41] for Section 1.5.

1.1. Encoding of information. Error-correcting codes

In this section, we give a brief introduction to the digital information broadcasting processes and error-correcting codes. We will use the term *information* to refer to digital information.

Information is usually broadcasted through a channel after a previous encoding procedure. It is expressed as a sequence of symbols of a finite set named *alphabet*. When received, the information is decoded with the aim of recovering the original pre-encoded message. There are two main reasons for encoding information. First, because it should previously be adapted to the characteristics of the channel. Secondly, because it is useful for the broadcasting to be the fastest, safest and the most reliable possible. These goals are reached with three types of codes (see Definition 1.1.1):

- *Compressing* codes – to compress the information,
- *Cryptographic* codes – to guarantee the information privacy against third parties, and

- *Error-correcting* codes – to detect and correct the possible errors due to the channel, machinery used or other phenomena.

Let us recall some basic terminology. An *alphabet* is a finite set containing the symbols used to represent the information, tipically a field or a ring. A *word* $\boldsymbol{w}$ over the alphabet $\mathcal{A}$ is a finite sequence of elements of $\mathcal{A}$:

$$\boldsymbol{w} = w_1 \cdots w_n = (w_1, \ldots, w_n) \in \mathcal{A}^n, \quad n \in \mathbb{N}.$$

Each value w_i, $i = 1, \ldots, n$, is named the i-th *coordinate* of $\boldsymbol{w}$ or its coordinate at the *position* i. The number n of symbols of $\boldsymbol{w}$ is called its *length*. Let us denote by $W(\mathcal{A})$ the set of words over $\mathcal{A}$.

Notice that information may be originally expressed over an alphabet which is not adapted to the characteristics of the channel and then a change of alphabet is needed. *Encoding* an alphabet $\mathcal{A}_1$ to another alphabet $\mathcal{A}_2$ is to provide an injective map

$$f : \mathcal{A}_1 \to W(\mathcal{A}_2).$$

Then, words over $\mathcal{A}_1$ are *encoded* to words over $\mathcal{A}_2$ by the map f' that applies f in every symbol:

$$f' : W(\mathcal{A}_1) \to W(\mathcal{A}_2), \quad f'(w_1, \ldots, w_n) = (f(w_1), \ldots, f(w_n)).$$

Definition 1.1.1. A *code* $\mathcal{C}$ over (the alphabet) $\mathcal{A}$ is a subset $\mathcal{C} \subseteq W(\mathcal{A})$.

Every word $\boldsymbol{c} \in \mathcal{C}$ is called a *codeword*. One can distinguish between two types of codes depending on the length of their codewords. A *block code* of length n is a code where all the codewords have the same length n. Otherwise, it is called a *variable-length code*. For example, compressing codes are variable-length such that they encode frequent symbols to short codewords.

A block code $\mathcal{C}$ of length n over an alphabet $\mathcal{A}$ with Q symbols has at most Q^n codewords. Then, a block code over $\mathcal{A}$ with m codewords has length at least $\lceil \log_Q(m) \rceil$. One can consider that $\lceil \log_Q(m) \rceil$ of the n symbols of a codeword contain the information and the remaining ones are redundant symbols. Thus, any block code of length n with m codewords over an alphabet with Q symbols has an *information rate* of $\frac{\log_Q(m)}{n}$ and a *redundancy* of $n - \log_Q(m)$.

We are only interested in block codes, which are suitable to detection and correction of errors. They are named error-correcting codes, in the sequel simply *codes*. They are based on redundant information inclusion (control symbols) that allows us to detect and eventually correct the corrupted part during broadcasting. Indeed, assume that the information to send is a word $\boldsymbol{w} \in W(\mathcal{A})$ that is divided into blocks of words of length k:

$$\boldsymbol{w} = \boldsymbol{w}_1 \cdots \boldsymbol{w}_l, \quad \boldsymbol{w}_i \in \mathcal{A}^k, \quad i = 1, \ldots, l.$$

Considering the blocks on $\mathcal{A}^k$, we add to each block $\boldsymbol{x} \in \mathcal{A}^k$ redundancy, encoding it and giving rise to a codeword of a (error-correcting) code $\mathcal{C}$ of length n. $\mathcal{C}$ is the image of an injective map

$$g : \mathcal{A}^k \to \mathcal{A}^n.$$

Notice that the information rate of $\mathcal{C}$ is $\frac{k}{n}$ and it has redundancy $n-k$.

Figure 1.1 shows a scheme where the channel suffers from interferences, commonly called *noise*. In such scheme, each block $\boldsymbol{x} \in \mathcal{A}^k$ is encoded to a codeword $\boldsymbol{c} = g(\boldsymbol{x}) \in \mathcal{C}$ that is sent over the channel. Noise may corrupt $\boldsymbol{c}$ producing an error $\boldsymbol{e} \in \mathcal{A}^n$ so that the output of the channel is a word $\boldsymbol{y} = \boldsymbol{c} + \boldsymbol{e} \in \mathcal{A}^n$. Then a process, named decodification, to try to remove the error from the received word $\boldsymbol{y}$ is made. It gives an estimated sent codeword $\widehat{\boldsymbol{c}} \in \mathcal{C}$. Since there is a bijection between codewords and messages, $\widehat{\boldsymbol{c}}$ gives rise to the estimated sent message $\widehat{\boldsymbol{x}} \in \mathcal{A}^k$. Whenever the error is not very high for the error-correcting capability of $\mathcal{C}$, it holds that $\widehat{\boldsymbol{c}} = \boldsymbol{c}$, and therefore $\widehat{\boldsymbol{x}} = \boldsymbol{x}$.

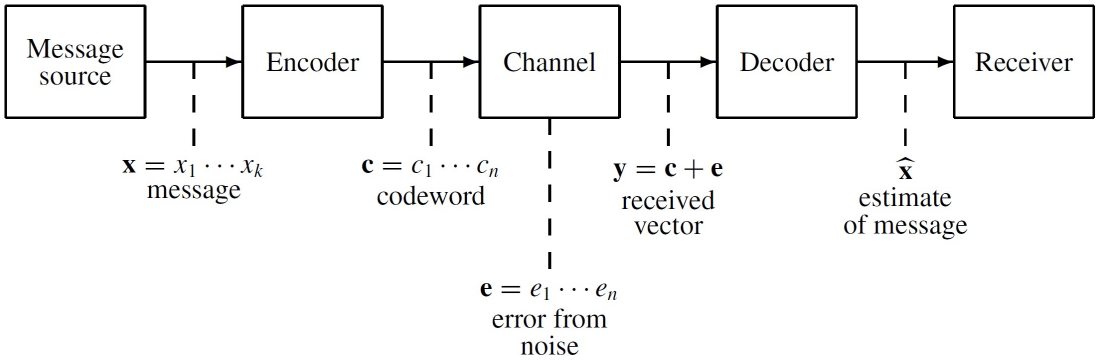


Figure 1.1: Information broadcasting scheme on a noisy channel [71]

Although the corrupted information can be of two types, we generally refer to them as errors, but it is convenient to distinguish between

- *Erasures* – unreadable symbols; or
- *Errors* – different symbols from the original ones.

Notice that erasures are detectable by the receptor but errors cannot be distinguished from well-broadcasted symbols. Because of this, erasures are usually thought as errors whose position is known.

It is desirable that a code corrects as many errors as possible with a high information rate, that is, by introducing the least amount of redundancy as possible. These two requirements are contradictory and one has to settle with a certain balance between them. We will explain this fact in Subsection 1.2.2 for a class of codes named linear codes. Concerning error-correction, it is desirable that codewords are as different as possible so that noise unlikely converts a codeword into another. The following concept measures the difference among words.

Definition 1.1.2. Let $\mathcal{A}$ be an alphabet and n be a positive integer. Given two words $\boldsymbol{w} = (w_1, \ldots, w_n)$, $\boldsymbol{w}' = (w'_1, \ldots, w'_n) \in \mathcal{A}^n$, the *Hamming distance* between $\boldsymbol{w}$ and $\boldsymbol{w}'$ is

$$\mathrm{d}(\boldsymbol{w}, \boldsymbol{w}') := \#\{i \mid 1 \leq i \leq n,\, w_i \neq w'_i\}.$$

The map d above defined gives rise to a metric on $\mathcal{A}^n$ which allows us to decode following the minimum distance principle. In this way, when a word is received, one

looks for a nearest one in terms of the Hamming distance. Schemes where one has a unique choice at minimum distance are preferred.

Definition 1.1.3. Let $\mathcal{C}$ be a code. Its *minimum distance* is defined as

$$d := \mathrm{d}(\mathcal{C}) := \min\left\{\mathrm{d}(\boldsymbol{c}, \boldsymbol{c}'),\, \boldsymbol{c}, \boldsymbol{c}' \in \mathcal{C},\, \boldsymbol{c} \neq \boldsymbol{c}'\right\}.$$

The next proposition formalizes the detection/correction procedure suggested in the above paragraph.

Proposition 1.1.4. *A code $\mathcal{C}$ with minimum distance d is able to detect $d-1$ errors and correct $\left\lfloor \frac{d-1}{2} \right\rfloor$ errors (respectively, $d-1$ erasures).*

Proof. Assume that $\boldsymbol{c} \in \mathcal{C} \subseteq \mathcal{A}^n$ is the sent codeword and $\boldsymbol{y} \in \mathcal{A}^n$ is the received word, containing $0 \leq t < d$ errors. When $t > 0$, then $\boldsymbol{y} \notin \mathcal{C}$ because any codeword is at distance at least d of $\boldsymbol{c}$. Thus, it suffices to check the condition $\boldsymbol{y} \in \mathcal{C}$ to detect if errors were produced.

Suppose now that $\boldsymbol{y}$ contains $t < \frac{d}{2}$ errors. Euclidean balls of radius $\left\lfloor \frac{d-1}{2} \right\rfloor$ in $\mathcal{A}^n$ whose center is each codeword in $\mathcal{C}$ are disjoint by definition of d, see Figure 1.2. Then, $\boldsymbol{y}$ is decoded by the codeword which is the center of the unique ball containing it.

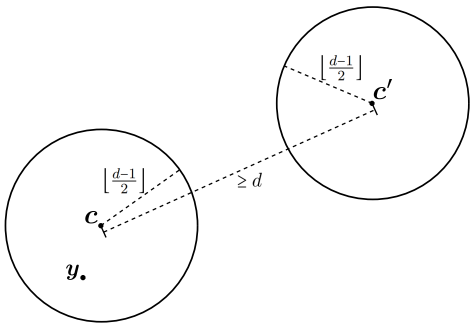


Figure 1.2: Two Euclidean balls of radius $\left\lfloor \frac{d-1}{2} \right\rfloor$ centered in the codewords $\boldsymbol{c}$ and $\boldsymbol{c}'$

Lastly, assume that $\boldsymbol{y}$ contains $t < d$ erasures. Then, it is decoded by the codeword which coincides with $\boldsymbol{y}$ in the remaining $n - t$ coordinates. □

Therefore, the higher the minimum distance is, the better the error-correcting capability of the code is. Computing the minimum distance of a code is, in general, a hard problem. Thus, lower bounds on the minimum distance are usually used to ensure a minimum value on the error-correcting capability of a code.

Block codes encoding and decoding processes are computationally expensive because they require to save in memory all the codewords. In order to solve this problem, algebraic structures are useful. Linear codes are the most common structure for error-correcting codes.

1.2. Linear codes

Let Q be a prime power and set $\mathbb{F}_Q$ the finite field with cardinality Q. $\mathbb{F}_Q$ will be the alphabet for our linear codes, which will be referred as *supporting field*. We use a capital letter for such cardinality in order not to lead to confusion, this is because we will use the symbol q for a (possibly) different prime power. Some references for finite fields can be found in [83, 71, 96, 101].

Definition 1.2.1. A *linear code* of length n over $\mathbb{F}_Q$ is a vector subspace of $\mathbb{F}_Q^n$.

As a vector space, a linear code $\mathcal{C}$ has a dimension k. Then, $\#\mathcal{C} = Q^k$, its information rate is $\frac{k}{n}$ and its redundancy is $n-k$. The fundamental parameters of a linear code are the length, dimension and minimum distance and are usually written as $[n,k,d]_Q$, or $[n,k,d]$ when the alphabet is not relevant. In order to specify the alphabet, it is also said that $\mathcal{C}$ is a Q-ary code. Notice that with this algebraic structure, it suffices to store in memory nk elements of $\mathbb{F}_Q$, coming from the k codewords of a basis of C, instead of nQ^k ones, coming from storing all the codewords of a general block code.

A linear code $\mathcal{C}$, as a k-dimensional vector subspace of $\mathbb{F}_Q^n$, is the image of an injective linear map

$$g : \mathbb{F}_Q^k \to \mathbb{F}_Q^n.$$

We can think of $\mathbb{F}_Q^k$ as the information source encoded into $\mathcal{C}$ by the map g.

Definition 1.2.2. A *generator matrix* G of a linear code $\mathcal{C}$ is a $k \times n$ matrix over $\mathbb{F}_Q$ of rank k whose rows constitute a basis of $\mathcal{C}$.

Of course, a linear code has different (similar) generator matrices or, equivalently, different encodings maps g. In addition, $\mathcal{C}$ can be described as a system of implicit equations given by the kernel of a linear map

$$h : \mathbb{F}_Q^n \to \mathbb{F}_Q^{n-k}$$

whose matrix is the transpose $H^\top$ of the following matrix.

Definition 1.2.3. A *parity-check matrix* H of a linear code $\mathcal{C}$ is an $(n-k) \times n$ matrix over $\mathbb{F}_Q$ of rank $n-k$ such that for every $\boldsymbol{x} \in \mathbb{F}_Q^n$, $\boldsymbol{x} \in \mathcal{C}$ if and only if $H\boldsymbol{x}^\top = 0$.

Then, $\mathcal{C} = \mathrm{Im}(g) = \mathrm{Ker}(h)$ and $GH^\top = 0$.

Since H has maximum rank, it can be seen as the generator matrix of another linear code over $\mathbb{F}_Q$.

Definition 1.2.4. Let $\mathcal{C} \subseteq \mathbb{F}_Q^n$ be a linear code with parity-check matrix H. The *dual code*, $\mathcal{C}^\perp$, of $\mathcal{C}$ is the $n-k$-dimensional linear code over $\mathbb{F}_Q$ that admits H as a generator matrix.

Indeed, $\mathcal{C}^\perp$ is the orthogonal subspace of $\mathcal{C}$ with respect to the following non-degenerate symmetric bilinear form, that we call *Euclidean inner product*:

$$\cdot_e : \mathbb{F}_Q^n \times \mathbb{F}_Q^n \to \mathbb{F}_Q, \quad \boldsymbol{x} \cdot_e \boldsymbol{y} = \sum_{i=1}^{n} x_i y_i.$$

Sometimes we write $\mathcal{C}^{\perp_e}$ instead of $\mathcal{C}^{\perp}$ to distinguish among different inner products we will use. Moreover, the equality $GH^{\top} = 0$ implies that G is a parity-check matrix of $\mathcal{C}^{\perp}$.

A linear code admits different denominations depending on its relation with its dual code.

Definition 1.2.5. Let $\mathcal{C}$ be a linear code.

- If $\mathcal{C} \cap \mathcal{C}^{\perp} = \{\mathbf{0}\}$, then $\mathcal{C}$ is called *linear complementary-dual* (*LCD*).
- If $\mathcal{C} \subseteq \mathcal{C}^{\perp}$, then $\mathcal{C}$ is called *self-orthogonal*.
- If $\mathcal{C} = \mathcal{C}^{\perp}$, then $\mathcal{C}$ is called *self-dual*.

The parity-check matrix of a linear code allows us to compute its minimum distance. To show it, we define the following concept.

Definition 1.2.6. Let $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{F}_Q^n$. The *(Hamming) weight* of $\boldsymbol{x}$ is

$$\mathrm{w}(\boldsymbol{x}) := \#\{i \mid 1 \leq i \leq n,\, x_i \neq 0\} = \mathrm{d}(\boldsymbol{x}, \mathbf{0}),$$

where $\mathbf{0} := (0, \ldots, 0)$.

Definition 1.2.7. Two linear codes $\mathcal{C}_1, \mathcal{C}_2$ are said to be *isometric* if there exists a bijective mapping between them that preserves Hamming weights.

Notice that $\mathrm{d}(\boldsymbol{x}, \boldsymbol{y}) = \mathrm{w}(\boldsymbol{x} - \boldsymbol{y})$, for all $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_Q^n$. Therefore,

$$d = \mathrm{d}(\mathcal{C}) = \min\left\{\mathrm{d}(\boldsymbol{c}, \boldsymbol{c}'),\, \boldsymbol{c}, \boldsymbol{c}' \in \mathcal{C},\, \boldsymbol{c} \neq \boldsymbol{c}'\right\} = \min\left\{\mathrm{w}(\boldsymbol{c}) \mid \boldsymbol{c} \in \mathcal{C},\, \boldsymbol{c} \neq \mathbf{0}\right\}.$$

Proposition 1.2.8. *Let $\mathcal{C}$ be a linear code with minimum distance d and parity-check matrix H. Then, d coincides with the least cardinality of a set of linearly dependent columns of H.*

Proof. By definition of H, a word $\boldsymbol{x} \in \mathbb{F}_Q^n$ belongs to $\mathcal{C}$ if and only if $H\boldsymbol{x}^{\top} = 0$. Then, there exists a codeword of weight $w > 0$ if and only if there exist w columns of H which are linearly dependent. The coordinates of $\boldsymbol{x}$ are the coefficients of such a linear combination. □

The computation of the minimum distance of a linear code is an NP-hard problem [125]. For large dimensions, it is unsolvable, but for relatively small values of dimension and length it can be solved in a reasonable time. The so-called Brouwer-Zimmerman algorithm [134], described in [61], is the fastest general algorithm designed to compute the minimum distance.

One can construct new linear codes from old by raising (raising the coordinates of every codeword to a fixed power), lengthening (adding new coordinates), puncturing (deleting some coordinates) and shortening (discarding all but the codewords with 0's in some prefixed coordinates and puncturing those codewords in those coordinates). In the sequel we will work with raised and punctured codes, so we introduce the following

notation. Let $\mathcal{C}$ be an $[n,k,d]_Q$ linear code. Let s be a nonnegative integer and $\boldsymbol{c} = (c_1,\dots,c_n) \in \mathcal{C}$ be a codeword. We denote $\boldsymbol{c}^s = (c_1^s,\dots,c_n^s)$ and define

$$\mathcal{C}^s := \{\boldsymbol{c}^s \mid \boldsymbol{c} \in \mathcal{C}\} \subseteq \mathbb{F}_Q^n.$$

Let $R \subseteq \{1,\dots,n\}$ be a subset of cardinality r. Set $\pi_R : \mathbb{F}_Q^n \to \mathbb{F}_Q^r$ the projection map on the coordinates of R and let

$$\mathcal{C}[R] := \{\pi_R(\boldsymbol{c}) \mid \boldsymbol{c} \in \mathcal{C}\}.$$

This is the code obtained after puncturing $\mathcal{C}$ in the coordinates with positions in $\{1,\dots,n\}\backslash R$.

1.2.1. Decoding processes

The algebraic structure of linear codes eases the decoding processes, being computationally cheaper. Here we expose a general decoding method, but we remark that each particular linear code may have other much more efficient ones. Our next definition considers the parity-check matrix to give information about the error produced when transmitting a codeword.

Let $\mathcal{C} \subseteq \mathbb{F}_Q^n$ be an $[n,k,d]$ linear code with parity-check matrix H. Suppose that one sends a codeword $\boldsymbol{c} \in \mathcal{C}$ and receives $\boldsymbol{y} = \boldsymbol{c} + \boldsymbol{e} \in \mathbb{F}_Q^n$, where $\boldsymbol{e} \in \mathbb{F}_Q^n$ is the error produced.

Definition 1.2.9. The *syndrome* of a word $\boldsymbol{w} \in \mathbb{F}_Q^n$ is defined to be the vector

$$\mathrm{sy}(\boldsymbol{w}) := H\boldsymbol{w}^\top \in \mathbb{F}_Q^{n-k}.$$

Since $\mathrm{sy}(\boldsymbol{c}) = 0$, then $\mathrm{sy}(\boldsymbol{y}) = \mathrm{sy}(\boldsymbol{e})$ and the syndrome of $\boldsymbol{y}$ is a linear combination of the columns of H corresponding to positions where errors occurred.

Define the equivalence relation in $\mathbb{F}_Q^n$: $\boldsymbol{w}_1 \sim \boldsymbol{w}_2$ if and only if $\boldsymbol{w}_1 - \boldsymbol{w}_2 \in \mathcal{C}$ and consider its quotient space vector $\mathbb{F}_Q^n / \mathcal{C}$. Then, the equivalence classes are of the form $\boldsymbol{w} + \mathcal{C} = \{\boldsymbol{w} + \boldsymbol{x} \mid \boldsymbol{x} \in \mathcal{C}\}$, $\boldsymbol{w} \in \mathbb{F}_Q^n$. Notice that the condition $\boldsymbol{w}_1 \sim \boldsymbol{w}_2$ is equivalent to $\mathrm{sy}(\boldsymbol{w}_1) = \mathrm{sy}(\boldsymbol{w}_2)$.

Then, once received $\boldsymbol{y}$, we know the equivalence class $\boldsymbol{e}$ belongs to. Assuming unique decodification, decoding $\boldsymbol{y}$ means to find its nearest codeword. That is, to find that $\boldsymbol{x} \in \mathcal{C}$ whose value $\mathrm{d}(\boldsymbol{y},\boldsymbol{x}) = \mathrm{w}(\boldsymbol{y}-\boldsymbol{x})$ is a minimum. Since every vector $\boldsymbol{y}-\boldsymbol{x}$, $\boldsymbol{x} \in \mathcal{C}$, belongs to the equivalence class of $\boldsymbol{y}$, that minimum is obtained when $\boldsymbol{y}-\boldsymbol{x}$ is the minimum weight element of the equivalence class of $\boldsymbol{y}$, and $\boldsymbol{y}-\boldsymbol{x}$ is assumed as the error $\boldsymbol{e}$ produced. Therefore, the decoding is possible whenever there is a unique minimum weight element in the equivalence class of $\boldsymbol{y}$. If the number of errors does not overcome the error-correcting capacity of the code, the decoding will be correct, because each equivalence class has at most an element of weight at most $\left\lfloor \frac{d-1}{2} \right\rfloor$. Indeed, if $\boldsymbol{w}_1 \neq \boldsymbol{w}_2$, both belonging to the same equivalence class and with weight less than or equal to $\left\lfloor \frac{d-1}{2} \right\rfloor$, then $\boldsymbol{w}_1 - \boldsymbol{w}_2 \in \mathcal{C}$ and $\mathrm{w}(\boldsymbol{w}_1 - \boldsymbol{w}_2) \leq \mathrm{w}(\boldsymbol{w}_1) + \mathrm{w}(\boldsymbol{w}_2) \leq 2\left\lfloor \frac{d-1}{2} \right\rfloor < d$, a contradiction.

For the code $\mathcal{C}$, one constructs a two-column table whose rows are the equivalence classes of $\mathbb{F}_Q^n / \mathcal{C}$. In each row, the first column contains the syndrome of any element of the corresponding equivalence class. The second column contains the element of minimum weight not larger than $\left\lfloor \frac{d-1}{2} \right\rfloor$, if it exists. Otherwise, the column is empty. The decoding method is as follows:

Algorithm 1.2.10 (General decoding method for linear codes)**.** *Received* $\boldsymbol{y}$*:*

1. *Compute* $\mathrm{sy}(\boldsymbol{y})$ *and search the row where it appears in the above table.*
2. *If the second entry of that row is empty, the decoding fails. Otherwise, the second entry is assumed to be the error* $\boldsymbol{e}$ *produced and the decoded codeword is* $\boldsymbol{y} - \boldsymbol{e}$*. End of the algorithm.*

Notice that this (general) method requires the storage of a table of Q^{n-k} rows with syndromes and words involving a total of $Q^{n-k}(n-k+n)$ elements of $\mathbb{F}_Q$. Thus, the practical efficiency of this method reduces to codes with small length and dimension. Much more efficient decoding algorithms are known but they are not object of study in this work.

1.2.2. Singleton bound

As said, it is desirable for a code to have both the minimum distance and the information rate as high as possible, but these requirements are contradictory. In the setting of linear codes, this fact is reflected in the well-known Singleton bound. It relates the parameters of a linear code regardless of the supporting field, that is, this bound is independent of the cardinality of the field.

Theorem 1.2.11 (Singleton bound)**.** *Let* $\mathcal{C}$ *be an* $[n,k,d]_Q$ *code. Then,* $k + d \leq n + 1$*.*

Proof. By Proposition 1.2.8 , d coincides with the minimum number of linearly dependent columns of a parity-check matrix H of $\mathcal{C}$, which is at most $n-k+1$ because the rank of H is $n-k$. Therefore, $d \leq n-k+1$. □

There are several other bounds, such as Plotkin's, Hamming's, Gilbert-Varshamov's, Griesmer's and Elias-Bassalygo's bounds, but in this thesis we will only use the Singleton one.

Fixed the length of a linear code, it is clear that the larger one of the two remaining parameters is, the smaller the other is. That is the price one has to pay when desiring a large dimension or minimum distance. Fixed length and dimension, the Singleton bound shows that there is a maximum on its error-correcting capability.

1.2.3. MDS codes

Codes attaining equality in the Singleton bound are called *maximum distance separable* (*MDS*) codes.

In 1955, Segre posed the so-called MDS conjecture [111], which has been proved in certain cases. One of the more recent ones is when Q is prime [8]. The conjecture gives an upper bound on the length of an MDS code.

Conjecture 1.2.12 (MDS conjecture). *Let $\mathcal{C}$ be an $[n,k,d]_Q$ MDS code, then*

$$n \leq Q+1$$

unless Q is even and $k=3$ or $k=Q-1$, in which case

$$n \leq Q+2.$$

The MDS conjecture implies that whenever one wishes to maximize the minimum distance of a code by using an MDS code, one has to decide between having a limited length or working in a larger field. The first option restricts the number of symbols needed to broadcast information and a larger field implies a greater difficulty on the operations.

We end this section by stating the next result about the dual of an MDS code.

Proposition 1.2.13. *The dual of an MDS code is also an MDS code.*

Proof. Let $\mathcal{C}$ be an MDS code with parameters $[n,k,n-k+1]$ and assume that its dual $\mathcal{C}^\perp$ is not MDS. Then, there exists a codeword $\boldsymbol{c} \in \mathcal{C}^\perp$ of weight $0 < \mathrm{w}(\boldsymbol{c}) \leq k$. Let H be a generator matrix of $\mathcal{C}^\perp$ constructed by enlarging $\boldsymbol{c}$ to some basis of $\mathcal{C}^\perp$. H is a parity-check matrix of $\mathcal{C}$ whose first row is given by the coordinates of $\boldsymbol{c}$ and by Proposition 1.2.8 any $n-k$ columns of H are linear independent. Clearly, there are $n-k$ columns such that its first coordinate equals 0 and it is a contradiction because these columns are $n-k$ elements of $\mathbb{F}_Q^{n-k}$. □

1.3. Evaluation codes

In this section, we introduce the so-called *evaluation codes*. Their codewords are n-tuples obtained by evaluating specific functions at certain n fixed points. The properties of these codes can be deduced from the algebraic structure of the space of functions and the geometry of the involved points.

Keep the notation as in Section 1.2. Let $P = \{\alpha_1, \ldots, \alpha_n\}$ be a set of n distinct points of a set $\mathcal{X}$. Let $V = \{f : \mathcal{X} \to \mathbb{F}_Q\}$ a vector space of functions on the finite field $\mathbb{F}_Q$. Consider the *evaluation map*

$$\mathrm{ev}_P : V \to \mathbb{F}_Q^n, \quad \mathrm{ev}_P(f) = (f(\alpha_1), \ldots, f(\alpha_n)).$$

When this map is linear, its image is a vector subspace of $\mathbb{F}_Q^n$ and thus a linear code of length n over $\mathbb{F}_Q$.

Definition 1.3.1. An *evaluation code* is a linear code of the form $\mathcal{C}_V^P = \mathrm{ev}_P(V)$ for some linear map ev_P as above introduced.

The codewords of an evaluation code are of the form $\mathrm{ev}_P(f)$, $f \in V$, and there is a correspondence between positions and points in P.

Set $V = \mathbb{F}_Q[X_1, \ldots, X_m]$ the ring of polynomials in m variables. Let r be a positive integer. Denote by $\mathbb{F}_Q[X_1, \ldots, X_m]^{(r)}$ the vector space of polynomials in m variables over $\mathbb{F}_Q$ with degree less than or equal to r. A classical example of evaluation code is the *Reed-Muller* code. It is an evaluation code where $\mathcal{X} = P = \mathbb{F}_Q^m$ and $V = \mathbb{F}_Q[X_1, \ldots, X_m]^{(r)}$.

Reed-Solomon codes are another important class of evaluation codes. Let us define them.

Definition 1.3.2. Let k and n be positive integers such that $1 \leq k < n \leq Q$. Let $P = \{\alpha_1, \ldots, \alpha_n\} \subseteq \mathbb{F}_Q$. The *Reed-Solomon code* $\mathrm{RS}_{Q,P}[n,k]$ is the following evaluation code:

$$\mathrm{RS}_{Q,P}[n,k] = \{\mathrm{ev}_P(f) \mid f \in \mathbb{F}_Q[X]^{(k-1)}\}.$$

The length and dimension of the code $\mathrm{RS}_{Q,P}[n,k]$ are n and k, respectively. Images by ev_P of bases of $\mathbb{F}_Q[X]^{(k-1)}$ are bases of $\mathrm{RS}_{Q,P}[n,k]$. Reed-Solomon codes are MDS, and thus their minimum distance $d = n - k + 1$. This is because every codeword, as evaluation of a polynomial of degree less than k, has at most $k-1$ coordinates equal to 0, and at least weight $n - k + 1$. Then, $d \geq n - k + 1$ and the Singleton bound proves the equality.

Examples of evaluation codes arise when $\mathcal{X}$ is an affine or projective space, P is a subset of points determined by some constraints, and V is determined by polynomial or rational functions. P could be an algebraic variety, roughly speaking the set of solutions of a system of polynomial equations in either the affine or projective space. Only affine varieties are considered in this thesis. *Affine variety codes* were introduced in [40], where P is an affine variety and V is a subspace of classes of polynomials of the quotient ring modulo the vanishing ideal of P.

1.3.1. Monomial-Cartesian codes

This subsection introduces monomial-Cartesian codes, a family of codes present in a good part of our work. They were introduced in [54]. In [93] the authors defined them using only algebraic tools. We, similarly to [54], prefer to consider them as affine variety codes.

Let Q be a prime power, m a positive integer and consider a family $\{P_j\}_{j=1}^m$ of subsets of $\mathbb{F}_Q$ with cardinality larger than one. Set

$$P = P_1 \times \cdots \times P_m = \{\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_n\} \subseteq \mathbb{F}_Q^m.$$

We usually write $\boldsymbol{\alpha}_i = (\alpha_{i1}, \ldots, \alpha_{im})$. Consider the quotient ring

$$\mathcal{R} = \mathbb{F}_Q[X_1, \ldots, X_m] / I,$$

where I is the ideal of $\mathbb{F}_Q[X_1, \ldots, X_m]$ vanishing at P. Then, I is the $\mathbb{F}_Q$-vector space

$$I = \langle f_1(X_1), \ldots, f_m(X_m) \rangle,$$

where

$$f_j(X_j) = \prod_{\beta \in P_j} (X_j - \beta)$$

and $\deg(f_j) = \#P_j =: n_j \geq 2$ [94]. Let

$$E = \{0, 1, \ldots, n_1 - 1\} \times \cdots \times \{0, 1, \ldots, n_m - 1\}.$$

Any m-tuple $\boldsymbol{e} = (e_1, \ldots, e_m) \in E$ is called an exponent and we denote $\boldsymbol{X}^{\boldsymbol{e}} = X_1^{e_1} \cdots X_m^{e_m}$. Given $f \in \mathcal{R}$, f denotes both the equivalence class in $\mathcal{R}$ and the unique polynomial in $\mathbb{F}_Q[X_1, \ldots, X_m]$ with degree in X_j less than n_j, $1 \leq j \leq m$, representing f. Thus

$$f(X_1, \ldots, X_m) = \sum_{(e_1, \ldots, e_m) \in E} f_{e_1, \ldots, e_m} X_1^{e_1} \cdots X_m^{e_m},$$

with $f_{e_1, \ldots, e_m} \in \mathbb{F}_Q$. Set $\operatorname{supp}(f) = \{(e_1, \ldots, e_m) \in E \mid f_{e_1, \ldots, e_m} \neq 0\}$. For each subset $\varnothing \neq \Delta \subseteq E$, define

$$V_\Delta := \{f \in \mathcal{R} \mid \operatorname{supp}(f) \subseteq \Delta\} \cup \{0\}.$$

Then, V_Δ is the $\mathbb{F}_Q$-vector space $\langle \boldsymbol{X}^{\boldsymbol{e}} \mid \boldsymbol{e} \in \Delta \rangle_{\mathbb{F}_Q}$. The linear evaluation map

$$\operatorname{ev}_P : \mathcal{R} \to \mathbb{F}_Q^n, \qquad \operatorname{ev}_P(f) = (f(\boldsymbol{\alpha}_1), \ldots, f(\boldsymbol{\alpha}_n)),$$

gives rise to the following class of evaluation codes.

Definition 1.3.3. Keep the notation of this subsection. The *monomial-Cartesian code* (MCC) $\mathcal{C}_\Delta^P$ is the following $\mathbb{F}_Q$-vector subspace of $\mathbb{F}_Q^n$:

$$\mathcal{C}_\Delta^P := \operatorname{ev}_P(V_\Delta) = \langle \operatorname{ev}_P(\boldsymbol{X}^{\boldsymbol{e}}) \mid \boldsymbol{e} \in \Delta \rangle \subseteq \mathbb{F}_Q^n.$$

We say that $\mathcal{C}_\Delta^P$ is univariate (respectively, bivariate, multivariate) when $m = 1$ (respectively, $m = 2$, $m > 2$).

MCCs are a family of codes that extend J-affine variety codes, previously introduced in [49]. In [49] the authors used the term "affine variety codes", however one must not confuse them with those satisfying the more general definition of an affine variety code, given at the end of Section 1.3. J-affine variety codes are MCCs where the evaluation points belong to a Cartesian product of some multiplicative subgroups of $\mathbb{F}_Q$ to which we could also add the element $0 \in \mathbb{F}_Q$. The mentioned multiplicative structure eases the control of these codes, and the possibility of introducing 0 increases the range of lengths. These codes can be thought as a generalization of cyclic codes to multiple variables, and we define them next as particular instances of MCCs. Denote by $U_t \subseteq \mathbb{F}_Q$ the set of t-th roots of unity for some $t \mid Q - 1$.

Definition 1.3.4. Consider a subset $J \subseteq \{1, \ldots, m\}$, that is used to detect the variables where $0 \in \mathbb{F}_Q$ is not evaluated. A *J-affine variety code*, $\mathcal{C}_\Delta^{P,J}$, is an MCC, $\mathcal{C}_\Delta^P$, where $P_j = U_{n_j}$, for some $n_j \mid Q - 1$, when $j \in J$, and $P_j = U_{n_j - 1} \cup \{0\}$, for some $n_j - 1 \mid Q - 1$, otherwise.

Sometimes in the future, we will consider J-affine variety codes since the subgroup structure of the sets P_j will be useful for our purposes.

We also introduce the following definition which will be used in the next sections.

Definition 1.3.5. Two subsets Δ_1 and Δ_2 of E are *pseudoisometric* if there exists $\boldsymbol{v} = (v_1, \ldots, v_m) \in \mathbb{Z}^m$ such that

$$\Delta_2 = \boldsymbol{v} + \Delta_1 := \{(e_1 + v_1, \ldots, e_m + v_m) \mid (e_1, \ldots, e_m) \in \Delta_1\}.$$

In that case, we say that the codes $\mathcal{C}^P_{\Delta_1}$ and $\mathcal{C}^P_{\Delta_2}$ are *pseudoisometric*.

Remark 1.3.6. Let us explain why we speak of pseudoisometric codes. Firstly, recall the definition of $*$-product given at the beginning of Part I, and Definition 1.2.7 of isometric codes. Note that $\mathrm{ev}_P(fg) = \mathrm{ev}_P(f) * \mathrm{ev}_P(g)$ for all $f, g \in \mathcal{R}$.

Assume that Δ_1, $\Delta_2 \subseteq E$ are pseudoisometric sets such that $\Delta_2 = \boldsymbol{v} + \Delta_1$. For simplicity, suppose $v_j \leq 0$, $1 \leq j \leq m_1$, and $v_j \geq 0$, $m_1 + 1 \leq j \leq m$ for some index m_1. Consider

$$\Delta_2' = (-v_1, -v_2, \ldots, -v_{m_1}, 0, \ldots, 0) + \Delta_2$$

and

$$\Delta_1' = (0, \ldots, 0, v_{m_1+1}, \ldots, v_m) + \Delta_1,$$

and then $\Delta_2' = \Delta_1'$. Thus

$$V_{\Delta_2'} = \left\{X_1^{-v_1} \cdots X_{m_1}^{-v_{m_1}} g \mid g \in V_{\Delta_2}\right\},$$

and the codewords in $\mathcal{C}^P_{\Delta_2'}$ are of the form

$$\mathrm{ev}_P(X_1^{-v_1} \cdots X_{m_1}^{-v_{m_1}} g) = \mathrm{ev}_P(X_1^{-v_1} \cdots X_{m_1}^{-v_{m_1}}) * \mathrm{ev}_P(g),$$

where $g \in V_{\Delta_2}$. *When $0 \notin P_j$ for all $1 \leq j \leq m$ such that $v_j \neq 0$*, we have just proved that $\mathcal{C}^P_{\Delta_2'}$ and $\mathcal{C}^P_{\Delta_2}$ are isometric codes. The same reasoning proves that $\mathcal{C}^P_{\Delta_1'}$ and $\mathcal{C}^P_{\Delta_1}$ are isometric. Thus *$C^P_{\Delta_1}$ and $C^P_{\Delta_2}$ are isometric* and this also happens when the v_j are always negative or positive. The proof is the same but we need no auxiliary code.

When $0 \in P_j$ for some index $1 \leq j \leq m$, $\mathcal{C}^P_{\Delta_1}$ and $\mathcal{C}^P_{\Delta_2}$ need not be isometric.

Length, dimension and a bound for the minimum distance of an MCC, $\mathcal{C}^P_\Delta$, are provided in the forthcoming Proposition 1.3.7 and Corollary 1.3.10.

Proposition 1.3.7. *Keep the above notation. The length n and dimension k of an MCC, $\mathcal{C}^P_\Delta$, are $n = \prod_{j=1}^m n_j$ and $k = \#\Delta$.*

Proof. The claim on the length is immediate because it is equal to the number of points to evaluate, $n = \#P = \prod_{j=1}^m n_j$. As for the dimension, notice that the restriction map of ev_P to the vector space V_Δ, $\mathrm{ev}_P\big|_{V_\Delta}: V_\Delta \to \mathcal{C}^P_\Delta$, is an isomorphism of vector spaces. Indeed, the kernel of this map vanishes because I is the ideal of polynomials vanishing at P. Then, setting $\mathrm{Im}\left(\mathrm{ev}_P\big|_{V_\Delta}\right)$ the image of the map $\mathrm{ev}_P\big|_{V_\Delta}$, it holds that

$$k = \dim\left(\mathcal{C}^P_\Delta\right) = \dim\left(\mathrm{Im}\left(\mathrm{ev}_P\big|_{V_\Delta}\right)\right) = \dim(V_\Delta) = \#\Delta,$$

which finishes the proof. □

Now, we are going to give a bound on the minimum distance of MCCs. Our bound is deduced of the so-called *footprint bound* [52, 51] which can be proved with techniques of the Gröbner basis theory [32] (see [24, Proposition 2.3]). Very close bounds are, on the one hand, the *Feng-Rao bound* for the dual code which was initially stated for algebraic geometry codes [37, 38] and called *order bound* for evaluation codes [67]. Finally it was generalized to linear codes (see [97]). And, on the other hand, the *Feng-Rao bound* for the primal code (i.e., for the code itself, not for the dual one) [2].

Definition 1.3.8. Let E be as at the beginning of this subsection. We call *footprint* of an exponent $\boldsymbol{e} \in E$ the value $\mathrm{F}(\boldsymbol{e}) := \prod_{j=1}^{m}(n_j - e_j)$.

In the bivariate case ($m = 2$), we represent the set E as a grid. Each coordinate (e_1, e_2) in the grid is an exponent and it is labelled with its footprint $\mathrm{F}(\boldsymbol{e})$. Figure 1.3 shows the grid representation of E in the case when $n_1 = 10$ and $n_2 = 9$.

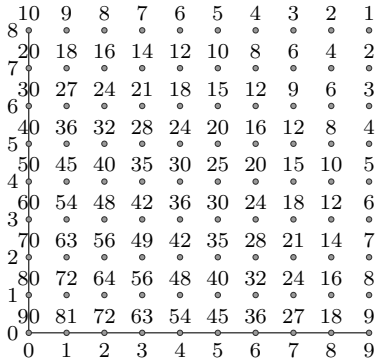


Figure 1.3: Grid representation of E, where $m = 2$, $n_1 = 10$ and $n_2 = 9$

Proposition 1.3.9. *Let $\mathcal{C}_\Delta^P$ be an MCC and let $\boldsymbol{c} = \mathrm{ev}_P(f) \in \mathcal{C}_\Delta^P$ be a codeword, $f \in \mathcal{R}$. Fix a monomial ordering on $\mathbb{N}_0^m$ and let $\boldsymbol{X}^{\boldsymbol{e}}$ be the leading monomial of f. Then, $\mathrm{w}(\boldsymbol{c}) \geq \mathrm{F}(\boldsymbol{e})$.*

Proof. Recall that $f_1(X_1), \ldots, f_m(X_m)$ are the generators of the ideal I. They have leading monomials, respectively, $X_1^{n_1}, \ldots, X_m^{n_m}$. Let

$$I' := \langle f(X_1, \ldots, X_m), f_1(X_1), \ldots, f_m(X_m) \rangle$$

and denote by $\mathrm{V}(I')$ the affine variety defined by I'. Set $\mathrm{F}(I')$ the footprint of I', that is, the set of monomials that are not leading monomials of any polynomial in I' or, equivalently, that are not multiple of any of the leading monomials of the polynomials in a Gröbner basis for I'. Then, $\mathrm{F}(I') \subseteq \mathrm{F}(\langle \boldsymbol{X}^{\boldsymbol{e}}, X_1^{n_1}, \ldots, X_m^{n_m} \rangle)$. Also, since $\mathrm{F}(I')$ is a finite set, $\#\mathrm{V}(I') \leq \#\mathrm{F}(I')$ [32, Section 5.3]. Then,

$$\#\mathrm{V}(I') \leq \#\mathrm{F}(I') \leq \#\mathrm{F}(\langle \boldsymbol{X}^{\boldsymbol{e}}, X_1^{n_1}, \ldots, X_m^{n_m} \rangle).$$

Notice that $\#\mathrm{F}(\langle \boldsymbol{X}^{\boldsymbol{e}}, X_1^{n_1}, \ldots, X_m^{n_m} \rangle) = n - \prod_{i=1}^{m}(n_i - e_i)$, since there are n monomials that are not multiple of $X_1^{n_1}, \ldots, X_m^{n_m}$ but we must also remove from that set the number

of monomials that are not multiple of $\boldsymbol{X}^{\boldsymbol{e}}$. An illustration for the case $m = 2$ is shown in Figure 1.4.

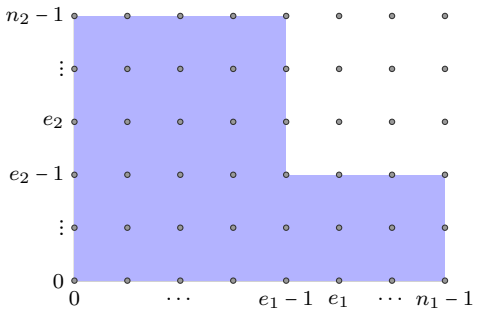


Figure 1.4: Shaded region representing $\mathrm{F}(\langle \boldsymbol{X}^{\boldsymbol{e}}, X_1^{n_1}, X_2^{n_2} \rangle)$

Therefore,

$$\mathrm{w}(\boldsymbol{c}) = \mathrm{w}(\mathrm{ev}_P(f)) = n - \#\,\mathrm{V}(I') \geq n - \#\,\mathrm{F}(\langle \boldsymbol{X}^{\boldsymbol{e}}, X_1^{n_1}, \ldots, X_m^{n_m} \rangle) = \prod_{i=1}^{m} (n_i - e_i) = \mathrm{F}(\boldsymbol{e}).$$

□

We will frequently use the following result which follows from Proposition 1.3.9.

Corollary 1.3.10. *Let $\mathcal{C}_\Delta^P$ be an MCC and let d be its minimum distance. Define $d_0 := d_0(\mathcal{C}_\Delta^P) := \min\{\mathrm{F}(\boldsymbol{e}) \mid \boldsymbol{e} \in \Delta\}$. Then, $d \geq d_0$.*

The above bound is attained in some cases:

Remark 1.3.11. With the above notation, given $\varnothing \neq \Delta \subseteq E$, define $M_\Delta := \{\boldsymbol{X}^{\boldsymbol{e}} \mid \boldsymbol{e} \in \Delta\}$. According to [22, Definition 3.1], a code $\mathcal{C}_\Delta^P$ is named *decreasing monomial-Cartesian* whenever

$$\boldsymbol{X}^{\boldsymbol{e}} \in M_\Delta \text{ implies } \boldsymbol{X}^{\boldsymbol{e}'} \in M_\Delta \text{ for all } \boldsymbol{e}' \in E \text{ such that } \boldsymbol{X}^{\boldsymbol{e}'} \text{ divides } \boldsymbol{X}^{\boldsymbol{e}}. \tag{1.3.1}$$

By [22, Theorem 3.9], the values d and d_0 corresponding to any decreasing MCC coincide.

Definition 1.3.12. A set $\Delta \subseteq E$ that satisfies Condition (1.3.1) is called *decreasing*.

Example 1.3.13. From now on when displayed in a picture the exponents in a set $\Delta \subseteq E$ are coloured in blue. Figure 1.5 shows the case when $m = 2$, $n_1 = 8$, $n_2 = 6$ and $\Delta = (\{0,1,2\} \times \{0,1\}) \cup \{(0,2),(1,2)\}$. By Corollary 1.3.10 a lower bound for the minimum distance of the code $\mathcal{C}_\Delta^P$, for any $P = P_1 \times P_2 \subseteq \mathbb{F}_Q^2$, is $d_0 = d_0(\mathcal{C}_\Delta^P) = \min\{\mathrm{F}(\boldsymbol{e}) \mid \boldsymbol{e} \in \Delta\} = 28$. Moreover, since Δ is decreasing, $d = d_0$ by Remark 1.3.11.

1.4. Locally recoverable codes

In large scale distributed and cloud storage systems, information is disseminated in several nodes in a redundant form to ensure reliability against node failures causing loss

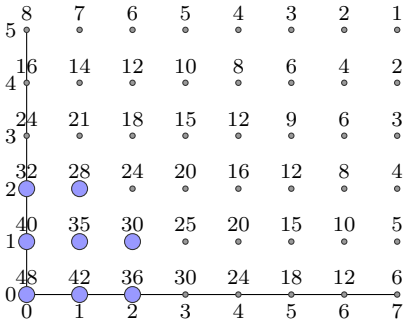


Figure 1.5: Grid representation of E, where $m = 2$, $n_1 = 8$, $n_2 = 6$. In blue, the points in $\Delta = (\{0,1,2\} \times \{0,1\}) \cup \{(0,2),(1,2)\}$

of data. This is known as the repair problem, which nowadays is gaining importance because of the growth of the amount of stored data. It is then required a reliable storage so that, when a node fails or it is temporarily unavailable due to maintenance or other reasons, the data it contains can be recovered by using information from other nodes. A natural method consists of replicating the information across several nodes, but protecting the data using error-correcting codes is a more clever method. This way *locally recoverable* (or *locally repairable*) *codes* (LRCs) arise. They were introduced in [55] and since we know the affected position we desire to repair erasures. Here we abuse language by referring to positions as coordinates, following the terminology used in literature.

Definition 1.4.1. An LRC is an error-correcting code such that any erasure in a coordinate of a codeword can be recovered from a set of other few coordinates.

Keep the notation as in Section 1.2. Let $\mathcal{C}$ be an $[n,k,d]_Q$ code. A coordinate $i \in \{1,\dots,n\}$ is *locally recoverable* if there is a *recovery set* $R \subseteq \{1,\dots,n\}$ with cardinality $r \in \mathbb{N}$ and $i \notin R$ such that for any codeword $\boldsymbol{c} = (c_1,\dots,c_n) \in \mathcal{C}$, an erasure in the coordinate c_i of $\boldsymbol{c}$ can be recovered from the coordinates of $\boldsymbol{c}$ with positions in R. Let us denote $\overline{R} := R \cup \{i\}$. The *locality* of a coordinate is the smallest cardinality of a recovery set for that coordinate. An *LRC with locality* r is an LRC such that every coordinate is locally recoverable and r is the largest locality of its coordinates. Recall, from Section 1.2, that $\pi_R : \mathbb{F}_Q^n \to \mathbb{F}_Q^r$ is the projection map on the coordinates of R and $\mathcal{C}[R] = \{\pi_R(\boldsymbol{c}) \mid \boldsymbol{c} \in \mathcal{C}\}$. Next we give two important bounds on the locality of an LRC.

Proposition 1.4.2. *Let r be the locality of an LRC $\mathcal{C}$. Then, $r \geq \mathrm{d}(\mathcal{C}^\perp) - 1$.*

Proof. Let n be the length of $\mathcal{C}$ and $\boldsymbol{g}_1,\dots,\boldsymbol{g}_n$ be the columns of a generator matrix of $\mathcal{C}$. Let $i \in \{1,\dots,n\}$ be any coordinate. Let $r_0 \leq r$ be the locality of i and set R a recovery set for i with cardinality r_0. Then, $\boldsymbol{g}_i \in \langle \boldsymbol{g}_l \mid l \in R \rangle$. Notice that this is equivalent to $\dim(\mathcal{C}[R]) = \dim(\mathcal{C}[\overline{R}])$ and this shows that the notion of recovery set does not depend on the generator matrix. Thus, there exists $\boldsymbol{w} = (w_1,\dots,w_n) \in \mathcal{C}^\perp$, that is, $\sum_{l=1}^n w_l \boldsymbol{g}_l = 0$, with $w_i \neq 0$ and $w_l = 0$ for all $l \notin \overline{R}$. Therefore, $r \geq r_0 = \#R \geq \mathrm{d}(\mathcal{C}^\perp) - 1$. □

The parameters and locality of an LRC satisfy the following Singleton-like inequality [55].

$$k + d + \left\lceil \frac{k}{r} \right\rceil \leq n + 2.$$

When the equality holds, the code is called an *optimal r-LRC*.

The following result gives an equivalent condition of recovery set and motivates the forthcoming definition.

Proposition 1.4.3. *A set $R \subseteq \{1, \ldots, n\}$ is a recovery set for a coordinate $i \notin R$ if and only if* $\mathrm{d}(\mathcal{C}[\overline{R}]) \geq 2$.

Proof. By [105, Proposition 4.3.12] the minimum distance d' of any code $\mathcal{C}'$ with length n' satisfies $d' \geq d^*$, $(n' >)$ d^* being a fixed positive integer, if and only if, for all $S \subseteq \{1, \ldots, n'\}$ with $\#S > n' - d^*$, we have $\dim(\mathcal{C}'[S]) = \dim(\mathcal{C}')$. The proof of Proposition 1.4.2 shows that R is a recovery set for i if and only if $\dim(\mathcal{C}[R]) = \dim(\mathcal{C}[\overline{R}])$. Then, the result follows by taking $\mathcal{C}' = \mathcal{C}[\overline{R}]$ and $d^* = 2$. □

By Proposition 1.4.3, if R is a recovery set for i, then $\mathrm{d}(\mathcal{C}[\overline{R}]) \geq 2$ and thus only one erasure can be corrected (also only up to to one error can be detected). At the beginning, locally recoverable codes were introduced by assuming that no erasures occur in the coordinates $\pi_R(\boldsymbol{c})$ used to recover the desired one c_i. The previous definition covers this situation, but it is limited because erasures can also occur in $\pi_R(\boldsymbol{c})$. The fact that simultaneous multiple device failures may happen leads us to the concept of LRCs with locality (r, δ) (or (r, δ)-LRCs), introduced in [106].

Definition 1.4.4. Let r and $\delta \geq 2$ be positive integers. A code $\mathcal{C}$ is *locally recoverable with locality* (r, δ) if, for any coordinate $i \in \{1, \ldots, n\}$, there exists a set of coordinates $\overline{R} = \overline{R}(i) \subseteq \{1, \ldots, n\}$ such that:

1. $i \in \overline{R}$ and $\#\overline{R} \leq r + \delta - 1$; and
2. $\mathrm{d}(\mathcal{C}[\overline{R}]) \geq \delta$.

Such a set $\overline{R}$ is called an (r, δ)-*recovery set for* i, and $\mathcal{C}$ an (r, δ)-*LRC*.

In this thesis we only consider this last type of locality. Sometimes, abusing the notation, we will use locality r but understanding locality (r, δ) for some δ inferred from the context. In this definition, r refers to the number of coordinates used to recover another one and $\delta - 1$ refers to the number of erasures that can occur in an (r, δ)-recovery set. We remark that by definition one can speak about several localities (r, δ), corresponding to the $\mathrm{d}(\mathcal{C}) - 1$ values of $\delta = 2, 3, \ldots, \mathrm{d}(\mathcal{C})$, and that r is not necessarily the minimum possible value. The second condition in Definition 1.4.4 allows us to correct an erasure at coordinate i plus any other $\delta - 2$ erasures in $\overline{R} \backslash \{i\}$ by using the remaining r coordinates (also it allows us to detect an error at coordinate i plus any other $\delta - 2$ errors in $\overline{R} \backslash \{i\}$). Notice that, when $\mathcal{C}$ is an LRC with locality (r, δ), the original definition

of locality of $\mathcal{C}$ is $\leq r$. In fact, any subset $R \subseteq \overline{R}$ such that $\#R = r$ and $i \notin R$ fulfills $d(\mathcal{C}([R] \cup \{i\})) \geq 2$. Thus, by Proposition 1.4.3, R is a recovery set for the coordinate i.

There is also a Singleton-like inequality for (r, δ)-LRCs:

Proposition 1.4.5. *[106] The parameters $[n, k, d]_Q$ of an (r, δ)-LRC, $\mathcal{C}$, satisfy*

$$k + d + \left(\left\lceil \frac{k}{r} \right\rceil - 1\right)(\delta - 1) \leq n + 1. \tag{1.4.1}$$

A code $\mathcal{C}$ as above is called an *optimal* (r, δ)-*LRC* (or simply, an *optimal* LRC) whenever equality holds in (1.4.1).

1.5. Subfield-subcodes

A Q-ary code $\mathcal{C}$ may have codewords with all their coordinates in a subfield $\mathbb{F}_{Q'}$ of $\mathbb{F}_Q$. Sometimes we will be interested in the subcode consisting of such codewords.

Definition 1.5.1. Let $\mathcal{C}$ be a Q-ary code with length n and $\mathbb{F}_{Q'}$ be a subfield of $\mathbb{F}_Q$. The *subfield-subcode* $\mathcal{S}$ of $\mathcal{C}$ over $\mathbb{F}_{Q'}$ is the linear code $\mathcal{S} = \mathcal{C} \cap \mathbb{F}_{Q'}^n$.

Suppose that $Q = p^l$ and $Q' = p^h$, where p is a prime and l and h are distinct positive integers such that $h \mid l$. Let $[n, k, d]_Q$ and $[n', k', d']_{Q'}$ be the parameters of $\mathcal{C}$ and $\mathcal{S}$, respectively. Obviously, $n' = n$ and $d' \geq d$. A parity-check matrix of $\mathcal{S}$ can be constructed from a parity-check matrix of $\mathcal{C}$. We start by replacing each entry by the $\frac{l}{h} \times 1$ column containing the coordinates of such an entry with respect a basis of $\mathbb{F}_Q$ over $\mathbb{F}_{Q'}$. The resulting matrix is an $\frac{l}{h}(n-k) \times n$ matrix over $\mathbb{F}_{Q'}$ and, by deleting dependent rows, one obtains a parity-check matrix of $\mathcal{S}$. Then, the dimension of $\mathcal{S}$ satisfies $n - \frac{l}{h}(n-k) \leq k' \leq k$. Furthermore, if $\mathcal{C}$ has a basis of codewords in $\mathbb{F}_{Q'}^n$, then it is also a basis of $\mathcal{S}$ and in such case $k' = k$ [71, Section 3.8].

We recall the concept of *trace map*. It is a key tool to describe subfield-subcodes. This map sends every element of $\mathbb{F}_Q (= \mathbb{F}_{p^l})$ into the sum of its conjugates over $\mathbb{F}_{Q'} (= \mathbb{F}_{p^h})$:

$$\mathrm{tr} := \mathrm{tr}_l^h : \mathbb{F}_{p^l} \to \mathbb{F}_{p^h}, \quad \mathrm{tr}_l^h(x) = x + x^{p^h} + \cdots + x^{p^{h\left(\frac{l}{h}-1\right)}}.$$

Properties of finite fields imply that this map indeed evaluates in $\mathbb{F}_{Q'}$ because $\mathrm{tr}_l^h(x)$ is a root of the polynomial $X^{Q'} - X$. Moreover, tr is surjective and a nontrivial linear functional on the vector space $\mathbb{F}_Q$ over $\mathbb{F}_{Q'}$, that is, $\mathrm{tr}_l^h(\gamma(\alpha + \beta)) = \gamma\,\mathrm{tr}_l^h(\alpha) + \gamma\,\mathrm{tr}_l^h(\beta)$ for all $\alpha, \beta \in \mathbb{F}_Q$ and $\gamma \in \mathbb{F}_{Q'}$.

We also define another trace type map which will be useful:

$$\mathbf{tr} := \mathbf{tr}_l^h : \mathbb{F}_{p^l}^n \to \mathbb{F}_{p^h}^n, \text{ determined by } \mathrm{tr}_l^h \text{ componentwise.}$$

Definition 1.5.2. The *trace code* of a Q-ary code $\mathcal{C}$ is the following linear code of length n over $\mathbb{F}_{Q'}$:

$$\mathbf{tr}(\mathcal{C}) := \mathbf{tr}_l^h(\mathcal{C}) := \{\mathbf{tr}_l^h(\boldsymbol{c}) \mid \boldsymbol{c} \in \mathcal{C}\}.$$

We will omit the indexes l and h of the above maps and code when they are clear from the context.

The following theorem by Delsarte [33] provides a relation between subfield-subcodes, duality and trace map (see [71, Theorem 3.8.6]).

Theorem 1.5.3 (Delsarte). *Let $\mathcal{S}$ be a p^h-ary subfield-subcode of a p^l-ary code $\mathcal{C}$. Then*

$$\mathcal{S}^\perp = \mathbf{tr}_l^h(\mathcal{C}^\perp).$$

Proof. Let $\boldsymbol{c} = (c_1, \dots, c_n) \in \mathcal{C}^\perp$ and let $\boldsymbol{s} = (s_1, \dots, s_n) \in \mathcal{S} \subseteq \mathcal{C}$. Then, recalling that $\cdot_e$ means Euclidean inner product,

$$\mathbf{tr}(\boldsymbol{c}) \cdot_e \boldsymbol{s} = \sum_{i=1}^{n} \mathrm{tr}(c_i)s_i = \mathrm{tr}\left(\sum_{i=1}^{n} c_i s_i\right) = \mathrm{tr}(0) = 0,$$

by definition of $\boldsymbol{c}$ and $\boldsymbol{s}$ and the linearity of the trace functional. Then, $\mathbf{tr}(\boldsymbol{c}) \in \mathcal{S}^\perp$, proving that $\mathbf{tr}(\mathcal{C}^\perp) \subseteq \mathcal{S}^\perp$.

Now, we show that $\mathcal{S}^\perp \subseteq \mathbf{tr}(\mathcal{C}^\perp)$ by proving that $(\mathbf{tr}(\mathcal{C}^\perp))^\perp \subseteq \mathcal{S}$. Let $\boldsymbol{t} = (t_1, \dots, t_n) \in (\mathbf{tr}(\mathcal{C}^\perp))^\perp \subseteq \mathbb{F}_{p^h}^n$ and then it suffices to prove $\boldsymbol{t} \in \mathcal{C}$ (or $\boldsymbol{t} \cdot_e \boldsymbol{c} = 0$ for all $\boldsymbol{c} = (c_1, \dots, c_n) \in \mathcal{C}^\perp$). For such a $\boldsymbol{c}$, since $\alpha\boldsymbol{c} \in \mathcal{C}^\perp$ for all $\alpha \in \mathbb{F}_{p^l}$, then

$$0 = \boldsymbol{t} \cdot_e \mathbf{tr}(\alpha\boldsymbol{c}) = \sum_{i=1}^{n} t_i \,\mathrm{tr}(\alpha c_i) = \mathrm{tr}\left(\alpha \sum_{i=1}^{n} t_i c_i\right)$$

by the linearity of the trace functional. Finally, $\sum_{i=1}^{n} t_i c_i = 0$ because, otherwise, we would contradict the fact that the trace functional is nontrivial. □

1.5.1. Subfield-subcodes of J-affine variety codes

J-affine variety codes were introduced in Definition 1.3.4. The structure of J-affine variety codes eases their management and allows us to provide some results on their subfield-subcodes that will be useful in the forthcoming chapters.

Keep the notation of this section and Subsection 1.3.1. Consider a subset $J \subseteq \{1, \dots, m\}$. Recall that it is used to detect the variables where $0 \in \mathbb{F}_Q$ is not evaluated. Assume that the polynomials $f_j(X_j)$ generating the ideal I are of the form

$$f_j(X_j) = X_j^{n_j} - 1,$$

for some $n_j \mid Q - 1$ if $j \in J$, and

$$f_j(X_j) = X_j^{n_j} - X_j,$$

where $n_j - 1 \mid Q - 1$, otherwise. Consider the J-affine variety code $\mathcal{C}_\Delta^{P,J}$ and denote by

$$\mathcal{S}_\Delta^{P,J} := \mathcal{C}_\Delta^{P,J} \cap \mathbb{F}_{p^h}^n$$

its subfield-subcode over the field $\mathbb{F}_{p^h}$. We define another trace type map as follows:

$$\mathcal{T} := \mathcal{T}_l^h : \mathcal{R} \to \mathcal{R}, \quad \mathcal{T}(f) = f + f^{p^h} + \cdots + f^{p^{h(\frac{l}{h}-1)}},$$

$\mathcal{R}$ being the quotient ring defined at the beginning of Subsection 1.3.1. Some of its properties are listed below [43, Propositions 4 and 5].

Proposition 1.5.4. *Let $f \in \mathcal{R}$. Then,*

1. $\mathcal{T}(af) = a\,\mathcal{T}(f)$, *for all* $a \in \mathbb{F}_{p^h}$.
2. $\mathcal{T}(f)^{p^h} = \mathcal{T}\left(f^{p^h}\right) = \mathcal{T}(f)$.
3. $\mathrm{ev}_P(\mathcal{T}(f)) = \mathbf{tr}(\mathrm{ev}_P(f))$.
4. $f = \mathcal{T}(g)$ *for some* $g \in \mathcal{R}$ *if and only if* f *evaluates to* $\mathbb{F}_{p^h}$.

Proof. The definition of the map $\mathcal{T}$, properties of finite fields and the fact that $\mathcal{R}$ is a quotient ring modulo I imply *1*, *2* and *3*.

To prove *4*, suppose that $f = \mathcal{T}(g)$ for some $g \in \mathcal{R}$. Then, *2* implies

$$f^{p^h} = \mathcal{T}(g)^{p^h} = \mathcal{T}(g) = f$$

and thus for any $\boldsymbol{\alpha} \in \mathbb{F}_{p^l}^m$, $f(\boldsymbol{\alpha})^{p^h} = f(\boldsymbol{\alpha})$, so $f(\boldsymbol{\alpha}) \in \mathbb{F}_{p^h}$. Reciprocally, suppose that f evaluates to $\mathbb{F}_{p^h}$. The fact that $\mathbf{tr}$ is surjective allows us to consider $\boldsymbol{w} \in \mathbb{F}_{p^l}^n$ such that $\mathrm{ev}_P(f) = \mathbf{tr}(\boldsymbol{w})$. Let $f' \in \mathcal{R}$ be the class of an interpolating polynomial satisfying $\mathrm{ev}_P(f') = \boldsymbol{w}$. Then, Item *3* implies

$$\mathrm{ev}_P(\mathcal{T}(f')) = \mathbf{tr}(\mathrm{ev}_P(f')) = \mathrm{ev}_P(f)$$

and the fact that ev_P is an isomorphism gives $f = \mathcal{T}(f')$. □

The above introduced set

$$E = \{0, 1, \ldots, n_1 - 1\} \times \cdots \times \{0, 1, \ldots, n_m - 1\}$$

can be endowed with an additive and multiplicative structure which will allow us to determine a basis for the subfield-subcode $S_\Delta^{P,J}$ and a formula for its dimension. Notice that, when $j \notin J$, the evaluation of monomials containing X_j^0 or containing $X_j^{n_j-1}$ may be different, since when evaluating at zero $X_j^0\big|_0 = 1$ but $X_j^{n_j-1}\Big|_0 = 0$. This explains the difference on the powers of the variables when equipping E with the following structure which we will assume in the sequel. When $j \in J$, we identify the set $\{0, 1, \ldots, n_j - 1\}$ of possible exponents of the variable X_j with the ring $\mathbb{Z}/n_j\mathbb{Z}$, because the identification $X_j^{n_j} - 1 = 0$ gives the identification on the exponents $n_j = 0$. Otherwise, if $j \notin J$, we have the identification $X_j^{n_j} - X_j = 0$, then we can identify the set $\{1, \ldots, n_j - 1\}$ with $\mathbb{Z}/(n_j - 1)\mathbb{Z}$, and extend the addition and multiplication in this ring to $\{0, 1, \ldots, n_j - 1\}$, by setting $0 + e = e$, $0 \cdot e = 0$ for all $e = 0, 1, \ldots, n_j - 1$. Therefore,

$$\{0, 1, \ldots, n_j - 1\} := \begin{cases} \mathbb{Z}/n_j\mathbb{Z}, & \text{when } j \in J, \\ \{0\} \cup \mathbb{Z}/(n_j - 1)\mathbb{Z}, & \text{otherwise.} \end{cases}$$

Notice that X_j^0 and $X_j^{n_j-1}$ have the same evaluation at all the elements of P_j with the exception of zero.

Our next definition generalizes that of a *cyclotomic coset*, related to minimal polynomials and cyclic codes, see for example [71]. It will allow us to obtain subfield-subcodes of J-affine variety codes with the same dimension as the code they come from.

Definition 1.5.5. With the above identification of the sets in the Cartesian product E, a set $\Omega \subseteq E$ is called *closed set* (*with respect to* p^h) if $p^h \boldsymbol{\omega} \in \Omega$ for all $\boldsymbol{\omega} = (\omega_1, \dots, \omega_m) \in \Omega$.

Minimal closed sets are those of the form

$$\Lambda = \{p^{hi}\boldsymbol{e} \mid i \geq 0\},$$

for some element $\boldsymbol{e} \in E$. Notice that closed sets are union of minimal closed sets. For each minimal closed set Λ, denote by $\boldsymbol{a}$ the minimum element in Λ with respect to the lexicographic order in $\mathbb{N}_0^m$, that we fix, and set $\Lambda = \Lambda_{\boldsymbol{a}}$ and $c_{\boldsymbol{a}} := \#\Lambda_{\boldsymbol{a}}$. Hence,

$$\Lambda_{\boldsymbol{a}} := \{\boldsymbol{a}, p^h\boldsymbol{a}, \dots, p^{h(c_{\boldsymbol{a}}-1)}\boldsymbol{a}\}.$$

Fixed an index $j \in \{1, \dots, m\}$, if we replace E by $\{0, 1, \dots, n_j - 1\}$, the same definition gives rise to sets $\Omega^j \subseteq \{0, 1, \dots, n_j - 1\}$ (respectively, $\Lambda^j \subseteq \{0, 1, \dots, n_j - 1\}$) called *closed* (respectively, *minimal closed) sets in a single variable* with respect to p^h. Again, denoting by a the minimum element in Λ^j, we set $\Lambda^j = \Lambda^j_a$.

Example 1.5.6. Assume that: (1) the number of variables is $m = 3$; (2) the field is $\mathbb{F}_8$ and we consider its subfield $\mathbb{F}_2$, so $p = 2$, $h = 1$, $l = 3$; (3) in each variable, the polynomials are evaluated at all the elements in $\mathbb{F}_8$, thus $J = \varnothing$, $n_1 = n_2 = n_3 = 8$; and (4) we pick the exponent $\boldsymbol{a} = (1, 4, 5)$. Then, the set of possible exponents $E = \{0, 1, \dots, 7\}^3$ has the same structure as $(\{0\} \cup \mathbb{Z}/7\mathbb{Z})^3$. The minimal closed set of $\boldsymbol{a}$ with respect to 2 is obtained from $\boldsymbol{a}$ by succesive multiplications by 2 in each variable taking into account the identification $8 = 1$, and it equals $\Lambda_{\boldsymbol{a}} = \{(1, 4, 5), (2, 1, 3), (4, 2, 6)\} \subseteq E$. The corresponding minimal closed set in a single variable for $j = 3$ is the set $\Lambda_3^j = \{3, 5, 6\} \subseteq \{0, 1, \dots, 7\}$. It is constructed like $\Lambda_{\boldsymbol{a}}$ but considering only the third coordinate of the exponents, where $\{0, 1, \dots, 7\}$ is identified with $\{0\} \cup \mathbb{Z}/7\mathbb{Z}$.

In addition, minimal closed sets constitute a partition of E. Let us denote

$$\mathcal{A} := \{\boldsymbol{a}_0 < \boldsymbol{a}_1 < \cdots < \boldsymbol{a}_\nu\} \subseteq E$$

the ordered set of minimum elements of all minimal closed sets. Then,

$$E = \bigcup_{\boldsymbol{a} \in \mathcal{A}} \Lambda_{\boldsymbol{a}}.$$

For any set $\Delta \subseteq E$, we define $\mathcal{A}(\Delta) = \{\boldsymbol{a} \in \mathcal{A} \mid \Lambda_{\boldsymbol{a}} \subseteq \Delta\}$. We end by defining a last trace type map. For an $\boldsymbol{a} \in \mathcal{A}$, let

$$\mathcal{T}_{\boldsymbol{a}} := \mathcal{T}^h_{\boldsymbol{a}} : \mathcal{R} \to \mathcal{R}, \quad \mathcal{T}_{\boldsymbol{a}}(f) = f + f^{p^h} + \cdots + f^{p^{h(c_{\boldsymbol{a}}-1)}}.$$

Now we are ready to state the main result of this subsection [47, Theorem 2.3], [43, Theorem 4].

Theorem 1.5.7. *Keep the above notation. Let Δ be a subset of E. For every $\boldsymbol{a} \in \mathcal{A}(\Delta)$, let $\xi_{\boldsymbol{a}}$ be a primitive element of $\mathbb{F}_{p^{hc_{\boldsymbol{a}}}}$. Then, the set*

$$\bigcup_{\boldsymbol{a}\in\mathcal{A}(\Delta)} \left\{ \mathrm{ev}_P\left(\mathcal{T}_{\boldsymbol{a}}\left(\xi_{\boldsymbol{a}}^k \boldsymbol{X}^{\boldsymbol{a}}\right)\right) \mid 0 \le k \le c_{\boldsymbol{a}} - 1 \right\}$$

is a basis of the subfield-subcode over $\mathbb{F}_{p^h}$, $\mathcal{S}_{\Delta}^{P,J}$. In particular

$$\dim\left(\mathcal{S}_{\Delta}^{P,J}\right) = \sum_{\boldsymbol{a}\in\mathcal{A}(\Delta)} c_{\boldsymbol{a}}$$

and, if Δ is closed, then $\dim\left(\mathcal{S}_{\Delta}^{P,J}\right) = \dim\left(\mathcal{C}_{\Delta}^{P,J}\right) = \#\Delta$.

Proof. We are going to prove that the set

$$S := \bigcup_{\boldsymbol{a}\in\mathcal{A}} \left\{ \mathcal{T}_{\boldsymbol{a}}\left(\xi_{\boldsymbol{a}}^k \boldsymbol{X}^{\boldsymbol{a}}\right) \mid 0 \le k \le c_{\boldsymbol{a}} - 1 \right\}$$

constitutes a basis of the vector space over $\mathbb{F}_{p^h}$ of elements in $\mathcal{R}$ evaluating to $\mathbb{F}_{p^h}$. Then, the facts

$$\mathcal{S}_{\Delta}^{P,J} = \{\mathrm{ev}_P(f) \mid f \in \langle S \rangle, \mathrm{supp}(f) \subseteq \Delta\},$$

for every $\boldsymbol{a} \in \mathcal{A}$ and $k \in \{0, \ldots, c_{\boldsymbol{a}} - 1\}$, $\mathrm{supp}\left(\mathcal{T}_{\boldsymbol{a}}\left(\xi_{\boldsymbol{a}}^k \boldsymbol{X}^{\boldsymbol{a}}\right)\right) = \Lambda_{\boldsymbol{a}}$, and the map ev_P is linear imply that the set given in the statement of the theorem is a basis of $\mathcal{S}_{\Delta}^{P,J}$. The statements on the dimension are straightforward. Let us prove our first statement on S at the beginning of the proof.

Let us start by proving that S generates the vector space over $\mathbb{F}_{p^h}$ of elements $f \in \mathcal{R}$ evaluating to $\mathbb{F}_{p^h}$. Recall that the polynomials we are using to represent classes in $\mathcal{R}$ are representatives modulo I. First, let us see that when $\mathrm{supp}(f) \subseteq \Lambda_{\boldsymbol{a}}$ for some $\boldsymbol{a} \in \mathcal{A}$, then $f \in \left\langle \mathcal{T}_{\boldsymbol{a}}\left(\xi_{\boldsymbol{a}}^k \boldsymbol{X}^{\boldsymbol{a}}\right) \mid 0 \le k \le c_{\boldsymbol{a}} - 1 \right\rangle$. Indeed, since $f^{p^h} = f$, there exists some $\alpha \in \mathbb{F}_{p^l}$ such that $f = \sum_{s=0}^{c_{\boldsymbol{a}}-1} (\alpha \boldsymbol{X}^{\boldsymbol{a}})^{p^{hs}}$. The fact that $\alpha^{p^{hc_{\boldsymbol{a}}}} = \alpha$ implies $\alpha \in \mathbb{F}_{p^{hc_{\boldsymbol{a}}}}$. Then, $\alpha = \sum_{k=0}^{c_{\boldsymbol{a}}-1} \beta_k \xi_{\boldsymbol{a}}^k$, with $\beta_k \in \mathbb{F}_{p^h}$ for all k since $\{1, \xi_{\boldsymbol{a}}, \ldots, \xi_{\boldsymbol{a}}^{c_{\boldsymbol{a}}-1}\}$ is a basis of $\mathbb{F}_{p^{hc_{\boldsymbol{a}}}}$ over $\mathbb{F}_{p^h}$. Therefore,

$$\begin{aligned} f &= \sum_{s=0}^{c_{\boldsymbol{a}}-1} \alpha^{p^{hs}} \boldsymbol{X}^{p^{hs}\boldsymbol{a}} = \sum_{s=0}^{c_{\boldsymbol{a}}-1} \left(\sum_{k=0}^{c_{\boldsymbol{a}}-1} \beta_k \xi_{\boldsymbol{a}}^k \right)^{p^{hs}} \boldsymbol{X}^{p^{hs}\boldsymbol{a}} \\ &= \sum_{k=0}^{c_{\boldsymbol{a}}-1} \beta_k \left(\sum_{s=0}^{c_{\boldsymbol{a}}-1} \xi_{\boldsymbol{a}}^{kp^{hs}} \boldsymbol{X}^{p^{hs}\boldsymbol{a}} \right) = \sum_{k=0}^{c_{\boldsymbol{a}}-1} \beta_k \mathcal{T}_{\boldsymbol{a}}\left(\xi_{\boldsymbol{a}}^k \boldsymbol{X}^{\boldsymbol{a}}\right). \end{aligned}$$

Now, assume that f is a general element in $\mathcal{R}$ evaluating to $\mathbb{F}_{p^h}$ and suppose that $\boldsymbol{X}^{\boldsymbol{a}_1}$ is the monomial in f with smallest exponent with respect to the lexicographic order. Then, by the above discussion, $\mathcal{T}_{\boldsymbol{a}_1}\left(\xi_{\boldsymbol{a}_1}^{k_1} \boldsymbol{X}^{\boldsymbol{a}_1}\right)$, for some $k_1 \in \{0, \ldots, c_{\boldsymbol{a}_1} - 1\}$, must appear in f because it evaluates to $\mathbb{F}_{p^h}$. Since $\xi_{\boldsymbol{a}_1}^{k_1} \boldsymbol{X}^{\boldsymbol{a}_1}$ is the term in f with smallest exponent, then $\boldsymbol{a}_1 \in \mathcal{A}$. Let $f_1 = f - \mathcal{T}_{\boldsymbol{a}_1}\left(\xi_{\boldsymbol{a}_1}^{k_1} \boldsymbol{X}^{\boldsymbol{a}_1}\right)$ and let $\xi_{\boldsymbol{a}_2}^{k_2} \boldsymbol{X}^{\boldsymbol{a}_2}$ be the term in f_1 with smallest exponent. Again, $\mathcal{T}_{\boldsymbol{a}_2}\left(\xi_{\boldsymbol{a}_2}^{k_2} \boldsymbol{X}^{\boldsymbol{a}_2}\right)$ must appear in f_1 and $\boldsymbol{a}_2 \in \mathcal{A}$. We can then pick $f_2 = f_1 - \mathcal{T}_{\boldsymbol{a}_2}\left(\xi_{\boldsymbol{a}_2}^{k_2} \boldsymbol{X}^{\boldsymbol{a}_2}\right)$ and repeat this procedure, that will finish in a finite number of steps, to obtain the desired expression of f as a linear combination of elements in S.

It remains to prove that those elements in S are linearly independent. Indeed, this holds for elements in S supported on different minimal closed sets because they contain

different monomials. For elements supported on the same minimal closed set $\Lambda_{\boldsymbol{a}}$, $\boldsymbol{a} \in \mathcal{A}$, we reason by contradiction. If $\sum_{k=0}^{c_{\boldsymbol{a}}-1} \beta_k \mathcal{T}_{\boldsymbol{a}}\left(\xi_{\boldsymbol{a}}^k \boldsymbol{X}^{\boldsymbol{a}}\right) = 0$ with $\beta_k \in \mathbb{F}_{p^h}$ for all k, then the coefficient of $\boldsymbol{X}^{\boldsymbol{a}}$ in such expression is $\beta_0 + \beta_1 \xi_{\boldsymbol{a}} + \cdots + \beta_{c_{\boldsymbol{a}}-1} \xi_{\boldsymbol{a}}^{c_{\boldsymbol{a}}-1}$ and it must vanish. This contradicts the fact that the minimal polynomial of $\xi_{\boldsymbol{a}}$ has degree $c_{\boldsymbol{a}}$. □

The next result will be useful for studying LRCs. It shows that, when Δ is closed, the operators on a J-affine variety code "taking its projection" and "taking its subfield-subcode" commute. Recall, from Section 1.4, that the projection map $\mathbb{F}_Q^n \to \mathbb{F}_Q^r$ on the coordinates of a subset $R \subseteq \{1, \ldots, n\}$ of cardinality r is denoted by π_R.

Proposition 1.5.8. *With the above notation, let $R \subseteq \{1, \ldots, n\}$. If $\Delta \subseteq E$ is closed, then $\pi_R\left(\mathcal{S}_\Delta^{P,J}\right) = \pi_R\left(\mathcal{C}_\Delta^{P,J}\right) \cap \mathbb{F}_{p^h}^{\#R}$.*

Proof. First we prove that $\mathcal{S}_\Delta^{P,J} = \mathbf{tr}\left(\mathcal{C}_\Delta^{P,J}\right)$. By Proposition 1.5.4, the following chain of equalities holds:

$$\begin{aligned} \mathbf{tr}\left(\mathcal{C}_\Delta^{P,J}\right) &= \left\{\mathbf{tr}(\boldsymbol{c}) \mid \boldsymbol{c} \in \mathcal{C}_\Delta^{P,J}\right\} = \{\mathbf{tr}(\mathrm{ev}_P(f)) \mid f \in \mathcal{R},\, \mathrm{supp}(f) \subseteq \Delta\} \\ &= \{\mathrm{ev}_P(\mathcal{T}(f)) \mid f \in \mathcal{R},\, \mathrm{supp}(f) \subseteq \Delta\} \\ &= \{\mathrm{ev}_P(\mathcal{T}(f)) \mid f \in \mathcal{R},\, \mathrm{supp}(\mathcal{T}(f)) \subseteq \Delta\} = \mathcal{S}_\Delta^{P,J}. \end{aligned} \tag{1.5.1}$$

Notice that the last but one equality is true because Δ is closed. Now define

$$\mathbf{tr}' : \mathbb{F}_{p^l}^{\#R} \to \mathbb{F}_{p^h}^{\#R},$$

determined by tr_l^h componentwise. Then,

$$\pi_R\left(\mathcal{C}_\Delta^{P,J}\right) \cap \mathbb{F}_{p^h}^{\#R} = \mathbf{tr}'\left(\pi_R\left(\mathcal{C}_\Delta^{P,J}\right)\right).$$

Finally consider any element in $\mathcal{S}_\Delta^{P,J}$, $\mathbf{tr}(\boldsymbol{c})$, $\boldsymbol{c} \in \mathcal{C}_\Delta^{P,J}$. Then, the fact that the maps $\mathbf{tr}$ and $\mathbf{tr}'$ are defined componentwise implies $\pi_R(\mathbf{tr}(\boldsymbol{c})) = \mathbf{tr}'(\pi_R(\boldsymbol{c}))$, which proves the result. □

We conclude this chapter with a result for the case when $m = 1$, $J = \{1\}$ and Δ is a union of minimal closed sets whose representatives are consecutive and start at the smallest one. We show that we can bound the minimum distance of the dual of the subfield-subcode by considering the BCH approach.

Proposition 1.5.9. *Keep the above notation, particularly that around Example 1.5.6. Assume that $m = 1$ and $J = \{1\}$. Let τ be a positive integer such that $\tau < \nu$ and let*

$$\Delta = \Lambda_{a_0} \cup \Lambda_{a_1} \cup \cdots \cup \Lambda_{a_\tau} \subseteq E.$$

Then,

$$\mathrm{d}\left(\left(\mathcal{S}_\Delta^{P,J}\right)^\perp\right) \geq a_{\tau+1} + 1.$$

Proof. First, notice that

$$\mathrm{d}\left(\left(\mathcal{C}_{\Delta}^{P,J}\right)^{\perp}\right) \geq a_{\tau+1}+1$$

by Proposition 1.2.8, since Δ contains $a_{\tau+1}$ consecutive elements ($a_0 = 0$, $a_1 = 1$, $\ldots$, $a_{\tau+1}-1$) and a parity-check matrix of $\left(\mathcal{C}_{\Delta}^{P,J}\right)^{\perp}$ contains a Vandermonde matrix of rank $a_{\tau+1}$. Setting $n := n_1$, $\alpha \in \mathbb{F}_Q$ a primitive n-th root of unity and

$$\Delta^{\perp} := \{0,1,\ldots,n-1\}\backslash\{n-e \mid e \in \Delta\},$$

where each element before represents a class in $\mathbb{Z}/n\mathbb{Z}$, it holds that $\left(\mathcal{C}_{\Delta}^{P,J}\right)^{\perp} = \mathcal{C}_{\Delta^{\perp}}^{P,J}$ because for any e, $e' \in \{0,1,\ldots,n-1\}$, we have

$$\mathrm{ev}_P(X^e) \cdot_e \mathrm{ev}_P(X^{e'}) = \sum_{i=0}^{n-1} \alpha^{i(e+e')} = 0$$

if and only if $e + e' \not\equiv 0 \mod n$. Notice that $\Delta^{\perp}$ is closed because Δ so is. Then, Theorem 1.5.3 and Equalities (1.5.1) in Proposition 1.5.8 prove

$$\left(\mathcal{S}_{\Delta}^{P,J}\right)^{\perp} = \mathbf{tr}_l^h\left(\left(\mathcal{C}_{\Delta}^{P,J}\right)^{\perp}\right) = \mathbf{tr}_l^h\left(\mathcal{C}_{\Delta^{\perp}}^{P,J}\right) = \mathcal{S}_{\Delta^{\perp}}^{P,J}.$$

Therefore, the fact that $\mathcal{S}_{\Delta^{\perp}}^{P,J} \subseteq \mathcal{C}_{\Delta^{\perp}}^{P,J}$ implies

$$\mathrm{d}\left(\left(\mathcal{S}_{\Delta}^{P,J}\right)^{\perp}\right) \geq \mathrm{d}\left(\mathcal{C}_{\Delta^{\perp}}^{P,J}\right) \geq a_{\tau+1}+1,$$

which concludes the proof. □

Chapter 2

Quantum error-correcting codes

The second chapter in Part I introduces quantum error-correcting codes, we will construct codes of this type in Chapters 4 and 5 of Part III of this thesis. Our quantum codes are always stabilizer ones and thus the most relevant section of this chapter is Section 2.3. For completeness we give an overall idea of the basics of quantum mechanics with the aim that the construction and properties of these codes become understandable. A substantial part of the results and notation of this chapter will not be used in what remains. We only desire to give a fast-reading introduction of the underlying matter. The main references for this chapter are [104, 65, 58, 75, 10, 57, 73, 6].

Some companies affirm to have primitive quantum computers and the simple existence of the Shor algorithm of factorization of positive integers on a quantum computer in a polynomial time [113], breaking the RSA public-key system, shows the huge potential of this computers.

However there is a big difference between classical and quantum computers. For a start a (classical) bit only has the states 0 or 1, but the quantum bit (or *qubit*, for short) can be in a superposition of these states. Moreover, when considering multiple qubits, there exist *entangled* states; they are those that cannot be written as the product of the states of each single qubit. Additionally, quantum computers are more prone to errors compared to modern classical digital computers. This susceptibility is due to the delicate and challenging nature of controlling quantum mechanical systems. Classical error-correction techniques rely on the assumption that all bits in a computer can be measured and this cannot be directly applied to quantum computers. In classical digital computers, to prevent small errors from accumulating into larger ones, the hardware resets the bit to the nearer value of 0 or 1 at each time step. However, this approach cannot be employed in quantum computers because entangled states would be disrupted if a continuous measurement of each qubit was made. Classical error-correction techniques to correct sequences of bits cannot neither be similarly applied on quantum codes. Furthermore, unlike classical, quantum information is unclonable [128].

Thus, quantum error-correcting codes demand a somewhat different approach. The first quantum error-correcting codes were discovered by Shor [112] and Steane [118]. We will work with the widely used class of stabilizer codes.

First we introduce some basics of quantum mechanics to understand the setting of quantum codes.

2.1. A basic introduction to quantum mechanics

Quantum mechanics serves as a framework to describe the laws governing a physical system. This theory was formulated in the period 1925–1926 supported in the works of Heisenberg, Schrödinger, and Born. It emerged in response to a series of experiments that aimed at reconsidering the existing physical theories. They gave rise to new concepts such as the wave-particle duality and the probabilistic behavior of particles, making the principles of quantum mechanics seem counterintuitive.

According to these experiments, every particle is associated with a wave function that determines the probability of finding the particle in a certain position, but this wave function behavior cannot be observed directly on the particle because everytime one examines its position, it does not change. This behavior is exhibited, for example, in the double-slit experiment.

Wave functions can be understood as elements in a Hilbert space, where the tools of linear algebra can be applied. A wave function corresponds to a complex-valued function which indicate the probabilities of the system to be in a certain basis state. This function evolves in continuous time as a wave function by the Schrödinger equation, from which the discrete time version given in Postulate 2 is derived.

Next we present the basic postulates of quantum mechanics, which provide a connection between the physical world and its mathematical formalism.

2.1.1. Postulates of quantum mechanics

We follow [104, 65] for stating the postulates of quantum mechanics.

The first postulate establishes how to describe the system under analysis. We understand by system a portion of the physical universe chosen for study in such a way that everything outside that portion is regarded as external to the system, and its effects are not taken into consideration.

Postulate 1: State space *Associated to any isolated physical system there is a complex vector space with inner product (a Hilbert space) known as the "state space" of the system. The system is completely described, at a fixed time, by its "state vector", which is a unit vector in the system's state space.*

In quantum mechanics we work with complex finite-dimensional Hilbert spaces, denoted $H = \mathbb{C}^r$, $1 \leq r \in \mathbb{N}$, and we use the bra-ket notation for the quantum states, introduced by Paul Dirac in 1958. In quantum mechanics, a column vector in the Hilbert space is denoted by $|v\rangle \in H$; an inner product of two vectors $|v\rangle, |w\rangle \in H$ is written $\langle v \,|\, w\rangle$, the conjugate of $z \in \mathbb{C}$ is denoted by z^* and the modulus of z is denoted by $|z|$.

Recall that an inner product on H is a map $\langle \cdot \,|\, \cdot \rangle : H \times H \to \mathbb{C}$ such that it is:

- Conjugate linear on the left: $\langle c_1 v_1 + c_2 v_2 \,|\, w\rangle = c_1^* \langle v_1 \,|\, w\rangle + c_2^* \langle v_2 \,|\, w\rangle$, for all $c_1, c_2 \in \mathbb{C}$, $v_1, v_2, w \in H$;
- Linear on the right: $\langle v \,|\, c_1 w_1 + c_2 w_2\rangle = c_1 \langle v \,|\, w_1\rangle + c_2 \langle v \,|\, w_2\rangle$, for all $c_1, c_2 \in \mathbb{C}$, $v, w_1, w_2 \in H$;
- Hermitian: $\langle v \,|\, w\rangle = \langle w \,|\, v\rangle^*$, for all $v, w \in H$;
- Positive definite: $\langle v \,|\, v\rangle \in \mathbb{R}$ with $\langle v \,|\, v\rangle \geq 0$, and $\langle v \,|\, v\rangle = 0$ if and only if $v = 0$, for all $v \in H$.

The bra-ket notation is related with the inner product. Given a vector or *ket* $|v\rangle$, its *bra* $\langle v|$ is defined as its conjugate transpose. An inner product of $|v\rangle = (v_1, \ldots, v_r)^\top$ and $|w\rangle = (w_1, \ldots, w_r)^\top$, with coordinates in an orthonormal basis, is the following:

$$\langle v \,|\, w\rangle := \langle v || w\rangle = (v_1^*, \ldots, v_r^*)(w_1, \ldots, w_r)^\top := v_1^* w_1 + \cdots + v_r^* w_r.$$

Quantum mechanics does not specify the state space nor the system's state vector. An interpretation derived from Postulate 1 is that quantum systems have a probabilistic nature. Denoting by $\{|e_i\rangle \mid i = 1, \ldots, r\}$ an orthonormal basis of H, state vectors are unit vectors ($|v\rangle$ such that $\langle v \,|\, v\rangle = 1$), and they satisfy

$$|v\rangle = \sum_{i=1}^{r} v_i |e_i\rangle, \quad v_i \in \mathbb{C}, \quad \sum_{i=1}^{r} v_i^* v_i = 1.$$

It indicates that the system is in the state $|e_i\rangle$ with probability $|v_i|^2 = v_i^* v_i$, $i = 1, \ldots, r$. When some $v_i \neq 1$ it is also said that the system is in a *superposition* of states. Taking the atom model as an example, $r = 2$ and the electron can be in the *ground* or *excited* state, which we denote by $|0\rangle$ and $|1\rangle$, respectively, see Figure 2.1. By shining light on the atom, it is possible to move the electron from one state to the other and even into the state $|+\rangle := \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$.

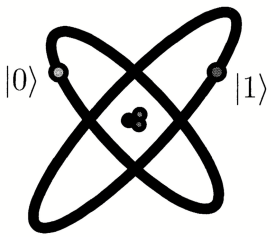


Figure 2.1: Instance of the qubit as two states of an electron orbiting an atom [104]

The second postulate describes the evolution of the system as time evolves, prescribing the change of state.

Postulate 2: Evolution *The evolution of a closed quantum system is described by a unitary transformation. That is, the state $|v\rangle$ of the system at time t_1 is related to the*

state $|v'\rangle$ *of the system at time* t_2 *by a unitary operator* U *which depends only on the times* t_1 *and* t_2,

$$|v'\rangle = U|v\rangle.$$

Again, quantum mechanics only assures that one can describe the evolution of such a system in that way, without specifying which unitary operators U represent quantum dynamics.

Next we recall the definition of unitary operator. Let A be an operator, i.e., endomorphism A of H. Usually, we denote $|Av\rangle := A|v\rangle$.

Definition 2.1.1. Let A be an operator of H. The *adjoint* or (*Hermitian*) *conjugate* operator of A, denoted by $A^\dagger$, is the unique [7] operator $A^\dagger$ of H such that, for all $|v\rangle, |w\rangle \in H$,

$$\langle v \,|\, Aw\rangle = \langle A^\dagger v \,|\, w\rangle.$$

An operator A is called *Hermitian* or *self-adjoint* if $A^\dagger = A$.

The associated matrix $A^\dagger$ to the adjoint operator is constructed by conjugating the entries and transposing the associated matrix A of the operator, i.e., $A^\dagger = (A^*)^\top$. As said, for a vector $|v\rangle \in H$, $|v\rangle^\dagger = \langle v|$. A matrix has real eigenvalues iff it is Hermitian. Moreover, if A is Hermitian, there exists an orthonormal basis of H consisting of eigenvectors of A, so A is diagonalizable. Indeed, this result is more general, and holds for normal operators [66, Section 8.5, Theorem 22]. An operator A of H is called *normal* if $AA^\dagger = A^\dagger A$. Clearly, Hermitian operators are normal.

A normal (or, particularly, Hermitian) operator A can be written as a linear combination of pairwise orthogonal projections (to the eigenspaces) whose coefficients are the corresponding eigenvalues. This linear combination is called the *spectral decomposition* of A [66, Section 9.5, Theorem 9]. Given a subspace V of H with orthonormal basis $\{|e_i'\rangle \mid i = 1, \ldots, r'\}$, the projection onto V is the following Hermitian operator:

$$P := P_V : H \to V, \quad |v\rangle \mapsto \sum_{i=1}^{r'} \langle e_i' \,|\, v\rangle |e_i'\rangle.$$

Two projections are said to be orthogonal whenever their images are orthogonal spaces. The projection onto the orthogonal complement of V, $V^\perp$, is the operator $P^\perp := I - P$, where I denotes the identity.

Definition 2.1.2. An operator U of H is called *unitary* if $U^\dagger U = UU^\dagger = I$.

Equivalently, the associated matrices to the operators (with respect to some basis of H) satisfy the above condition. Unitary operators are normal and preserve inner products, that is, given $|v\rangle, |w\rangle \in H$,

$$\langle Uv \,|\, Uw\rangle = \langle U^\dagger U v \,|\, w\rangle = \langle v \,|\, w\rangle,$$

by definition of adjoint operator. In quantum mechanics, unitary operators produce change of basis and map orthonormal bases to orthonormal bases. Notice that applying unitary operators on H does not contradict Postulate 2.

The subsequent postulate addresses the influence of an external entity on the system itself, particularly the outcome of measuring the system, that is, extracting information from it. An observable refers to any measurable property of a system. Here, we present a restrictive version of the third postulate, which employs projective measurements (a specific instance of the general postulate) because it is commonly used in quantum computing. This version emphasizes that the measurement device should possess "favourite" states forming an orthonormal basis in the state space, and the result of the measurement will be one of these designated "favourite" states. As a consequence of this postulate, in quantum mechanics one cannot directly observe the state vector of a system, since it will generally change as a result of the invasive character of the measurement.

Postulate 3: Measurement *A projective measurement is described by an observable, M, a Hermitian operator on H. Thus, this operator has a spectral descomposition*

$$M = \sum_m m P_m,$$

where m denotes the eigenvalues of the operator M and P_m denotes the projection on the eigenspace of eigenvalue m. The possible results of the measurement correspond to the eigenvalues m of the observable M. If the system is in state $|v\rangle$ just before the measurement, the probability of obtaining the result m is

$$\langle v|P_m|v\rangle$$

and the state of the system after the measurement will be

$$\frac{P_m|v\rangle}{\sqrt{\langle v|P_m|v\rangle}}.$$

We conclude this section by stating the last postulate which describes the state space of a quantum system composed by several different physical systems.

Postulate 4: Composite systems *The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. Moreover, if we have systems numbered 1 through n, and system number i is prepared in the state $|v_i\rangle$, then the joint state of the total system is $|v_1\rangle \otimes \cdots \otimes |v_n\rangle$.*

For example, given two quantum systems of state spaces $H_1 = \mathbb{C}^{r_1}$, $H_2 = \mathbb{C}^{r_2}$, with respective bases

$$\{|e_i\rangle \mid i = 1, \ldots, r_1\}, \quad \{|e'_j\rangle \mid j = 1, \ldots, r_2\},$$

there is an isomorphism of vector spaces between $\mathbb{C}^{r_1} \otimes \mathbb{C}^{r_2}$ and $\mathbb{C}^{r_1 r_2}$, and a basis of $\mathbb{C}^{r_1} \otimes \mathbb{C}^{r_2}$ is

$$\{|e_i\rangle \otimes |e'_j\rangle \mid i = 1, \ldots, r_1,\ j = 1, \ldots, r_2\}.$$

Then an element in $H_1 \otimes H_2$ is written as

$$|\boldsymbol{v}\rangle = \sum_{i,j} a_{ij} |e_i\rangle \otimes |e'_j\rangle,$$

where $a_{ij} \in \mathbb{C}$. If A and B are operators of H_1 and H_2 respectively, we can define the operator $A \otimes B$ of $H_1 \otimes H_2$ as

$$A \otimes B\left(\sum_{i,j} a_{ij}|e_i\rangle \otimes |e'_j\rangle\right) = \sum_{i,j} a_{ij} A|e_i\rangle \otimes B|e'_j\rangle.$$

An inner product on $H_1 \otimes H_2$ can be derived from inner products on H_1 and H_2 as follows. Consider

$$|\boldsymbol{w}\rangle = \sum_{k,l} b_{kl}|e_k\rangle \otimes |e'_l\rangle$$

in $H_1 \otimes H_2$ and then

$$\langle \boldsymbol{v} \,|\, \boldsymbol{w}\rangle = \sum_{i,j,k,l} a^*_{ij} b_{kl} \langle e_i \,|\, e_k\rangle \langle e'_j \,|\, e'_l\rangle.$$

A quantum state $|\boldsymbol{v}\rangle$ in a composite system that cannot be descomposed as a product $|\boldsymbol{v}\rangle = |v_1\rangle \otimes \cdots \otimes |v_n\rangle$ of states of the component systems is called an *entangled* state. Otherwise, it is called a *separable* state. For instance, an entangled state is the two qubit state

$$\frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle),$$

while a separable state is the two qubit state

$$\frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |0\rangle \otimes |1\rangle) = |0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle).$$

Entangled states are generally quite delicate and a measurement on one of them usually makes it collapse into a "less" entangled state. Minor interactions with the environment act as a continuous form of measurement on the system, and as the system becomes larger (the number of tensor components grows), these interactions become more difficult to ignore. Consequently, the system undergoes *decoherence* and tends to resemble a classical system, being this the cause of the classical appearance of the world at a human scale.

2.2. Quantum error-correcting codes

2.2.1. Generalities

In this subsection we briefly revise detection and correction of quantum codes. Subsection 2.2.2 introduces an error model and a specific and useful class of error-correcting codes is given in the forthcoming Section 2.3.

In classic computation, a unit of information (or bit), has only two possible states: 0 and 1. A unit of quantum information, (or quantum bit, or qubit) can be thought as a physical system of "two" states, which correspond to those of the classical bit, $|0\rangle$ and $|1\rangle$, and they form an orthonormal basis of the Hilbert space representing the qubit. Following the first postulate of quantum mechanics, a qubit's state $|v\rangle$ is a unit vector in $\mathbb{C}^2$. Thus, it is a linear combination

$$|v\rangle = v_1|0\rangle + v_2|1\rangle,$$

where $v_1, v_2 \in \mathbb{C}$ are such that $|v_1|^2+|v_2|^2 = 1$. A qubit is in a continuum of states between $|0\rangle$ and $|1\rangle$ until one observes it, getting either the result 0 with probability $|v_1|^2$ or the result 1 with probability $|v_2|^2$. The normalization ensures that the probability of getting some result is exactly 1. A quantum computer with n qubits is represented by states in the 2^n-dimensional Hilbert space $\mathbb{C}^2 \otimes \overset{n)}{\cdots} \otimes \mathbb{C}^2$.

There is ongoing work to develop quantum computers which can manipulate *qudits*, the generalization of qubits, i.e., quantum states in r-dimensional Hilbert spaces $\mathbb{C}^r$, $r \geq 2$. Here we will consider quantum error-correcting codes dealing with qudits for $r = Q$, a prime power, because it allows us to take advantage of the structure of finite fields. As in Chapter 1, we use a capital letter Q to denote the cardinality of a finite field $\mathbb{F}_Q$, that will become some power of q in the following chapters. The vectors of an orthonormal basis of $\mathbb{C}^Q$ will be denoted by the elements of $\mathbb{F}_Q$: $|x\rangle$, $x \in \mathbb{F}_Q$.

Definition 2.2.1. Set $1 \leq l, n \in \mathbb{N}$ and let Q be a prime power. A *quantum error-correcting code* (*QECC*) is a linear subspace $\mathcal{Q}$ of $\mathbb{C}^{Q^n} = \mathbb{C}^Q \otimes \overset{n)}{\cdots} \otimes \mathbb{C}^Q$.

We notice that some authors consider a more general case where a QECC is not imposed to be linear. QECCs are designed to protect quantum information from errors due to decoherence or other quantum noise, for example that produced by the faulty quantum gates. We describe the errors (also called *error operators*) by means of operators as those described in Subsection 2.1.1. We assume that errors are unitary by the argument we will give in the paragraph before Theorem 2.2.2, unless specified otherwise. Also, the encoding of quantum states into a QECC is made by means of a unitary operator.

Quantum information is rather different from classical information what makes new ideas should be introduced for error-correction. Following [104] (see also [10, 58]), three challenges have to be overcome for a reliable quantum correction:

- No cloning. Since an arbitrary quantum state cannot be cloned [128], to perform quantum error correction, unlike the classical setting, one cannot create redundancy by making copies of a quantum state.

- Measurement disturbance. In classical error-correction, in order to apply a decoding procedure, syndromes are obtained to acquire information about the error produced. However, in quantum mechanics syndromes observation alteres the quantum state.

- Errors are continuous. When manipulating classical information, errors are discrete, but in the quantum world the set of errors that may occur on a single qudit is continuous.

Thus, one desires to have a suitable syndrome measurement to diagnose the type of error occurred without knowing any information stored in the encoded state (so as not to disturb the superposition of quantum information). The idea is that when the syndromes are computed, all states in the code space $\mathcal{Q}$ remain the same and erroneous states (in

$\boldsymbol{E}\mathcal{Q}$ for errors $\boldsymbol{E}$) are changed in a way that can be reversed. Then, a unitary correction based on the syndrome ($\boldsymbol{E}^\dagger$ if $\boldsymbol{E}$ is observed) is applied with the aim of returning the erroneous state to the original state in $\mathcal{Q}$. In addition, the fact that nonorthogonal states are not distinguishable [104] leads one to think that, in order that the syndrome measurement allows us to distinguish different errors, a QECC should be defined (as a linear subspace of some larger Hilbert space) so that the different errors it is intended to detect move encoded states into orthogonal subspaces (among them) of the Hilbert space. Furthermore, these subspaces should be undeformed with respect to the code space $\mathcal{Q}$, that is, orthogonal codewords are mapped by errors into orthogonal states, and thus can be corrected. See Figure 2.2 (taken from [104]) for an illustration of this phaenomenon. The syndrome measurement works by projecting the state into one of these subspaces so that the one that is observed will determine the unitary correction applied to recover the original state.

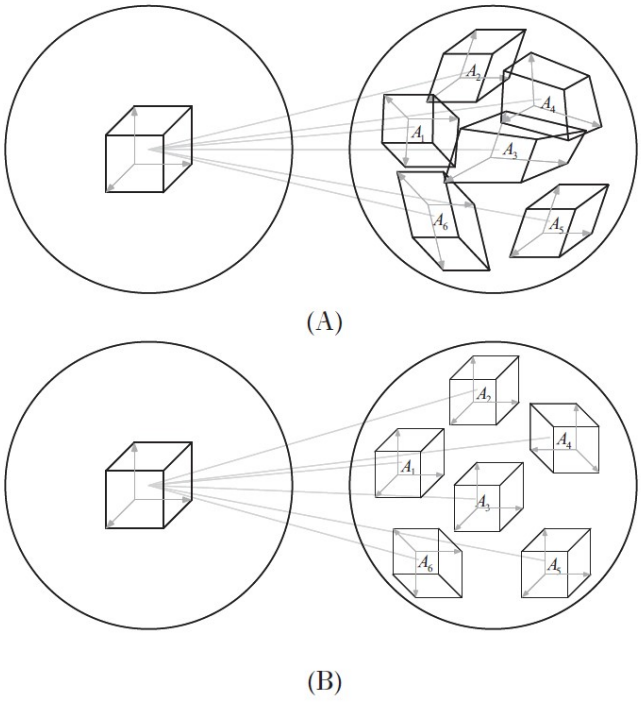


Figure 2.2: Two codes in a Hilbert space: (A) A not desired code $\mathcal{Q}$, with non-orthogonal, deformed "error" subspaces $A_i := \boldsymbol{E}_i\mathcal{Q}$; (B) A desired code, with orthogonal, undeformed subspaces [104]

The conditions discussed in the above paragraph are sufficient but not necessary for a QECC to be able to correct errors. To do it in a generic situation, the forthcoming Theorem 2.2.2 determines necessary and sufficient conditions. Next we describe the generic situation where Theorem 2.2.2 works [75]. The measurement that one applies to control whether a state is in the QECC $\mathcal{Q}$ is the pair $\boldsymbol{P}$ and $\boldsymbol{P}^\perp$ of projections onto Q and $Q^\perp$, respectively. A (non necessarily unitary) error $\boldsymbol{E}$ is said to be *detectable* by the QECC $\mathcal{Q}$ if, for all $|\boldsymbol{v}\rangle \in \mathcal{Q}$, it holds that $\boldsymbol{P}\boldsymbol{E}|\boldsymbol{v}\rangle = c_{\boldsymbol{E}}|\boldsymbol{v}\rangle$ for some $c_{\boldsymbol{E}} \in \mathbb{C}$, that is,

codewords affected by $\boldsymbol{E}$ do not change excepting to get a multiple only depending on $\boldsymbol{E}$. Other two equivalent conditions for detectability are the following:

$$\boldsymbol{PEP} = c_{\boldsymbol{E}}\boldsymbol{P}, \quad \text{for some } c_{\boldsymbol{E}} \in \mathbb{C}$$

and

$$\text{for all } |\boldsymbol{v}\rangle, |\boldsymbol{w}\rangle \in \mathcal{Q}, \quad \text{it holds that} \quad \langle \boldsymbol{v}|\boldsymbol{E}|\boldsymbol{w}\rangle = c_{\boldsymbol{E}}\langle \boldsymbol{v}\,|\,\boldsymbol{w}\rangle, \quad \text{for some } c_{\boldsymbol{E}} \in \mathbb{C}.$$

A set $\mathcal{E}$ of (non necessarily unitary) error operators is said to be *correctable* by the QECC $\mathcal{Q}$ if there exists a decoding procedure for $\mathcal{E}$. Notice that this definition involves a set of errors, while that of detectability only considers individual errors. This is because one must be able to distinguish among the errors to determine which one ocurred and therefore correct it.

Next we give a characterization of the sets $\mathcal{E} = \{\boldsymbol{E}_\gamma\}_{\gamma\geq 1}$ of error operators that are correctable. A necessary and sufficient condition for $\mathcal{E}$ to be correctable is the existence of a linear transformation of the set $\mathcal{E}$ such that the images $\boldsymbol{E}'_\gamma$ of $\boldsymbol{E}_\gamma$ satisfy two properties. First, the spaces $\boldsymbol{E}'_\gamma\mathcal{Q}$ are orthogonal between them and second, the restriction of $\boldsymbol{E}'_\gamma$ to $\mathcal{Q}$ is a scalar multiple of the restriction to $\mathcal{Q}$ of a unitary operator. Moreover, this characterization implies (i) each restriction of $\left(\boldsymbol{E}'_\gamma\right)^\dagger \boldsymbol{E}'_\gamma$ to $\mathcal{Q}$ is a scalar multiple to the identity operator on $\mathcal{Q}$ and (ii) the spaces $\left(\boldsymbol{E}'_\mu\right)^\dagger \boldsymbol{E}'_\gamma\mathcal{Q}$, $\mu \neq \gamma$, and $\mathcal{Q}$ are orthogonal. This means that the errors $\left(\boldsymbol{E}'_\mu\right)^\dagger \boldsymbol{E}'_\gamma$ are detectable, and the fact that detectability is preserved under linear combinations provide conditions of correctability of $\mathcal{E}$ which we state in the following Theorem 2.2.2. They were found by Knill and Laflamme [74] and by Bennett et al. [14]. Here we give a similar statement to [10, Theorem 1.5], an equivalent one can be found in [75, Theorem 7] or [104, Theorem 10.1].

Theorem 2.2.2 (Knill-Laflamme conditions)**.** *A QECC $\mathcal{Q}$ is able to correct a set $\mathcal{E}$ of (non necessarily unitary) error operators if and only if for all $|\boldsymbol{v}\rangle, |\boldsymbol{w}\rangle \in \mathcal{Q}$ and $\boldsymbol{E}_\mu, \boldsymbol{E}_\gamma \in \mathcal{E}$, it holds that*

$$\left\langle \boldsymbol{v}\middle|\boldsymbol{E}_\mu^\dagger \boldsymbol{E}_\gamma\middle|\boldsymbol{w}\right\rangle = c_{\mu\gamma}\langle \boldsymbol{v}\,|\,\boldsymbol{w}\rangle,$$

for some $c_{\mu\gamma} \in \mathbb{C}$.

The situation discussed in the paragraph before Figure 2.2 (orthogonal error subspaces and orthogonality preservation by errors) corresponds to the particular cases in Theorem 2.2.2 where $c_{\mu\gamma} = 0$ for all indices $\mu \neq \gamma$ and when $\langle \boldsymbol{v}\,|\,\boldsymbol{w}\rangle = 0$. However, Knill-Laflamme conditions leave room for the case where two different errors have the same effect on the code $\mathcal{Q}$. That is, these conditions do not impose that different errors map the same codeword to different subspaces. This fact is allowed by the superposition principle of quantum mechanics but it cannot occur in classical error-correction. Let us complete this information. Let $\boldsymbol{E}_\mu, \boldsymbol{E}_\gamma \in \mathcal{E}$ be different errors such that $\boldsymbol{E}_\mu\mathcal{Q}$ and $\boldsymbol{E}_\gamma\mathcal{Q}$ are not orthogonal. Suppose that a codeword $|\boldsymbol{v}\rangle \in \mathcal{Q}$ was affected by $\boldsymbol{E}_\mu$, so let $|\boldsymbol{v}'\rangle = \boldsymbol{E}_\mu|\boldsymbol{v}\rangle$, but we measure whether $|\boldsymbol{v}'\rangle$ is in $\boldsymbol{E}_\gamma\mathcal{Q}$, in order to determine if $|\boldsymbol{v}\rangle$ was instead affected by $\boldsymbol{E}_\gamma$. This would disturb $|\boldsymbol{v}'\rangle$ unless $|\boldsymbol{v}'\rangle$ collapsed to the state $\boldsymbol{E}_\gamma|\boldsymbol{v}\rangle$ (that is, $c_{\mu\gamma} \neq 0$), and in this case $|\boldsymbol{v}'\rangle$ can be corrected as though $\boldsymbol{E}_\gamma$ had happened.

2.2.2. A quantum error model

In this subsection, we show an error model to represent errors acting locally on a quantum system. Other equivalent definitions can be provided, we follow the approach of the seminal paper [73]. We will work under the scenario that noise affects qudits independently, since it is often a good approximation, although there are errors which cannot be described by a product of errors in individual qudits.

We also notice an important fact concerning the third challenge indicated in pg 51. Despite the set of quantum errors is continuous, it can be discretized. Then, to correct all the continuum of errors that may occur on a single qudit it is enough to correct the discrete subset of errors that span the continuum. This is a consequence of the linearity of quantum mechanics [60, Theorem 2], [82].

The following notations and results will be used in the next subsection devoted to stabilizer codes. Recall that Q is a power of a prime p and that, in Section 1.5, we denoted by $\mathrm{tr}_l^1 =: \mathrm{tr}$ the trace map from the extension field $\mathbb{F}_Q$ to the prime field $\mathbb{F}_p$. Set $\omega := e^{\frac{2\pi i}{p}} \in \mathbb{C}$. As mentioned before, $\{|x\rangle \mid x \in \mathbb{F}_Q\}$ denotes an orthonormal basis of $\mathbb{C}^Q$.

Let $a, b \in \mathbb{F}_Q$. We define the unitary error operators on $\mathbb{C}^Q$ (in a single qudit) that correspond, respectively, with qudit flip and phase shift errors:

$$X(a) : \mathbb{C}^Q \to \mathbb{C}^Q, \quad X(a)|x\rangle = |x + a\rangle,$$

and

$$Z(b) : \mathbb{C}^Q \to \mathbb{C}^Q, \quad Z(b)|x\rangle = \omega^{\mathrm{tr}(bx)}|x\rangle.$$

We define the set of (unitary) error operators on $\mathbb{C}^Q$ as

$$\mathcal{E}_1 := \{X(a)Z(b) \mid a, b \in \mathbb{F}_Q\}.$$

Regarding the elements in $\mathcal{E}_1$ as matrices in the mentioned basis, it holds that $\mathcal{E}_1$ is a (*nice error*) basis of the vector space of complex $Q \times Q$ matrices. Notice that the identity operator is also considered as an "error". The following result describes the product of elements in $\mathcal{E}_1$.

Proposition 2.2.3. *Let a, b, a' and b' be elements in $\mathbb{F}_Q$. Then,*

$$X(a)Z(b)X(a')Z(b') = \omega^{\mathrm{tr}(a'b)}X(a + a')Z(b + b').$$

Proof. The equalities

$$X(a)Z(b)|x\rangle = \omega^{\mathrm{tr}(bx)}X(a)|x\rangle = \omega^{\mathrm{tr}(bx)}|x + a\rangle$$

and

$$Z(b)X(a)|x\rangle = Z(b)|x + a\rangle = \omega^{\mathrm{tr}(b(x+a))}|x + a\rangle$$

prove $\omega^{\mathrm{tr}(ab)}X(a)Z(b) = Z(b)X(a)$ and thus the result holds. □

We can consider tensor products of n error operators as above to get an error basis on $\mathbb{C}^{Q^n}$. Indeed, given $\boldsymbol{a} = (a_1, \ldots, a_n)$ and $\boldsymbol{b} = (b_1, \ldots, b_n) \in \mathbb{F}_Q^n$, we define the error operators on $\mathbb{C}^{Q^n}$:

$$\boldsymbol{X}(\boldsymbol{a}) \coloneqq X(a_1) \otimes \cdots \otimes X(a_n)$$

and

$$\boldsymbol{Z}(\boldsymbol{b}) \coloneqq Z(b_1) \otimes \cdots \otimes Z(b_n),$$

and the set of error operators on $\mathbb{C}^{Q^n}$

$$\mathcal{E}_n \coloneqq \left\{ \boldsymbol{X}(\boldsymbol{a})\boldsymbol{Z}(\boldsymbol{b}) \mid \boldsymbol{a}, \boldsymbol{b} \in \mathbb{F}_Q^n \right\}.$$

$\mathcal{E}_n$ (whose elements we regard as matrices) is a (*nice error*) basis of the vector space of complex $Q^n \times Q^n$ matrices. The coordinates of the vectors $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{F}_Q^n$ indicate, respectively, the occurred qudit flip or the phase shift error.

Definition 2.2.4. The *error group* $\mathcal{G}_n$ associated with $\mathcal{E}_n$ is the group of operators generated by $\mathcal{E}_n$ with respect to the product. By Proposition 2.2.3,

$$\mathcal{G}_n = \left\{ \omega^c \boldsymbol{X}(\boldsymbol{a})\boldsymbol{Z}(\boldsymbol{b}) \mid \boldsymbol{a}, \boldsymbol{b} \in \mathbb{F}_Q^n, c \in \mathbb{F}_p \right\}.$$

The following two definitions are used to define the minimum distance of $\mathcal{Q}$. Given two vectors $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{F}_Q^n$, we denote $(\boldsymbol{a} \mid \boldsymbol{b}) \coloneqq (a_1, \ldots, a_n, b_1, \ldots, b_n) \in \mathbb{F}_Q^{2n}$.

Definition 2.2.5. The *symplectic weight* sw of a vector $(\boldsymbol{a} \mid \boldsymbol{b}) \in \mathbb{F}_Q^{2n}$ is

$$\mathrm{sw}((\boldsymbol{a} \mid \boldsymbol{b})) \coloneqq \#\{i \in \{1, \ldots, n\} \mid (a_i, b_i) \neq (0, 0)\}.$$

The *minimum symplectic weight* of a subset of $\mathbb{F}_Q^{2n}$ is the minimum value of the symplectic weights of its elements.

Definition 2.2.6. The number of nonidentity tensor components of an error $\boldsymbol{E} = \omega^c \boldsymbol{X}(\boldsymbol{a})\boldsymbol{Z}(\boldsymbol{b}) \in \mathcal{G}_n$ is called the *weight* of $\boldsymbol{E}$ and it is denoted $\mathrm{w}(\boldsymbol{E})$. In fact

$$\mathrm{w}(\boldsymbol{E}) \coloneqq \mathrm{sw}((\boldsymbol{a} \mid \boldsymbol{b})).$$

Notice that the weight of a scalar multiple of the identity operator $\boldsymbol{I}$ equals 0.

Definition 2.2.7. The *minimum distance* of a quantum code $\mathcal{Q}$ is the smallest weight of the errors in $\mathcal{G}_n$ that $\mathcal{Q}$ does not detect.

Notice that if $\mathcal{Q}$ has minimum distance d, then it detects all errors in $\mathcal{G}_n$ of weight less than d and corrects all errors in $\mathcal{G}_n$ of weight $\left\lfloor \frac{d-1}{2} \right\rfloor$ or less. This is because, given $\boldsymbol{E}_1, \boldsymbol{E}_2 \in \mathcal{G}_n$, the weight of $\boldsymbol{E}_1^\dagger \boldsymbol{E}_2$ is at most $\mathrm{w}(\boldsymbol{E}_1) + \mathrm{w}(\boldsymbol{E}_2)$. A quantum code $\mathcal{Q} \subseteq \mathbb{C}^{Q^n}$ with dimension K and minimum distance d is said to be an $((n, K, d))_q$ code. If $K = Q^k$ it is also called an $[[n, k, d]]_Q$ code. Some authors only use the bracket notation for stabilizer codes.

In order to compare different quantum codes one may use the *length extension*, *subcode* and *smaller distance* propagation rules, as stated in [89] for example. We therefore say that a quantum $[[n, k, d]]_Q$ code *beats* a quantum $[[n', k', d']]_Q$ code if at least one of the following holds:

- $n < n'$ and $k = k'$ and $d = d'$ (*length extension*);
- $n = n'$ and $k > k'$ and $d = d'$ (*subcode*);
- $n = n'$ and $k = k'$ and $d > d'$ (*smaller distance*).

In other words, decreasing n, or increasing k or d, while keeping other parameters fixed, results in a better code. This is well known, see [89] for example, where the authors say that "... all other parameters being equal, we record the smallest n, the largest k, the largest d, ...".

For detection of errors purposes, it is useful to know which elements in $\mathcal{G}_n$ commute. The following proposition characterizes them. First we need to define the *trace-symplectic form* of two vectors $(\boldsymbol{a} \mid \boldsymbol{b}), (\boldsymbol{a}' \mid \boldsymbol{b}') \in \mathbb{F}_Q^{2n}$. It is defined as follows.

$$\cdot_s : \mathbb{F}_Q^{2n} \times \mathbb{F}_Q^{2n} \to \mathbb{F}_p, \quad (\boldsymbol{a} \mid \boldsymbol{b}) \cdot_s (\boldsymbol{a}' \mid \boldsymbol{b}') = \operatorname{tr}(\boldsymbol{b} \cdot_e \boldsymbol{a}' - \boldsymbol{b}' \cdot_e \boldsymbol{a}).$$

Proposition 2.2.8. *Let* $\boldsymbol{E} = \omega^c \boldsymbol{X}(\boldsymbol{a})\boldsymbol{Z}(\boldsymbol{b})$ *and* $\boldsymbol{E}' = \omega^{c'} \boldsymbol{X}(\boldsymbol{a}')\boldsymbol{Z}(\boldsymbol{b}')$ *be two elements in the error group* $\mathcal{G}_n$*. Then,*

$$\boldsymbol{E}\boldsymbol{E}' = \omega^{\operatorname{tr}(\boldsymbol{b} \cdot_e \boldsymbol{a}' - \boldsymbol{b}' \cdot_e \boldsymbol{a})} \boldsymbol{E}'\boldsymbol{E}.$$

Therefore they commute if and only if $(\boldsymbol{a} \mid \boldsymbol{b}) \cdot_s (\boldsymbol{a}' \mid \boldsymbol{b}') = 0$.

Proof. Proposition 2.2.3 and the properties of the trace map tr imply that

$$\boldsymbol{E}\boldsymbol{E}' = \omega^{\operatorname{tr}(\boldsymbol{b} \cdot_e \boldsymbol{a}')} \boldsymbol{X}(\boldsymbol{a} + \boldsymbol{a}')\boldsymbol{Z}(\boldsymbol{b} + \boldsymbol{b}')$$

and

$$\boldsymbol{E}'\boldsymbol{E} = \omega^{\operatorname{tr}(\boldsymbol{b}' \cdot_e \boldsymbol{a})} \boldsymbol{X}(\boldsymbol{a} + \boldsymbol{a}')\boldsymbol{Z}(\boldsymbol{b} + \boldsymbol{b}').$$

Hence, $\omega^{\operatorname{tr}(\boldsymbol{b} \cdot_e \boldsymbol{a}' - \boldsymbol{b}' \cdot_e \boldsymbol{a})} \boldsymbol{E}'\boldsymbol{E} = \boldsymbol{E}\boldsymbol{E}'$. □

We end Part I, devoted to preliminaries, by introducing stabilizer codes, an important class of QECCs that can be developed from the theory of classical codes.

2.3. Stabilizer codes

Stabilizer (quantum) codes, which are also named additive quantum codes, were defined by Gottesman [57]. They are a class of QECCs which takes advantage of the fact that, in the quantum setting, nontrivial error operators may have no effect on the encoded state. These codes are designed to protect the encoded states against most common errors (since no code can protect against all possible errors). Stabilizer codes have two main virtues. On the one hand, many quantum states (and quantum codes) are described more easily by working with their stabilizer operators than with their own states. On the other hand, stabilizer codes work in an efficient way because of their connection with classical codes. Most of the known QECCs are stabilizer codes.

Definition 2.3.1. A *stabilizer code* $\mathcal{Q}$ is a nontrivial subspace of $\mathbb{C}^{q^n}$ which is the intersection of the eigenspaces with eigenvalue 1 corresponding to the elements of an abelian subgroup S of the error group $\mathcal{G}_n$:

$$\mathcal{Q} = \bigcap_{\boldsymbol{E}\in S} \left\{ |\boldsymbol{v}\rangle \in \mathbb{C}^{q^n} \mid \boldsymbol{E}|\boldsymbol{v}\rangle = |\boldsymbol{v}\rangle \right\}.$$

The subgroup S is called the *stabilizer* of $\mathcal{Q}$.

Definition 2.3.2. A stabilizer code is *pure to* a positive integer t if its stabilizer does not contain errors other than identity of weight less than t, and it is *pure* if it is pure to its minimum distance.

Let us denote by $Z(\mathcal{G}_n)$ the center of the group $\mathcal{G}_n$, by $C_{\mathcal{G}_n}(S)$ the centralizer of the subgroup S in $\mathcal{G}_n$ and by $SZ(\mathcal{G}_n)$ the group generated by S and $Z(\mathcal{G}_n)$. An error $\boldsymbol{E} \in SZ(\mathcal{G}_n)$ is a scalar multiple of some element in S, since $Z(\mathcal{G}_n)$ consists of the scalar multiples of $\boldsymbol{I}$. Then, the restriction of $\boldsymbol{E}$ to $\mathcal{Q}$ equals $c_{\boldsymbol{E}}\boldsymbol{I}$ for some scalar $c_{\boldsymbol{E}} \in \mathbb{C}$ and therefore $\boldsymbol{E}$ is detectable. When an error $\boldsymbol{E} \in \mathcal{G}_n$ does not commute with an element $\boldsymbol{F}$ of the stabilizer, that is, $\boldsymbol{EF} = c\boldsymbol{FE}$ for some complex $c \neq 1$ by Proposition 2.2.8, then the error takes the stabilizer code to an orthogonal subspace because all $|\boldsymbol{v}\rangle, |\boldsymbol{w}\rangle \in \mathcal{Q}$ satisfy

$$\langle \boldsymbol{v}|\boldsymbol{E}|\boldsymbol{w}\rangle = \langle \boldsymbol{v}|\boldsymbol{EF}|\boldsymbol{w}\rangle = c\,\langle \boldsymbol{v}|\boldsymbol{FE}|\boldsymbol{w}\rangle = c\,\langle \boldsymbol{v}|\boldsymbol{E}|\boldsymbol{w}\rangle$$

and therefore $\langle \boldsymbol{v}|\boldsymbol{E}|\boldsymbol{w}\rangle = 0$. Hence, the error is also detectable. In fact, we have showed all detectable errors by a stabilizer code as the following result proved in [73, Lemma 11] states.

Proposition 2.3.3. *An error $\boldsymbol{E} \in \mathcal{G}_n$ is detectable by a stabilizer code $\mathcal{Q}$ of dimension larger than one, with stabilizer S, if and only if either $\boldsymbol{E} \in SZ(\mathcal{G}_n)$ or $\boldsymbol{E} \notin C_{\mathcal{G}_n}(S)$.*

Let t be a positive integer and assume that a stabilizer code $\mathcal{Q}$ is pure to t. The following corollary eases to understand the meaning of pureness. It states that detectable errors which are not a scalar multiple of the identity and with weight less than t take the stabilizer code to an orthogonal subspace.

Corollary 2.3.4. *Let $\mathcal{Q}$ be a pure to (a positive integer) t stabilizer code with minimum distance d. Then, all errors $\boldsymbol{E} \in \mathcal{G}_n$ with $1 \leq \mathrm{w}(\boldsymbol{E}) < \min\{t, d\}$ satisfy $\langle \boldsymbol{v}|\boldsymbol{E}|\boldsymbol{w}\rangle = 0$ for all $|\boldsymbol{v}\rangle, |\boldsymbol{w}\rangle \in \mathcal{Q}$.*

Proof. An error $\boldsymbol{E}$ as in the statement is detectable because $\mathrm{w}(\boldsymbol{E}) < d$. Since $\mathcal{Q}$ is pure to $t > \mathrm{w}(\boldsymbol{E})$, then $\boldsymbol{E} \notin SZ(\mathcal{G}_n)$. Then, Proposition 2.3.3 and its preceding paragraph imply the claim. □

Next, we give a description based in [104, Page 466] of how to perform error-correction on stabilizer codes. Let $\mathcal{Q}$ be a stabilizer code and $S = \langle \boldsymbol{G}_1, \ldots, \boldsymbol{G}_{n-k} \rangle$ be its stabilizer group. Suppose that $\{\boldsymbol{E}_j \mid j = 1, \ldots, m\}$, for some $m \in \mathbb{N}$, is the set of correctable errors by $\mathcal{Q}$. We may assume that those errors are unitary by the argument given in the

paragraph before Theorem 2.2.2. Then, we know that every $\boldsymbol{E}_j$, $j = 1, \ldots, m$, commutes with S (equivalently, commutes with its generators) up to a scalar factor, that is:

$$\boldsymbol{G}_l \boldsymbol{E}_j = \beta_l^j \boldsymbol{E}_j \boldsymbol{G}_l, \quad \beta_l^j \in \mathbb{C}, \quad l = 1, \ldots, n-k.$$

Let us call the vector $(\beta_1^j, \ldots, \beta_{n-k}^j) \in \mathbb{C}^{n-k}$ the *syndrome* of the error $\boldsymbol{E}_j$. Syndromes are previously computed and stored as the rows of a matrix

$$\left(\beta_l^j\right)_{m \times (n-k)}.$$

Notice that each row refers to a correctable error. Suppose that a codeword $|\phi\rangle \in \mathcal{Q}$ is affected by the error $\boldsymbol{E}_{j_0}$ and let $|\psi\rangle = \boldsymbol{E}_{j_0}|\phi\rangle$. Then, one applies on $|\psi\rangle$ the $n-k$ syndrome measurements that consist of computing $\boldsymbol{G}_l|\psi\rangle$ for all $l = 1, \ldots, n-k$. Then

$$\boldsymbol{G}_l|\psi\rangle = \boldsymbol{G}_l \boldsymbol{E}_{j_0}|\phi\rangle = \beta_l^{j_0} \boldsymbol{E}_{j_0} \boldsymbol{G}_l|\phi\rangle = \beta_l^{j_0} \boldsymbol{E}_{j_0}|\phi\rangle = \beta_l^{j_0}|\psi\rangle.$$

Once obtained the syndrome $(\beta_1^{j_0}, \ldots, \beta_{n-k}^{j_0})$, if it equals $(1, \ldots, 1)$, it means that $\boldsymbol{E}_{j_0} \in SZ(\mathcal{G}_n)$ and therefore we correct $|\psi\rangle$ by normalizing it. Otherwise, $(\beta_1^{j_0}, \ldots, \beta_{n-k}^{j_0})$ will coincide with the j'-th row, $1 \leq j' \leq m$, in the syndrome matrix and correct $|\psi\rangle$ by applying the adjoint of the error $\boldsymbol{E}_{j'}$. This operation will recover $|\phi\rangle$. Indeed:

- Suppose that there exists a unique row with that syndrome. Then, $j' = j_0$ and therefore $\boldsymbol{E}_{j'}^\dagger|\psi\rangle = \boldsymbol{E}_{j_0}^\dagger|\psi\rangle = \boldsymbol{E}_{j_0}^\dagger \boldsymbol{E}_{j_0}|\phi\rangle = |\phi\rangle$.
- Suppose that there exist two rows with that syndrome and $j' \neq j_0$. Since

  $$\boldsymbol{G}_l \boldsymbol{E}_{j'} = \beta_l^{j_0} \boldsymbol{E}_{j'} \boldsymbol{G}_l, \quad l = 1, \ldots, n-k,$$

  then the following chain of equalities holds for all $l = 1, \ldots, m$:

  $$\boldsymbol{E}_{j_0} \boldsymbol{G}_l \boldsymbol{E}_{j_0}^\dagger = \left(\beta_l^{j_0}\right)^{-1} \boldsymbol{G}_l \boldsymbol{E}_{j_0} \boldsymbol{E}_{j_0}^\dagger = \left(\beta_l^{j_0}\right)^{-1} \boldsymbol{G}_l = \left(\beta_l^{j_0}\right)^{-1} \boldsymbol{G}_l \boldsymbol{E}_{j'} \boldsymbol{E}_{j'}^\dagger = \boldsymbol{E}_{j'} \boldsymbol{G}_l \boldsymbol{E}_{j'}^\dagger.$$

  The above equality and the fact that the projection $\boldsymbol{P}$ onto $\mathcal{Q}$ can be written as $\boldsymbol{P} = \frac{1}{\#S} \sum_{\boldsymbol{E} \in S} \boldsymbol{E}$ [73, Lemma 9] imply

  $$\boldsymbol{E}_{j_0} \boldsymbol{P} \boldsymbol{E}_{j_0}^\dagger = \frac{1}{\#S} \sum_{\boldsymbol{E} \in S} \boldsymbol{E}_{j_0} \boldsymbol{E} \boldsymbol{E}_{j_0}^\dagger = \frac{1}{\#S} \sum_{\boldsymbol{E} \in S} \boldsymbol{E}_{j'} \boldsymbol{E} \boldsymbol{E}_{j'}^\dagger = \boldsymbol{E}_{j'} \boldsymbol{P} \boldsymbol{E}_{j'}^\dagger,$$

  where we have used that any $\boldsymbol{E} \in S$ can be written as a product $\prod_{i \in A \subseteq \{1, \ldots, n-k\}} \boldsymbol{G}_i$ and the fact that $\boldsymbol{I} = \boldsymbol{E}_{j_0}^\dagger \boldsymbol{E}_{j_0} = \boldsymbol{E}_{j'}^\dagger \boldsymbol{E}_{j'}$. Then,

  $$\boldsymbol{E}_{j'}^\dagger \boldsymbol{E}_{j_0} \boldsymbol{P} \boldsymbol{E}_{j_0}^\dagger \boldsymbol{E}_{j'} = \boldsymbol{P},$$

  so $\boldsymbol{E}_{j'}^\dagger \boldsymbol{E}_{j_0} \in S$, because otherwise $\boldsymbol{P} \boldsymbol{E}_{j'}^\dagger \boldsymbol{E}_{j_0} \boldsymbol{P} = \boldsymbol{0}$ [104, Theorem 10.8] and this fact, together with the above equation, would lead to $\boldsymbol{P} = \boldsymbol{0}$, a contradiction. Therefore, $\boldsymbol{E}_{j'}^\dagger|\psi\rangle = \boldsymbol{E}_{j'}^\dagger \boldsymbol{E}_{j_0}|\phi\rangle = |\phi\rangle$.

Next we connect stabilizer codes to additive codes. A $\mathfrak{q}$-ary additive code is a closed under addition subgroup of $\mathbb{F}_\mathfrak{q}^t$ for some $t \in \mathbb{N}$. We are interested in those that allow us to characterize the detectable errors in $\mathcal{G}_n$ by a stabilizer code.

2.3.1. Stabilizer codes from additive codes over $\mathbb{F}_Q$

The phase information ω^c of an element in $\mathcal{G}_n$ does not affect the detectability. This means that we can suppose $\omega^c = 1$ and considering the map

$$\mathcal{G}_n \to \mathbb{F}_Q^{2n}, \quad \omega^c \boldsymbol{X}(\boldsymbol{a})\boldsymbol{Z}(\boldsymbol{b}) \mapsto (\boldsymbol{a} \mid \boldsymbol{b}),$$

it holds that $SZ(\mathcal{G}_n)$ is mapped to the additive code

$$\mathcal{C} := \{(\boldsymbol{a} \mid \boldsymbol{b}) \mid \omega^c \boldsymbol{X}(\boldsymbol{a})\boldsymbol{Z}(\boldsymbol{b}) \in SZ(\mathcal{G}_n)\} = {}^{SZ(\mathcal{G}_n)}\!/_{Z(\mathcal{G}_n)}.$$

Moreover, by Proposition 2.2.8, $C_{\mathcal{G}_n}(S)$ is mapped onto the trace-symplectic dual code $\mathcal{C}^{\perp_s}$ of $\mathcal{C}$. That is,

$$\mathcal{C}^{\perp_s} = \{(\boldsymbol{a} \mid \boldsymbol{b}) \mid \omega^c \boldsymbol{X}(\boldsymbol{a})\boldsymbol{Z}(\boldsymbol{b}) \in C_{\mathcal{G}_n}(S)\}.$$

Next theorem provides the connection between additive codes over $\mathbb{F}_Q$ and stabilizer codes [73, 6].

Theorem 2.3.5. *[73, Theorem 13] The existence of an $((n, K, d))_Q$ stabilizer code is equivalent to that of an additive code $\mathcal{C} \subseteq \mathbb{F}_Q^{2n}$ of cardinality $\#\mathcal{C} = \frac{Q^n}{K}$ such that $\mathcal{C} \subseteq \mathcal{C}^{\perp_s}$ and d is the minimum symplectic weight of $\mathcal{C}^{\perp_s} \backslash \mathcal{C}$ if $K > 1$ (and whenever $K = 1$, d is the minimum symplectic weight of $\mathcal{C}^{\perp_s} = \mathcal{C}$).*

2.3.2. Stabilizer codes from additive codes over $\mathbb{F}_{Q^2}$

The literature about the symplectic weight is limited. A well-known inner product is the Hermitian one. Stabilizer codes obtained from Hermitian self-orthogonal codes can be regarded as a particular case of the following situation where we relate stabilizer codes and additive codes over $\mathbb{F}_{Q^2}$.

Let $\{\alpha, \alpha^Q\}$ be a normal basis of the field $\mathbb{F}_{Q^2}$ over $\mathbb{F}_Q$. We define the map

$$\theta : \mathbb{F}_Q^{2n} \to \mathbb{F}_{Q^2}^n, \quad \theta((\boldsymbol{a} \mid \boldsymbol{b})) = \alpha\boldsymbol{a} + \alpha^Q\boldsymbol{b},$$

which is bijective and isometric. This last expression means that θ preserves weights (symplectic in $\mathbb{F}_Q^{2n}$ and Hamming in $\mathbb{F}_{Q^2}^n$), that is, $\mathrm{sw}((\boldsymbol{a} \mid \boldsymbol{b})) = \mathrm{w}(\theta((\boldsymbol{a} \mid \boldsymbol{b})))$ for all $(\boldsymbol{a} \mid \boldsymbol{b}) \in \mathbb{F}_Q^{2n}$. Now we define the *trace-alternating form* of two vectors $\boldsymbol{x}$ and $\boldsymbol{y}$ in $\mathbb{F}_{Q^2}^n$ as

$$\cdot_a : \mathbb{F}_{Q^2}^n \times \mathbb{F}_{Q^2}^n \to \mathbb{F}_p, \quad \boldsymbol{x} \cdot_a \boldsymbol{y} = \mathrm{tr}\left(\frac{\boldsymbol{x} \cdot_e \boldsymbol{y}^Q - \boldsymbol{x}^Q \cdot_e \boldsymbol{y}}{\alpha^{2Q} - \alpha^2}\right),$$

which is bi-additive, linear over $\mathbb{F}_p$ and satisfies that $\boldsymbol{x} \cdot_a \boldsymbol{x} = 0$ for all $\boldsymbol{x} \in \mathbb{F}_{Q^2}^n$. Moreover, for every $\boldsymbol{x}$ and $\boldsymbol{y}$ in $\mathbb{F}_Q^{2n}$, it holds that

$$\boldsymbol{x} \cdot_s \boldsymbol{y} = \theta(\boldsymbol{x}) \cdot_a \theta(\boldsymbol{y}).$$

The previous equality clearly implies that $\boldsymbol{x}$ and $\boldsymbol{y}$ are trace-symplectic orthogonal if and only if $\theta(\boldsymbol{x})$ and $\theta(\boldsymbol{y})$ are trace-alternating orthogonal. Let the symbol $\perp_a$ denote dual with respect to the trace-alternating form $\cdot_a$. The relation between stabilizer codes and additive codes over $\mathbb{F}_{Q^2}$ follows from Theorem 2.3.5 and the isometry θ:

Theorem 2.3.6. *[73, Theorem 15] The existence of an $((n, K, d))_Q$ stabilizer code is equivalent to that of an additive code $\mathcal{C} \subseteq \mathbb{F}_{Q^2}^n$ of cardinality $\#\mathcal{C} = \frac{Q^n}{K}$ such that $\mathcal{C} \subseteq \mathcal{C}^{\perp_a}$, where d is the minimum distance of $\mathcal{C}^{\perp_a} \backslash \mathcal{C}$ if $K > 1$ (and whenever $K = 1$, d is the minimum distance of $\mathcal{C}^{\perp_a} = \mathcal{C}$).*

An immediate consequence is

Corollary 2.3.7. *Let $\mathcal{C} \subseteq \mathbb{F}_{Q^2}^n$ be an $[n, k]_{Q^2}$ additive code such that $\mathcal{C} \subseteq \mathcal{C}^{\perp_a}$. Denote by $d^{\perp_a}$ the minimum distance of $\mathcal{C}^{\perp_a}$. Then, there exists an $[[n, n-2k, \geq d^{\perp_a}]]_Q$ stabilizer code that is pure to $d^{\perp_a}$.*

2.3.3. Stabilizer codes from linear codes over $\mathbb{F}_{Q^2}$

As we have explained, when considering additive codes over $\mathbb{F}_{Q^2}$, a trace-alternating form as above can be used to construct stabilizer codes. However, when one has linear codes over $\mathbb{F}_{Q^2}$, it suffices to consider the more common *Hermitian inner product*. It is defined as the map

$$\cdot_h : \mathbb{F}_{Q^2}^n \times \mathbb{F}_{Q^2}^n \to \mathbb{F}_{Q^2}, \quad \boldsymbol{x} \cdot_h \boldsymbol{y} = \boldsymbol{x} \cdot_e \boldsymbol{y}^Q = \sum_{i=1}^{n} x_i y_i^Q.$$

Let the symbol $\perp_h$ mean dual with respect to the Hermitian inner product. Given $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_{Q^2}^n$ such that $\boldsymbol{x} \cdot_h \boldsymbol{y} = 0$, then it is clear that $\boldsymbol{x} \cdot_a \boldsymbol{y} = 0$. Thus, for a code $\mathcal{C} \subseteq \mathbb{F}_{Q^2}^n$, it holds that $\mathcal{C}^{\perp_h} \subseteq \mathcal{C}^{\perp_a}$ so, whenever $\mathcal{C} \subseteq \mathcal{C}^{\perp_h}$, then $\mathcal{C} \subseteq \mathcal{C}^{\perp_a}$. In general, $\mathcal{C}^{\perp_h} \subset \mathcal{C}^{\perp_a}$, but provided that $\mathcal{C}$ is linear over $\mathbb{F}_{Q^2}$, a dimensional argument shows that $\mathcal{C}^{\perp_h} = \mathcal{C}^{\perp_a}$ (see [73, Lemma 18]). Then one can use Corollary 2.3.7 to prove the following corollary. It will be one of our main results to construct stabilizer codes from classical linear codes.

Corollary 2.3.8. *[1, 73] Let $\mathcal{C}$ be an $[n, k]$ linear code over $\mathbb{F}_{Q^2}$ such that $\mathcal{C} \subseteq \mathcal{C}^{\perp_h}$. Denote by $d^{\perp_h}$ the minimum distance of $\mathcal{C}^{\perp_h}$. Then, there exists an $[[n, n-2k, \geq d^{\perp_h}]]_Q$ stabilizer code that is pure to $d^{\perp_h}$.*

2.3.4. Bounds on stabilizer codes

When studying quantum codes, this thesis only considers stabilizer codes. For this reason, in this last subsection of Chapter 2 we provide some bounds on the parameters of stabilizer codes. We notice that most of the bounds here given are also valid for general quantum codes.

The quantum analogue of the classical Singleton bound is stated in the following result, which was proved in [109] for general nonbinary quantum codes.

Theorem 2.3.9 (Quantum Singleton bound)**.** *Let $[[n, k, d]]_Q$ be the parameters of a quantum code with $k \geq 1$, then the following bound holds:*

$$n \geq k + 2(d-1).$$

Quantum codes reaching the quantum Singleton bound are called *(quantum) MDS codes*.

There is also a quantum version [69] of the MDS conjecture. It follows by applying the classical MDS conjecture to the classical codes over $\mathbb{F}_{Q^2}$ giving rise to stabilizer codes. Therefore, this bound is only valid for MDS stabilizer quantum codes. Even if the classical MDS conjecture were true, one could find non-stabilizer MDS codes contradicting the quantum MDS conjecture.

Conjecture 2.3.10 (Quantum MDS conjecture)**.** *Let $[[n, n-2d+2, d]]_Q$ be the parameters of a stabilizer quantum MDS code with $d \geq 3$. Then, the following bound holds:*

$$n \leq Q^2 + 1,$$

excepting the case when Q even and $d = 4$, where $n \leq Q^2 + 2$.

We finish the two chapters on preliminaries by stating the quantum version of the classical Gilbert-Varshamov bound. It helps to decide when parameters of a quantum code have a good behavior. We say that a parameter set $[[n, k, d]]_Q$ *beats* this bound if the inequality in Theorem 2.3.11 is not satisfied.

Theorem 2.3.11 (Quantum Gilbert-Varshamov bound)**.** *[39] Suppose that $n > k \geq 2$, $d \geq 2$, and $n \equiv k \mod 2$. If*

$$\frac{Q^{n-k+2} - 1}{Q^2 - 1} \geq \sum_{i=1}^{d-1} (Q^2 - 1)^{i-1} \binom{n}{i},$$

then there exists a pure stabilizer quantum code with parameters $[[n, k, d]]_Q$.

Part II

Locally recoverable codes from evaluation codes

Chapter 3

Optimal (r,δ)-locally recoverable codes from monomial-Cartesian codes and their subfield subcodes

Let q be a prime power. In this chapter we keep the same notations as in Subsection 1.3.1 with $Q = q$, and consider MCCs with $m \geq 2$ to construct (r,δ)-locally recoverable codes. Recall from Definition 1.3.3 that a q-ary MCC $\mathcal{C}_\Delta^P$ is an $\mathbb{F}_q$-vector subspace of $\mathbb{F}_q^n$

$$\mathcal{C}_\Delta^P = \mathrm{ev}_P(V_\Delta) = \langle \mathrm{ev}_P(X_1^{e_1}\cdots X_m^{e_m}) \mid (e_1,\ldots,e_m) \in \Delta \rangle \subseteq \mathbb{F}_q^n$$

obtained as the image of a map

$$\mathrm{ev}_P : V_\Delta \subset \mathcal{R} = \mathbb{F}_q[X_1,\ldots,X_m]/I \to \mathbb{F}_q^n, \qquad \mathrm{ev}_P(f) = (f(\boldsymbol{\alpha}_1),\ldots,f(\boldsymbol{\alpha}_n)),$$

where $m \geq 1$ is a positive integer, $P = P_1 \times \cdots \times P_m = \{\boldsymbol{\alpha}_1,\ldots,\boldsymbol{\alpha}_n\}$ a Cartesian product subset of $\mathbb{F}_q^m$, $I = \langle f_1(X_1),\ldots,f_m(X_m)\rangle$ the vanishing ideal at P of $\mathbb{F}_q[X_1,\ldots,X_m]$ (i.e., $f_j(X_j) = \prod_{\beta\in P_j}(X_j - \beta)$ for $j = 1,\ldots,m$) and

$$V_\Delta = \left\langle X_1^{e_1}\cdots X_m^{e_m} \mid (e_1,\ldots,e_m) \in \Delta \right\rangle_{\mathbb{F}_q}$$

an $\mathbb{F}_q$-linear space generated by classes of monomials with exponents in some subset $\Delta \subseteq E = \{0,1,\ldots,n_1-1\} \times \cdots \times \{0,1,\ldots,n_m-1\}$. This set E is that containing the possibilities of exponents of any monomial reduced modulo I. Other important notations are $n_j = \#P_j$ and $n = \#P = \prod_{j=1}^m n_j$.

Recall also from Definition 1.4.4 that an $[n,k,d]$ code $\mathcal{C}$ is an (r,δ)-LRC, with r and $\delta \geq 2$ positive integers, if, for any coordinate $i \in \{1,\ldots,n\}$, there exists a set of coordinates $\overline{R} = \overline{R}(i) \subseteq \{1,\ldots,n\}$ such that:

1. $i \in \overline{R}$ and $\#\overline{R} \leq r + \delta - 1$; and
2. $\mathrm{d}(\mathcal{C}[\overline{R}]) \geq \delta$.

We are interested in optimal codes, that is, those attaining the Singleton-like bound for (r,δ)-LRCs we reproduce in Proposition 1.4.5:

$$k + d + \left(\left\lceil \frac{k}{r} \right\rceil - 1\right)(\delta - 1) \leq n + 1.$$

The goal of this chapter is to obtain many new optimal LRCs coming from MCCs, we refer the reader to pages 5 to 6 of the introduction of this PhD thesis for a detailed summary of this chapter.

In Proposition 3.1.1 of Section 3.1 we show how MCCs can be considered as LRCs. Section 3.2 is devoted to determine the set of optimal MCCs we can obtain, they are given in Propositions 3.2.1, 3.2.2 and 3.2.3, 3.2.13 and 3.2.14. We divide our study in two cases: bivariate and multivariate performed respectively in Subsections 3.2.1 and 3.2.2. Parameters of codes in the above five propositions are grouped in Corollary 3.2.12 for the bivariate case and in Corollary 3.2.17 for the multivariate case. They are not new but, unlike the literature, they can be obtained by a unique procedure.

Finally our main results concerning new LRCs obtained from subfield-subcodes of some subfamilies of the above MCCs are given in Section 3.3. These new LRCs are given in Subsection 3.3.1, where the bivariate case is treated, and in Subsection 3.3.2 devoted to the multivariate case. Propositions 3.3.4 and 3.3.6 for the bivariate case, and Propositions 3.3.11 and 3.3.12 for the multivariate case, explain how to construct new optimal (r,δ)-LRCs. The main results of this chapter are Theorems 3.3.9, 3.3.10, 3.3.14 and 3.3.15. Theorem 3.3.9 (respectively, 3.3.14) gives parameters of new optimal LRCs over any field coming from the bivariate (respectively, multivariate) case.

The entire contents in this chapter, except for Remark 3.2.4 and its proof, were published in the journal *Designs, Codes and Cryptography*, see [45]. The notation has been adapted to ease the reading of this thesis.

3.1. Locally recoverable monomial-Cartesian codes

In this section we regard MCCs with $m \geq 2$ as (r,δ)-LRCs. MCCs were previously used to provide LRCs with availability [93]. Next proposition and its proof show how to regard MCCs as LRCs with locality (r,δ). To do it, we need to introduce some definitions. For each $1 \leq j \leq m$, define the support of V_Δ at X_j as

$$\operatorname{supp}_{X_j}(V_\Delta) := \left\{ e_j \in \{0,1,\ldots,n_j-1\} \mid \text{there exists a monomial } X_1^{e_1}\cdots X_j^{e_j}\cdots X_m^{e_m} \text{ in } V_\Delta \right\},$$

and set $\mathcal{K}_j := \#\operatorname{supp}_{X_j}(V_\Delta)$ and $k_j := \max\left(\operatorname{supp}_{X_j}(V_\Delta)\right)$. Now, and as the beginning of Subsection 1.3.1, consider the set $P_j = \left\{\alpha_1^j,\ldots,\alpha_{n_j}^j\right\} \subseteq \mathbb{F}_q$, the ideal I_j of $\mathbb{F}_q[X_j]$ generated by $f_j = \prod_{i=1}^{n_j}\left(X_j - \alpha_i^j\right)$ and the map

$$\operatorname{ev}_{P_j}\colon \mathcal{R}_j := \mathbb{F}_q[X_j]/I_j \to \mathbb{F}_q^{n_j}$$

given by

$$\operatorname{ev}_{P_j}(f) = \left(f\left(\alpha_1^j\right),\ldots,f\left(\alpha_{n_j}^j\right)\right).$$

Finally define the $\mathbb{F}_q$-vector space $V_\Delta^j := \langle X_j^e \mid e \in \operatorname{supp}_{X_j}(V_\Delta)\rangle_{\mathbb{F}_q} \subseteq \mathcal{R}_j$.

Proposition 3.1.1. *Let $\mathcal{C}_\Delta^P$ be an MCC. Then, for each $1 \le l \le m$ such that $k_l + 1 < n_l$, $\mathcal{C}_\Delta^P$ is an LRC with locality $(\ge \mathcal{K}_l, \le n_l - \mathcal{K}_l + 1)$. In addition, if $\mathrm{ev}_{P_l}\left(V_\Delta^l\right)$ is an MDS code, then the locality is $(\mathcal{K}_l, n_l - \mathcal{K}_l + 1)$.*

Proof. Let $\boldsymbol{c} = (c_1, \ldots, c_n) = \mathrm{ev}_P(f) \in \mathcal{C}_\Delta^P$ be a codeword whose i-th coordinate c_i we desire to recover. We know that $\mathrm{supp}(f) \subseteq \Delta$ and thus $\deg_{X_j}(f) \le k_j$ for all $j = 1, \ldots, m$. Choose a variable X_l (we will interpolate with respect to it), write $c_i = f(\boldsymbol{\alpha}_i) = f(\alpha_{i1}, \ldots, \alpha_{im})$ and consider the following subset of P:

$$\begin{aligned}\overline{R}_P &= \left\{\boldsymbol{\alpha}_t \in P \mid \alpha_{tj} = \alpha_{ij} \text{ for all } j \in \{1, \ldots, m\} \backslash \{l\}\right\} \\ &= \left\{(\alpha_{i1}, \ldots, \alpha_{il-1}, x, \alpha_{il+1}, \ldots, \alpha_{im}) \mid x \in P_l\right\},\end{aligned}$$

whose cardinality is $\#\overline{R}_P = n_l$. A polynomial in V_Δ can be expressed as

$$\begin{aligned}f(X_1, \ldots, X_m) &= \sum_{(e_1, \ldots, e_m) \in \Delta} f_{e_1, \ldots, e_m} X_1^{e_1} \cdots X_m^{e_m} \\ &= \sum_{h=0}^{k_l} f_h(X_1, \ldots, X_{l-1}, X_{l+1}, \ldots, X_m) X_l^h \in \mathbb{F}_q[X_1, \ldots, X_{l-1}, X_{l+1}, \ldots, X_m][X_l].\end{aligned}$$

Replacing each X_j, $j \ne l$, by α_{ij}, we get a polynomial in X_l, $g(X_l)$, with constant coefficients, of degree at most k_l:

$$g(X_l) = f(\alpha_{i1}, \ldots, \alpha_{il-1}, X_l, \alpha_{il+1}, \ldots, \alpha_{im}) = \sum_{h=0}^{k_l} g_h X_l^h,$$

where $g_h = f_h(\alpha_{i1}, \ldots, \alpha_{il-1}, \alpha_{il+1}, \ldots, \alpha_{im})$. So we can interpolate g by using $k_l + 1$ points in $\overline{R}_P$ (since $k_l + 1 < n_l$) to obtain the coefficients g_h. Let us denote those $k_l + 1$ points by $\boldsymbol{\beta}_t = (\alpha_{i1}, \ldots, \alpha_{il-1}, \beta_t, \alpha_{il+1}, \ldots, \alpha_{im}) \in \overline{R}_P$, $\boldsymbol{\beta}_t \ne \boldsymbol{\alpha}_i$, where $\beta_t \in P_l$, $t = 0, \ldots, k_l$, and let $v_t := f(\boldsymbol{\beta}_t) = g(\beta_t)$. Thus, the interpolation consists of solving the following linear system of $k_l + 1$ equations with indeterminates $g_0, \ldots, g_{k_l}$.

$$\begin{pmatrix} 1 & \beta_0 & \beta_0^2 & \cdots & \beta_0^{k_l} \\ 1 & \beta_1 & \beta_1^2 & \cdots & \beta_1^{k_l} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \beta_{k_l} & \beta_{k_l}^2 & \cdots & \beta_{k_l}^{k_l} \end{pmatrix} \begin{pmatrix} g_0 \\ g_1 \\ \vdots \\ g_{k_l} \end{pmatrix} = \begin{pmatrix} v_0 \\ v_1 \\ \vdots \\ v_{k_l} \end{pmatrix}. \tag{3.1.1}$$

The coefficient matrix of this system is a Vandermonde matrix, which is nonsingular, and therefore the system has a unique solution. Consequently, we can recover c_i by evaluating g. Let

$$\overline{R} = \{t \in \{1, \ldots, n\} \mid \boldsymbol{\alpha}_t \in \overline{R}_P\}.$$

The set $\overline{R}$ is an (r, δ)-recovery set for i with $r := k_l + 1$ and $\delta := n_l - k_l$ since $i \in \overline{R}$, $\#\overline{R} = n_l = r + \delta - 1$ and

$$\mathrm{d}(\mathcal{C}[\overline{R}]) = \mathrm{d}\left(\mathrm{ev}_{P_l}\left(V_\Delta^l\right)\right) \ge \mathrm{d}\left(\mathrm{ev}_{P_l}\left(V'^l\right)\right) = \delta,$$

where $V'^l := \langle X_l^e \mid e \in \{0, 1, \ldots, k_l\}\rangle_{\mathbb{F}_q} \subseteq \mathcal{R}_l$. The above inequality holds because $\mathcal{C}[\overline{R}] = \mathrm{ev}_{P_l}\left(V_\Delta^l\right)$ is a subcode of the Reed-Solomon (and thus MDS) code $\mathrm{ev}_{P_l}\left(V'^l\right)$. The facts that $r \ge \mathcal{K}_l$ and $\delta \le n_l - \mathcal{K}_l + 1$ prove the first part of our statement.

To prove the last one, notice that we have $k_l + 1 - \mathcal{K}_l$ conditions

$$g_h = f_h(\alpha_{i1}, \ldots, \alpha_{il-1}, \alpha_{il+1}, \ldots, \alpha_{im}) = 0 \tag{3.1.2}$$

$h \notin \operatorname{supp}_{X_l}(V_\Delta)$, and then we actually need $\mathcal{K}_l$ points in $\overline{R}_P$ to obtain the coefficients of g. The system of equations (3.1.1) can be reduced to a linear system where, for those indices h involved in Equality (3.1.2), we remove, for example, the equations whose independent terms are v_h and, also, the variables g_h (together with their coefficients) of the remaining equations. Indeed, $\mathcal{C}[\overline{R}]$ is now an MDS code with parameters $[n_l, \mathcal{K}_l, n_l - \mathcal{K}_l + 1]$, the coefficient matrix of this reduced system is a $\mathcal{K}_l \times \mathcal{K}_l$ submatrix of the transpose of a parity-check matrix of the code $\mathcal{C}[\overline{R}]^\perp$ whose minimum distance is $\mathcal{K}_l + 1$, so it is nonsingular, and therefore the system has a unique solution. Finally, the locality is $(r,\delta) := (\mathcal{K}_l, \mathrm{d}(\mathcal{C}[\overline{R}])) = (\mathcal{K}_l, n_l - \mathcal{K}_l + 1)$. □

Remark 3.1.2. With the above notation and when $\operatorname{supp}_{X_l}(V_\Delta) = \{0, 1, \ldots, k_l\}$, it holds that $\mathrm{ev}_{P_l}\left(V_\Delta^l\right)$ is a Reed-Solomon code (and thus an MDS code), and then the locality of $\mathcal{C}_\Delta^P$ is $(\mathcal{K}_l, n_l - \mathcal{K}_l + 1)$.

Remark 3.1.3. Let $\mathcal{C}_\Delta^P$ be an MCC with parameters $[n,k,d]_q$ and locality (r,δ). Then by Proposition 1.4.5 and Corollary 1.3.10, the following inequalities

$$k + d_0 + \left(\left\lceil \frac{k}{r} \right\rceil - 1\right)(\delta - 1) \le k + d + \left(\left\lceil \frac{k}{r} \right\rceil - 1\right)(\delta - 1) \le n + 1 \tag{3.1.3}$$

hold.

Let $\mathcal{C}_\Delta^P$ be an MCC with parameters $[n,k,d]_q$ and locality (r,δ). We define its *defect* (with respect to d_0) as the value D:

$$D := D\left(\mathcal{C}_\Delta^P\right) := n + 1 - k - d_0 - \left(\left\lceil \frac{k}{r} \right\rceil - 1\right)(\delta - 1) \ge 0.$$

Definition 3.1.4. The code $\mathcal{C}_\Delta^P$ is called d_0-*optimal* whenever D vanishes. That is, $\mathcal{C}_\Delta^P$ is optimal and $d = d_0$.

Remarks 3.1.5. The next facts will be useful:

1. The locality (r,δ) provided in Proposition 3.1.1 depends on the variable X_l we choose to interpolate, which allows us to make the best choice of X_l.

2. A d_0-optimal code is always optimal but a code that is not d_0-optimal may be optimal.

3.2. Optimal monomial-Cartesian codes

In this section we give optimal (r,δ)-LRCs which are decreasing MCCs. MCCs are well suited to provide good LRCs. Fixed a supporting field $\mathbb{F}_q$, MCCs are error-correcting codes with unbounded lengths that are constructed by a very simple procedure. This

procedure determines in a very easy way their length, dimension and a bound for the minimum distance (Proposition 1.3.7 and Corollary 1.3.10). The recovery procedure based on interpolation (described in the proof of Proposition 3.1.1) allows us to regard MCCs as LRCs which are very versatile and capable of giving good parameters.

As mentioned, in this section we provide optimal LRCs, but their parameters are not new. Nonetheless we get a large family of optimal LRCs, constructed by a unique and simple procedure, that includes the family of codes introduced in [3] (see Remark 3.2.19 for details) and provides, on the one hand, the parameters of those LRCs over $\mathbb{F}_q$ given in [28] whose lengths are of the form $N(r+\delta-1)$ where N can be written as a product of integers less than or equal to q and, on the other hand, the parameters of those LRCs in [90] with length less than or equal to q^2+q.

Our results will allow us to provide, in the next section, *new* optimal (r,δ)-LRCs coming from subfield-subcodes of MCCs.

We start with the bivariate case.

3.2.1. The bivariate case ($m = 2$)

For simplicity let us denote X_1 by X and X_2 by Y. We look for decreasing sets $\Delta \subseteq E$, E being the set introduced in Subsection 1.3.1, such that the code $\mathcal{C}_\Delta^P$ is optimal, that is, its parameters satisfy

$$k + d_0 + \left(\left\lceil \frac{k}{r} \right\rceil - 1\right)(\delta - 1) = n + 1.$$

Note that, by Remark 1.3.11, $d = d_0$.

Recall we represented E by a grid, see Figure 1.3. From now on, we use shaded regions to represent sets formed by the points in E inside that region. By rectangle we will always refer to a subset of E whose representation as shaded set is a rectangle. The first result in this subsection shows when codes $\mathcal{C}_\Delta^P$, where Δ is decreasing and has the shape of a rectangle, are optimal.

Proposition 3.2.1. *Keep the notation as at the beginning of Section 3.1, where q is a prime power, $m = 2$ and n_1, $n_2 \geq 2$ are the cardinalities of P_1 and P_2. Consider the sets*

$$\Delta = \Delta_{i,j} := \{(e_1, e_2) \mid 0 \leq e_1 \leq i,\ 0 \leq e_2 \leq j\} \subseteq E = \{0, \ldots, n_1 - 1\} \times \{0, \ldots, n_2 - 1\}$$

(see Figure 3.1). Then, the MCC, $\mathcal{C}_\Delta^P$, defined by a set Δ as above is an optimal (r,δ)-LRC if and only if one of the following conditions hold:

- *$i = 0$ and $0 \leq j \leq n_2 - 1$, in which case $(r,\delta) = (1, n_1)$.*
- *$1 \leq i \leq n_1 - 2$ and $j = n_2 - 1$, in which case $(r,\delta) = (i+1, n_1 - i)$.*
- *$0 \leq i \leq n_1 - 1$ and $j = 0$, in which case $(r,\delta) = (1, n_2)$.*
- *$i = n_1 - 1$ and $1 \leq j \leq n_2 - 2$, in which case $(r,\delta) = (j+1, n_2 - j)$.*

Sets Δ as above are denoted by $\Delta_{i,j}^1$.

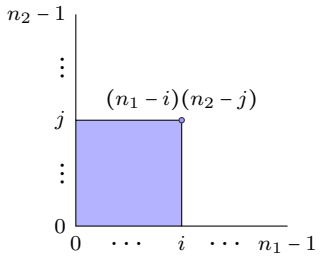


Figure 3.1: Sets $\Delta_{i,j}$ in Proposition 3.2.1

Proof. Clearly, $k=(i+1)(j+1)$ and $d_0=(n_1-i)(n_2-j)$. By interpolating with respect to X, $r=i+1$ and $\delta-1=n_1-i-1$. Then,

$$k+d_0+\left(\left\lceil\frac{k}{r}\right\rceil-1\right)(\delta-1)=(i+1)(j+1)+(n_1-i)(n_2-j)$$
$$+\left(\left\lceil\frac{(i+1)(j+1)}{i+1}\right\rceil-1\right)(n_1-i-1)=n_1n_2+1+i(j+1-n_2),$$

and the code is optimal if and only if $i=0$ or $j=n_2-1$. Note that when $j=n_2-1$ and $i=n_1-1$ one does not get an LRC.

The remaining LRCs are obtained by interpolating with respect to Y, so that $r=j+1$ and $\delta-1=n_2-j-1$. □

In the sequel, we will perform the procedure of considering a subset $\Delta\subseteq E$ (*starting set*) and adding or removing elements to obtain a new subset $\Delta^*\subseteq E$ (*resulting set*). The expression *gaining* (or *losing*) x *units in* a parameter refers to the fact that the resulting code $\mathcal{C}^P_{\Delta^*}$ has a larger (or smaller) value for that parameter in a quantity of x units. We can also say that the parameter *increases* (or *decreases*) x (*units*).

The sets Δ^* obtained by removing the least footprint point on the n_2-1-th row (or n_1-1-th column) of a rectangle $\Delta^1_{i,j}$ with $j=n_2-1$ and $i\geq 1$ (or $i=n_1-1$ and $j\geq 1$) also provide optimal codes since the left-hand side (LHS) of Inequalities (3.1.3) remains the same. Indeed, when removing that point we lose one unit in dimension but we gain one unit in the bound for the minimum distance and r, δ and $\left\lceil\frac{k}{r}\right\rceil$ do not change. The following result generalizes this situation.

Proposition 3.2.2. *With notation as in Proposition 3.2.1, consider the subsets of E*

$$\Delta=\Delta^2_{i,s}:=\{(e_1,e_2)\mid 0\leq e_1\leq i,\ 0\leq e_2\leq n_2-2\}\cup\{(e_1,n_2-1)\mid 0\leq e_1\leq s\},$$

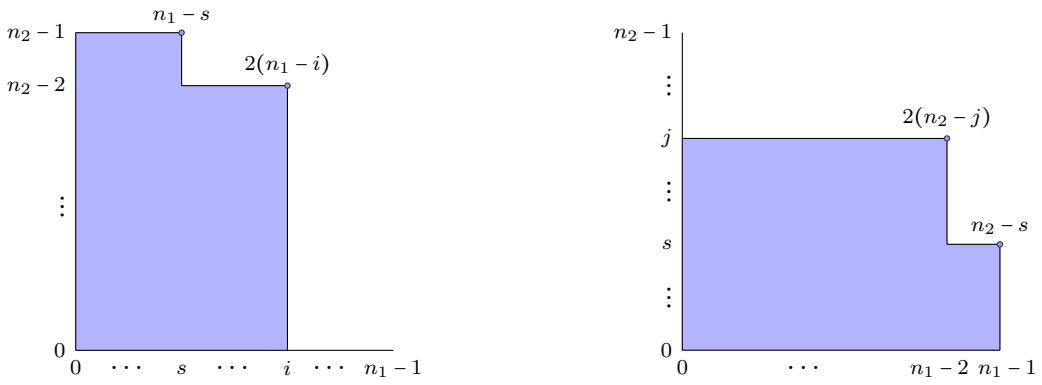
where $\max\{0,2i-n_1\}\leq s<i\leq n_1-2$ *(see Figure 3.2 (1)).*

Then, the MCCs, $\mathcal{C}^P_\Delta$, are optimal $(r,\delta)=(i+1,n_1-i)$-LRCs.

Analogously, the MCCs, $\mathcal{C}^P_\Delta$, where

$$\Delta=\Delta^{2,\sigma}_{j,s}:=\{(e_1,e_2)\mid 0\leq e_1\leq n_1-2,\ 0\leq e_2\leq j\}\cup\{(n_1-1,e_2)\mid 0\leq e_2\leq s\}\subseteq E,$$

$\max\{0,2j-n_2\}\leq s<j\leq n_2-2$ *(see Figure 3.2 (2)) are optimal $(r,\delta)=(j+1,n_2-j)$-LRCs.*



(1) Sets $\Delta^2_{i,s}$ (2) Sets $\Delta^{2,\sigma}_{j,s}$

Figure 3.2: Sets $\Delta^2_{i,s}$ and $\Delta^{2,\sigma}_{j,s}$ in Proposition 3.2.2

Proof. Let us see a proof for the case $\Delta = \Delta^2_{i,s}$. Δ is obtained by removing the $(i-s)$ least footprint points of Δ^1_{i,n_2-1} on the n_2-1-th row with $0 \le s < i$ as long as the footprint

$$\mathrm{F}(s, n_2 - 1) \le \mathrm{F}(i, n_2 - 2).$$

In fact, this last inequality is equivalent to $n_1 - s \le 2(n_1 - i)$ and to $s \ge 2i - n_1$. Interpolating with respect to X, the parameters of the code $\mathcal{C}^P_\Delta$ are $k = (i+1)(n_2-1)+s+1$, $d_0 = n_1 - s$, $r = i+1$ and $\delta - 1 = n_1 - i - 1$, and therefore

$$k + d_0 + \left(\left\lceil \frac{k}{r} \right\rceil - 1\right)(\delta - 1) = (i+1)(n_2-1) + s + 1 + n_1 - s + \left(\left\lceil \frac{(i+1)(n_2-1)+s+1}{i+1} \right\rceil - 1\right)(n_1 - i - 1) = n_1 n_2 + 1.$$

The case $\Delta = \Delta^{2,\sigma}_{j,s}$ can be proved analogously. It suffices to consider the symmetric situation, interpolate with respect to Y and replace i by j and n_1 by n_2. □

The following result completes our family of decreasing sets Δ, that correspond to MCCs, where $m = 2$, giving rise to optimal (r, δ)-LRCs.

Proposition 3.2.3. *With notation as in Proposition 3.2.1, consider the family of subsets of E*

$$\Delta = \Delta^3_{i,j} := \{(e_1, e_2) \mid 0 \le e_1 \le i,\ 0 \le e_2 \le j-1\} \cup \{(0, j)\},$$

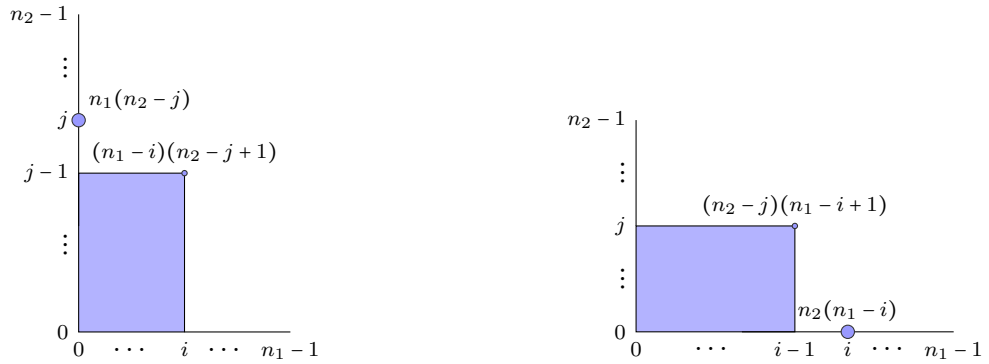
where $1 \le i \le n_1 - 2$ and $\max\left\{1, \frac{i(n_2+1)-n_1}{i}\right\} \le j \le n_2 - 2$ (see Figure 3.3 (1)).

Then, the MCCs, $\mathcal{C}^P_\Delta$, are optimal $(r, \delta) = (i+1, n_1 - i)$-LRCs.

Analogously, the MCCs, $\mathcal{C}^P_\Delta$, where

$$\Delta = \Delta^{3,\sigma}_{i,j} := \{(e_1, e_2) \mid 0 \le e_1 \le i-1,\ 0 \le e_2 \le j\} \cup \{(i, 0)\} \subseteq E,$$

$1 \le j \le n_2 - 2$, and $\max\left\{1, \frac{j(n_1+1)-n_2}{j}\right\} \le i \le n_1 - 2$ (see Figure 3.3 (2)) are optimal $(r, \delta) = (j+1, n_2 - j)$-LRCs.



(1) Sets $\Delta^3_{i,j}$ (2) Sets $\Delta^{3,\sigma}_{i,j}$

Figure 3.3: Sets $\Delta^3_{i,j}$ and $\Delta^{3,\sigma}_{i,j}$ in Proposition 3.2.3

Proof. As before, we only give the proof for the case $\Delta = \Delta^3_{i,j}$ since a proof for $\Delta^{3,\sigma}_{i,j}$ follows as described in the symmetric situation of the proof of Propositon 3.2.2.

Δ is obtained by removing the points (e_1, j), $1 \le e_1 \le i$, of a rectangle

$$\Delta_{i,j} = \{(e_1, e_2) \mid 0 \le e_1 \le i,\ 0 \le e_2 \le j\}$$

with $1 \le i \le n_1 - 2$ and $1 \le j \le n_2 - 2$ such that $\mathrm{F}(0, j) \le \mathrm{F}(i, j-1)$. As a consequence, $n_1(n_2 - j) \le (n_1 - i)(n_2 - j + 1)$, which is equivalent to $i \le \frac{n_1}{n_2 - j + 1}$, or $j \ge \frac{i(n_2+1)-n_1}{i}$. In this case, we interpolate with respect to X and the parameters of the code $\mathcal{C}^P_\Delta$ are $k = (i+1)j + 1$, $d_0 = n_1(n_2 - j)$, $r = i + 1$ and $\delta - 1 = n_1 - i - 1$. Thus,

$$\begin{aligned} k + d_0 + \left(\left\lceil \frac{k}{r} \right\rceil - 1\right)(\delta - 1) &= (i+1)j + 1 + n_1(n_2 - j) + \left(\left\lceil \frac{(i+1)j+1}{i+1} \right\rceil - 1\right)(n_1 - i - 1) \\ &= n_1 n_2 + 1. \end{aligned}$$

□

Remark 3.2.4. The families of (decreasing) MCCs given in Propositions 3.2.1, 3.2.2 and 3.2.3 determine the parameters of all d_0-optimal bivariate ($m = 2$) (r,δ)-LRCs $\mathcal{C}^P_\Delta$ (with any set $\Delta \subseteq E$). That is to say, if $\mathcal{C}^P_\Delta$ is a d_0-optimal LRC, then there exists an MCC, $\mathcal{C}^P_{\Delta^*}$, as in Propositions 3.2.1, 3.2.2 and 3.2.3 having the same parameters n, k, d, r and δ as $\mathcal{C}^P_\Delta$. Therefore, by Remark 1.3.11, we have characterized the optimal bivariate decreasing MCCs. We devote the following subsubsection to prove the first mentioned fact. Since the proof is long, to help the reader, we give a sketch in the next paragraphs.

Without loss of generality, we can suppose that our recovery method interpolates with respect to the variable X. Recall two key facts: (i) the locality (r,δ) of an MCC is bounded by Proposition 3.1.1, and this bound is sharp for decreasing MCCs $\mathcal{C}^P_{\Delta'}$ by Remark 3.1.2, being $r = \#\mathrm{supp}_X(V_{\Delta'})$; and (ii) the footprints of the exponents in the grid E increase when going to the left and to the down.

Now, fixed P and therefore n, and $\#\mathrm{supp}_X(V_\Delta)$ of an arbitrary MCC $\mathcal{C}^P_\Delta$, the first inequality in Inequalities (3.1.3) shows that to reach d_0-optimality it is desirable r to be small and k and d_0 (also, $\delta = n_1 - r + 1$) to be large. We can optimize in this sense the parameters of $\mathcal{C}^P_\Delta$ by "compacting" Δ to get a decreasing set Δ^*, so that the defect of

the above codes satisfies $D\left(\mathcal{C}^P_{\Delta^*}\right) \leq D\left(\mathcal{C}^P_{\Delta}\right)$. By "compacting" we roughly mean: (1) to translate Δ to touch both axis X and Y, (2) to remove empty columns and, (3) for each exponent in the resulting set, to add every element which is inside the rectangle that the exponent "forms" with $(0,0)$. Notice that this way $\#\operatorname{supp}_X(V_\Delta) = \#\operatorname{supp}_X(V_{\Delta^*})$, and performing (1) and (2) (respectively, (3)) we optimize d_0, r -and δ- (respectively, k). Thus, if $\mathcal{C}^P_\Delta$ were d_0-optimal, then $\mathcal{C}^P_{\Delta^*}$ would be too. This reasoning summarizes the main idea behind the forthcoming Lemma 3.2.6 in Subsubsection 3.2.1.1 and allows us to restrict our study to decreasing MCCs.

It remains to show that, fixed P and r, the only decreasing sets $\Delta \subseteq E$ giving rise to d_0-optimal MCCs $\mathcal{C}^P_\Delta$ are those in Propositions 3.2.1, 3.2.2 and 3.2.3. Those sets Δ we are looking for must satisfy $\Delta \subseteq \Delta^1_{r-1,n_2-1}$, and since $\mathcal{C}^P_{\Delta^1_{r-1,n_2-1}}$ is d_0-optimal by Proposition 3.2.1, successively removing the least footprint points in Δ^1_{r-1,n_2-1} is the optimal way to get the mentioned sets Δ. Assume that $r-1 \leq \frac{n_1}{2}$, the opposite case follows similarly. Before reaching the smallest (with respect to inclusion) set $\mathfrak{M} \subseteq E$ among those considered in the above mentioned propositions (that will be $\mathfrak{M} = \Delta^3_{r-1,b}$ for some b or $\mathfrak{M} = \Delta^2_{r-1,0}$ –denoted $\mathfrak{M} = M^i_1$– when $i = r-1 \leq \frac{n_1}{2}$, and $\mathfrak{M} = \Delta^2_{i,2i-n_1}$ –denoted $\mathfrak{M} = M^i_2$–, otherwise), the removed exponents go from right to left coming from upper to lower rows. The first $r-1$ removed exponents provide every set of Proposition 3.2.2.

If $\mathfrak{M} = \Delta^3_{r-1,b}$, the following removed exponents before reaching $\mathfrak{M}$ provide sets Δ such that $\Delta' \subseteq \Delta \subseteq \Delta''$, where $(\Delta', \Delta'') \in \left\{\left(\Delta^3_{r-1,n_2-2}, \Delta^2_{r-1,0}\right), \left(\Delta^3_{r-1,j-1}, \Delta^3_{r-1,j}\right)\right\}$ for some j. A set $\Delta \neq \Delta', \Delta''$, does not provide a d_0-optimal code since in the LHS of Inequalities (3.1.3) the term $\left(\left\lceil \frac{k}{r} \right\rceil - 1\right)(\delta - 1)$ is the same for both Δ and Δ', but the term $k + d_0$ is less for Δ than for Δ'. The above two paragraphs are a summary of the first part of the proof of Theorem 3.2.11. This paragraph summarizes the statements of Lemmas 3.2.8 and 3.2.9 (under the case $r-1 \leq \frac{n_1}{2}$).

Finally, once reached the set $\mathfrak{M}$, we are forced to remove points from lower rows, causing the difference between the footprints of the exponents removed becomes smaller, and, then, the resulting sets Δ do not give either d_0-optimal codes. This fact is showed in the rest of the proof of Theorem 3.2.11.

Notice that when one removes exponents from right to left inside a row, the bound on the minimum distance increases the same quantity (a multiple of one unit more than its second coordinate), but when we remove exponents from lower rows, the gain on the bound of the minimum distance is smaller, worsening the defect of the code. See Figure 3.4 for an example, where $\Delta^3_{2,5}$ gives a d_0-optimal code (defect 0) but, by removing its four exponents from lowest to higher footprint, we do not get d_0-optimality as the obtained sequence of defects is 8, 4, 2, 8.

3.2.1.1. Proof of Remark 3.2.4

The forthcoming Theorem 3.2.11 proves the assertion in the first paragraph of Remark 3.2.4. Before proving our theorem we need some previous definitions and results.

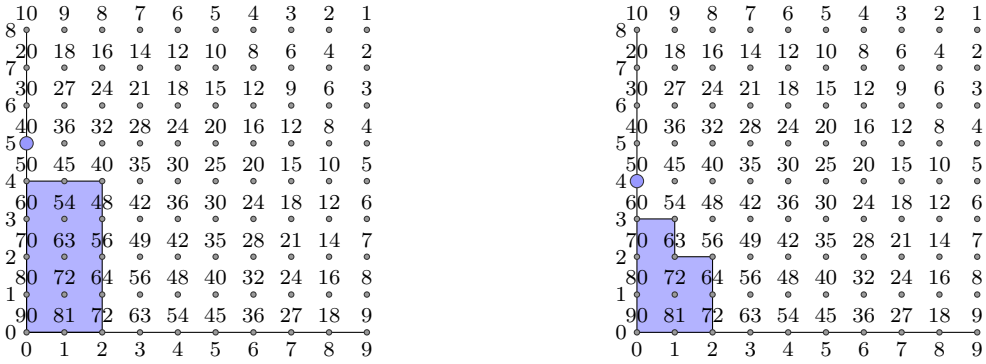


Figure 3.4: On the right, the set obtained by removing four exponents of $\Delta^3_{2,5}$ (on the left) as described in Remark 3.2.4

Remark 3.2.4 may be used to facilitate reading of this subsubsection.

Definition 3.2.5. A set $\Delta \subseteq E$ is said to be *optimal* if the code $\mathcal{C}^P_\Delta$ is d_0-optimal, that is, $D = 0$, D being the defect of $\mathcal{C}^P_\Delta$ given above Definition 3.1.4.

Let Δ (respectively, Δ^*) be a starting (respectively, resulting) set included in E. We say that Δ^* is obtained following a *natural order* if Δ^* comes from Δ by succesively removing (respectively, adding) points of least footprint in Δ (respectively, largest footprint in $E\backslash\Delta$). Assume that $[n,k,\geq d_0]_q$ (respectively, $[n^*,k^*,\geq d_0^*]_q$) are the parameters, and (r,δ) (respectively, (r^*,δ^*)) the locality of the code $\mathcal{C}^P_\Delta$ (respectively, $\mathcal{C}^P_{\Delta^*}$). Then, we define *variation (of the code $\mathcal{C}^P_{\Delta^*}$ with respect to $\mathcal{C}^P_\Delta$) produced in the LHS of Inequalities* (3.1.3) as the value

$$k^* + d_0^* + \left(\left\lceil \frac{k^*}{r^*} \right\rceil - 1\right)(\delta^* - 1) - \left(k + d_0 + \left(\left\lceil \frac{k}{r} \right\rceil - 1\right)(\delta - 1)\right).$$

Denote $\boldsymbol{\epsilon}_1 = (1,0)$ and $\boldsymbol{\epsilon}_2 = (0,1)$.

Lemma 3.2.6. *Let Δ be a subset of E. Set*

$$a := \min\{e_1 \mid (e_1,e_2) \in \Delta\} \quad \textit{and} \quad b := \min\{e_2 \mid (e_1,e_2) \in \Delta\}.$$

Fix an index $l \in \{1,2\}$ and construct the set Δ^* as follows:

(1) Set $\Delta_0 := (-a,-b) + \Delta$. Define

$$T_0 := \{t \in \{1,2,\ldots,n_l - 1\} \mid \textit{ there is no } \boldsymbol{e} \in \Delta_0 \textit{ such that } e_l = t\},$$

$c_0 := \#T_0$ *and* $t_0 := \min T_0$.

(2) For every $i = 1,\ldots,c_0$, define inductively

$$\Delta_i := \{\boldsymbol{e} \in \Delta_{i-1} \mid e_l < t_{i-1}\} \cup \{\boldsymbol{e} - \boldsymbol{\epsilon}_l \mid \boldsymbol{e} \in \Delta_{i-1} \textit{ with } e_l > t_{i-1}\},$$

$T_i := \{t-1 \mid t \in T_{i-1}\backslash\{t_{i-1}\}\}$ *and* $t_i := \min T_i$.

(3) Set $l' := j \in \{1,2\}\backslash\{l\}$ *and define*

$$M := \max\{e_l \in \{0,1,\dots,n_l-1\} \mid \boldsymbol{e} \in \Delta_{c_0}\}$$

and

$$v_M := \max\{e_{l'} \mid e_l = M \text{ and } \boldsymbol{e} \in \Delta_{c_0}\}.$$

Consider the set

$$\Delta'_M = \Delta_{c_0} \cup \{\boldsymbol{e} \in E\backslash\Delta_{c_0} \mid e_l \le M,\ e_{l'} \le v_M\}.$$

(4) For every $i = M-1, M-2, \dots, 0$, *let*

$$v_i := \max\{e_{l'} \mid e_l = i \text{ and } \boldsymbol{e} \in \Delta'_{i+1}\}$$

and inductively set

$$\Delta'_i := \Delta'_{i+1},$$

when $v_i \le v_{i+1}$, *and*

$$\Delta'_i := \Delta'_{i+1} \cup \{\boldsymbol{e} \in E\backslash\Delta'_{i+1} \mid e_l \le i,\ e_{l'} \le v_i\},$$

when $v_i > v_{i+1}$.

(5) Finally, $\Delta^* := \Delta'_0$.

Then, when comparing Δ^* *with* Δ, *the variation produced in the LHS of Inequalities* (3.1.3) *is* ≥ 0, *that is,* $D(C^P_{\Delta^*}) \le D(C^P_\Delta)$.

Proof. Let $[n,k,\ge d_0]_q$ and (r,δ) (respectively, $[n_0,k_0,\ge (d_0)_0]_q$ and (r_0,δ_0)) be the parameters and locality of the code $\mathcal{C}^P_\Delta$ (respectively, $\mathcal{C}^P_{\Delta_0}$). The MCCs $\mathcal{C}^P_\Delta$ and $\mathcal{C}^P_{\Delta_0}$ are pseudoisometric, so $n = n_0$, $k = k_0$ but $d_0 \le (d_0)_0$ because the footprints of the elements in E increase when one considers exponents going to the left and to the down. As for the localities, we know from Proposition 3.1.1 that r, $r_0 \ge \mathcal{K}_l$ and δ, $\delta_0 \le n_l - \mathcal{K}_l + 1$. Let $[n_{c_0},k_{c_0},\ge (d_0)_{c_0}]_q$ be the parameters and (r_{c_0},δ_{c_0}) the locality of $\mathcal{C}^P_{\Delta_{c_0}}$. Suppose $l = 1$ (the remaining case is analogue), Step (2) removes vertical segments in $E\backslash\Delta_0$ and then $\#\operatorname{supp}_{X_l}(V_{\Delta_{c_0}}) = \max\left(\operatorname{supp}_{X_l}(V_{\Delta_{c_0}})\right) + 1$, thus $n = n_{c_0}$, $k = k_{c_0}$ but $r \ge r_{c_0} = \mathcal{K}_l$, $\delta \le \delta_{c_0} = n_l - \mathcal{K}_l + 1$ (see Remark 3.1.2) and $d_0 \le (d_0)_{c_0}$. Let $(i,j) \in \Delta_{c_0}$. Since every element in E inside the rectangle that (i,j) sets from $(0,0)$ has larger footprint than (i,j), it makes sense to include all of them in the new set Δ in order to increase the dimension of the code and thus decreasing the defect. We perform it on Step (4), so that if $[n^*,k^*,\ge d_0^*]_q$ are the parameters and (r^*,δ^*) the locality of $\mathcal{C}^P_{\Delta^*}$, then $n = n^*$, $k \le k^*$, $d_0 \le d_0^*$, $r \ge r^* = \mathcal{K}_l$ and $\delta \le \delta^* = n_l - \mathcal{K}_l + 1$. Therefore,

$$k + d_0 + \left(\left\lceil \frac{k}{r} \right\rceil - 1\right)(\delta - 1) - \left(k^* + d_0^* + \left(\left\lceil \frac{k^*}{r^*} \right\rceil - 1\right)(\delta^* - 1)\right) \le 0. \qquad \square$$

Remark 3.2.7. Let Δ and Δ^* be as in Lemma 3.2.6. Then, $\#\operatorname{supp}_{X_l}(V_\Delta) = \#\operatorname{supp}_{X_l}(V_{\Delta^*})$. Figure 3.5 shows some simple cases where that procedure (for $l = 1$) is applied.

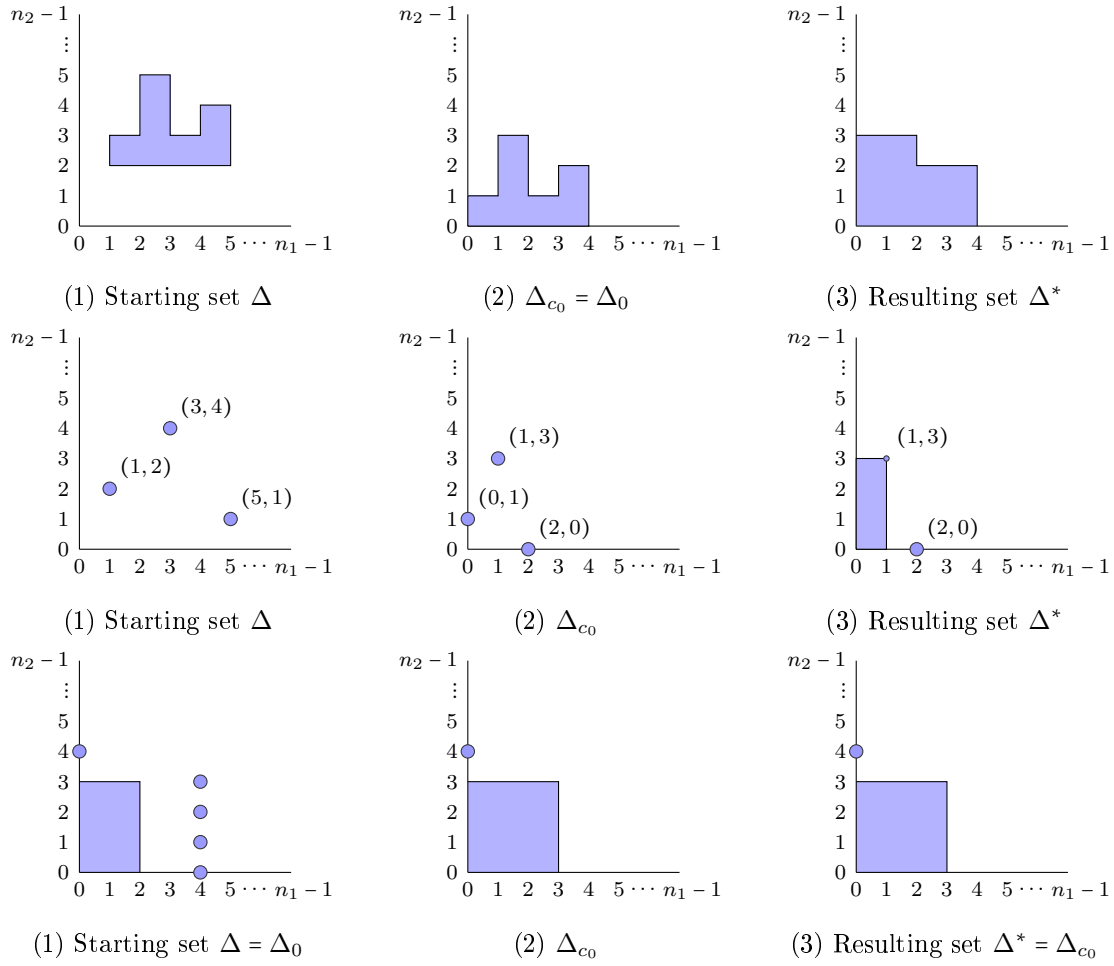


Figure 3.5: Examples in Remark 3.2.7

Lemma 3.2.8. *Keep the notation as in Proposition 3.2.3. Let Δ_1 and Δ_2 be two subsets of E of the form $\Delta^3_{i,j}$ (respectively, $\Delta^{3,\sigma}_{i,j}$) for some indices i, j, and such that Δ_2 is obtained by removing points of Δ_1 following a natural order (see the paragraph below Definition 3.2.5 where this concept was introduced). Then, there is no d_0-optimal code $\mathcal{C}^P_\Delta$ such that:*

1. $\Delta_2 \subsetneq \Delta \subsetneq \Delta_1$, *and*
2. Δ *is not of the form* $\Delta^3_{i,j}$ *(respectively,* $\Delta^{3,\sigma}_{i,j}$*).*

Proof. We perform the proof for the case when Δ_1 and Δ_2 are of the form $\Delta^3_{i,j}$. The proof for the remaining case is analogue. It suffices to assume that

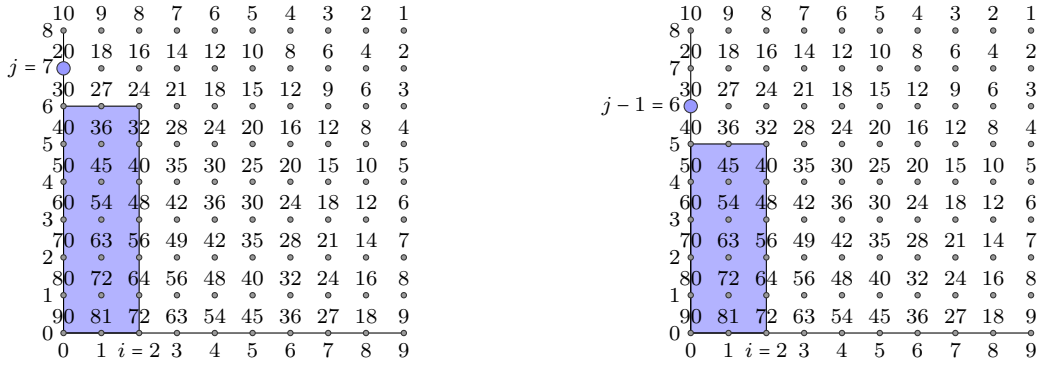
$$\Delta_1 = \Delta^3_{i,j} = \{(e_1,e_2) \mid 0 \le e_1 \le i,\ 0 \le e_2 \le j-1\} \cup \{(0,j)\}$$

and

$$\Delta_2 = \Delta^3_{i,j-1} = \{(e_1,e_2) \mid 0 \le e_1 \le i,\ 0 \le e_2 \le j-2\} \cup \{(0,j-1)\},$$

where $1 \le i \le n_1 - 2$ and $\left\lceil \frac{i(n_2+1)-n_1}{i} \right\rceil + 1 \le j \le n_2 - 2$. Thus, we have to prove that there is

no optimal set Δ such that $\Delta_2 \subsetneq \Delta \subsetneq \Delta_1$. A toy example in the case $n_1 = 10$ and $n_2 = 9$ is showed in Figure 3.6.



(1) Set Δ_1 (2) Set Δ_2

Figure 3.6: Sets Δ_1 and Δ_2 in the proof of Lemma 3.2.8

We start by removing the point $(0, j)$ in Δ_1 ($(0, 7)$ in the example). Then the LHS of Inequalities (3.1.3) loses one unit in dimension and also $\delta - 1$ units (since $\left\lceil \frac{k}{r} \right\rceil$ decreases one unit), whereas in the bound for the minimum distance we gain

$$\mathrm{F}(i, j-1) - \mathrm{F}(0, j) = (n_1 - r + 1)(n_2 - j + 1) - n_1(n_2 - j) = n_1 - (r-1)(n_2 - j + 1).$$

Thus, the variation produced in the LHS of Inequalities (3.1.3) is

$$n_1 - (r-1)(n_2 - j + 1) - \delta = n_1 - (r-1)(n_2 - j + 1) - (n_1 - r + 1) = -(r-1)(n_2 - j) < 0$$

(because $r = i + 1 \geq 2$). In our example we lose $\delta = 8$ (units) and gain 4, with a variation equal to -4.

Iterating our procedure, for each point on the $(j-1)$-th row we remove (excepting $(0, j-1)$), we lose 1 in dimension, the bound on the minimum distance increases $n_2 - j + 1$ and the remaining summands of the LHS of Inequalities (3.1.3) remain the same. Therefore the only way to sum $(r-1)(n_2 - j)$ units so that the variation produced in the LHS of Inequalities (3.1.3) equals 0, and the defect D vanishes, holds when we remove the next $r-1$ points on the $(j-1)$-th row following a natural order. Then we get Δ_2 and our result is proved. □

Lemma 3.2.9. *Keep the notation as in Proposition 3.2.2. Consider a set $S = \Delta^2_{i,0}$, where $1 \leq i \leq n_1 - 2$, and a set $S^\sigma = \Delta^{2,\sigma}_{j,0}$, where $1 \leq j \leq n_2 - 2$. Then, there is no d_0-optimal code $\mathcal{C}^P_\Delta$, Δ being the resulting set of removing less than $i+1$ points from S (or less than $j+1$ points from S^σ) following a natural order.*

Proof. Consider the set $S = \{(e_1, e_2) \mid 0 \leq e_1 \leq i,\ 0 \leq e_2 \leq n_2 - 2\} \cup \{(0, n_2 - 1)\}$, which we show in Figure 3.7. The proof for S^σ is analogue and we omit it.

Recall from the proof of Proposition 3.2.3 that $\mathrm{F}(0, n_2 - 1) \leq \mathrm{F}(i, n_2 - 2)$ if and only if $i \leq \frac{n_1}{2}$ and in such case S is optimal. We divide our proof in two cases according to

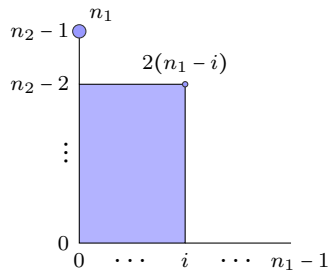
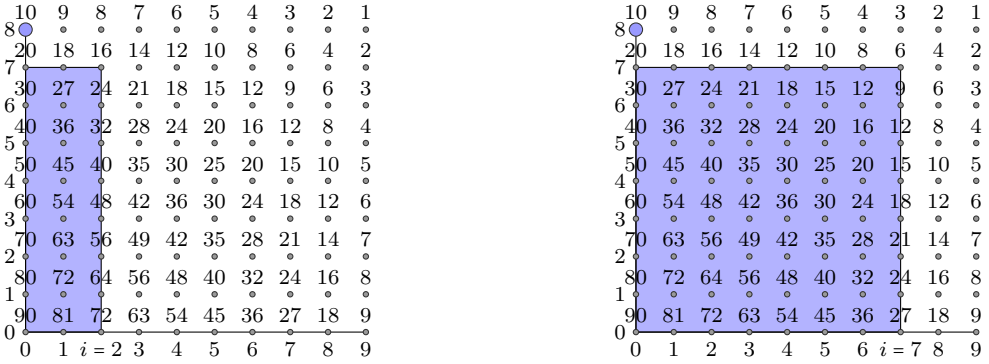


Figure 3.7: Set S in the proof of Lemma 3.2.9

$i \leq \frac{n_1}{2}$ or $i > \frac{n_1}{2}$. Figure 3.8 shows an example of the case $n_1 = 10$ and $n_2 = 9$ showing sets S, where $i = 2 \leq \frac{n_1}{2}$ (Figure 3.8 (1)) and $i = 7 > \frac{n_1}{2}$ (Figure 3.8 (2)), with the aim of making easier the understanding of the proof.



(1) Set S for $i \leq \frac{n_1}{2}$ (2) Set S for $i > \frac{n_1}{2}$

Figure 3.8: Toy example in the proof of Lemma 3.2.9

Assume $i \leq \frac{n_1}{2}$, following a natural order the first point to remove is $(0, n_2-1)$. Then, in the LHS of Inequalities (3.1.3) we lose 1 (unit) in dimension plus $\delta - 1$ and gain

$$\mathrm{F}(i, n_2-2) - \mathrm{F}(0, n_2-1) = 2(n_1 - r + 1) - n_1 = n_1 - 2r + 2$$

in the bound for the minimum distance. Thus, the variation produced in the LHS of Inequalities (3.1.3) is

$$n_1 - 2r + 2 - \delta = n_1 - 2r + 2 - (n_1 - r + 1) = -r + 1 < 0$$

(because $r = i + 1 \geq 2$).

Notice that for each point on the (n_2-2)-th row we remove (excepting $(0, n_2-2)$), the values r, δ and $\left\lceil \frac{k}{r} \right\rceil$ do not change, we lose 1 in dimension and gain 2 in the footprint of the exponents in that row. Keeping our procedure of removing points by following a natural order, if we were in the best situation, that is, the natural order was to remove points of least footprint on the (n_2-2)-th row, then the quantity gained in the footprints of the exponents would just be the quantity gained in the bound of the minimum distance, so in the LHS of Inequalities (3.1.3) we would sum 1 every time we remove a point. Therefore,

removing the next $r-1=i$ points on the (n_2-2)-th row, we would obtain the set

$$\{(e_1,e_2)\mid 0\leq e_1\leq i,\ 0\leq e_2\leq n_2-3\}\cup\{(0,n_2-2)\},$$

which in the best situation would be optimal, and no optimal set is obtained by removing less than $i+1$ points from S.

To conclude suppose now that $i>\frac{n_1}{2}$. In this case the set S is not optimal. Indeed, the LHS of Inequalities (3.1.3) for the code $\mathcal{C}_S^P$ is

$$n_1n_2+1+n_1-2i,$$

which is less than n_1n_2+1. Removing the point with least footprint, we lose δ units in the LHS of Inequalities (3.1.3). Then, we need to add

$$2i-n_1+\delta=2i-n_1+(n_1-i)=i$$

units to the LHS of Inequalities (3.1.3). These units should come from the sum $k+d_0$ so that the resulting set is optimal. The same reasoning given in the above paragraph explains that the best situation for gaining units happens by removing points on the (n_2-2)-th row and again, by removing less than i more points from S, we cannot get an optimal set, which concludes the proof. □

Example 3.2.10. Consider the example showed in Figure 3.8, where $n_1=10$ and $n_2=9$, and let us apply Lemma 3.2.9. If $i=2\leq\frac{n_1}{2}$, then $(r,\delta)=(3,8)$ and we must show that the resulting set of removing less than 3 points from S following a natural order is not optimal. When we remove the first point, $(0,8)$, then we lose $\delta=8$ and gain 6 in the LHS of Inequalities (3.1.3), thus we lose 2. The next and last point to remove is $(2,7)$. Here, we lose 1 unit in dimension and gain 2 in the bound for the minimum distance, but the resulting set Δ is not optimal since $D(\mathcal{C}_\Delta^P)=1$.

As for the case $i=7\geq\frac{n_1}{2}$, we have $(r,\delta)=(8,3)$ and the resulting set of removing less than 8 points from S following a natural order is not optimal. Indeed, when we remove the first point, $(7,7)$, then we lose $\delta=3$ and gain 2 units in the LHS of Inequalities (3.1.3), thus we lose 1. The next six points to remove (together with the defect of the resulting code) are $(6,7)$ $(D=1)$, $(7,6)$ $(D=1)$, $(0,8)$ $(D=2)$, $(5,7)$ $(D=1)$, $(4,7)$ $(D=2)$ and $(6,6)$ $(D=3)$ and no such a set is optimal.

Now we are ready to prove the assertion given in Remark 3.2.4.

Theorem 3.2.11. *The families of MCCs given in Propositions 3.2.1, 3.2.2 and 3.2.3 determine the parameters of all bivariate ($m=2$) MCCs which are d_0-optimal (r,δ)-LRCs. That is to say, if $\mathcal{C}_\Delta^P$ is a d_0-optimal LRC, then there exists a MCC, $\mathcal{C}_{\Delta^*}^P$, as in Propositions 3.2.1, 3.2.2 or 3.2.3 having the same parameters n, k, d, r and δ as $\mathcal{C}_\Delta^P$.*

Proof. We start by checking d_0-optimality when interpolating with respect to X. Unless we say otherwise, every process of removing (or adding) points of (or to) a subset in E is performed by following a natural order (see the definition below Definition 3.2.5). We

also exemplify the proof for the case $n_1 = 10$ and $n_2 = 9$. Let us fix $\mathcal{K} := \#\mathrm{supp}_X(V_\Delta)$ the cardinality of the set $\mathrm{supp}_X(V_\Delta)$ of the optimal sets $\Delta \subseteq E$ that we want to find. By Lemma 3.2.6, we can restrict to decreasing sets Δ (the resulting sets in the construction presented in that lemma), so $\mathrm{supp}_X(V_\Delta) = \{0, 1, \ldots, i\}$ and $r = \mathcal{K} = i + 1$, by Remark 3.1.2). Since we know that every set Δ with $i = 0$ is optimal (Proposition 3.2.1) and we are not interested in those where $i = n_1 - 1$ as they do not provide LRCs, we assume $1 \leq i = r - 1 \leq n_1 - 2$. Thus, it suffices to start with the following set:

$$\Delta^1_{i,n_2-1} = \{(e_1, e_2) \mid 0 \leq e_1 \leq i, 0 \leq e_2 \leq n_2 - 1\}$$

(see Figure 3.9 corresponding to our example where $n_1 = 10$, $n_2 = 9$) and to remove points from it to get the sets Δ we are looking for.

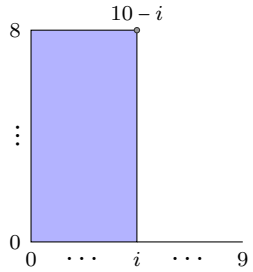


Figure 3.9: Set Δ^1_{i,n_2-1} in the proof of Theorem 3.2.11

This set is optimal by Proposition 3.2.1 and the largest optimal set with $r = i + 1$. Proposition 3.2.2 proves that the $i - s$ sets obtained from Δ^1_{i,n_2-1} by removing one by one until $i - s$ points on the $(n_2 - 1)$-th row are also optimal for $s = 0$ if $i \leq \frac{n_1}{2}$ and $s = 2i - n_1$ if $i > \frac{n_1}{2}$. The last obtained set is

$$\Delta^2_{i,0} = \{(e_1, e_2) \mid 0 \leq e_1 \leq i,\ 0 \leq e_2 \leq n_2 - 2\} \cup \{(0, n_2 - 1)\},$$

when $i \leq \frac{n_1}{2}$, and

$$M^i_2 := \Delta^2_{i,2i-n_1} = \{(e_1, e_2) \mid 0 \leq e_1 \leq i,\ 0 \leq e_2 \leq n_2 - 2\} \cup \{(e_1, n_2 - 1) \mid 0 \leq e_1 \leq 2i - n_1\},$$

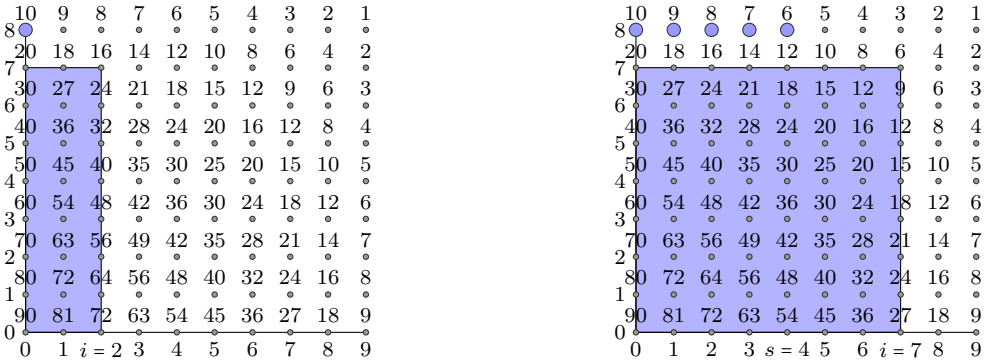
if $i > \frac{n_1}{2}$.

Figure 3.10 (1) shows $\Delta^2_{2,0}$ for the case $n_1 = 10$, $n_2 = 9$. Within the same case, one can see M^7_2 in Figure 3.10 (2).

Now if $i > \frac{n_1}{2}$, M^i_2 is the least (with respect to inclusion) optimal set such that $r = i+1$ considered in Propositions 3.2.1 and 3.2.2. With respect to $i \leq \frac{n_1}{2}$, define

$$M^i_1 := \{(e_1, e_2) \mid 0 \leq e_1 \leq i, 0 \leq e_2 \leq b - 1\} \cup \{(0, b)\},$$

where $b = \left\lceil \frac{i(n_2+1)-n_1}{i} \right\rceil$ (Figure 3.11 shows M^2_1 for the case $n_1 = 10$, $n_2 = 9$) and the unique optimal sets Δ such that $M^i_1 \subseteq \Delta \subseteq \Delta^2_{i,0}$ are among those given in Proposition 3.2.3 (see Proposition 3.2.3 and Lemmas 3.2.8 and 3.2.9). Then, M^i_1 is the least optimal set such that $r = i + 1$ considered in Propositions 3.2.1, 3.2.2 and 3.2.3 when $i \leq \frac{n_1}{2}$. Notice that M^i_1 may be denoted either $\Delta^2_{i,0}$ or $\Delta^3_{i,b}$.



(1) $\Delta^2_{2,0}$ (2) M^7_2

Figure 3.10: Sets $\Delta^2_{2,0}$ and M^7_2 in the proof of Theorem 3.2.11

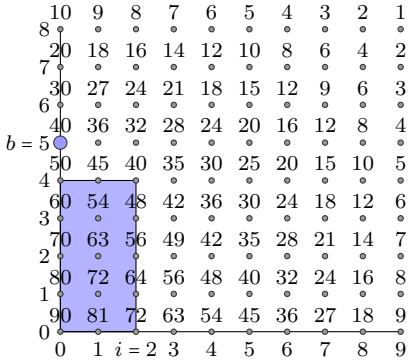


Figure 3.11: Set M^2_1 in the proof of Theorem 3.2.11

Therefore, it only remains to prove that under the above cases, there is no optimal set Δ such that $\Delta \subset M^i_1$ or $\Delta \subset M^i_2$. Recall that the parameters corresponding to an optimal set must attain the bound

$$k + d_0 + \left(\left\lceil \frac{k}{r} \right\rceil - 1\right)(\delta - 1) \leq n_1 n_2 + 1.$$

Let us start with M^i_2. If we remove up to s $(= 2i - n_1)$ points, then r, δ and $\left\lceil \frac{k}{r} \right\rceil$ do not change. The first point to remove is $(s, n_2 - 1)$, but then we lose one unit in dimension, and it cannot be recovered by adding one unit in the bound for the minimum distance because $\mathrm{F}(i, n_2 - 2) = \mathrm{F}(s, n_2 - 1)$. Then, the variation produced in the LHS of Inequalities (3.1.3) considering M^i_2 as the starting set is $V := V(M^i_2) := -1$. In order to achieve $V = 0$, the best situation would hold when the process of removing points was from right to left on the $(n_2 - 1)$-th row (without removing points from rows below with the same footprint that the previous removed point) because that way, for every removed point we would lose one unit in dimension and gain one unit in the bound for the minimum distance. But even in those cases we would not get $V = 0$.

Suppose that, in our next step, we have removed the s points in M^i_2 on the $(n_2 - 1)$-th row from right to left obtaining the set

$$S^i := \{(e_1, e_2) \mid 0 \leq e_1 \leq i, 0 \leq e_2 \leq n_2 - 2\} \cup \{(0, n_2 - 1)\},$$

which is not optimal by the reasoning just given (see Figure 3.12 for the case $n_1 = 10$, $n_2 = 9$ and $i = 7$).

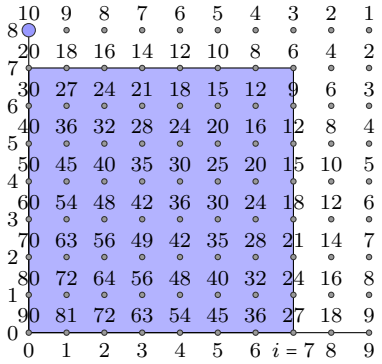


Figure 3.12: Set S^7 in the proof of Theorem 3.2.11

Next we study what happens when removing points of either M_1^i or S^i according to our two cases $i \leq \frac{n_1}{2}$, $i > \frac{n_1}{2}$. Our reasoning differentiates each previous case in two new subcases. The first subcase corresponds to remove a multiple of r points and the second one to delete an intermediate number of points. Since we are looking for sets Δ with fixed value r corresponding to their locality, the reasoning will finish when we delete the last remaining point in the i-th column because if one performs a new step, the new code will have smaller locality.

Suppose that we remove λr points of the starting sets M_1^i or S^i. Then, in the LHS of Inequalities (3.1.3) we lose λr units (corresponding to the dimension) plus $\lambda(\delta-1)$ units (because for every r points removed, $\left\lceil \frac{k}{r} \right\rceil$ decreases one unit), and we gain at most λn_1 in the bound for the minimum distance (because the best situation holds by deleting $(0,j)$ and every point at the right of $(0,j-1)$, $j = b,\ldots,b-\lambda+1$, for M_1^i, and $j = n_2-1,\ldots,n_2-\lambda$ for S^i). Then, the variation produced in LHS of Inequalities (3.1.3) would be smaller than or equal to

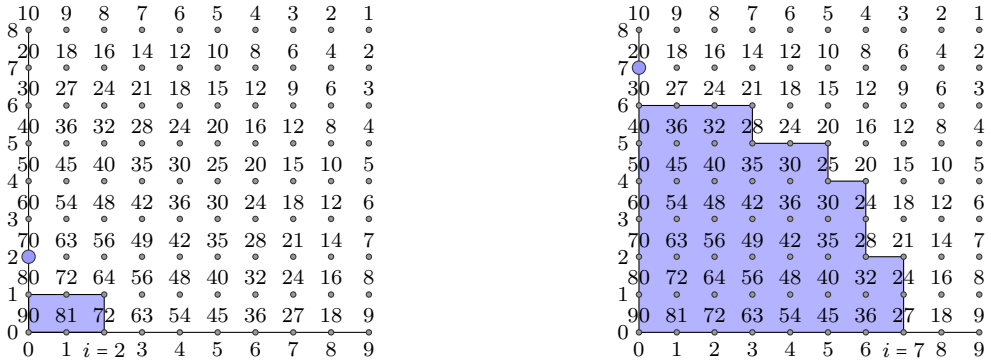
$$-\lambda r - \lambda(\delta-1) + \lambda n_1 = -\lambda r - \lambda(n_1 - r) + \lambda n_1 = 0.$$

Nevertheless, the mentioned gaining does not happen because for every $j < b$ (for M_1^i) and $j \leq n_2 - 1$ (for S^i) there are points in rows below with lower footprint than $(0,j)$, at least the point $(i, j-1)$. Thus, we cannot get the mentioned best situation and if we remove a multiple of r points from M_1^i or S^i, we do not find optimal sets. Figure 3.13 (1) (respectively, 3.13 (2)) shows what happens in our example with $n_1 = 10$, $n_2 = 9$ when removing $3 \cdot (3 = r)$ (respectively, $2 \cdot (8 = r)$) points from M_1^2 (respectively, S^7).

Suppose now that we remove an intermediate number of points, that is, $\lambda r - s$ $(1 \leq s < r)$ points from M_1^i or S^i. For this end, it suffices to start with the set

$$\overline{S}^i = \{(e_1,e_2) \mid 0 \leq e_1 \leq i, 0 \leq e_2 \leq n_2 - 2\} \cup \{(0, n_2-1)\},$$

where we do not impose any restriction to the index i. Notice that $\overline{S}^i = S^i$ when $i > \frac{n_1}{2}$ and $M_1^i \subseteq \overline{S}^i$ otherwise. When $i \leq \frac{n_1}{2}$, there is no loss of generality if one considers $\overline{S}^i$



(1) (2)

Figure 3.13: Resulting set (1) (respectively, (2)) when removing 9 (respectively, 16) points from M_1^2 (respectively, S^7) in the proof of Theorem 3.2.11

instead of M_1^i because the sets obtained by removing an intermediate number of points can be obtained either by removing $\lambda_0 r - s$ points from M_1^i or by removing $\lambda r - s$ points from $\overline{S}^i$, where $\lambda = \lambda_0 + n_2 - 1 - b$.

Then, removing points of $\overline{S}^i$ as mentioned, we obtain a set S' whose bound on the minimum distance is $d_0 \leq n_1(\lambda+1) - (\lambda+1)$ which is not optimal. We prove it by contradiction. Assume that this set is optimal, that is, $k + d_0 + t = n_1 n_2 + 1$, where $t = \left(\left\lceil \frac{k}{r} \right\rceil - 1\right)(n_1 - r)$. Now, if we add to this set the next $(\lambda-1)r$ points (following a natural order) without altering the locality r, we obtain a new set S'' that satisfies

$$\begin{aligned} n_1 n_2 + 1 &\geq k + (\lambda-1)r + d_0 + \Delta d + \left(\left\lceil \frac{k + (\lambda-1)r}{r} \right\rceil - 1\right)(n_1 - r) \\ &= k + (\lambda-1)r + d_0 + \Delta d + t + (\lambda-1)(n_1 - r) = k + d_0 + \Delta d + t + (\lambda-1)n_1 \\ &= n_1 n_2 + 1 + \Delta d + (\lambda-1)n_1 \geq n_1 n_2 + 1 - (\lambda-1)n_1 + (\lambda-1)n_1 \\ &= n_1 n_2 + 1, \end{aligned}$$

where Δd is the variation produced in the bound on the minimum distance when obtaining S'' from S'. Then $-(\lambda-1)n_1 \leq \Delta d < 0$ and thus, $\Delta d = -(\lambda-1)n_1$. Therefore, we get an optimal set S'' that could be also obtained by removing less than r points of $\overline{S}^i$, a contradiction by Lemma 3.2.9. To illustrate this last part of the proof, in Figures 3.14 (1), 3.15 (1) and 3.16 (1) (respectively, 3.14 (2), 3.15 (2) and 3.16 (2)) we show (within the example where $n_1 = 10$, $n_2 = 9$) the sets $\overline{S}^2$ (corresponding to the case $i \leq \frac{n_1}{2}$), S' obtained by removing $\lambda r - s = 6 \cdot 3 - 2$ points from $\overline{S}^2$ and S'' obtained by adding $(\lambda-1)r = (6-1)3$ points to S' (respectively, $\overline{S}^7$ (corresponding to the case $i > \frac{n_1}{2}$), S' obtained by removing $\lambda r - s = 2 \cdot 8 - 5$ from $\overline{S}^7$ and S'' obtained by adding $(\lambda-1)r = (2-1)8$ points to S').

We have checked that fixed $\#\mathrm{supp}_X(V_\Delta)$, the only d_0-optimal codes obtained by interpolating with respect to X are of the type of those given in Propositions 3.2.1, 3.2.2 and 3.2.3. It is clear that one can perform the same reasoning by interpolating with respect to Y. This concludes the proof after noticing that although in the procedure of

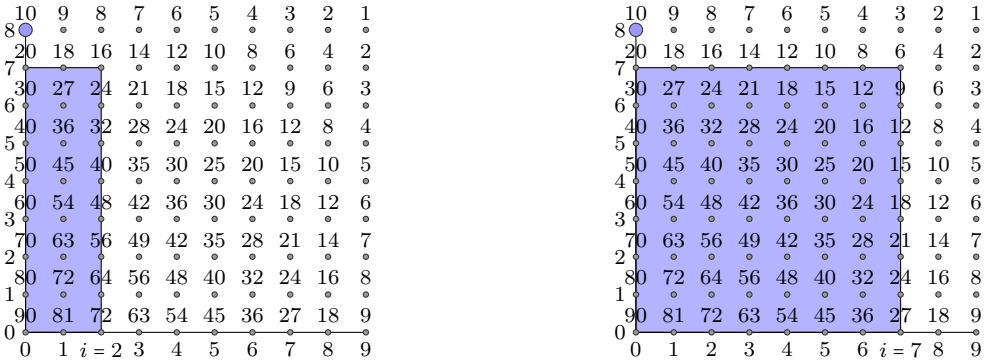


Figure 3.14: Sets $\overline{S}^2$ and $\overline{S}^7$ in the proof of Theorem 3.2.11

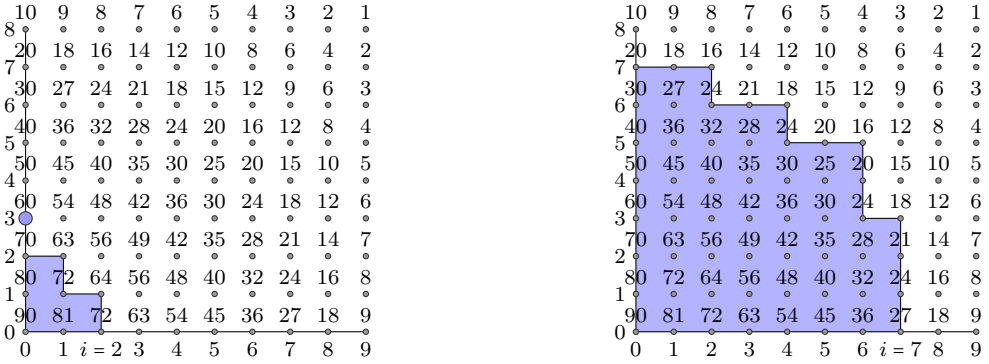


Figure 3.15: Sets S' obtained by removing points from $\overline{S}^i$ in the proof of Theorem 3.2.11

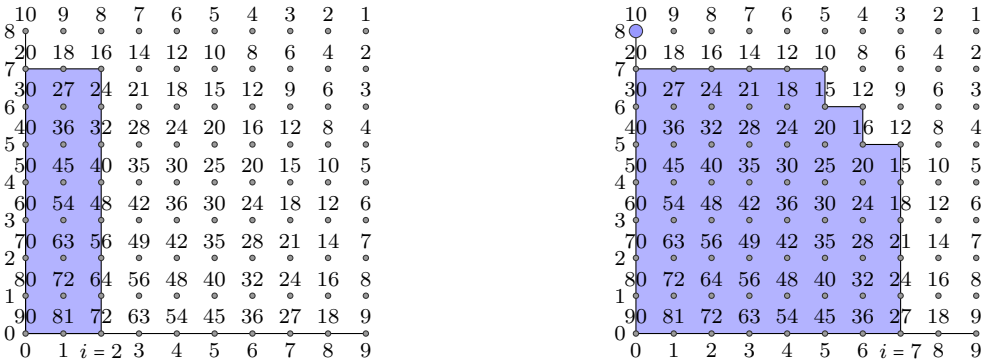


Figure 3.16: Sets S'' obtained by adding points to S' in the proof of Theorem 3.2.11

interpolating with respect to X (respectively, Y), with starting set Δ and resulting set Δ^*, $\mathcal{C}^P_{\Delta^*}$ would have less defect when interpolating with respect to Y (respectively, X), we would not find new optimal sets because this optimality would be discarded in the process of interpolating with respect to Y (respectively, X). □

As a consequence of Theorem 3.2.11, the next Corollary 3.2.12 determines the parameters and (r,δ)-localities of the optimal (r,δ)-LRCs we can obtain with the bound d_0 on the minimum distance. Notice that, in order not to repeat cases and since the variables X and Y play the same role, the parameters are written only with the notation we have used to interpolate with respect to X.

Corollary 3.2.12. *Let $\mathbb{F}_q$ be a finite field. For each pair (n_1,n_2) of integers such that $2 \le n_1, n_2 \le q$, there exists an optimal (r,δ)-LRC with length $n = n_1 n_2$, parameters $[n,k,d]_q$ and locality (r,δ) as follows:*

(1) $k = (i+1)(j+1)$, $d = (n_1 - i)(n_2 - j)$, *where*

- $i = 0$ *and* $0 \le j \le n_2 - 1$, *being the locality* $(r,\delta) = (1, n_1)$; *or*
- $1 \le i \le n_1 - 2$ *and* $j = n_2 - 1$, *being the locality* $(r,\delta) = (i+1, n_1 - i)$.

(2) $k = (i+1)(n_2 - 1) + s + 1$, $d = n_1 - s$ *and* $(r,\delta) = (i+1, n_1 - i)$, *where*

$$\max\{0, 2i - n_1\} \le s < i \le n_1 - 2.$$

(3) $k = (i+1)j + 1$, $d = n_1(n_2 - j)$ *and* $(r,\delta) = (i+1, n_1 - i)$, *where* $1 \le i \le n_1 - 2$ *and* $\max\left\{1, \frac{i(n_2+1)-n_1}{i}\right\} \le j \le n_2 - 2$.

3.2.2. The multivariate case $(m \ge 3)$

In Subsection 3.2.1 we have studied bivariate codes $\mathcal{C}_\Delta^P$, obtained from decreasing sets $\Delta \subseteq \{0,1,\dots,n_1-1\} \times \{0,1,\dots,n_2-1\}$, which give rise to optimal LRCs. Moreover we have determined all the parameters of the d_0-optimal bivariate MCCs. We devote this subsection to the same purpose in the multivariate case. Thus $\mathcal{R} = \mathbb{F}_q[X_1,\dots,X_m]/I$, where $m \ge 3$ and $\Delta \subseteq \{0,1,\dots,n_1-1\} \times \cdots \times \{0,1,\dots,n_m-1\}$. The forthcoming Propositions 3.2.13 and 3.2.14 are the analogues to Propositions 3.2.1 and 3.2.2 for multivariate MCCs and allow us to determine the parameters of the d_0-optimal LRCs of the type $\mathcal{C}_\Delta^P$, $m \ge 3$.

Proposition 3.2.13. *Keep the notation as given at the beginning of Section 3.1. For each index $j_0 \in \{1,\dots,m\}$, set $i_j = n_j - 1$ for all $j \in \{1,\dots,m\}\backslash\{j_0\}$ and $i_{j_0} \in \{0,1,\dots,n_{j_0}-2\}$, and consider*

$$\Delta = \Delta^1_{i_1,\dots,i_m} := \{(e_1,\dots,e_m) \mid 0 \le e_j \le i_j, \text{ for all } j = 1,\dots,m\}.$$

Then, the MCC, $\mathcal{C}_\Delta^P$, is an optimal LRC with locality $(r,\delta) = (i_{j_0}+1, n_{j_0} - i_{j_0})$. Furthermore, $\Delta^1_{i_1,\dots,i_m}$ are the unique sets of the form $\Delta' = \{(e_1,\dots,e_m) \mid 0 \le e_j \le l_j \text{ for all } j = 1,\dots,m\}$, where $0 \le l_j \le n_j - 1$, providing optimal LRCs.

Proof. We interpolate with respect to X_1 (the proof is analogue if we interpolate with respect to any other variable). Consider a set Δ' as in the statement.

We start by assuming that $l_j = n_j - 1$ for $m-2$ indices j. Without loss of generality suppose that $l_j = n_j - 1$ for all $j = 3,\dots,m$. Then, the point that defines the bound on the minimum distance is $(l_1, l_2, n_3 - 1, \dots, n_m - 1)$ and the parameters of this code give the following value for the LHS of Inequalities (3.1.3):

$$\begin{aligned} d_0 + k + \left(\left\lceil \frac{k}{r} \right\rceil - 1\right)(\delta - 1) &= (n_1 - l_1)(n_2 - l_2) + (l_1 + 1)(l_2 + 1)n_3 n_4 \cdots n_m \\ &\quad + [(l_2 + 1)n_3 n_4 \cdots n_m - 1](n_1 - l_1 - 1) \\ &= (n_1 - l_1)(n_2 - l_2) + n_1(l_2 + 1)n_3 n_4 \cdots n_m - (n_1 - l_1 - 1) \\ &= n_1(l_2 + 1)n_3 n_4 \cdots n_m + (n_1 - l_1)(n_2 - l_2 - 1) + 1. \end{aligned}$$

Thus, the code is optimal if and only if $l_2 = n_2 - 1$ (and $l_1 \in \{0, 1, \dots, n_1 - 2\}$ for being an LRC).

We conclude the proof after noticing that the same reasoning allows us to prove the proposition when the number of indices j in Δ' such that $l_j = n_j - 1$ is less than $m-2$. □

Our next result shows that deleting, from a set $\Delta^1_{i_1,\dots,i_m}$, a suitable number of successive minimum footprint points on the line $e_j = n_j - 1$, $j \neq j_0$, an optimal LRC is also obtained. This is because for each removed point we lose one unit in dimension but we gain one unit in the bound for the minimum distance and r, δ and $\left\lceil \frac{k}{r} \right\rceil$ do not change. As a consequence the LHS in Inequalities (3.1.3) remains constant.

Proposition 3.2.14. *Keep the notation as in Proposition 3.2.13. Define*

$$\Delta = \Delta^2_{i_{j_0},s} := \Delta^1_{i_1,\dots,i_m} \setminus \{(n_1 - 1, \dots, n_{j_0-1} - 1, e_{j_0}, n_{j_0+1} - 1, \dots, n_m - 1) \mid s \le e_{j_0} \le i_{j_0}\},$$

where s satisfies $\max\{1, 2i_{j_0} - n_{j_0} + 1\} \le s \le i_{j_0} \le n_{j_0} - 2$ or $i_{j_0} = s = 0$.

Then the MCC, $\mathcal{C}^P_\Delta$, is an optimal LRC with locality $(r,\delta) = (i_{j_0} + 1, n_{j_0} - i_{j_0})$.

Proof. The footprint $\mathrm{F}(\boldsymbol{p})$ of the point

$$\boldsymbol{p} = (n_1 - 1, n_2 - 1, \dots, n_{j_0-1} - 1, i_{j_0}, n_{j_0+1} - 1, \dots, n_{m-1} - 1, n_m - 1)$$

determines the bound d_0 for the minimum distance of the code $\mathcal{C}^P_{\Delta^1_{i_1,\dots,i_m}}$. We look for an index $0 \le s \le i_{j_0}$ such that $i_{j_0} - s + 1$ is the number of points in $\Delta^1_{i_1,\dots,i_m}$ that meet the line $e_j = n_j - 1$, $j \neq j_0$, and have footprint less than $2(n_{j_0} - i_{j_0})$. The candidate set Δ for $\mathcal{C}^P_\Delta$ to be optimal is obtained by deleting from $\Delta^1_{i_1,\dots,i_m}$ those points because $2(n_{j_0} - i_{j_0})$ is the footprint of any point in the set

$$V = \{\boldsymbol{p} - \boldsymbol{\epsilon}_j \text{ for all } j \in \{1, \dots, m\} \setminus \{j_0\}\},$$

where $\boldsymbol{\epsilon}_j = (\delta_{j1}, \dots, \delta_{jm})$, δ_{ij} being the Kronecker delta, and $V \subseteq \Delta^1_{i_1,\dots,i_m} \setminus \{\boldsymbol{p}\}$. Thus, $n_{j_0} - s < 2(n_{j_0} - i_{j_0})$, what is equivalent to $s \ge 2i_{j_0} - n_{j_0} + 1$.

Therefore, in order to Δ be a candidate for $\mathcal{C}^P_\Delta$ to be optimal, $s \ge \max\{0, 2i_{j_0} - n_{j_0} + 1\}$. The dimension of the code $\mathcal{C}^P_\Delta$ is

$$k = n_1 n_2 \cdots n_{j_0-1}(i_{j_0} + 1)n_{j_0+1} \cdots n_{m-1} n_m - (i_{j_0} - s + 1),$$

and the bound on the minimum distance of $\mathcal{C}_\Delta^P$ is given by the point with coordinates $e_j = n_j - 1$, $j \neq j_0$, $e_{j_0} = s - 1$ when $s \geq 1$ or by any point of V when $s = 0$. Then $d_0 = n_{j_0} - s + 1$ for $s \geq 1$ and $d_0 = 2(n_{j_0} - i_{j_0})$ when $s = 0$. Moreover we interpolate with respect to X_{j_0} (it is the only way to obtain an LRC), so $r = i_{j_0} + 1$ and $\delta - 1 = n_{j_0} - i_{j_0} - 1$. Thus, the value for $k + d_0 + \left(\left\lceil \frac{k}{r} \right\rceil - 1\right)(\delta - 1)$ (the LHS of Inequalities (3.1.3)) is

$$\begin{aligned} &n_1 n_2 \cdots n_{j_0-1}(i_{j_0}+1)n_{j_0+1}\cdots n_{m-1}n_m - (i_{j_0} - s + 1) + n_{j_0} - s + 1 \\ &\quad + \left(\left\lceil \frac{n_1 n_2 \cdots n_{j_0-1}(i_{j_0}+1)n_{j_0+1}\cdots n_{m-1}n_m - (i_{j_0} - s + 1)}{i_{j_0}+1} \right\rceil - 1\right) \cdot (n_{j_0} - i_{j_0} - 1) \\ &\qquad = n_1 n_2 \cdots n_m - i_{j_0} + n_{j_0} - (n_{j_0} - i_{j_0} - 1) = n_1 n_2 \cdots n_m + 1, \end{aligned}$$

if $s \geq 1$ and

$$\begin{aligned} &n_1 n_2 \cdots n_{j_0-1}(i_{j_0}+1)n_{j_0+1}\cdots n_{m-1}n_m - (i_{j_0} - s + 1) + 2(n_{j_0} - i_{j_0}) \\ &\quad + \left(\left\lceil \frac{n_1 n_2 \cdots n_{j_0-1}(i_{j_0}+1)n_{j_0+1}\cdots n_{m-1}n_m - (i_{j_0} - s + 1)}{i_{j_0}+1} \right\rceil - 1\right) \cdot (n_{j_0} - i_{j_0} - 1) \\ &\qquad = n_1 n_2 \cdots n_m - i_{j_0} - 1 + 2(n_{j_0} - i_{j_0}) - 2(n_{j_0} - i_{j_0} - 1) = n_1 n_2 \cdots n_m + 1 - i_{j_0}, \end{aligned}$$

otherwise. This, together with the condition $i_{j_0} = 0$ in the case $s = 0$, proves that $\mathcal{C}_\Delta^P$ is optimal and concludes the proof. □

Remark 3.2.15. As in the bivariate case, the families of (decreasing) MCCs given in Propositions 3.2.13 and 3.2.14 determine the parameters of all d_0-optimal multivariate ($m \geq 3$) (r, δ)-LRCs $\mathcal{C}_\Delta^P$ (with any set $\Delta \subseteq E$). The following Theorem 3.2.16 proves the analogue of Theorem 3.2.11 in the multivariate case. Therefore, by Remark 1.3.11, we have characterized the optimal multivariate decreasing MCCs.

Theorem 3.2.16. *Let $\mathcal{C}_\Delta^P$ be a multivariate MCC. If $\mathcal{C}_\Delta^P$ is a d_0-optimal LRC, then there exists a MCC, $\mathcal{C}_{\Delta^*}^P$, as in Propositions 3.2.13 or 3.2.14 having the same parameters n, k, d, r and δ as $\mathcal{C}_\Delta^P$.*

Proof. The proof follows by a close reasoning to that given in Theorem 3.2.11. By a multivariate version of Lemma 3.2.6, one can start with a set Δ as that given in Proposition 3.2.13 and remove points following a natural order. The main difference with the case $m = 2$ is that when $m \geq 3$, we should delete points out of a plane, which enlarges the defect, giving rise to the two possibilities described in Propositions 3.2.13 and 3.2.14 for sets Δ such that $\mathcal{C}_\Delta^P$ is d_0-optimal. □

Corollary 3.2.17 determines parameters and (r, δ)-localities of the multivariate d_0-optimal (r, δ)-LRCs.

Corollary 3.2.17. *Let $\mathbb{F}_q$ be a finite field and consider an integer $m \geq 3$. For every m-tuple $(n_1, \ldots, n_m)$ of integers such that $2 \leq n_j \leq q$, $j \in \{1, \ldots, m\}$, there exists an optimal (r, δ)-LRC with length $n = n_1 \cdots n_m$, parameters $[n, k, d]_q$ and locality (r, δ) as follows:*

1. $k = n_1 \cdots n_{j_0-1}(i_{j_0}+1)n_{j_0+1}\cdots n_m$, $d = n_{j_0} - i_{j_0}$ *and* $(r,\delta) = (i_{j_0}+1, n_{j_0}-i_{j_0})$, *where* $i_{j_0} \in \{0,1,\ldots,n_{j_0}-2\}$.

2. $k = n_1 \cdots n_{j_0-1}(i_{j_0}+1)n_{j_0+1}\cdots n_m - (i_{j_0}-s+1)$, $d = n_{j_0}-s+1$ *and* $(r,\delta) = (i_{j_0}+1, n_{j_0}-i_{j_0})$, *where*
$$\max\{1, 2i_{j_0} - n_{j_0} + 1\} \leq s \leq i_{j_0} \leq n_{j_0} - 2.$$

3. $k = n_1 \cdots n_{j_0-1} n_{j_0+1} \cdots n_m - 1$, $d = 2n_{j_0}$ *and* $(r,\delta) = (1, n_{j_0})$.

Remark 3.2.18. Keep the notation as in Section 3.1, so let $m \geq 2$. Let Δ be a subset of E satisfying some of the conditions in Propositions 3.2.1, 3.2.2, 3.2.3, 3.2.13 or 3.2.14. Define $\Delta^* := \boldsymbol{v} + \Delta$ for any $\boldsymbol{v} \in \mathbb{N}_0^m$ such that $\Delta^* \subseteq E$. If $0 \notin P_j$ for all $1 \leq j \leq m$, then the MCC $C^P_{\Delta^*}$ is optimal with the same parameters and locality as $\mathcal{C}^P_\Delta$. This result follows straightforwardly from Remark 1.3.6.

Remark 3.2.19. MCCs include the family of codes introduced in [3], codes whose evaluation map is the same as MCCs but their evaluation sets V_Δ are only a subset of those used for MCCs. Specifically, the codes in [3] are subcodes of affine Cartesian codes (of order t), where the corresponding set V_Δ is the set of polynomials f in $\mathbb{F}_q[X_1,\ldots,X_m]$ with total degree bounded by t and such that a fixed variable X_{j_0} has degree $\deg_{X_{j_0}}(f) \leq i_{j_0} < n_{j_0} - 1$ for some fixed integer i_{j_0} (see [3, Definitions 2.2 and 2.3]). Therefore, while MCCs allow arbitrary sets $\Delta \subset E$, the sets Δ of those codes considered in [3] are of the form

$$\Delta = \{(e_1,\ldots,e_m) \in E \mid e_1 + \cdots + e_m \leq t,\ e_{j_0} \leq i_{j_0}\}.$$

As a consequence we obtain many more (r,δ)-optimal LRCs than those given in [3, Corollaries 4.2 and 4.3]. Thus, if we fix the locality $r = i_{j_0}+1$ for some $1 \leq j_0 \leq m$, then we obtain optimal codes which are not considered in [3]. These are those of Proposition 3.2.1 for $i_{j_0} = i = 0$, $j < n_2 - 2$, and $i < n_1 - 2$, $i_{j_0} = j = 0$; those of Proposition 3.2.2 for $s \leq i_{j_0} - 2$; those of Proposition 3.2.3 for $i_{j_0} > 1$ and for $i_{j_0} = 1$ and $n_{j_0} < n_{j'}$, where $j' \in \{1,2\}\backslash\{j_0\}$; and those of Proposition 3.2.14 for $i_{j_0} \geq 2$ and $\max\{1, 2i_{j_0} - n_{j_0}\} \leq s \leq i_{j_0} - 1$. Moreover, in this chapter, we also give many more optimal LRCs, regarded as subfield-subcodes of MCCs, as we will explain in the next section.

3.3. Optimal subfield-subcodes

Fix $q = p^l$, p a prime. We devote this section to obtain new optimal (r,δ)-LRCs. These are subfield-subcodes of J-affine variety codes which were introduced in Definition 1.3.4. In this section we keep the notations and use the results in Subsection 1.5.1. Notice that we set $Q = q$. We prove that subfield-subcodes of some J-affine variety codes keep the parameters and (r,δ)-locality of certain decreasing MCCs considered in Section 3.2, being then optimal. Thus, we get optimal (r,δ)-LRCs over smaller supporting fields, which are new and behave as MCCs.

To show the novelty of our codes, we compare them with those in the references [29, 81, 92, 121, 72, 27, 129, 28, 36, 131, 132, 108, 31, 90, 79]. They group the known codes whose parameters $[n, k, d]$ and locality (r, δ) satisfy Formula (1.4.1) with equality and their lenghts n are divisible by $r + \delta - 1$.

LRCs we provide in this section are p^h-ary, such that $r + \delta - 1$ equals either $p^h + 1$ or $p^h + 2$, their length n is a multiple of some of these values, $r > 1$ and $\delta > 2$. In some cases, when $r + \delta - 1 = p^h + 1$, we also impose gcd-type conditions to obtain novelty.

Our codes are new because they are optimal and there is no code in the literature with the same parameters and locality. The following paragraph shows some requeriments that the codes in the above given list of references must satisfy showing that, taking into account the above paragraph, our codes give optimal codes over the same field with a wider range for the pairs (r, δ).

Parameters and locality of the previously mentioned literature codes, assumed also p^h-ary, satisfy the following conditions, which differ from ours:

- $r + \delta - 1 \leq p^h$ [28, 36, 131, 132, 31, 79];
- $r + \delta - 1 \leq p^h + 1$ with either minimum distances other than ours [121, 90] or opposite gcd-type conditions [121], see the future Remarks 3.3.7 and 3.3.13;
- either $n \mid p^h - 1$ or $n \mid p^h + 1$ [29, 27, 108], but our codes have $n \geq 2(p^h + 1)$ since $n = (r + \delta - 1)n_2 \cdots n_m$ with $n_j \geq 2$ for all $j \in \{1, \ldots, m\}$;
- $r = 1$ [129];
- $\delta = 2$ [81, 92, 72, 79]; and
- $2\delta + 1 \leq d \leq r + \delta$ [79] but, in case our codes have $d \leq r + \delta$, then $d \leq 2\delta$, see the future Remarks 3.3.7 and 3.3.13.

Subfield-subcodes of J-affine variety codes were also used in [47] to provide (r, δ)-LRCs but unlike this chapter, most of them are non-optimal. The recovery procedure proposed in [47] is different from the one in this chapter; it was designed to be applied on subfield-subcodes and it mainly uses the structure of closed sets introduced in Definition 1.5.5. As a consequence, LRCs in [47] have different parameters than those in this section. In particular, the values r and δ in [47] of p^h-ary subfield-subcodes (of a q-ary code) satisfy $r + \delta - 1 = p^h - 1$, while those in this section are such that $r + \delta - 1$ is either $p^h + 1$ or $p^h + 2$. Finally, setting $q = p^h$ and $n \leq (p^h)^m$, we also notice that our codes in Section 3.2 extend those in [47] because, here, our restriction is $r + \delta - 1 \leq p^h$.

Closed sets will be the key for obtaining optimal (r, δ)-LRCs coming from subfield-subcodes. To explain it, we recall, on the one hand, that if Δ is a closed set, then $\dim(\mathcal{S}_\Delta^{P,J}) = \dim(\mathcal{C}_\Delta^{P,J}) = \#\Delta$. On the other hand, the minimum distance of a subfield-subcode $\mathcal{S}_\Delta^{P,J}$ admits the bound on the MCC $\mathcal{C}_\Delta^{P,J}$ it comes from. Since Δ is closed, it is not decreasing (see Definition 1.3.12) because the construction of closed sets produces non-consecutive elements in some coordinate. Then Δ contains gaps, see for example the

future Figure 3.19. Therefore, the bound given in Corollary 1.3.10 is not sharp, which forces us to use an improved bound for each particular case that depends on the shape of Δ. This new bound coincides with that of Corollary 1.3.10 on a certain decreasing MCC $\mathcal{C}_{\Delta'}^{P,J}$ obtained, roughly speaking, after "compacting" Δ to a decreasing set Δ' such that $\#\Delta = \#\Delta'$. Roughly speaking, "to compact" a set $\Delta \subseteq E$ (represented as a shaded region in the grid E) means to move Δ by a translation vector vanishing out of the variable used to interpolate in such a way that the first segments of exponents in that variable are as full as possible, and to remove empty segments (see the forthcoming Figure 3.17 d), where we use the identification $9 = 0$ and points where $X = 2$ go to points with $X = 8$). This procedure is very close to that described in the third paragraph of Remark 3.2.4, but adapted to the current shapes of the sets Δ. Thus, if we choose Δ to be closed, the code over $\mathbb{F}_{p^h}$, $\mathcal{S}_{\Delta}^{P,J}$, has the same parameters n and k and the same bound for the minimum distance as $\mathcal{C}_{\Delta'}^{P,J}$. Moreover, the recovery method presented in Proposition 3.1.1 can also be applied to $\mathcal{S}_{\Delta}^{P,J}$ obtaining the same locality (r,δ) as $\mathcal{C}_{\Delta'}^{P,J}$. Therefore, we deduce optimality of subfield-subcodes $\mathcal{S}_{\Delta}^{P,J}$ from the optimality of the codes $\mathcal{C}_{\Delta'}^{P,J}$ studied in Section 3.2.

3.3.1. Optimal (r,δ)-LRCs coming from subfield-subcodes of bivariate MCCs

In this subsection, we use some results in Section 3.2 and the ideas described in the above paragraph to provide some families of *new* optimal (r,δ)-LRCs coming from subfield-subcodes of q-ary bivariate J-affine variety codes. We will give p^h-ary optimal (r,δ)-LRCs whose length is a multiple of $r+\delta-1$, where $r+\delta-1$ equals p^h+1 or p^h+2, $r>1$, $\delta>2$, and for some codes we impose certain gcd-type conditions so that all the codes provided are new (see the introduction of Section 3.3 and the future Remark 3.3.7). The forthcoming Propositions 3.3.4 and 3.3.6 (in characteristic two) prove the optimality while Theorems 3.3.9 and 3.3.10 show the parameters of our codes.

Recall from Definition 1.3.4 that $U_t \subseteq \mathbb{F}_q$ denotes the multiplicative subgroup of $\mathbb{F}_q$ of t-th roots of unity, $t \mid q-1$. Keep the notation as in Section 3.1 and Subsection 1.5.1. Fix $i \in \{1,2\}$ (it refers to the variable X_i with respect to which we will interpolate when applying our recovery method) and denote i' the unique element $i' \in \{1,2\}\backslash\{i\}$.

Pick $p^h \geq 4$ if p equals 2 ($p^h \geq 5$, otherwise) such that $p^h+1 \mid q-1$. Here, the set of points to evaluate in the variable X_i is $P_i = U_{p^h+1} \subseteq \mathbb{F}_q$, and thus its cardinality equals $n_i = p^h+1$. Our (two-dimensional) set P of evaluation points is $P = P_1 \times P_2$, where $P_{i'}$ is either some multiplicative subgroup $U_{n_{i'}} \subseteq \mathbb{F}_q$, with $n_{i'} \mid q-1$ and $J = \{1,2\}$, or, allowing also the element 0 to be evaluated, $U_{n_{i'}-1} \cup \{0\} \subseteq \mathbb{F}_q$, with $n_{i'}-1 \mid q-1$ and $J = \{i\}$.

The following two families of sets will be used to define the sets Δ of our codes $\mathcal{S}_{\Delta}^{P,J}$ since they will constitute the sets $\mathrm{supp}_{X_i}(V_\Delta)$ defined at the beginning of Section 3.1. For each nonnegative integer $a \leq \left\lfloor \frac{p^h}{2} \right\rfloor - 1$ (and, if $p=2$, $b \leq \frac{p^h}{2} - 2$), we consider the sets Λ^i introduced in Subsection 1.5.1, and define

$$\Omega_a := \left\{0, 1, \ldots, a, p^h+1-a, p^h+2-a, \ldots, p^h\right\} = \Lambda_0^i \cup \Lambda_1^i \cup \cdots \cup \Lambda_a^i$$

when $a > 0$, $\Omega_0 := \{0\}$ and

$$\Omega_b^* := \left\{ \frac{p^h}{2} - b, \frac{p^h}{2} - b + 1, \ldots, \frac{p^h}{2} + b + 1 \right\} = \Lambda^i_{\frac{p^h}{2}-b} \cup \Lambda^i_{\frac{p^h}{2}-b+1} \cup \cdots \cup \Lambda^i_{\frac{p^h}{2}}.$$

These are closed sets (in the fixed variable i with respect to p^h) of the set $\{0, 1, \ldots, n_i - 1\} = \{0, 1, \ldots, p^h\}$ (identified with $\mathbb{Z}/(p^h+1)\mathbb{Z}$) of possible exponents, in the variable X_i, of evaluation polynomials. Indeed, with the above mentioned identification, $p^h + 1 = 0$ and then $\Lambda_0^i = \{0\}$ and $\Lambda_t^i = \{t, p^h - (t-1)\}$.

Example 3.3.1. Set $(i, p^h, q, a, b) = (1, 8, 64, 3, 2)$, that is we fix the first variable to interpolate and we take the field $\mathbb{F}_{64}$ and its subfield $\mathbb{F}_8$. Then the above defined sets are $\Omega_a = \{0,1,2,3,6,7,8\} = \Lambda_0^i \cup \Lambda_1^i \cup \Lambda_2^i \cup \Lambda_3^i = \{0\} \cup \{1,8\} \cup \{2,7\} \cup \{3,6\}$, where, for example, $\Lambda_2^i = \{2, 2 \cdot 8 = 16 = 7\}$ because the exponents in the variable i fulfill the identification $9 = 0$ and $\Omega_b^* = \{2, \ldots, 7\} = \Lambda_2^i \cup \Lambda_3^i \cup \Lambda_4^i = \{2,7\} \cup \{3,6\} \cup \{4,5\}$, and they coincide, respectively, with the set $\mathrm{supp}_{X_i}(V_\Delta)$ in Figure 3.17 a) (i) and b) (i).

Now, let $0 \le t < z \le \left\lfloor \frac{p^h}{2} \right\rfloor - 1$ be nonnegative integers such that $2t \ge \max\{0, 4z - p^h - 1\}$. In addition, when $p = 2$, consider a nonnegative integer $0 \le u \le \frac{p^h}{2} - 2$ and if $u \ge 1$, let $0 \le v < u$ be a nonnegative integer such that $2v + 1 \ge \max\{0, 4u + 1 - p^h\}$. Let us define the following four types of sets Δ (named Δ_1, Δ_2, Δ_1^* and Δ_2^*) which will allow us to give our *first family of optimal codes* $\mathcal{S}_\Delta^{P,J}$. Sets Δ_1 and Δ_2 provide codes defined over finite fields of arbitrary characteristic, while sets Δ_1^* and Δ_2^* work only in characteristic two.

$$\Delta_1(z) := \Delta_1 := \begin{cases} \Omega_z \times \{0, 1, \ldots, n_2 - 1\}, & \text{when } i = 1, \\ \{0, 1, \ldots, n_1 - 1\} \times \Omega_z, & \text{otherwise;} \end{cases}$$

$$\Delta_2(z,t) := \Delta_2 := \begin{cases} \Omega_z \times \{0, 1, \ldots, n_2 - 2\} \cup \Omega_t \times \{n_2 - 1\}, & \text{when } i = 1, \\ \{0, 1, \ldots, n_1 - 2\} \times \Omega_z \cup \{n_1 - 1\} \times \Omega_t, & \text{otherwise;} \end{cases}$$

$$\Delta_1^*(u) := \Delta_1^* := \begin{cases} \Omega_u^* \times \{0, 1, \ldots, n_2 - 1\}, & \text{when } i = 1, \\ \{0, 1, \ldots, n_1 - 1\} \times \Omega_u^*, & \text{otherwise;} \end{cases}$$

and

$$\Delta_2^*(u,v) := \Delta_2^* := \begin{cases} \Omega_u^* \times \{0, 1, \ldots, n_2 - 2\} \cup \Omega_v^* \times \{n_2 - 1\}, & \text{when } i = 1, \\ \{0, 1, \ldots, n_1 - 2\} \times \Omega_u^* \cup \{n_1 - 1\} \times \Omega_v^*, & \text{otherwise.} \end{cases}$$

Our choice of sets Δ is supported on the ideas exposed before Subsection 3.3.1. We will prove that they are closed in the forthcoming Proposition 3.3.4. It must hold in each variable and happens in the variable i' by picking all the possible exponents or all but $n_{i'} - 1$ (notice that $\Lambda^{i'}_{n_{i'}-1} = \{n_{i'} - 1\}$ when $i' \notin J$). A key fact is that we force the projected code in the variable i, $\mathrm{ev}_{P_i}\left(V_\Delta^i\right)$, to be MDS in order to have the explicit values of r and δ from Proposition 3.1.1. Finally, the above sets Δ are those that, as described before Subsection 3.3.1, can be "compacted" to some of the sets provided in Propositions 3.2.1, 3.2.2 or 3.2.3 and admit their same (improved) bounds on the minimum distance.

Example 3.3.2. This is a continuation of Example 3.3.1. With the same notation, set $z = a$ and $t = b$, consider also $(u,v) = (2,1)$. Then, $\Omega_t = \{0,1,2,7,8\}$ and $\Omega_v^* = \{3,\dots,6\}$. Figure 3.17 c) (i) and d) (i) show, respectively, the sets Δ_2 and Δ_2^* in this case.

Lemma 3.3.3. *Keep the above notation. Let $a \leq \left\lfloor \frac{p^h}{2} \right\rfloor - 1$ and, if $p = 2$, $b \leq \frac{p^h}{2} - 2$ be nonnegative integers. Consider the $\mathbb{F}_q$-vector spaces $V_1 = \langle (X_i)^e \mid e \in \Omega_a \rangle$ and $V_2 = \langle (X_i)^e \mid e \in \Omega_b^* \rangle$ contained in the quotient ring $\mathcal{R}_i$ defined before Proposition 3.1.1. Then, $\mathrm{ev}_{P_i}(V_1)$ and $\mathrm{ev}_{P_i}(V_2)$ are MDS codes.*

Proof. Let $\Omega := \{0,1,\dots,2a\} = \Omega_a + a$ regarded as representatives of elements in $\mathbb{Z}/(p^h+1)\mathbb{Z}$. Define $V = \langle (X_i)^e \mid e \in \Omega \rangle$. Codewords in $\mathrm{ev}_{P_i}(V)$ are of the form

$$\mathrm{ev}_{P_i}((X_i)^a f) = \mathrm{ev}_{P_i}((X_i)^a) * \mathrm{ev}_{P_i}(f),$$

where $f \in V_1$, $*$ denoting the $*$-product as introduced at the beginning of Part I. Since $0 \notin P_i$, $\mathrm{ev}_{P_i}(V_1)$ and $\mathrm{ev}_{P_i}(V)$ are isometric codes. The code $(\mathrm{ev}_{P_i}(V))^\perp$ is a $[p^h+1, p^h-2a, \leq 2a+2]_q$ code and, since Ω contains $2a+1$ consecutive elements, $\mathrm{d}\left((\mathrm{ev}_{P_i}(V))^\perp\right) \geq 2a+2$ because its corresponding parity-check matrix contains a Vandermonde matrix of rank $2a+1$. Thus, $(\mathrm{ev}_{P_i}(V))^\perp$ is an MDS code and therefore $\mathrm{ev}_{P_i}(V)$ and $\mathrm{ev}_{P_i}(V_1)$ are MDS codes. The fact that Ω_b^* contains $2b+2$ consecutive elements proves that $(\mathrm{ev}_{P_i}(V_2))^\perp$ is an MDS code and therefore so is $\mathrm{ev}_{P_i}(V_2)$. □

The following result shows sets P, J and Δ giving rise to our *first family of new optimal LRCs* $\mathcal{S}_\Delta^{P,J}$ in the bivariate case. Sets in Items (1), (2) and (3) provide codes over fields of any characteristic, while the remaining items only give characteristic two codes. We note that the proof is based on the ideas exposed in the paragraphs before Subsection 3.3.1 and Example 3.3.2. The specific parameters of the LRCs corresponding to this result are given in the next Theorem 3.3.9.

Proposition 3.3.4. *Keep the the notation as above where $\mathbb{F}_{p^h}$ is regarded as a subfield of $\mathbb{F}_{q=p^l}$ and $p^h+1 \mid q-1$. Fixed i and $P_i = U_{p^h+1}$, the set of p^h+1-th roots of unity, the following statements determine sets $P_{i'}$, J and Δ such that the subfield-subcodes $\mathcal{S}_\Delta^{P,J}$ over the field $\mathbb{F}_{p^h}$ are optimal (r,δ)-LRCs.*

(1) $P_{i'} = U_{n_{i'}}$ for some $n_{i'}$ such that $n_{i'} \mid q-1$; $J = \{1,2\}$ and $\Delta = \Delta_1$, in which case

$$(r,\delta) = (2z+1, p^h - 2z + 1).$$

(2) $P_{i'} = U_{n_{i'}-1} \cup \{0\}$ for some $n_{i'}$ such that $n_{i'} - 1 \mid q-1$; $J = \{i\}$ and $\Delta = \Delta_1$, in which case

$$(r,\delta) = (2z+1, p^h - 2z + 1).$$

(3) $P_{i'} = U_{n_{i'}-1} \cup \{0\}$ for some $n_{i'}$ such that $n_{i'} - 1 \mid q-1$ and, if p is odd, either $\gcd(n_{i'}, p^h) \neq 1$ or $\gcd(n_{i'}, p^h+1) \neq 1$; $J = \{i\}$ and $\Delta = \Delta_2$, in which case

$$(r,\delta) = (2z+1, p^h - 2z + 1).$$

(4) $P_{i'} = U_{n_{i'}}$ *for some* $n_{i'}$ *such that* $n_{i'} \mid q-1$; $J = \{1,2\}$ *and* $\Delta = \Delta_1^*$, *in which case*

$$(r,\delta) = (2u+2, p^h - 2u).$$

(5) $P_{i'} = U_{n_{i'}-1} \cup \{0\}$ *for some* $n_{i'}$ *such that* $n_{i'} - 1 \mid q-1$; $J = \{i\}$ *and* $\Delta = \Delta_1^*$, *in which case*

$$(r,\delta) = (2u+2, p^h - 2u).$$

(6) $P_{i'} = U_{n_{i'}-1} \cup \{0\}$ *for some* $n_{i'}$ *such that* $n_{i'} - 1 \mid q-1$; $J = \{i\}$ *and* $\Delta = \Delta_2^*$, *in which case* $(r,\delta) = (2u+2, p^h - 2u)$.

Proof. We start by proving that the sets Δ in the statements (1)-(6) are closed with respect to p^h. As we said, in the single variable i, the subsets of $\{0,1,\dots,n_i-1\} = \{0,1,\dots,p^h\}$ (identified with $\mathbb{Z}/(p^h+1)\mathbb{Z}$),

$$\Omega_a = \Lambda_0^i \cup \Lambda_1^i \cup \cdots \cup \Lambda_a^i$$

and

$$\Omega_b^* = \Lambda^i_{\frac{p^h}{2}-b} \cup \Lambda^i_{\frac{p^h}{2}-b+1} \cup \cdots \cup \Lambda^i_{\frac{p^h}{2}},$$

for $a \in \{z,t\}$ and $b \in \{u,v\}$ are clearly closed. In the single variable i', $\{0,1,\dots,n_{i'}-1\}$ is closed. In addition, when $0 \in P_{i'}$, the minimal closed set in a single variable $\Lambda^{i'}_{n_{i'}-1} \subseteq \{0,1,\dots,n_{i'}-1\}$ is the set $\Lambda^{i'}_{n_{i'}-1} = \{n_{i'}-1\}$. Indeed, with the identification $n_{i'} = 1$ described in Subsection 1.5.1, the following chain of equalities holds:

$$p^h(n_{i'}-1) = (p^h-1)(n_{i'}-1) + n_{i'} - 1 = (p^h-1)n_{i'} + n_{i'} - p^h = p^h - 1 + n_{i'} - p^h = n_{i'} - 1.$$

Therefore, $\{0,1,\dots,n_{i'}-2\} = \{0,1,\dots,n_{i'}-1\}\backslash\{n_{i'}-1\}$ is also closed. The Cartesian product and the union of closed sets are closed, so the sets Δ in (1)-(6) are closed and $\dim(\mathcal{S}_\Delta^{P,J}) = \dim(\mathcal{C}_\Delta^{P,J})$.

Now we are going to prove that the subfield-subcodes $\mathcal{S}_\Delta^{P,J}$ are LRCs. Let $i = 1$ and V_1 as in Lemma 3.3.3 with $a = z$. Since Ω_z is closed, $\dim(\mathrm{ev}_{P_i}(V_1) \cap \mathbb{F}_{p^h}^{p^h+1}) = \dim(\mathrm{ev}_{P_i}(V_1))$ and the fact that $\mathrm{d}(\mathrm{ev}_{P_i}(V_1) \cap \mathbb{F}_{p^h}^{p^h+1}) \geq \mathrm{d}(\mathrm{ev}_{P_i}(V_1))$ (see Definition 1.1.3 to recall this notation) and Lemma 3.3.3 imply that $\mathrm{ev}_{P_i}(V_1) \cap \mathbb{F}_{p^h}^{p^h+1}$ is an MDS code with minimum distance $p^h - 2z + 1$. Taking $\overline{R}$ such that $\pi_{\overline{R}}(\mathcal{C}_\Delta^{P,J}) = \mathrm{ev}_{P_i}(V_1)$, Proposition 1.5.8 shows that $\pi_{\overline{R}}(\mathcal{S}_\Delta^{P,J}) = \mathrm{ev}_{P_i}(V_1) \cap \mathbb{F}_{p^h}^{p^h+1}$ is also MDS. Then, Proposition 3.1.1 applied to $\mathcal{S}_\Delta^{P,J}$, Δ being either Δ_1 or Δ_2, proves that $\mathcal{S}_\Delta^{P,J}$ is an LRC with locality $(2z+1, p^h - 2z + 1)$. Replacing (V_1, a, z, Ω_z) by (V_2, b, u, Ω_u^*) one deduces that $\mathcal{S}_\Delta^{P,J}$ is an LRC with locality $(2u+2, p^h - 2u)$, whenever Δ is either Δ_1^* or Δ_2^*. Notice that r and δ do not depend neither on t nor on v, unlike dimension and minimum distance.

The case $i = 2$ can be proved analogously noticing that we are in the symmetric situation. It suffices to interpolate with respect to Y and change i by i' and n_2 by n_1.

With notation as in Section 3.2 page 69 and $i = 1$, we assert that the minimum distance of the code $\mathcal{S}_{\Delta}^{P,J}$ admits the bound on the minimum distance of $\mathcal{C}_{\Delta'}^{P,J}$, $d_0\left(\mathcal{C}_{\Delta'}^{P,J}\right)$, whenever

$$(\Delta,\Delta') \in \left\{ \left(\Delta_1, \Delta^1_{2z,n_2-1}\right), \left(\Delta_2, \Delta^2_{2z,2t}\right), \left(\Delta_1^*, \Delta^1_{2u+1,n_2-1}\right), \left(\Delta_2^*, \Delta^2_{2u+1,2v+1}\right) \right\}.$$

Let us prove the statement. Figure 3.17 considers the case $(p,h,l,z,t,u,v) = (2,3,6,3,2,2,1)$ to illustrate our reasoning. Let $\boldsymbol{c} = \mathrm{ev}_P(f)$, $f(X,Y) \in V_{\Delta}$ be a codeword in $\mathcal{S}_{\Delta}^{P,J}$.

a) Assume firstly that $\Delta = \Delta_1$. A no-root (α,β) in P of $f(X,Y)$ must satisfy that α is a no-root of $f(X,\beta)$ as a polynomial in X and β is a no-root of $f(\alpha,Y)$ as a polynomial in Y. Denote n_β (respectively, n_α) the cardinality of the set of no-roots of $f(X,\beta)$ (respectively, $f(\alpha,Y)$). Set n_X (respectively, n_Y) the minimum of n_β (respectively, n_α) when β (respectively, α) runs over P_2 (respectively, P_1). Then, the number of no-roots of f in P is at least $n_X n_Y$. Since $\mathrm{d}\left(\mathrm{ev}_{P_1}(V_1) \cap \mathbb{F}_{p^h}^{p^h+1}\right) = p^h + 1 - 2z$ and $\mathrm{d}\left(\mathrm{ev}_{P_2}\left(\langle Y^e \mid e \in \{0,1,\ldots,n_2-1\}\rangle\right) \cap \mathbb{F}_{p^h}^{n_2}\right) = 1$ (they are MDS codes), then $\mathrm{w}(\boldsymbol{c}) \geq p^h + 1 - 2z$ and $\mathrm{d}\left(\mathcal{S}_{\Delta}^{P,J}\right) \geq p^h + 1 - 2z = d_0\left(\mathcal{C}_{\Delta'}^{P,J}\right)$. See a) in Figure 3.17.

b) Consider now the case $\Delta = \Delta_1^*$. Since $\mathrm{d}\left(\mathrm{ev}_{P_1}(V_2) \cap \mathbb{F}_{p^h}^{n_2}\right) = p^h - 2u$, the same argument as in a) proves $\mathrm{d}\left(\mathcal{S}_{\Delta}^{P,J}\right) \geq p^h - 2u = d_0\left(\mathcal{C}_{\Delta'}^{P,J}\right)$. See b) in Figure 3.17.

c) For proving the case $\Delta = \Delta_2$, we use the following ordering in E:

$$(e_1,e_2) \leq (e_1',e_2') \iff e_2 < e_2' \text{ or } (e_2 = e_2' \text{ and } e_1 \leq e_1'),$$

and we distinguish two cases:

- The leading monomial of f is in $\Omega_z \times \{0,1,\ldots,n_2-2\}$, then an analogue argument as in a) proves $\mathrm{w}(\boldsymbol{c}) \geq 2(p^h + 1 - 2z)$.
- The leading monomial of f is in $\Omega_t \times \{n_2-1\}$, then consider $\Delta'' := \Delta + (t,0) \subseteq E$ because of the relation $p^h + 1 = 0$ in $\{0,1,\ldots,p^h\}$. Consider the codeword in $\mathcal{C}_{\Delta''}^{P}$

  $$\mathrm{ev}_P(X^t f) = \mathrm{ev}_P(X^t) * \mathrm{ev}_P(f) = \mathrm{ev}_P(X^t) * \boldsymbol{c}.$$

  Since $0 \notin P_1$, $\mathrm{w}(\boldsymbol{c}) = \mathrm{w}(\mathrm{ev}_P(X^t f)) \geq \mathrm{F}(2t, n_2-1) = p^h + 1 - 2t$, F denoting footprint as introduced in Definition 1.3.8, by Proposition 1.3.9 (the leading monomial of $X^t f$ is $\mu X^\gamma Y^{n_2-1}$ with $\gamma \leq 2t$).

Then, $\mathrm{w}(\boldsymbol{c}) \geq \min\{2(p^h + 1 - 2z), p^h + 1 - 2t\} = p^h + 1 - 2t$ and therefore

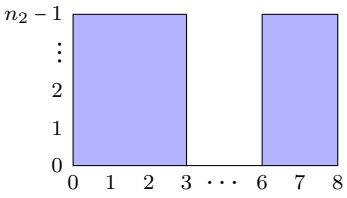
$$\mathrm{d}\left(\mathcal{S}_{\Delta}^{P,J}\right) \geq p^h + 1 - 2t = d_0\left(\mathcal{C}_{\Delta'}^{P,J}\right).$$

See c) in Figure 3.17.

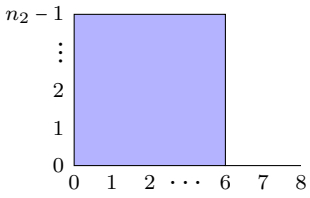
d) Finally, when $\Delta = \Delta_2^*$, reasoning as in c) with $\Delta'' := \Delta + (\frac{p^h}{2} + v + 1, 0)$, one gets the desired bound:

$$\mathrm{d}\left(\mathcal{S}_{\Delta}^{P,J}\right) \geq p^h - 2v = d_0\left(\mathcal{C}_{\Delta'}^{P,J}\right).$$

See d) in Figure 3.17.

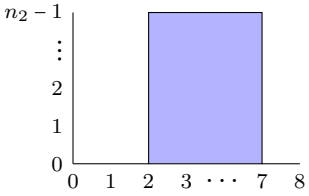


(i) $\Delta = \Delta_1 = \Omega_3 \times \{0, 1, \ldots, n_2 - 1\}$

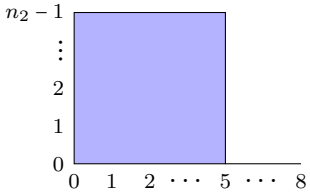


(ii) $\Delta' = (\Delta_1)' = \Delta^1_{6,n_2-1}$

a) Either $P_2 = U_{n_2}$, $n_2 \mid q-1$ and $J = \{1,2\}$, or $P_2 = U_{n_2-1} \cup \{0\}$, $n_2 - 1 \mid q-1$ and $J = \{1\}$

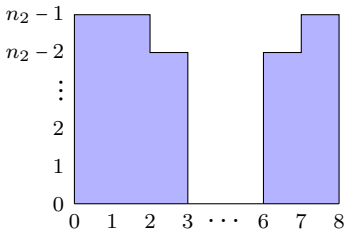


(i) $\Delta = \Delta_1^* = \Omega_2^* \times \{0, 1, \ldots, n_2 - 1\}$

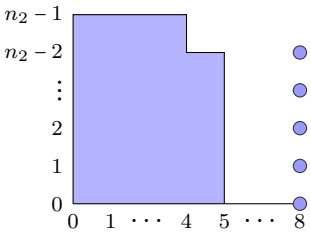


(ii) $\Delta' = (\Delta_1^*)' = \Delta^1_{5,n_2-1}$

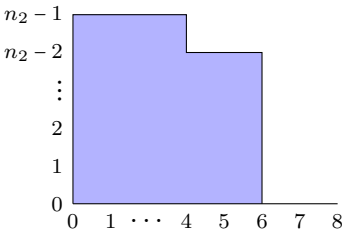
b) Either $P_2 = U_{n_2}$, $n_2 \mid q-1$ and $J = \{1,2\}$, or $P_2 = U_{n_2-1} \cup \{0\}$, $n_2 - 1 \mid q-1$ and $J = \{1\}$



(i) $\Delta = \Delta_2 = \Omega_3 \times \{0, 1, \ldots, n_2 - 2\} \cup \Omega_2 \times \{n_2 - 1\}$

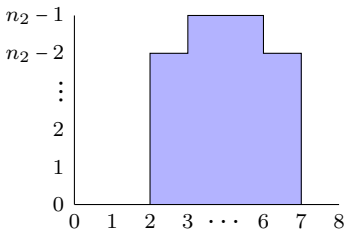


(ii) $\Delta'' = (\Delta_2)'' = \Delta_2 + (2,0)$

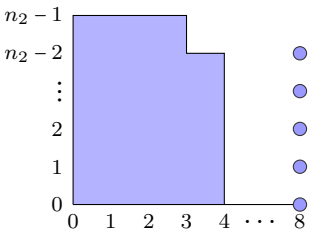


(iii) $\Delta' = (\Delta_2)' = \Delta^2_{6,4}$

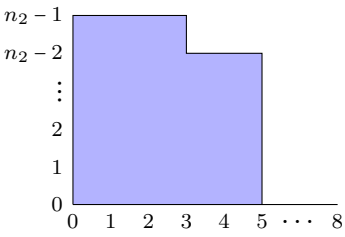
c) $P_2 = U_{n_2-1} \cup \{0\}$, $n_2 - 1 \mid q-1$ and $J = \{1\}$



(i) $\Delta = \Delta_2^* = \Omega_2^* \times \{0, 1, \ldots, n_2 - 2\} \cup \Omega_1^* \times \{n_2 - 1\}$



(ii) $\Delta'' = (\Delta_2^*)'' = \Delta_2^* + (6,0)$



(iii) $\Delta' = (\Delta_2^*)' = \Delta^2_{5,3}$

d) $P_2 = U_{n_2-1} \cup \{0\}$, $n_2 - 1 \mid q-1$ and $J = \{1\}$

Figure 3.17: Sets Δ, Δ' (and Δ'') considered in the proof of Proposition 3.3.4 for values $(i, p^h, q, P_1, z, t, u, v) = (1, 8, 64, U_9, 3, 2, 2, 1)$

The case $i = 2$ follows by symmetry. It suffices to replace P_1 by P_2, n_2 by n_1 and consider

$$(\Delta, \Delta') \in \left\{ \left(\Delta_1, \Delta^1_{n_1-1,2z}\right), \left(\Delta_2, \Delta^{2,\sigma}_{2z,2t}\right), \left(\Delta^*_1, \Delta^1_{n_1-1,2u+1}\right), \left(\Delta^*_2, \Delta^{2,\sigma}_{2u+1,2v+1}\right) \right\}.$$

Notice that $\#\Delta = \#\Delta'$ and $\dim(\mathcal{S}^{P,J}_{\Delta}) = \dim(\mathcal{C}^{P,J}_{\Delta}) = \dim(\mathcal{C}^{P,J}_{\Delta'})$. Moreover, $\mathrm{d}(\mathcal{S}^{P,J}_{\Delta}) \geq \mathrm{d}(\mathcal{C}^{P,J}_{\Delta}) \geq d_0(\mathcal{C}^{P,J}_{\Delta'})$ and the locality of $\mathcal{C}^{P,J}_{\Delta'}$ is the same as the locality of $\mathcal{S}^{P,J}_{\Delta}$. Then, the fact that $\mathcal{C}^{P,J}_{\Delta'}$ is optimal (Corollary 3.2.12 (1) when Δ is Δ_1 or Δ^*_1, and Corollary 3.2.12 (2) when Δ is Δ_2 or Δ^*_2) implies that the subfield-subcode $\mathcal{S}^{P,J}_{\Delta}$ over the field $\mathbb{F}_{p^h}$ is optimal, which concludes the proof. □

At the beginning of this subsection we announced the introduction of two families of new optimal codes. One of them contains codes over fields of any characteristic and it has already been described. Next we introduce *the second one* that only works in characteristic two. We start by giving some sets that will be useful for it. In this case, $p = 2$, $l \geq 4$ is an even positive integer, $h = \frac{l}{2}$ (recall that the field and subfield we are considering are denoted, respectively, $\mathbb{F}_{q=p^l}$ and $\mathbb{F}_{p^h}$) and the set of points to evaluate in the variable X_i is the set of $2^h + 1$-th roots of unity together with the element 0, $P_i = U_{2^h+1} \cup \{0\} \subseteq \mathbb{F}_q$. Recall also that $\{i, i'\} = \{1, 2\}$ means that X_i is the variable we use to interpolate. Then, the cardinality of P_i is $n_i = 2^h + 2$ and $P = P_1 \times P_2$, where $P_{i'}$ is either $U_{n_{i'}} \subseteq \mathbb{F}_q$, with $n_{i'} \mid q-1$ and $J = \{i'\}$, or $U_{n_{i'}-1} \cup \{0\} \subseteq \mathbb{F}_q$, with $n_{i'} - 1 \mid q-1$ and $J = \varnothing$.

Now we introduce some sets which will be the sets $\mathrm{supp}_{X_i}(V_\Delta)$ corresponding to the sets Δ that we are going to consider. Let $1 \leq j \leq n_{i'} - 1$ and $2 \leq z \leq 3$, $2^h - 2z + 1 \geq \max\{0, 2^h - 6\}$ be positive integers and denote

$$\Omega := \{0, 1, 2^h\} = \Lambda^i_0 \cup \Lambda^i_1,$$

$$\Omega^\perp := \{0, 2, 3, \ldots, 2^h - 1\} = \{0, 1, \ldots, 2^h + 1\} \setminus \left(\Lambda^i_1 \cup \Lambda^i_{2^h+1}\right)$$

and

$$\Omega^*(z) = \Omega^* := \{z, z+1, \ldots, 2^h - z + 1\} = \Lambda^i_z \cup \Lambda^i_{z+1} \cup \cdots \cup \Lambda^i_{2^h-1}.$$

These are closed sets (in the fixed variable i with respect to 2^h) of the set $\{0, 1, \ldots, n_i - 1\} = \{0, 1, \ldots, 2^h + 1\}$ (identified with $\{0\} \cup \mathbb{Z}/(2^h+1)\mathbb{Z}$) of possible exponents, in the variable X_i, of evaluation polynomials. Define the following four types of sets Δ (named Δ_1, $\Delta^\perp_1$, Δ_2 and $\Delta^\perp_2$) to be used in our second family of codes $\mathcal{S}^{P,J}_{\Delta}$:

$$\Delta_1 := \begin{cases} \Omega \times \{0, 1, \ldots, n_2 - 1\}, & \text{when } i = 1, \\ \{0, 1, \ldots, n_1 - 1\} \times \Omega, & \text{otherwise;} \end{cases}$$

$$\Delta^\perp_1 := \begin{cases} \Omega^\perp \times \{0, 1, \ldots, n_2 - 1\}, & \text{when } i = 1, \\ \{0, 1, \ldots, n_1 - 1\} \times \Omega^\perp, & \text{otherwise;} \end{cases}$$

$$\Delta_2(j) := \Delta_2 := \begin{cases} \Omega \times \{0,1,\dots,j-1\} \cup (0,j), & \text{when } i=1, \\ \{0,1,\dots,j-1\} \times \Omega \cup (j,0), & \text{otherwise;} \end{cases}$$

and

$$\Delta_2^{\perp}(z) := \Delta_2^{\perp} := \begin{cases} \Omega^{\perp} \times \{0,1,\dots,n_2-2\} \cup \Omega^* \times \{n_2-1\}, & \text{when } i=1, \\ \{0,1,\dots,n_1-2\} \times \Omega^{\perp} \cup \{n_1-1\} \times \Omega^*, & \text{otherwise.} \end{cases}$$

The reasons for choicing the above sets Δ are essentially the same ones we explained for our first family, however there are some minor difference. Here, in some cases, a smaller set of exponents is considered for the variable i' but we keep the closeness property because, in such cases, the minimal closed sets in the variable i' contain a single element. We also have MDS projected codes but our proof for this property is different.

Our next result plays the role of Lemma 3.3.3 for studying our second family of optimal codes.

Lemma 3.3.5. *Keep the above notation. Let* $V_1 = \langle X^e \mid e \in \Omega \rangle_{\mathbb{F}_q}$, $V_2 = \langle X^e \mid e \in \Omega^{\perp} \rangle_{\mathbb{F}_q} \subseteq \mathcal{R}_i$ *and define* $\mathcal{C}_1 := \mathrm{ev}_{P_i}(V_1) \cap \mathbb{F}_{2^h}^{\#P_i=2^h+2}$ *and* $\mathcal{C}_2 := \mathrm{ev}_{P_i}(V_2) \cap \mathbb{F}_{2^h}^{2^h+2}$. *Then,* $\mathcal{C}_1$ *and* $\mathcal{C}_2$ *are MDS codes.*

Proof. Notice that $\mathrm{ev}_{P_i}(V_2)$ is the dual code of $\mathrm{ev}_{P_i}(V_1)$ since

$$\Omega^{\perp} = \left\{0,1,\dots,2^h+1\right\} \setminus \left\{2^h+1-x \mid x \in \Omega\right\}$$

[49, Proposition 1] and, by Delsarte Theorem, $(\mathcal{C}_2)^{\perp} = (\mathrm{ev}_{P_i}(V_2))^{\perp} \cap \mathbb{F}_{2^h}^{2^h+2} = \mathcal{C}_1$, since $\Omega = \Lambda_0^i \cup \Lambda_1^i$ is closed and then $\Omega^{\perp}$ also is. Thus, it suffices to prove that $\mathcal{C}_1$ is an MDS code. Notice that its dimension coincides with the dimension of $\mathrm{ev}_{P_i}(V_1)$ because Ω is closed (Theorem 1.5.7), so the parameters of $\mathcal{C}_1$ are $[2^h+2, 3, \leq 2^h]_{2^h}$. Moreover, any codeword $\boldsymbol{c} \in \mathcal{C}_1$ is of the form $\boldsymbol{c} = \mathrm{ev}_{P_i}(f)$, where $f = \mathcal{T}(\lambda + \mu X)$, $\lambda, \mu \in \mathbb{F}_q = \mathbb{F}_{2^{2h}}$ and $\mathcal{T}: \mathcal{R}_i \to \mathcal{R}_i$ is the map given by $\mathcal{T}(g) = g + g^{2^h}$ (see Subsection 1.5.1). We have to prove that $\mathrm{d}(\mathcal{C}_1) = 2^h$, which is equivalent to prove that the number of roots of $f = \lambda + \lambda^{2^h} + \mu X + \mu^{2^h} X^{2^h}$ in $P_i = U_{2^h+1} \cup \{0\}$ is at most 2, or that the equation

$$\lambda + \mu X = \lambda^{2^h} + \mu^{2^h} X^{2^h} \tag{3.3.1}$$

has at most 2 solutions in P_i. Indeed, if $\lambda \notin \mathbb{F}_{2^h}$, $X = 0$ is not a solution since $\lambda \neq \lambda^{2^h}$. Thus, the above equation is equivalent to

$$\lambda X + \mu X^2 = \lambda^{2^h} X + \mu^{2^h} X^{2^h+1}$$

and to

$$\mu X^2 + \left(\lambda + \lambda^{2^h}\right) X + \mu^{2^h} = 0,$$

which has at most 2 solutions in P_i. Otherwise, if $\lambda \in \mathbb{F}_{2^h}$, then $\lambda = \lambda^{2^h}$ and Equation (3.3.1) is equivalent to

$$\mu X \left((\mu X)^{2^h-1} - 1\right) = 0.$$

We may suppose $\mu \neq 0$ since the case $\mu = 0$ is not relevant to compute the minimum distance. Then, the solutions are $X = 0$ and $X = \frac{\beta}{\mu}$ with $\beta \in \mathbb{F}_{2^h}$ such that $\beta^{2^h+1} = \mu^{2^h+1}$ (since $X^{2^h+1} = 1$), that is, $\beta^2 = \mu^{2^h+1}$. The solution $X = \frac{\beta}{\mu}$ exists if μ^{2^h+1} ($\in \mathbb{F}_{2^h}$) is a square in $\in \mathbb{F}_{2^h}$ and therefore $\beta = \sqrt{\mu^{2^h+1}}$. Hence, we obtain at most 2 solutions in P_i, as desired. □

As before, we give sets P, J and Δ providing our *second family of new optimal LRCs* $\mathcal{S}_\Delta^{P,J}$ in the bivariate case. Parameters for these codes are given in the forthcoming Theorem 3.3.10.

Proposition 3.3.6. *Keep the notation as before Lemma 3.3.5 where $\mathbb{F}_{2^h}$ is regarded as a subfield of $\mathbb{F}_{q=2^{2h}}$. Fixed $i \in \{1,2\}$ and $P_i = U_{2^h+1} \cup \{0\}$, the set of 2^h+1-th roots of unity together with 0, the following statements determine sets $P_{i'}$, J and Δ such that the subfield-subcodes $\mathcal{S}_\Delta^{P,J}$ over the field $\mathbb{F}_{2^h}$ are optimal (r,δ)-LRCs. Recall that $P = P_1 \times P_2$ and $\{i,i'\} = \{1,2\}$.*

(1) $P_{i'} = U_{n_{i'}}$ for some $n_{i'}$ such that $n_{i'} \mid q-1$; $J = \{i'\}$ and $\Delta = \Delta_1$, in which case $(r,\delta) = (3, 2^h)$.

(2) $P_{i'} = U_{n_{i'}-1} \cup \{0\}$ for some $n_{i'}$ such that $n_{i'} - 1 \mid q-1$; $J = \varnothing$ and $\Delta = \Delta_1$, in which case $(r,\delta) = (3, 2^h)$.

(3) $P_{i'} = U_{n_{i'}}$ for some $n_{i'}$ such that $n_{i'} \mid q-1$; $J = \{i'\}$ and $\Delta = \Delta_1^\perp$, in which case $(r,\delta) = (2^h-1, 4)$.

(4) $P_{i'} = U_{n_{i'}-1} \cup \{0\}$ for some $n_{i'}$ such that $n_{i'} - 1 \mid q-1$; $J = \varnothing$ and $\Delta = \Delta_1^\perp$, in which case $(r,\delta) = (2^h-1, 4)$.

(5) $P_{i'} = U_{n_{i'}}$ for some $n_{i'}$ such that $n_{i'} \mid 2^h-1$; $J = \{i'\}$ and $\Delta = \Delta_2$, where $j \geq \max\{1, n_{i'} - 2^{h-1}\}$. In this case $(r,\delta) = (3, 2^h)$.

(6) $P_{i'} = U_{n_{i'}-1} \cup \{0\}$ for some $n_{i'}$ such that $n_{i'} - 1 \mid 2^h-1$; $J = \varnothing$ and $\Delta = \Delta_2$, where $\max\{1, n_{i'} - 2^{h-1}\} \leq j < n_{i'} - 1$. In this case $(r,\delta) = (3, 2^h)$.

(7) $P_{i'} = U_{n_{i'}-1} \cup \{0\}$ for some $n_{i'}$ such that $n_{i'} - 1 \mid q-1$; $J = \varnothing$ and $\Delta = \Delta_2$, where $j = n_{i'} - 1$. In this case $(r,\delta) = (3, 2^h)$.

(8) $P_{i'} = U_{n_{i'}-1} \cup \{0\}$ for some $n_{i'}$ such that $n_{i'} - 1 \mid q-1$; $J = \varnothing$ and $\Delta = \Delta_2^\perp$, in which case $(r,\delta) = (2^h-1, 4)$.

Proof. The proof follows from a close reasoning to that given in the proof of Proposition 3.3.4. There are some minor differences which we next explain.

- Recall that $\{0,1,\ldots,2^h+1\}$ is a set of representatives of $\{0\} \cup \mathbb{Z}/(2^h+1)\mathbb{Z}$ and Λ_l^i is the minimal closed set in the variable i of the element $l \in \{0,1,\ldots,2^h+1\}$. Then, as we said before

$$\Omega = \Lambda_0^i \cup \Lambda_1^i,$$

$$\Omega^{\perp} = \left\{0, 1, \ldots, 2^h + 1\right\} \setminus \left(\Lambda_1^i \cup \Lambda_{2^h+1}^i\right),$$

and

$$\Omega^{\star} = \Lambda_z^i \cup \Lambda_{z+1}^i \cup \cdots \cup \Lambda_{2^h-1}^i,$$

are clearly closed sets, which proves that the sets Δ_1, $\Delta_1^{\perp}$ and $\Delta_2^{\perp}$, as well as Δ_2 in Item (7) are closed. The fact that the sets Δ_2 in Items (5) and (6) are closed follows by noticing that when $P_{i'} = U_{n_{i'}}$, $n_{i'} \mid 2^h - 1$ or $P_{i'} = U_{n_{i'}-1} \cup \{0\}$, $n_{i'} - 1 \mid 2^h - 1$, one can identify 2^h with 1 when computing minimal closed sets in the variable i'. Therefore, the sets $\{0, 1, \ldots, j-1\}$ and $\{j\}$ are closed because they are a union of single point minimal closed sets. This proves that Δ_2 is closed.

- Lemma 3.3.5 implies that $\mathrm{ev}_{P_i}(V_1) \cap \mathbb{F}_{2^h}^{2^h+2}$ and $\mathrm{ev}_{P_i}(V_2) \cap \mathbb{F}_{2^h}^{2^h+2}$ are MDS codes with respective minimum distances 2^h and 4. Proposition 3.1.1 applied to $\mathcal{S}_{\Delta}^{P,J}$ proves that it is an LRC with locality $(3, 2^h)$ when Δ equals Δ_1 or Δ_2 and $(2^h - 1, 4)$ in case Δ be $\Delta_1^{\perp}$ or $\Delta_2^{\perp}$.

- When $i = 1$, the minimum distance of $\mathcal{S}_{\Delta}^{P,J}$ admits the bound on the minimum distance of $\mathcal{C}_{\Delta'}^{P,J}$, $d_0\left(\mathcal{C}_{\Delta'}^{P,J}\right)$, whenever the pair (Δ, Δ') belongs to the following set:

$$\left\{\left(\Delta_1, \Delta_{2,n_2-1}^1\right), \left(\Delta_1^{\perp}, \Delta_{2^h-2,n_2-1}^1\right), \left(\Delta_2, \begin{cases} \Delta_{2,0}^2, & \text{when } j = n_2 - 1, \\ \Delta_{2,j}^3, & \text{otherwise.} \end{cases}\right), \left(\Delta_2^{\perp}, \Delta_{2^h-2,2^h-2z+1}^2\right)\right\}.$$

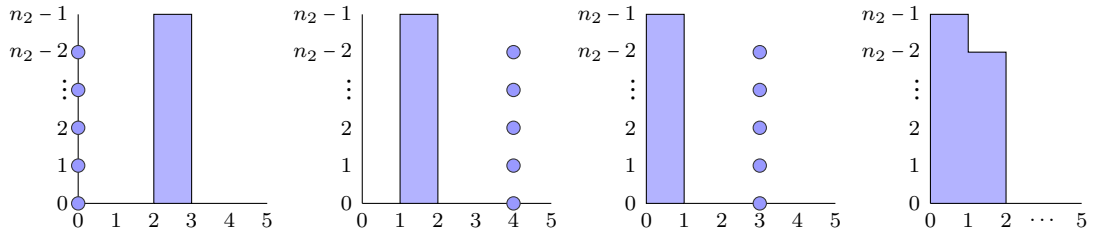
Recall that the sets $\Delta_{i,j}^l$, $1 \le l \le 3$ were introduced in Section 3.2. The cases where Δ equals Δ_1 or $\Delta_1^{\perp}$ (respectively, Δ_2 or $\Delta_2^{\perp}$) can be proved as in Item a) (respectively c)) in the proof of Proposition 3.3.4. However, when $\Delta = \Delta_2$ and the exponent of the leading monomial of f is $(0, j)$, we do not consider any set Δ'' but we immediately notice that $\mathrm{w}(\boldsymbol{c}) \ge n_1(n_2 - j)$. When $\Delta = \Delta_2^{\perp}$ and the exponent of the leading monomial of f is in $\Omega^{\star} \times \{n_2 - 1\}$, following the idea of the proof of Proposition 3.3.4, we consider the sets:

$$\Delta_0'' := \Delta + (2^h + 2 - z, 0) \subseteq E \quad \text{and} \quad \Delta'' := \Delta_0'' + (-1, 0) \subseteq E,$$

because of the relation $2^h + 2 = 1$ in $\{0, 1, \ldots, 2^h + 1\}$. We illustrate this part of the proof with the example in Figure 3.18. Since $0 \in P_1$, now we have

$$\mathrm{w}(\boldsymbol{c}) \ge \mathrm{w}(\mathrm{ev}_P(X^{-1}(X^{2^h+2-z} f))) \ge \mathrm{F}(2^h + 1 - 2z, n_2 - 1) = 2z + 1.$$

Then, wherever the exponent of the leading monomial of f is, $\mathrm{w}(\boldsymbol{c}) \ge \min\{8, 2z+1\} = 2z+1$ and therefore the minimum distance of $\mathcal{S}_{\Delta}^{P,J}$ admits the bound on the minimum distance of $\mathcal{C}_{\Delta'}^{P,J}$, that is, $\mathrm{d}(\mathcal{S}_{\Delta}^{P,J}) \ge 2z + 1 = d_0(\mathcal{C}_{\Delta'}^{P,J})$.



(1) $\Delta = \Delta_2^{\perp} = \Omega^{\perp} \times \{0,1,\ldots,n_2-2\} \cup \Omega^* \times \{n_2-1\}$ (2) $\Delta_0'' = (\Delta_2^{\perp})_0'' = \Delta_2^{\perp} + (4,0)$ (3) $\Delta'' = (\Delta_2^{\perp})'' = (\Delta_2^{\perp})_0'' + (-1,0)$ (4) $\Delta' = (\Delta_2^{\perp})' = \Delta_{2,1}^2$

Figure 3.18: Sets $\Delta_2^{\perp}$, Δ_0'', Δ'' and Δ' considered in the proof of Proposition 3.3.6 for values $(i, 2^h, q, P_1, P_2, J, z) = (1, 4, 16, U_5 \cup \{0\}, U_{n_2-1} \cup \{0\}, \varnothing, 2)$

The case $i = 2$ can also be proved following the same arguments as above. It suffices to consider the symmetric situation, replace P_1 by P_2, n_2 by n_1 and use pairs (Δ, Δ') such that

$$(\Delta,\Delta') \in \left\{ \left(\Delta_1, \Delta^1_{n_1-1,2}\right), \left(\Delta_1^{\perp}, \Delta^1_{n_1-1,2^h-2}\right), \left(\Delta_2, \begin{cases} \Delta^{2,\sigma}_{2,0}, & \text{when } j = 2^h+1, \\ \Delta^{3,\sigma}_{j,2}, & \text{otherwise.} \end{cases}\right), \left(\Delta_2^{\perp}, \Delta^{2,\sigma}_{2^h-2,2^h-2z+1}\right) \right\}.$$

We conclude with a last difference with respect to the proof of Proposition 3.3.4.

- The fact that $\mathcal{C}^{P,J}_{\Delta'}$ is optimal follows from Corollary 3.2.12 (1) when Δ is Δ_1 or $\Delta_1^{\perp}$, Corollary 3.2.12 (3) when $\Delta = \Delta_2$ and $j < n_{i'} - 1$ and Corollary 3.2.12 (2) when Δ equals $\Delta_2^{\perp}$ or Δ_2 and $j = n_{i'} - 1$. □

Remark 3.3.7. Propositions 3.3.4 and 3.3.6 do not give an exhaustive list of the optimal (r,δ)-codes one can find from subfield-subcodes of MCCs. These results are designed for providing p^h-ary optimal (r,δ)-LRCs such that $r+\delta-1$ is either p^h+1 or p^h+2 and their lengths are a multiple of $r+\delta-1$, $r>1$ and $\delta>2$. Notice that these codes are new with respect to those given in the literature, see the beginning of this section. The gcd-type condition given in Proposition 3.3.4 Item (3) is stated to provide new parameters with respect to those obtained in [121]. Moreover, excepting Proposition 3.3.6, Items (5), with $j \neq n_{i'} - 1$, and (7) (where $d \geq r+\delta$), codes in both propositions have minimum distances $d \leq \min\{r+\delta, 2\delta\}$, being new with respect to [79].

Examples 3.3.8. In these examples, we give some new optimal LRCs obtained by applying Propositions 3.3.4 and 3.3.6.

(1) Our first example corresponds to Proposition 3.3.4 (3). To help the reader, in this first example we are more explicit. Consider $(q, p^h, i, z, t, n_1, n_2) = (5^2, 5, 2, 1, 0, 9, 6)$ and the set $\Delta_2(z,t)$ in our first family. This means that we consider the field $\mathbb{F}_{25}$, its subfield $\mathbb{F}_5$ and we fix the second variable to interpolate. Moreover, the set

of points to evaluate in that variable (respectively, first variable) is the set of 6-th roots of unity (respectively, 8-th roots of unity together with the element 0), which has cardinality n_2 (respectively, n_1). Then, one gets a $[54, 25, 6]_5$ optimal $(3, 4)$-LRC.

(2) Consider $(q, p^h, i, z, n_1, n_2) = (7^2, 7, 2, 2, 17, 8)$, then by Proposition 3.3.4 (2) one gets a $[136, 85, 4]_7$ optimal $(5, 4)$-LRC.

(3) Consider $(q, p^h, i, z, t, n_1, n_2) = (9^2, 9, 1, 3, 1, 10, 21)$, then by Proposition 3.3.4 (3) one gets a $[210, 143, 8]_9$ optimal $(7, 4)$-LRC.

(4) Consider $(q, p^h, i, n_1, n_2) = (2^4, 4, 1, 6, 15)$, then by Proposition 3.3.6 (1) one gets a $[90, 45, 4]_4$ optimal $(3, 4)$-LRC.

(5) Consider $(q, p^h, i, j, n_1, n_2) = (2^6, 8, 2, 6, 8, 10)$, then by Proposition 3.3.6 (6) one gets a $[80, 19, 20]_8$ optimal $(3, 8)$-LRC.

(6) Consider $(q, p^h, i, z, n_1, n_2) = (2^6, 8, 1, 3, 10, 10)$, then by Proposition 3.3.6 (8) one gets a $[100, 58, 7]_8$ optimal $(7, 4)$-LRC.

Figure 3.19 shows the sets Δ introduced in Propositions 3.3.4 and 3.3.6 and used in the above examples. We make explicit the descomposition of the set $\Delta = \Delta_2 = \{0, 1, \ldots, 5\} \times \{0, 1, 8\} \cup \{(6, 0)\}$ in Example 3.3.8 (5) as a union of minimal closed sets. Indeed, $(i, P_1, P_2, J) = (2, U_7 \cup \{0\}, U_9 \cup \{0\}, \varnothing)$ and Δ is the union of the following minimal closed sets:

$$\Lambda_{(0,0)} = \{(0,0)\}, \quad \Lambda_{(1,0)} = \{(1,0)\}, \quad \Lambda_{(2,0)} = \{(2,0)\}, \quad \Lambda_{(3,0)} = \{(3,0)\},$$
$$\Lambda_{(4,0)} = \{(4,0)\}, \quad \Lambda_{(5,0)} = \{(5,0)\}, \quad \Lambda_{(6,0)} = \{(6,0)\}, \quad \Lambda_{(0,1)} = \{(0,1),(0,8)\},$$
$$\Lambda_{(1,1)} = \{(1,1),(1,8)\}, \quad \Lambda_{(2,1)} = \{(2,1),(2,8)\}, \quad \Lambda_{(3,1)} = \{(3,1),(3,8)\},$$
$$\Lambda_{(4,1)} = \{(4,1),(4,8)\}, \quad \Lambda_{(5,1)} = \{(5,1),(5,8)\}.$$

Now, we state our main results in this subsection which are Theorems 3.3.9 and 3.3.10. These results follow directly from Propositions 3.3.4 and 3.3.6 and provide explicitly the parameters and (r, δ)-localities of the new optimal LRCs we have obtained.

Theorem 3.3.9. *Let $\mathbb{F}_q$ be a finite field with $q = p^l$, p being a prime number and l a positive integer. Consider another positive integer h such that h divides l, $p^h \geq 4$ if $p = 2$ ($p^h \geq 5$, otherwise) and assume $p^h + 1 \mid q - 1$. Consider also nonnegative integers z and t satisfying $0 \leq t < z \leq \left\lfloor \frac{p^h}{2} \right\rfloor - 1$, $2t \geq \max\{0, 4z - p^h - 1\}$. Regard $\mathbb{F}_{p^h}$ as a subfield of $\mathbb{F}_q$.*

Then, there exists an optimal (r, δ)-LRC over $\mathbb{F}_{p^h}$ with the following parameters depending on two integer variables n' and a:

$$[n, k, d]_{p^h} = \left[(p^h + 1)n', (n' - 1)(2z + 1) + 2a + 1, p^h + 1 - 2a\right]_{p^h}$$

and

$$(r, \delta) = (2z + 1, p^h - 2z + 1),$$

whenever some of the following conditions hold:

(1) $n' \mid q-1$ *and* $a = z$.

(2) $n'-1 \mid q-1$ *and* $a = z$.

(3) $n'-1 \mid q-1$, $a = t$ *and, if* p *is odd, either* $\gcd(n', p^h) \neq 1$ *or* $\gcd(n', p^h+1) \neq 1$.

Assume now that $p = 2$ *and consider a nonnegative integer* u *and, if* $u \geq 1$, *a nonnegative integer* v, *satisfying* $0 \leq u \leq \frac{p^h}{2} - 2$, $0 \leq v < u$ *and* $2v + 1 \geq \max\{0, 4u + 1 - p^h\}$.

Then, there exists an optimal (r,δ)*-LRC over* $\mathbb{F}_{p^h}$ *with the following parameters depending on two integer variables* n' *and* a*:*

$$[n,k,d]_{p^h} = \left[(p^h+1)n', (n'-1)(2u+2) + 2a + 2, p^h - 2a\right]_{p^h}$$

and

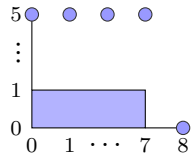
$$(r,\delta) = (2u+2, p^h - 2u),$$

whenever some of the following conditions hold:

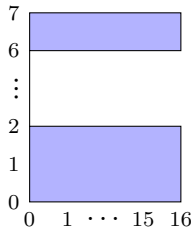
(1) $n' \mid q-1$ *and* $a = u$.

(2) $n'-1 \mid q-1$ *and* $a = u$.

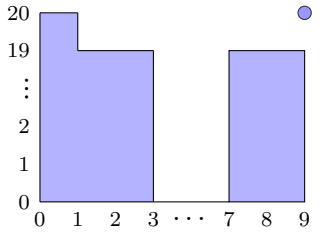
(3) $n'-1 \mid q-1$ *and* $a = v$.



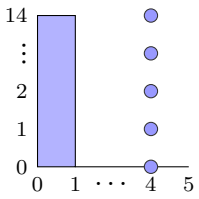
(1) $\Delta = \{0,1,\ldots,7\} \times \{0,1,5\} \cup \{(8,0)\}$



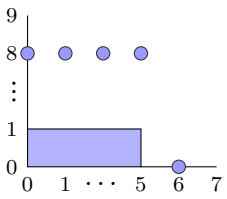
(2) $\Delta = \{0,1,\ldots,16\} \times \{0,1,2,6,7\}$



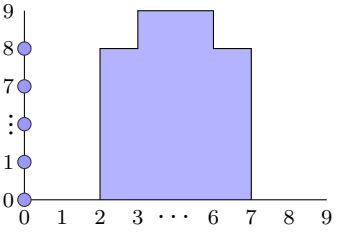
(3) $\Delta = \{0,1,2,3,7,8,9\} \times \{0,1,\ldots,19\} \cup \{0,1,9\} \times \{20\}$



(4) $\Delta = \{0,1,4\} \times \{0,1,\ldots,14\}$



(5) $\Delta = \{0,1,\ldots,5\} \times \{0,1,8\} \cup \{(6,0)\}$



(6) $\Delta = \{0,2,3,\ldots,7\} \times \{0,1,\ldots,8\} \cup \{3,4,5,6\} \times \{9\}$

Figure 3.19: Sets Δ considered in Examples 3.3.8

Theorem 3.3.10. *Let $\mathbb{F}_q$ be a finite field with $q = 2^l$, $l \geq 4$ being an even positive integer and $h = \frac{l}{2}$. Consider also a positive integer z satisfying $2 \leq z \leq 3$, $2^h - 2z + 1 \geq \max\{0, 2^h - 6\}$. Regard $\mathbb{F}_{2^h}$ as a subfield of $\mathbb{F}_q$.*

Then, there exists an optimal (r, δ)-LRC over $\mathbb{F}_{2^h}$ with the following parameters depending on the integer variables n', a, b and c:

$$[n, k, d]_{2^h} = \left[(2^h + 2)n', a(n' - 1) + b, 2h + 3 - b\right]_{2^h}$$

and

$$(r, \delta) = (a, c),$$

whenever some of the following conditions hold:

(1) $n' \mid q - 1$ *and* $(a, b, c) = (3, 3, 2^h)$.

(2) $n' - 1 \mid q - 1$ *and* $(a, b, c) = (3, 3, 2^h)$.

(3) $n' \mid q - 1$ *and* $(a, b, c) = (2^h - 1, 2^h - 1, 4)$.

(4) $n' - 1 \mid q - 1$ *and* $(a, b, c) = (2^h - 1, 2^h - 1, 4)$.

(5) $n' - 1 \mid q - 1$ *and* $(a, b, c) = (2^h - 1, 2^h - 2z + 2, 4)$.

Finally, consider n' and j positive integers such that $j \leq n' - 1$ and they satisfy some of the following conditions:

(1) $n' \mid 2^h - 1$ *and* $j \geq \max\{1, n' - 2^{h-1}\}$.

(2) $n' - 1 \mid 2^h - 1$ *and* $\max\{1, n' - 2^{h-1}\} \leq j < n' - 1$.

(3) $n' - 1 \mid q - 1$ *and* $j = n' - 1$.

Then, there exists an optimal (r, δ)-LRC over $\mathbb{F}_{2^h}$ with parameters

$$[n, k, d]_{2^h} = \left[(2^h + 2)n', 3j + 1, (2^h + 2)(n' - j)\right]_{2^h}$$

and

$$(r, \delta) = (3, 2^h).$$

Table 3.1 shows parameters of some new optimal (r, δ)-LRCs coming from subfield-subcodes deduced from Theorems 3.3.9 and 3.3.10.

3.3.2. Optimal (r, δ)-LRCs coming from subfield-subcodes of multivariate MCCs

This section is devoted to extend Propositions 3.3.4 and 3.3.6 and Theorems 3.3.9 and 3.3.10 to the multivariate case. The corresponding versions are stated in the below Propositions 3.3.11 and 3.3.12, and Theorems 3.3.14 and 3.3.15. Their proofs run parallel

Item in Theorem	p^h	q	n	k	d	r	δ
3.3.9 (3) (for $(n',z,t)=(25,1,0)$)	5	25	$150=6\cdot 25$	73	6	3	4
3.3.9 (1) (for $(n',z)=(48,1)$)	7	49	$384=8\cdot 48$	144	6	3	6
3.3.9 (2) (for $(n',u)=(16,0)$)	4	16	$80=5\cdot 16$	32	4	2	4
3.3.9 (3) (for $(n',z,t)=(22,2,0)$)	8	64	$198=9\cdot 22$	106	9	5	5
3.3.10 (2) (for $(n',j)=(8,5)$)	8	64	$80=10\cdot 8$	16	30	3	8
3.3.10 (3) (for $n'=18$)	4	256	$108=6\cdot 18$	144	6	3	6

Table 3.1: Optimal (r,δ)-subfield-subcodes over $\mathbb{F}_{p^h}$ in the bivariate case

to those given in the bivariate case and we omit them. The sets Δ extend the ones used for the bivariate case, but our multivariate case requires to write them in a different way.

Keep the notation as in Section 3.1 and Subsection 1.5.1. Fix $j_0 \in \{1,\dots,m\}$ (it refers to the variable X_{j_0} we use to interpolate when applying our recovery method) and S_1, $S_2 \subseteq \{1,\dots,m\}\backslash\{j_0\}$ such that $S_1 \cup S_2 = \{1,\dots,m\}\backslash\{j_0\}$ and $S_1 \cap S_2 = \varnothing$. These sets give a partition of $\{1,\dots,m\}\backslash\{j_0\}$ to decide which variables are (or not) evaluated at zero. As before, Propositions 3.3.11 and 3.3.12 determine two constructions of sets P, J and Δ to get optimal families of LRCs, and Theorems 3.3.14 and 3.3.15 give the parameters of the corresponding codes. Notice that Proposition 3.3.12 and Theorem 3.3.15 give rise to codes over fields of characteristic two.

For our first construction, keep the notation as in the paragraphs before Lemma 3.3.3 but changing i by j_0. In particular consider nonnegative integers z and t (and when $p=2$) u and v as in those paragraphs. Denote

$$O_{z,t} := \left\{t+1, t+2, \dots, z, p^h+1-z, p^h+2-z, \dots, p^h-t\right\}$$

and

$$O_{u,v} := \left\{\frac{p^h}{2}-u, \frac{p^h}{2}-u+1, \dots, \frac{p^h}{2}-v-1, \frac{p^h}{2}+v+2, \frac{p^h}{2}+v+3, \dots, \frac{p^h}{2}+u+1\right\}.$$

Define

$$\Delta_1 := \{0,1,\dots,n_1-1\}\times\cdots\times\{0,1,\dots,n_{j_0-1}-1\}\times\Omega_z\times\{0,1,\dots,n_{j_0+1}-1\}\times\cdots\times\{0,1,\dots,n_m-1\},$$

$$\Delta_2 := \Delta_1\Big\backslash\left\{(n_1-1,\dots,n_{j_0-1}-1,e_{j_0},n_{j_0+1}-1,\dots,n_m-1) \mid e_{j_0}\in O_{z,t}\right\},$$

$$\Delta_1^* := \{0,1,\dots,n_1-1\}\times\cdots\times\{0,1,\dots,n_{j_0-1}-1\}\times\Omega_u^*\times\{0,1,\dots,n_{j_0+1}-1\}\times\cdots\times\{0,1,\dots,n_m-1\}$$

and

$$\Delta_2^* := \Delta_1^*\Big\backslash\left\{(n_1-1,\dots,n_{j_0-1}-1,e_{j_0},n_{j_0+1}-1,\dots,n_m-1) \mid e_{j_0}\in O_{u,v}\right\}.$$

Proposition 3.3.11. *Keep the notation as above where $\mathbb{F}_{p^h}$ is regarded as a subfield of $\mathbb{F}_{q=p^l}$ and $p^h+1 \mid q-1$. Fixed j_0 and $P_{j_0}=U_{p^h+1}$, the set of p^h+1-th roots of unity, the following statements determine sets $P=P_1\times\cdots\times P_m$, J and Δ such that the subfield-subcodes $\mathcal{S}_\Delta^{P,J}$ over the field $\mathbb{F}_{p^h}$ are optimal (r,δ)-LRCs:*

(1) $P_j = U_{n_j}$ *for some* n_j *such that* $n_j \mid q-1$ *whenever* $j \in S_1$ *and when* $j \in S_2$ $P_j = U_{n_j-1} \cup \{0\}$ *for some* n_j *such that* $n_j - 1 \mid q-1$; $J = S_1 \cup \{j_0\}$ *and* $\Delta = \Delta_1$, *in which case*

$$(r, \delta) = (2z+1, p^h - 2z + 1).$$

(2) $S_1 = \varnothing$, *for all* $j \in S_2$ $P_j = U_{n_j-1} \cup \{0\}$ *for some* n_j *such that* $n_j - 1 \mid q-1$ *and, if* p *is odd, either* $\gcd\left(\prod_{j\in\{1,\ldots,m\}\setminus\{j_0\}} n_j, p^h\right) \neq 1$ *or* $\gcd\left(\prod_{j\in\{1,\ldots,m\}\setminus\{j_0\}} n_j, p^h+1\right) \neq 1$; $J = \{j_0\}$ *and* $\Delta = \Delta_2$, *in which case*

$$(r, \delta) = (2z+1, p^h - 2z + 1).$$

(3) $P_j = U_{n_j}$ *for some* n_j *such that* $n_j \mid q-1$ *when* $j \in S_1$ *and when* $j \in S_2$ $P_j = U_{n_j-1} \cup \{0\}$ *for some* n_j *such that* $n_j - 1 \mid q-1$; $J = S_1 \cup \{j_0\}$ *and* $\Delta = \Delta_1^*$, *in which case*

$$(r, \delta) = (2u+2, p^h - 2u).$$

(4) $S_1 = \varnothing$ *and for all* $j \in S_2$ $P_j = U_{n_j-1} \cup \{0\}$ *for some* n_j *such that* $n_j - 1 \mid q-1$; $J = \{j_0\}$ *and* $\Delta = \Delta_2^*$, *in which case*

$$(r, \delta) = (2u+2, p^h - 2u).$$

For the second construction, we use the notation as in the paragraph before Lemma 3.3.5 but changing i by j_0. Define

$$\Delta_1 := \{0,1,\ldots,n_1-1\}\times\cdots\times\{0,1,\ldots,n_{j_0-1}-1\}\times\Omega\times\{0,1,\ldots,n_{j_0+1}-1\}\times\cdots\times\{0,1,\ldots,n_m-1\},$$

$$\Delta_2 := \Delta_1 \setminus \left\{(n_1-1,\ldots,n_{j_0-1}-1, e_{j_0}, n_{j_0+1}-1,\ldots,n_m-1) \mid e_{j_0} \in \left\{1, 2^h\right\}\right\},$$

$$\Delta_1^\perp := \{0,1,\ldots,n_1-1\}\times\cdots\times\{0,1,\ldots,n_{j_0-1}-1\}\times\Omega^\perp\times\{0,1,\ldots,n_{j_0+1}-1\}\times\cdots\times\{0,1,\ldots,n_m-1\}$$

and

$$\Delta_2^\perp := \Delta_1^\perp \setminus \left\{ (n_1-1,\ldots,n_{j_0-1}-1, e_{j_0}, n_{j_0+1}-1,\ldots,n_m-1) \mid e_{j_0} \in \begin{cases} \{0\}, & \text{when } z=2, \\ \{0,2,2^h-1\}, & \text{otherwise.} \end{cases} \right\}.$$

Proposition 3.3.12. *Keep the notation as above where* $\mathbb{F}_{2^h}$ *is regarded as a subfield of* $\mathbb{F}_{q=2^{2h}}$. *Fixed* j_0 *and* $P_{j_0} = U_{2^h+1} \cup \{0\}$, *the set of* 2^h+1*-th roots of unity together with* 0, *the following statements determine sets* $P = P_1 \times \cdots \times P_m$, J *and* Δ *such that the subfield-subcodes* $\mathcal{S}_\Delta^{P,J}$ *over the field* $\mathbb{F}_{2^h}$ *are optimal* (r,δ)*-LRCs:*

(1) $P_j = U_{n_j}$ *for some* n_j *such that* $n_j \mid q-1$ *whenever* $j \in S_1$ *and when* $j \in S_2$ $P_j = U_{n_j-1} \cup \{0\}$ *for some* n_j *such that* $n_j - 1 \mid q-1$; $J = S_1$ *and* $\Delta = \Delta_1$, *in which case*

$$(r, \delta) = (3, 2^h).$$

(2) $P_j = U_{n_j}$ *for some* n_j *such that* $n_j \mid q-1$ *whenever* $j \in S_1$ *and when* $j \in S_2$ $P_j = U_{n_j-1} \cup \{0\}$ *for some* n_j *such that* $n_j - 1 \mid q-1$; $J = S_1$ *and* $\Delta = \Delta_1^\perp$, *in which case*

$$(r,\delta) = (2^h - 1, 4).$$

(3) $S_1 = \varnothing$ *and for all* $j \in S_2$ $P_j = U_{n_j-1} \cup \{0\}$ *for some* n_j *such that* $n_j - 1 \mid q-1$; $J = \varnothing$ *and* $\Delta = \Delta_2$, *in which case*

$$(r,\delta) = (3, 2^h).$$

(4) $S_1 = \varnothing$ *and for all* $j \in S_2$ $P_j = U_{n_j-1} \cup \{0\}$ *for some* n_j *such that* $n_j - 1 \mid q-1$; $J = \varnothing$ *and* $\Delta = \Delta_2^\perp$, *in which case*

$$(r,\delta) = (2^h - 1, 4).$$

Remark 3.3.13. As in the case of bivariate codes (see Remark 3.3.7), Propositions 3.3.11 and 3.3.12 do not give an exhaustive list of the optimal (r,δ)-LRCs one can get from subfield-subcodes of MCCs, in fact they impose conditions in order to obtain new families of optimal (r,δ)-LRCs. See the beginning of this section.

Finally, we state our main results for the multivariate case. They are Theorem 3.3.14 (respectively, 3.3.15) which give parameters and (r,δ)-localities of the optimal (r,δ)-LRCs we have obtained in Proposition 3.3.11 (respectively, 3.3.12).

Theorem 3.3.14. *Let* $\mathbb{F}_q$ *be a finite field with* $q = p^l$, p *being a prime number and* l *a positive integer. Consider another positive integer* h *such that* h *divides* l, $p^h \geq 4$ *if* $p = 2$ *(*$p^h \geq 5$ *otherwise) and assume* $p^h + 1 \mid q - 1$. *Consider also nonnegative integers* z *and* t *satisfying* $0 \leq t < z \leq \left\lfloor \frac{p^h}{2} \right\rfloor - 1$, $2t \geq \max\{0, 4z - p^h - 1\}$ *and subsets* S_1, $S_2 \subseteq \{1, \ldots, m-1\}$ *such that* $S_1 \cup S_2 = \{1, \ldots, m-1\}$ *and* $S_1 \cap S_2 = \varnothing$. *Regard* $\mathbb{F}_{p^h}$ *as a subfield of* $\mathbb{F}_q$.

Then, there exists an optimal (r,δ)*-LRC over* $\mathbb{F}_{p^h}$ *with the following parameters depending on the integer variables* $n_1, \ldots, n_{m-1}$ *and* a:

$$[n,k,d]_{p^h} = \left[(p^h+1)n_1 \cdots n_{m-1}, (2z+1)n_1 \cdots n_{m-1} - a, p^h + 1 - 2z + a\right]_{p^h}$$

and

$$(r,\delta) = (2z+1, p^h - 2z + 1),$$

whenever some of the following conditions hold:

(1) $n_j \mid q-1$ *for all* $j \in S_1$, $n_j - 1 \mid q-1$ *for all* $j \in S_2$ *and* $a = 0$.

(2) $S_1 = \varnothing$, $n_j - 1 \mid q - 1$ *for all* $j \in S_2$, $a = 2(z-t)$ *and, if* p *is odd, either* $\gcd\left(n_1 \cdots n_{m-1}, p^h\right) \neq 1$ *or* $\gcd\left(n_1 \cdots n_{m-1}, p^h + 1\right) \neq 1$.

Assume now that $p = 2$ *and consider a nonnegative integer* u *and, if* $u \geq 1$, *a nonnegative integer* v, *satisfying* $0 \leq u \leq \frac{p^h}{2} - 2$, $0 \leq v < u$ *and* $2v + 1 \geq \max\{0, 4u + 1 - p^h\}$.

Then, there exists an optimal (r,δ)*-LRC over* $\mathbb{F}_{p^h}$ *with parameters*

$$[n,k,d]_{p^h} = \left[(p^h+1)n_1 \cdots n_{m-1}, (2u+2)n_1 \cdots n_{m-1} - a, p^h - 2u + a\right]_{p^h}$$

and

$$(r, \delta) = (2u + 2, p^h - 2u),$$

whenever some of the following conditions hold:

(1) $n_j \mid q-1$ *for all* $j \in S_1$, $n_j - 1 \mid q-1$ *for all* $j \in S_2$ *and* $a = 0$.

(2) $S_1 = \varnothing$, $n_j - 1 \mid q-1$ *for all* $j \in S_2$ *and* $a = 2(u - v)$.

Theorem 3.3.15. *Let* $\mathbb{F}_q$ *be a finite field with* $q = 2^l$, $l \geq 4$ *being an even positive integer and* $h = \frac{l}{2}$. *Consider also a positive integer* z *satisfying* $2 \leq z \leq 3$, $2^h - 2z + 1 \geq \max\{0, 2^h - 6\}$ *and subsets* S_1, $S_2 \subseteq \{1, \ldots, m-1\}$ *such that* $S_1 \cup S_2 = \{1, \ldots, m-1\}$ *and* $S_1 \cap S_2 = \varnothing$. *Regard* $\mathbb{F}_{2^h}$ *as a subfield of* $\mathbb{F}_q$.

Then, there exists an optimal (r, δ)*-LRC over* $\mathbb{F}_{2^h}$ *with the following parameters depending on the integer variables* $n_1, \ldots, n_{m-1}$, a, b *and* c*:*

$$[n, k, d]_{2^h} = \left[(2^h + 2)n_1 \cdots n_{m-1}, an_1 \cdots n_{m-1} - b, c + b\right]_{2^h}$$

and

$$(r, \delta) = (a, c),$$

whenever some of the following conditions hold:

(1) $n_j \mid q-1$ *for all* $j \in S_1$, $n_j - 1 \mid q-1$ *for all* $j \in S_2$ *and* $(a, b, c) = (3, 0, 2^h)$.

(2) $n_j \mid q-1$ *for all* $j \in S_1$, $n_j - 1 \mid q-1$ *for all* $j \in S_2$ *and* $(a, b, c) = (2^h - 1, 0, 4)$.

(3) $S_1 = \varnothing$, $n_j - 1 \mid q-1$ *for all* $j \in S_2$ *and* $(a, b, c) = (3, 2, 2^h)$.

(4) $S_1 = \varnothing$, $n_j - 1 \mid q-1$ *for all* $j \in S_2$ *and* $(a, b, c) = (2^h - 1, 2z - 3, 4)$.

We finish this subsection by giving, in Table 3.2, the parameters of some new optimal (r, δ)-LRCs coming from subfield-subcodes deduced from Theorems 3.3.14 and 3.3.15.

Item in Theorem	p^h	q	n	k	d	r	δ
3.3.14 (1) (for $(m, z, t) = (3, 1, 0)$)	5	625	$480 = 6 \cdot 5 \cdot 16$	240	4	3	4
3.3.14 (2) (for $(m, z, t) = (3, 3, 1)$)	9	81	$800 = 10 \cdot 8 \cdot 10$	556	8	7	4
3.3.14 (2) (for $(m, z, t) = (4, 1, 0)$)	4	16	$320 = 5 \cdot 4 \cdot 4 \cdot 4$	190	5	3	3
3.3.14 (2) (for $(m, u, v) = (3, 2, 0)$)	8	64	$720 = 9 \cdot 8 \cdot 10$	476	8	6	4
3.3.15 (1) (for $m = 4$)	4	256	$900 = 6 \cdot 5 \cdot 5 \cdot 6$	450	4	3	4
3.3.15 (4) (for $(m, z) = (3, 2)$)	4	16	$576 = 6 \cdot 6 \cdot 16$	287	5	3	4

Table 3.2: Optimal (r, δ)-subfield-subcodes over $\mathbb{F}_{p^h}$ in the multivariate case

Acknowledgements. We thank O. Geil and H. H. López for explaining us when monomial-Cartesian codes were introduced and named. These facts had gone unnoticed by us. We named them *zero-dimensional affine variety codes* in a previous version of [45].

Part III

Quantum codes from evaluation codes

Chapter 4

Stabilizer quantum codes from generalized monomial-Cartesian codes

Let q be an odd prime power. In this chapter we construct q^2-ary classical linear codes that satisfy the hypotheses of Corollary 2.3.8; that is we present codes that are Hermitian self-orthogonal, and thereby they give rise to stabilizer quantum codes. We also aim for these quantum codes to have good parameters. For the codes we introduce in this chapter, we are going to use the same notations as for a monomial-Cartesian code, see Subsection 1.3.1, with $Q = q^2$. Recall from Definition 1.3.3 that a q^2-ary MCC $\mathcal{C}_\Delta^P$ is an $\mathbb{F}_{q^2}$-vector subspace of $\mathbb{F}_{q^2}^n$

$$\mathcal{C}_\Delta^P = \mathrm{ev}_P(V_\Delta) = \langle \mathrm{ev}_P(X_1^{e_1} \cdots X_m^{e_m}) \mid (e_1, \ldots, e_m) \in \Delta \rangle \subseteq \mathbb{F}_{q^2}^n$$

obtained as the image of a map

$$\mathrm{ev}_P \colon V_\Delta \subset \mathcal{R} = \mathbb{F}_{q^2}[X_1, \ldots, X_m] \big/ I \to \mathbb{F}_{q^2}^n, \qquad \mathrm{ev}_P(f) = (f(\boldsymbol{\alpha}_0), \ldots, f(\boldsymbol{\alpha}_{n-1})),$$

where $m \geq 1$ is a positive integer, $P = P_1 \times \cdots \times P_m = \{\boldsymbol{\alpha}_0, \ldots, \boldsymbol{\alpha}_{n-1}\}$ a Cartesian product subset of $\mathbb{F}_{q^2}^m$, $I = \langle f_1(X_1), \ldots, f_m(X_m) \rangle$ the vanishing ideal at P of $\mathbb{F}_{q^2}[X_1, \ldots, X_m]$ (i.e., $f_j(X_j) = \prod_{\beta \in P_j}(X_j - \beta)$ for $j = 1, \ldots, m$) and

$$V_\Delta = \left\langle X_1^{e_1} \cdots X_m^{e_m} \mid (e_1, \ldots, e_m) \in \Delta \right\rangle_{\mathbb{F}_{q^2}}$$

an $\mathbb{F}_{q^2}$-linear space generated by classes of monomials with exponents in some subset $\Delta \subseteq E = \{0, 1, \ldots, n_1 - 1\} \times \cdots \times \{0, 1, \ldots, n_m - 1\}$. This set E is that containing the possibilities of exponents of any monomial reduced modulo I. Notice that we reordered the evaluation points in P from 0 to $n-1$ as it will be suitable for our purposes. Other important notations are $n_j = \#P_j$ and $n = \#P = \prod_{j=1}^m n_j$.

In this chapter we use a generalized version of monomial-Cartesian codes (GMCCs) to construct Hermitian self-orthogonal classical linear codes. This choice lets the resulting quantum codes to have a wider range of dimensions that those previously obtained with

J-affine variety codes. GMCCs are obtained from MCCs by twisting each coordinate of their codewords by fixed nonzero elements of the field. This operation may help to manage the self-orthogonality conditions. To avoid repetitions, an abstract for this chapter can be found in pages 10 to 12 of the introduction of this PhD thesis.

This chapter is laid out as follows. We introduce GMCCs in Section 4.1. Our construction is presented in Section 4.2, first a general one (Theorem 4.2.4), and then a more specific construction that allows us to control the minimum distance, maximizing also the dimension of the quantum code (Theorem 4.2.7). We provide an explicit twist vector, see Equation (4.2.1), and formulae for the dimension and minimum distance. In Section 4.3 we show that our construction with $m = 1$ gives MDS codes, and when $m = 2$ and our lower bound for the minimum distance is 3, the codes are at least Hermitian almost MDS. Section 4.4 contains a proof that for an infinite family of parameters when $m = 2$, our codes beat the Gilbert-Varshamov bound. Finally, in Section 4.5 we present many examples obtained with our procedure, defined by small parameters and being better than any known code in the literature.

The entire contents in this chapter were carried out with B. Barbero-Lucas and G. McGuire and, except for Example 4.2.8, they were published in the journal *Quantum Information Processing*, see [11]. The notation has been adapted to ease the reading of this thesis.

4.1. Generalized monomial-Cartesian codes

In this chapter we assume that q is an odd prime power, although in this section the definitions hold for any q. Let us fix a finite field $\mathbb{F}_{q^2}$. Recall that $\mathbb{F}_{q^2}[X_1, \dots, X_m]$ denotes the polynomial ring in $m \geq 1$ variables over $\mathbb{F}_{q^2}$ and that for each element $\boldsymbol{e} = (e_1, \dots, e_m) \in \mathbb{N}_0^m$, we write $\boldsymbol{X}^{\boldsymbol{e}}$ for $X_1^{e_1} X_2^{e_2} \cdots X_m^{e_m}$. We use the lexicographic order in $\mathbb{N}_0^m$ for the exponents. That is, given $\boldsymbol{e}, \boldsymbol{e}' \in \mathbb{N}_0^m$, we say $\boldsymbol{e} < \boldsymbol{e}'$ if and only if $e_1 < e_1'$ or there exists $j \in \{2, \dots, m\}$ such that $e_1 = e_1', \dots, e_{j-1} = e_{j-1}'$ and $e_j < e_j'$.

Let $\lambda \in \mathbb{N}$ such that $\lambda \mid q-1$. Let P_1 be the set of roots of the polynomial $X_1^{\lambda(q+1)} - 1$ which lies in $\mathbb{F}_{q^2}$. We also consider arbitrary subsets $P_j \subseteq \mathbb{F}_{q^2}^*$ for $j = 2, \dots, m$ which have cardinality greater than or equal to 2. The rest of the notations are the same as the above introduced for a MCC. Notice that, in this setting, $f_1(X_1) = X_1^{\lambda(q+1)} - 1$ and $n_1 = \lambda(q+1)$. Again, given $f \in \mathcal{R}$, f denotes both the equivalence class in $\mathcal{R}$ and the unique polynomial representing f in $\mathbb{F}_{q^2}[X_1, \dots, X_m]$ with degree in X_j less than n_j, $1 \leq j \leq m$. Thus, one can write any $f \in \mathcal{R}$ uniquely as

$$f(X_1, \dots, X_m) = \sum_{(e_1, \dots, e_m) \in E} f_{e_1, \dots, e_m} X_1^{e_1} \cdots X_m^{e_m},$$

with $f_{e_1, \dots, e_m} \in \mathbb{F}_{q^2}$.

Now, for any positive integer t, set ζ_t a primitive t-th root of unity. Since P_j has n_j elements, we fix a bijection between P_j and the set $\{0, 1, \dots, n_j - 1\}$ which gives an ordering on P_j, $j = 2, \dots, m$. Let us represent by $\alpha_{(j,s)}$, $0 \leq s \leq n_j - 1$, the elements of P_j

under the mentioned ordering. For $\boldsymbol{\epsilon} = (\epsilon_1, \ldots, \epsilon_m) \in E$ we define $\boldsymbol{\alpha}_{\boldsymbol{\epsilon}} \in P$ by

$$\boldsymbol{\alpha}_{\boldsymbol{\epsilon}} := (\zeta_{\lambda(q+1)}^{\epsilon_1}, \alpha_{(1,\epsilon_2)}, \ldots \alpha_{(m,\epsilon_m)}),$$

where ϵ_1 indicates the exponent of $\zeta_{\lambda(q+1)}$ and $\epsilon_j \in \{0, 1, \ldots, n_j - 1\}$ gives the position of the element $\alpha_{(j,\epsilon_j)} \in P_j$ in the ordering on P_j, $j = 2, \ldots, m$. Every element of P has the form $\boldsymbol{\alpha}_{\boldsymbol{\epsilon}}$ for some $\boldsymbol{\epsilon} \in E$. This sets up a bijection between P and E.

We order the set P with the (lexicographic) order on $\mathbb{N}_0^m$ restricted to E. That is, given $\boldsymbol{\alpha}_{\boldsymbol{\epsilon}}$, $\boldsymbol{\alpha}_{\boldsymbol{\epsilon}'} \in P$, then $\boldsymbol{\alpha}_{\boldsymbol{\epsilon}} < \boldsymbol{\alpha}_{\boldsymbol{\epsilon}'}$ if and only if $\boldsymbol{\epsilon} < \boldsymbol{\epsilon}'$. Then, we can rename the points in P as

$$\boldsymbol{\alpha}_0 := \boldsymbol{\alpha}_{(0,\ldots,0)}, \quad \boldsymbol{\alpha}_1 := \boldsymbol{\alpha}_{(0,\ldots,0,1)}, \quad \ldots, \quad \boldsymbol{\alpha}_{n-1} := \boldsymbol{\alpha}_{(n_1-1,n_2-1,\ldots,n_m-1)}.$$

Let $\boldsymbol{v} = (v_0, \ldots, v_{n-1}) \in (\mathbb{F}_{q^2}^*)^n$, we will refer to this vector as the *twist vector*. We index the coordinates of $\boldsymbol{v}$ by the elements of E, and we order the coordinates of $\boldsymbol{v}$ in the same way as we ordered the elements of P. That is,

$$v_0 := v_{(0,\ldots,0)}, \quad v_1 := v_{(0,\ldots,0,1)}, \quad \ldots, \quad v_{n-1} := v_{(n_1-1,n_2-1,\ldots,n_m-1)}.$$

The following linear evaluation map in P:

$$\mathrm{ev}_{\boldsymbol{v},P}\colon \mathcal{R} \to \mathbb{F}_{q^2}^n, \qquad \mathrm{ev}_{\boldsymbol{v},P}(f) = (v_0 f(\boldsymbol{\alpha}_0), \ldots, v_{n-1} f(\boldsymbol{\alpha}_{n-1}))$$

is injective by the definition of $\mathcal{R}$. It provides the following class of evaluation codes.

Definition 4.1.1. Let P, $\boldsymbol{v}$ and Δ be as above. The *generalized monomial-Cartesian code (GMCC)* $\mathcal{C}_{\boldsymbol{v},\Delta}^P$ is the image of V_Δ via the evaluation map $\mathrm{ev}_{\boldsymbol{v},P}$, that is,

$$\mathcal{C}_{\boldsymbol{v},\Delta}^P := \mathrm{ev}_{\boldsymbol{v},P}(V_\Delta) = \langle \mathrm{ev}_{\boldsymbol{v},P}(\boldsymbol{X}^{\boldsymbol{e}}) \mid \boldsymbol{e} \in \Delta \rangle \subseteq \mathbb{F}_{q^2}^n.$$

Along this chapter, we fix an ordering on P as before and then use the notation $\mathrm{ev}_{\boldsymbol{v}} := \mathrm{ev}_{\boldsymbol{v},P}$ and $\mathcal{C}_{\boldsymbol{v},\Delta} := \mathcal{C}_{\boldsymbol{v},\Delta}^P$.

Remark 4.1.2. When all the sets $P_j \subseteq \mathbb{F}_{q^2}$, $j = 1, \ldots, m$, are arbitrary, GMCCs extend monomial-Cartesian codes. This should be the accurate definition, but for our purposes in this chapter we consider the above mentioned particular set P_1, namely that of $\lambda(q+1)$-th roots of unity, and sets P_j, $j = 2, \ldots, m$, not containing the element $0 \in \mathbb{F}_{q^2}$.

Next we show that the Hermitian dual of a GMCC is also a GMCC.

Lemma 4.1.3. *The dual code $(\mathcal{C}_{\boldsymbol{v},\Delta})^{\perp_h}$ is a GMCC $\mathcal{C}_{\boldsymbol{w},\Delta}$ for some twist vector $\boldsymbol{w}$.*

Proof. Consider any two codewords $\boldsymbol{c} = (c_0, \ldots, c_{n-1}) \in \mathcal{C}_{\mathbf{1},\Delta}$ and $\boldsymbol{b} = (b_0, \ldots, b_{n-1}) \in (\mathcal{C}_{\mathbf{1},\Delta})^{\perp_h}$. Then, the following equation holds:

$$c_0 b_0^q + \cdots + c_{n-1} b_{n-1}^q = 0. \tag{4.1.1}$$

Set $\boldsymbol{v} = (v_0, \ldots, v_{n-1})$ the twist vector in $(\mathbb{F}_{q^2}^*)^n$. It holds that $\boldsymbol{v} * \boldsymbol{c} = (v_0 c_0, \ldots, v_{n-1} c_{n-1}) \in \mathcal{C}_{\boldsymbol{v},\Delta}$ whenever $\boldsymbol{c} = (c_0, \ldots, c_{n-1}) \in \mathcal{C}_{\mathbf{1},\Delta}$, because the map

$$\mathcal{C}_{\mathbf{1},\Delta} \to \mathcal{C}_{\boldsymbol{v},\Delta}, \quad \text{given by} \quad \boldsymbol{c} \mapsto \boldsymbol{v} * \boldsymbol{c} \tag{4.1.2}$$

is bijective. We use this presentation of $\mathcal{C}_{\boldsymbol{v},\Delta}$.

We are going to prove that $(\mathcal{C}_{\boldsymbol{v},\Delta})^{\perp_h} = \mathcal{C}_{\boldsymbol{w},\Delta}$ where $\boldsymbol{w} = (w_0, \ldots, w_{n-1})$ is defined by $w_i := \frac{1}{v_i^q}$ for all $i = 0, \ldots, n-1$. This will conclude the proof.

First we claim that, for any $\boldsymbol{b} \in (\mathcal{C}_{\mathbf{1},\Delta})^{\perp_h}$, we have that $\boldsymbol{w} * \boldsymbol{b} = (w_0 b_0, \ldots, w_{n-1} b_{n-1}) \in (\mathcal{C}_{\boldsymbol{v},\Delta})^{\perp_h}$. To see it, choose $\boldsymbol{v} * \boldsymbol{c} \in \mathcal{C}_{\boldsymbol{v},\Delta}$ and note that

$$v_0 c_0 w_0^q b_0^q + \cdots + v_{n-1} c_{n-1} w_{n-1}^q b_{n-1}^q = 0,$$

where we use the fact that $w_i^q = \frac{1}{v_i^{q^2}} = \frac{1}{v_i}$ for all i, and Equation (4.1.1). This shows that all the vectors $\boldsymbol{w} * \boldsymbol{b}$ are in $(\mathcal{C}_{\boldsymbol{v},\Delta})^{\perp_h}$.

Finally note that the map

$$(\mathcal{C}_{\mathbf{1},\Delta})^{\perp_h} \to (\mathcal{C}_{\boldsymbol{v},\Delta})^{\perp_h}, \quad \text{defined by} \quad \boldsymbol{b} \mapsto \boldsymbol{w} * \boldsymbol{b}$$

is bijective, showing the required equality: $(\mathcal{C}_{\boldsymbol{v},\Delta})^{\perp_h} = \mathcal{C}_{\boldsymbol{w},\Delta}$. □

The length and the dimension of a GMCC are n and $\#\Delta$, respectively. A bound for the minimum distance is provided in the forthcoming Corollary 4.1.6. It follows from the fact that monomial-Cartesian codes $\mathcal{C}_{\mathbf{1},\Delta}$ in the sense of our Definition 4.1.1 admit the bound in Corollary 1.3.10 (see also Definition 1.3.8 where the notation F of footprint was introduced and Proposition 1.3.9) and, also, from the following result.

Lemma 4.1.4. *The GMCCs $\mathcal{C}_{\mathbf{1},\Delta}$ and $\mathcal{C}_{\boldsymbol{v},\Delta}$ are isometric.*

Proof. For any codeword $\boldsymbol{c} = (c_0, \ldots, c_{n-1}) \in \mathcal{C}_{\mathbf{1},\Delta}$, its twisted analogue codeword $\boldsymbol{v} * \boldsymbol{c} = (v_0 c_0, \ldots, v_{n-1} c_{n-1}) \in \mathcal{C}_{\boldsymbol{v},\Delta}$ under the bijective mapping (4.1.2) has the same Hamming weight. This holds because $v_i \neq 0$ for all $i = 1, \ldots, n$. □

Corollary 4.1.5. *Let $\mathcal{C}_{\boldsymbol{v},\Delta}$ be a GMCC and let $\boldsymbol{c} = \mathrm{ev}_{\boldsymbol{v}}(f) \in \mathcal{C}_{\boldsymbol{v},\Delta}$ be a codeword given by $f \in \mathcal{R}$. Fix a monomial ordering on $(\mathbb{N}_0)^m$ and let $\boldsymbol{X}^{\boldsymbol{e}}$ be the leading monomial of f. Then,* $\mathrm{w}(\boldsymbol{c}) \geq \mathrm{F}(\boldsymbol{e})$.

Corollary 4.1.6. *Let $\mathcal{C}_{\boldsymbol{v},\Delta}$ be a GMCC and let d be its minimum distance. Define $d_0 := d_0(\mathcal{C}_{\boldsymbol{v},\Delta}) := \min\{\mathrm{F}(\boldsymbol{e}) \mid \boldsymbol{e} \in \Delta\}$. Then, $d \geq d_0$.*

For example, pick $m = 2$, $n_1 = 8$, $n_2 = 6$ and $\Delta = (\{0,1,2\} \times \{0,1\}) \cup \{(0,2),(1,2)\}$. Following the same conventions as those in the paragraph above Figure 1.3, Figure 4.1 shows the grid representation of E in this case. Then, for any $\boldsymbol{v} \in (\mathbb{F}_{q^2}^*)^n$, by Corollary 4.1.6, a lower bound for the minimum distance of the code $\mathcal{C}_{\boldsymbol{v},\Delta}$ is $d_0(\mathcal{C}_{\boldsymbol{v},\Delta}) = \min\{\mathrm{F}(\boldsymbol{e}) \mid \boldsymbol{e} \in \Delta\} = 28$.

Lemma 4.1.7. *Let $\mathcal{C}_{\boldsymbol{v},\Delta}$ be a GMCC. Then $(\mathcal{C}_{\boldsymbol{v},\Delta})^{\perp_h}$ and $(\mathcal{C}_{\boldsymbol{v},\Delta})^{\perp_e}$ are isometric.*

Proof. It is straightforward because $(\mathcal{C}_{\boldsymbol{v},\Delta})^{\perp_h} = ((\mathcal{C}_{\boldsymbol{v},\Delta})^{\perp_e})^q$. □

Lemma 4.1.8. *Let $\mathcal{C}_{\boldsymbol{v},\Delta}$ be a GMCC. Then $(\mathcal{C}_{\mathbf{1},\Delta})^{\perp_h}$ and $(\mathcal{C}_{\boldsymbol{v},\Delta})^{\perp_h}$ are isometric.*

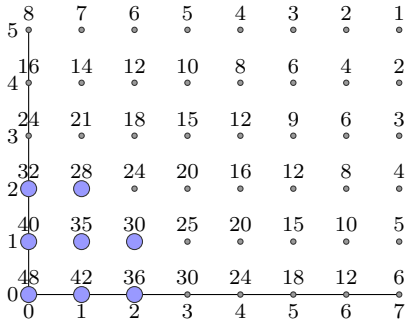


Figure 4.1: Grid representation of E, where $m = 2$, $n_1 = 8$, $n_2 = 6$, and $\Delta = (\{0,1,2\} \times \{0,1\}) \cup \{(0,2),(1,2)\}$

Proof. It follows from Lemma 4.1.4 and the fact that the family of GMCCs is closed under duality by Lemma 4.1.3. □

Corollary 4.1.9. *Let $\mathcal{C}_{\boldsymbol{v},\Delta}$ be a GMCC. Then $d((\mathcal{C}_{\boldsymbol{v},\Delta})^{\perp_h}) = d((\mathcal{C}_{\mathbf{1},\Delta})^{\perp_e})$.*

Proof. The equality is deduced from the isometry between $(\mathcal{C}_{\boldsymbol{v},\Delta})^{\perp_h}$ and $(\mathcal{C}_{\mathbf{1},\Delta})^{\perp_h}$ (by Lemma 4.1.8) and the fact that $(\mathcal{C}_{\mathbf{1},\Delta})^{\perp_h}$ is isometric to $(\mathcal{C}_{\mathbf{1},\Delta})^{\perp_e}$ (by Lemma 4.1.7). □

4.2. Constructions of stabilizer quantum codes from generalized monomial-Cartesian codes

In the present section we construct stabilizer quantum codes by applying Corollary 2.3.8 to GMCCs (Definition 4.1.1) with a specific twist vector. Recall from the beginning of this chapter that q is an odd prime power, ζ_{q^2-1} denotes a primitive q^2-1-th root of unity, λ is a natural number such that $\lambda \mid q-1$, $n_1 = \lambda(q+1)$, $2 \le n_j \le q^2-1$ for all $j = 2,\dots,m$, and $n = n_1 n_2 \cdots n_m$. We fix the following twist vector:

$$\boldsymbol{v} = (\underbrace{\zeta_{q^2-1}^{\frac{q-1}{2}},\dots,\zeta_{q^2-1}^{\frac{q-1}{2}}}_{\frac{n}{q+1}},\underbrace{1,\dots,1}_{\frac{n}{q+1}},\underbrace{\zeta_{q^2-1}^{\frac{q-1}{2}},\dots,\zeta_{q^2-1}^{\frac{q-1}{2}}}_{\frac{n}{q+1}},\dots,\underbrace{1,\dots,1}_{\frac{n}{q+1}}) \in (\mathbb{F}_{q^2}^*)^n. \tag{4.2.1}$$

The equality

$$\left(\zeta_{q^2-1}^{\frac{q-1}{2}}\right)^{q+1} = \zeta_{q^2-1}^{\frac{(q+1)(q-1)}{2}} = \zeta_{q^2-1}^{\frac{q^2-1}{2}} = -1$$

proves

$$\boldsymbol{v}^{q+1} = (\underbrace{-1,\dots,-1}_{\frac{n}{q+1}},\underbrace{1,\dots,1}_{\frac{n}{q+1}},\underbrace{-1,\dots,-1}_{\frac{n}{q+1}},\dots,\underbrace{1,\dots,1}_{\frac{n}{q+1}}).$$

The vector $\boldsymbol{v}^{q+1}$ has $q+1$ blocks of length $\frac{n}{q+1}$ and values -1's or 1's. Recall that the coordinates $v_{\boldsymbol{\epsilon}}$ of $\boldsymbol{v}$ are labelled and ordered in the same way as the points $\boldsymbol{\alpha}_{\boldsymbol{\epsilon}} \in P$. This twist vector works as follows. For each $\boldsymbol{\epsilon} \in E$,

$$v_{\boldsymbol{\epsilon}}^{q+1} = \begin{cases} -1 & \text{if } 0 \le (\epsilon_1 \bmod 2\lambda) \le \lambda - 1, \\ 1 & \text{if } \lambda \le (\epsilon_1 \bmod 2\lambda) \le 2\lambda - 1. \end{cases} \tag{4.2.2}$$

Notice that $v_{\boldsymbol{\epsilon}}$ only depends on ϵ_1. The reason why we choose this specific twist vector is going to become clear in the forthcoming Proposition 4.2.1.

4.2.1. Self-orthogonality conditions

First we present some conditions for the evaluation vectors (under the map $\mathrm{ev}_{\boldsymbol{v}}$) of monomials in $\mathcal{R}$ to be orthogonal for the Hermitian inner product, when our twist vector is used.

Proposition 4.2.1. *Keep the same notation as before. Let q be an odd prime power and consider the twist vector $\boldsymbol{v}$ defined in Equality (4.2.1). Let $\boldsymbol{e} = (e_1, \ldots, e_m)$, $\boldsymbol{e}' = (e'_1, \ldots, e'_m) \in E$ be exponents of two monomials $\boldsymbol{X}^{\boldsymbol{e}}$, $\boldsymbol{X}^{\boldsymbol{e}'} \in \mathcal{R}$. Then, the evaluation vectors under the map $\mathrm{ev}_{\boldsymbol{v}}$ of these monomials are orthogonal for the Hermitian inner product if one of the following conditions hold:*

- $e_1 \equiv e'_1 \mod q+1$, *or*
- $e_1 \not\equiv e'_1 \mod \frac{q+1}{2}$.

Proof. In order to compute some conditions under which two evaluations of monomials of the quotient ring $\mathcal{R}$ are orthogonal for the Hermitian inner product we have to see when the following sum vanishes:

$$\mathrm{ev}_{\boldsymbol{v}}(\boldsymbol{X}^{\boldsymbol{e}}) \cdot_h \mathrm{ev}_{\boldsymbol{v}}(\boldsymbol{X}^{\boldsymbol{e}'}) = \sum_{\boldsymbol{\epsilon} \in E} v_{\boldsymbol{\epsilon}}^{q+1} \zeta_{\lambda(q+1)}^{\epsilon_1(e_1+qe'_1)} \alpha_{(2,\epsilon_2)}^{(e_2+qe'_2)} \cdots \alpha_{(m,\epsilon_m)}^{(e_m+qe'_m)}.$$

Since $v_{\boldsymbol{\epsilon}}$ only depends on ϵ_1, we set $v_{\epsilon_1} := v_{(\epsilon_1,\ldots,\epsilon_m)} = v_{\boldsymbol{\epsilon}}$ and reorder the above sum in the following way:

$$\mathrm{ev}_{\boldsymbol{v}}(\boldsymbol{X}^{\boldsymbol{e}}) \cdot_h \mathrm{ev}_{\boldsymbol{v}}(\boldsymbol{X}^{\boldsymbol{e}'}) = \left(\sum_{\epsilon_1=0}^{\lambda(q+1)-1} v_{\epsilon_1}^{q+1} \zeta_{\lambda(q+1)}^{\epsilon_1(e_1+qe'_1)} \right) \left(\sum_{\epsilon_2=0}^{n_2-1} \alpha_{(2,\epsilon_2)}^{(e_2+qe'_2)} \right) \cdots \left(\sum_{\epsilon_m=0}^{n_m-1} \alpha_{(m,\epsilon_m)}^{(e_m+qe'_m)} \right). \tag{4.2.3}$$

The above equality is true because all coordinates $v_{\boldsymbol{\epsilon}}$ in $\boldsymbol{v}$ that have the same ϵ_1 coincide.

Now we study when the first factor in (4.2.3) equals 0. We ignore the remaining factors, since the first one gives enough information for the proof.

$$\sum_{\epsilon_1=0}^{\lambda(q+1)-1} v_{\epsilon_1}^{q+1} \zeta_{\lambda(q+1)}^{\epsilon_1(e_1+qe'_1)} \tag{4.2.4}$$

is a sum where ϵ_1 runs over $\{0, 1, \ldots, \lambda(q+1)-1\}$. Using the three following facts: i) each ϵ_1 can be written in the form $s\lambda + r$ where $0 \le s \le q$ and $0 \le r < \lambda$ to break the sum (4.2.4) into λ blocks of size $q+1$, ii) $\zeta_{q+1} := \zeta_{\lambda(q+1)}^{\lambda}$ is a primitive $(q+1)$-th root of unity, and iii) the structure of the twist vector $\boldsymbol{v}$, we can write the sum (4.2.4) as

$$\begin{aligned}
\sum_{\epsilon_1=0}^{\lambda(q+1)-1} v_{\epsilon_1}^{q+1} \zeta_{\lambda(q+1)}^{\epsilon_1(e_1+qe'_1)} &= \sum_{\substack{0 \le s \le q \\ 0 \le r < \lambda}} v_{s\lambda+r}^{q+1} \zeta_{\lambda(q+1)}^{(s\lambda+r)(e_1+qe'_1)} = \sum_{s=0}^{q} v_{s\lambda}^{q+1} \zeta_{q+1}^{s(e_1+qe'_1)} \\
&\quad + \zeta_{\lambda(q+1)}^{e_1+qe'_1} \sum_{s=0}^{q} v_{s\lambda+1}^{q+1} \zeta_{q+1}^{s(e_1+qe'_1)} + \cdots + \zeta_{\lambda(q+1)}^{(\lambda-1)(e_1+qe'_1)} \sum_{s=0}^{q} v_{s\lambda+\lambda-1}^{q+1} \zeta_{q+1}^{s(e_1+qe'_1)} \\
&= \left(1 + \zeta_{\lambda(q+1)}^{(e_1+qe'_1)} + \cdots + \zeta_{\lambda(q+1)}^{(\lambda-1)(e_1+qe'_1)} \right) \left(\sum_{s=0}^{q} v_{s\lambda}^{q+1} \zeta_{q+1}^{s(e_1+qe'_1)} \right).
\end{aligned}$$

We have considered Equality (4.2.2) and the fact that, for the above λ, $v_{s\lambda}^{q+1} = v_{s\lambda+1}^{q+1} = \cdots = v_{s\lambda+\lambda-1}^{q+1}$ for all $0 \le s \le q$. Now, Equality (4.2.2) and the fact that $\zeta_{\frac{q+1}{2}} := \zeta_{q+1}^2$ is a primitive $\frac{q+1}{2}$-th root of unity, allow us to rewrite the last sum as follows:

$$\begin{aligned}
\sum_{s=0}^{q} v_{s\lambda}^{q+1}\zeta_{q+1}^{s(e_1+qe_1')} &= \sum_{s=0}^{\frac{q-1}{2}} v_{2s\lambda}^{q+1}\zeta_{q+1}^{2s(e_1+qe_1')} + \sum_{s=0}^{\frac{q-1}{2}} v_{2s\lambda+1}^{q+1}\zeta_{q+1}^{(2s+1)(e_1+qe_1')} \\
&= \sum_{s=0}^{\frac{q-1}{2}} v_{2s\lambda}^{q+1}\zeta_{q+1}^{2s(e_1+qe_1')} - \zeta_{q+1}^{e_1+qe_1'}\sum_{s=0}^{\frac{q-1}{2}} v_{2s\lambda}^{q+1}\zeta_{q+1}^{2s(e_1+qe_1')} \\
&= \zeta_{q+1}^{e_1+qe_1'}\left(\sum_{s=0}^{\frac{q-1}{2}} \zeta_{\frac{q+1}{2}}^{s(e_1+qe_1')}\right) - \left(\sum_{s=0}^{\frac{q-1}{2}} \zeta_{\frac{q+1}{2}}^{s(e_1+qe_1')}\right) \\
&= (\zeta_{q+1}^{e_1+qe_1'} - 1)\left(\sum_{s=0}^{\frac{q-1}{2}} \zeta_{\frac{q+1}{2}}^{s(e_1+qe_1')}\right).
\end{aligned}$$

Thus, we have shown that we can express the sum (4.2.4) as

$$\sum_{\epsilon_1=0}^{\lambda(q+1)-1} v_{\epsilon_1}^{q+1}\zeta_{\lambda(q+1)}^{\epsilon_1(e_1+qe_1')} = P\left(\zeta_{\lambda(q+1)}^{e_1+qe_1'}\right)\left(\zeta_{q+1}^{e_1+qe_1'} - 1\right)\left(\sum_{s=0}^{\frac{q-1}{2}} \zeta_{\frac{q+1}{2}}^{s(e_1+qe_1')}\right),$$

where $P(X) = 1 + X + X^2 + \cdots + X^{\lambda-1}$. The above product equals 0 if and only if one of the following conditions holds:

- $\zeta_{q+1}^{e_1+qe_1'} - 1 = 0 \iff e_1 + qe_1' \equiv 0 \mod q+1$. That is, $e_1 \equiv e_1' \mod q+1$; either
- $\left(\sum_{s=0}^{\frac{q-1}{2}} \zeta_{\frac{q+1}{2}}^{s(e_1+qe_1')}\right) = 0 \iff e_1 + qe_1' \not\equiv 0 \mod \frac{q+1}{2}$. Since $q \equiv -1 \mod \frac{q+1}{2}$, this is equivalent to $e_1 \not\equiv e_1' \mod \frac{q+1}{2}$; or
- $P\left(\zeta_{\lambda(q+1)}^{(e_1+qe_1')}\right) = 0$. This is true if and only if $\zeta_{\lambda(q+1)}^{(e_1+qe_1')}$ is a λ-th root of unity other than 1. That is equivalent to $e_1 + qe_1' \equiv 0 \mod q+1$ and $e_1 + qe_1' \not\equiv 0 \mod \lambda(q+1)$, which is a particular case of the first condition.

Therefore, if either of the first two conditions hold, the sum (4.2.4) equals 0. It implies that $\mathrm{ev}_{\boldsymbol{v}}(\boldsymbol{X}^{\boldsymbol{e}})$ and $\mathrm{ev}_{\boldsymbol{v}}(\boldsymbol{X}^{\boldsymbol{e}'})$ are orthogonal for the Hermitian inner product. □

Remark 4.2.2. Suppose that the twist vector is $\mathbf{1} := (1, \ldots, 1) \in (\mathbb{F}_{q^2}^*)^n$, $\lambda = 1$ and P_j is the set of $q+1$-th roots of unity for every $j = 1, \ldots, m$. Then for any $\Delta \subseteq E$, the GMCC $\mathcal{C}_{\mathbf{1},\Delta}$ is a $\{1, \ldots, m\}$-affine variety code and it is not self-orthogonal (for the Hermitian inner product). This is because when we compute the Hermitian inner product of the evaluation of any monomial $\boldsymbol{X}^{\boldsymbol{e}} = \boldsymbol{X}^{(e_1,\ldots,e_m)}$ with itself, one obtains the equalities

$$\begin{aligned}
\mathrm{ev}_{\mathbf{1}}(\boldsymbol{X}^{\boldsymbol{e}}) \cdot_h \mathrm{ev}_{\mathbf{1}}(\boldsymbol{X}^{\boldsymbol{e}}) &= \sum_{\boldsymbol{\epsilon}\in E} \zeta_{q+1}^{\epsilon_1 e_1(1+q)}\zeta_{q+1}^{\epsilon_2 e_2(1+q)}\cdots\zeta_{q+1}^{\epsilon_m e_m(1+q)} \\
&= \left(\sum_{\epsilon_1=0}^{q} \zeta_{q+1}^{\epsilon_1 e_1(1+q)}\right)\left(\sum_{\epsilon_2=0}^{q} \zeta_{q+1}^{\epsilon_2 e_2(1+q)}\right)\cdots\left(\sum_{\epsilon_m=0}^{q} \zeta_{q+1}^{\epsilon_m e_m(1+q)}\right)
\end{aligned}$$

and every factor above is

$$\sum_{s=0}^{q} \zeta_{q+1}^{se_1(1+q)} = q+1 \neq 0.$$

The code $\mathcal{C}_{\mathbf{1},\Delta}$ is not self-orthogonal but the twist vector $\boldsymbol{v}$ given in Equality (4.2.1) provides a self-orthogonal GMCC $\mathcal{C}_{\boldsymbol{v},\Delta}$, and this code is isometric to $\mathcal{C}_{\mathbf{1},\Delta}$. We have chosen the twist vector carefully because many other GMCCs are not self-orthogonal.

4.2.2. Our general construction

Before stating a theorem with the general construction of this chapter, we introduce a subset of E which will be useful.

Definition 4.2.3. Let $E_0 := \left\{ \boldsymbol{e} = (e_1, \ldots, e_m) \in E \mid 0 \leq e_1 \leq \frac{q-1}{2} \right\} \subseteq E$.

The next theorem shows that the set E_0 introduced in Definition 4.2.3 is used as a reference to construct Hermitian self-orthogonal GMCCs.

Theorem 4.2.4. *Let q be an odd prime power and let $m \geq 1$, $\lambda \mid q-1$, $n_1 := \lambda(q+1)$ and $2 \leq n_j \leq q^2-1$, $j = 2, \ldots, m$, be positive integers. Let $n := n_1 \cdots n_m$. Consider the twist vector $\boldsymbol{v}$ defined in Equality (4.2.1) and the set $E_0 \subseteq E$ introduced in Definition 4.2.3. Let Δ be a subset of E_0. Then,*

$$\mathcal{C}_{\boldsymbol{v},\Delta} \subseteq (\mathcal{C}_{\boldsymbol{v},\Delta})^{\perp_h}.$$

Therefore, there exists a stabilizer quantum code with parameters

$$[[n, n-2\#\Delta, \geq d]]_q$$

where $d = \mathrm{d}((\mathcal{C}_{\mathbf{1},\Delta})^{\perp_e})$.

Proof. Since for all $(e_1, \ldots, e_m) \in \Delta$ we have $e_1 \leq \frac{q-1}{2}$, the self-orthogonality follows from Proposition 4.2.1. The existence and parameters of the stabilizer quantum code follow from Corollary 2.3.8. Notice that $d = \mathrm{d}((\mathcal{C}_{\boldsymbol{v},\Delta})^{\perp_h})$, but from Corollary 4.1.9 we can conclude that $d = \mathrm{d}((\mathcal{C}_{\mathbf{1},\Delta})^{\perp_e})$. □

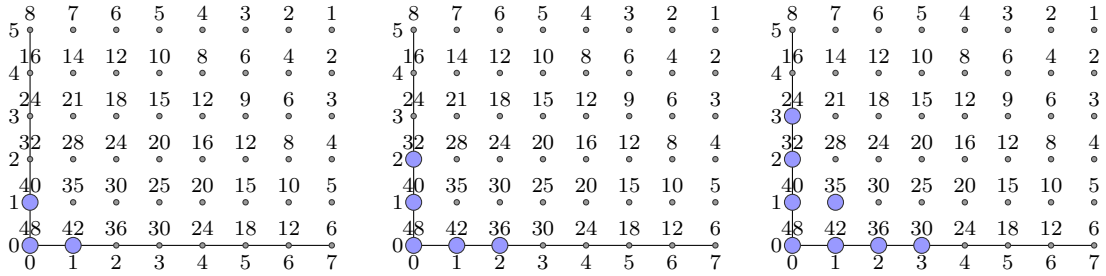
Notice that in the above theorem we do not give an explicit bound for the minimum distance, but it can be computed using Corollary 4.1.6 in every particular case.

4.2.3. Our specific construction

Following [53], we provide a strategy to choose a set $\Delta \subseteq E_0$ so that, on the one hand, we can control the minimum distance $\mathrm{d}((\mathcal{C}_{\mathbf{1},\Delta})^{\perp_e})$ and, on the other hand, the dimension of the resulting stabilizer quantum code is maximized. To that purpose, we need the following definition.

Definition 4.2.5. Let $2 \leq t \leq \frac{q+3}{2}$ be a positive integer. Define

$$\Delta_t := \left\{ \boldsymbol{e} = (e_1, \ldots, e_m) \in E \;\middle|\; \prod_{j=1}^{m} (e_j + 1) < t \right\} \subseteq E.$$



(1) Δ_3 (2) Δ_4 (3) Δ_5

Figure 4.2: Sets Δ_3, Δ_4 and Δ_5, where $m = 2$, $n_1 = 8$ and $n_2 = 6$. We use the same conventions as in the paragraph above Figure 1.3

Some instances of the above set are represented in Figure 4.2.

Lemma 4.2.6. *Let $\Delta_t \subseteq E$ be the set introduced in Definition 4.2.5. Then,*

$$\mathrm{d}\left((\mathcal{C}_{\mathbf{1},\Delta_t})^{\perp_e}\right) \geq t.$$

Proof. It follows from [42, Section 3]. □

Theorem 4.2.7. *Let q be an odd prime power and let $m \geq 1$, $\lambda \mid q-1$, $n_1 := \lambda(q+1)$ and $2 \leq n_j \leq q^2-1$, $j = 2, \ldots, m$, be positive integers. Let $n := n_1 \cdots n_m$. Consider the twist vector $\boldsymbol{v}$ defined in Equality (4.2.1), a positive integer t such that*

$$2 \leq t \leq \frac{q+3}{2}$$

and the set $\Delta_t \subseteq E$ introduced in Definition 4.2.5. Then, the following inclusion holds

$$\mathcal{C}_{\boldsymbol{v},\Delta_t} \subseteq (\mathcal{C}_{\boldsymbol{v},\Delta_t})^{\perp_h}.$$

Therefore, there exists a stabilizer quantum code with parameters

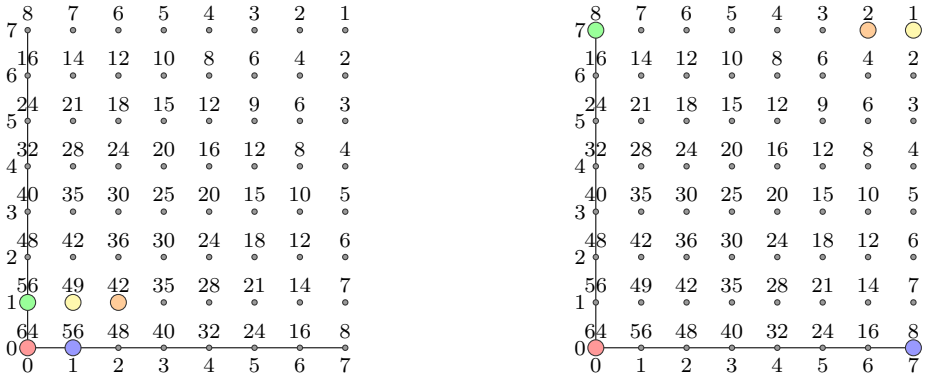
$$[[n, n - 2\#\Delta_t, \geq t]]_q.$$

Proof. Let $\boldsymbol{e} \in \Delta_t$. From $\prod_{j=1}^{m}(e_j+1) < t$ we have that $e_1 < t-1$. Since $t \leq \frac{q+3}{2}$, then $e_1 < t-1 \leq \frac{q+1}{2}$ and therefore $\Delta_t \subseteq E_0$. So, from Theorem 4.2.4 we have that $\mathcal{C}_{\boldsymbol{v},\Delta_t} \subseteq (\mathcal{C}_{\boldsymbol{v},\Delta_t})^{\perp_h}$.

The existence and parameters of the stabilizer quantum code follows from Corollary 2.3.8. Notice that from Corollary 4.1.9 and Lemma 4.2.6, we have $\mathrm{d}((\mathcal{C}_{\boldsymbol{v},\Delta_t})^{\perp_h}) = \mathrm{d}((\mathcal{C}_{\mathbf{1},\Delta_t})^{\perp_e}) \geq t$. □

Example 4.2.8. Let $m = 2$, $q = 7$ and $P_2 = P_1$, so $n_1 = n_2 = 8$. In this case, the code $\mathcal{C}_{\mathbf{1},\Delta_t}$ is a $\{1,2\}$-affine variety code and under this setting, we provide an illustrative strategy to obtain the same statement of Theorem 4.2.7. Notice that we are going to give a different argument than the one we gave in Theorem 4.2.7. From [41, Proposition

2.2], the evaluation of a monomial $X_1^{i_1}X_2^{i_2}$, $\mathrm{ev}_{\mathbf{1}}(X_1^{i_1}X_2^{i_2})$, admits a unique Euclidean non-orthogonal evaluation of a monomial. It is $\mathrm{ev}_{\mathbf{1}}(X_1^{r_1}X_2^{r_2})$, where $r_j := n_j - i_j \mod n_j$, $j = 1, 2$. Figure 4.3 shows an example of a set S of pairs of exponents of monomials whose evaluations under the map $\mathrm{ev}_{\mathbf{1}}$ are not Euclidean orthogonal. Those exponents are paired under the same colour.



(1) $X_1^{i_1}X_2^{i_2}$ (2) $X_1^{r_1}X_2^{r_2}$

Figure 4.3: Pairs $((i_1, i_2), (r_1, r_2))$ giving the set $S := \{((0,0),(0,0)), ((1,0),(7,0)), ((0,1),(0,7)), ((1,1),(7,7)), ((2,1),(6,7))\}$ in Example 4.2.8

Thus, if we consider a set $\Delta \subseteq E$, then a basis of the code $(\mathcal{C}_{\mathbf{1},\Delta})^{\perp_e}$ is

$$\{\mathrm{ev}_{\mathbf{1}}(X_1^{e_1}X_2^{e_2}) \mid (e_1, e_2) \in \Delta^{\perp_e}\},$$

where

$$\Delta^{\perp_e} := E \backslash \{(n_1 - i_1 \mod n_1,\, n_2 - i_2 \mod n_2) \mid (i_1, i_2) \in \Delta\}.$$

In this example $\Delta_0 = \{0,1,2,3\} \times \{0,1,\ldots,7\}$. Let us pick $t = \frac{q+3}{2} = 5$. Then we know that $\Delta_5 \subseteq \Delta_0$ and thus $\mathcal{C}_{\boldsymbol{v},\Delta_5} \subseteq (\mathcal{C}_{\boldsymbol{v},\Delta_5})^{\perp_h}$. Figure 4.4 (1) shows Δ_5. The minimum distance of $(\mathcal{C}_{\boldsymbol{v},\Delta_5})^{\perp_h}$ can be obtained from that of $(\mathcal{C}_{\mathbf{1},\Delta_5})^{\perp_e}$ since by Corollary 4.1.9 both coincide. Figure 4.4 (2) shows $(\Delta_5)^{\perp_e}$. Then we deduce that the bound given in Corollary 4.1.6 for the minimum distance of $(\mathcal{C}_{\mathbf{1},\Delta_5})^{\perp_e} = \mathcal{C}_{\mathbf{1},(\Delta_5)^{\perp_e}}$ is

$$d_0\left((\mathcal{C}_{\mathbf{1},\Delta_5})^{\perp_e}\right) = d_0\left(\mathcal{C}_{\mathbf{1},(\Delta_5)^{\perp_e}}\right) = 2.$$

However, we can enlarge the bound. To that purpose, consider $\mathbf{1}' := (1,\ldots,1) \in \mathbb{N}^m$, the code

$$\mathcal{C}_{\mathbf{1},\Delta_5}(\mathbf{1}') := \{\boldsymbol{c} * \mathrm{ev}_{\mathbf{1}}(X_1 \cdots X_m) \mid \boldsymbol{c} \in \mathcal{C}_{\mathbf{1},\Delta_5}\}$$

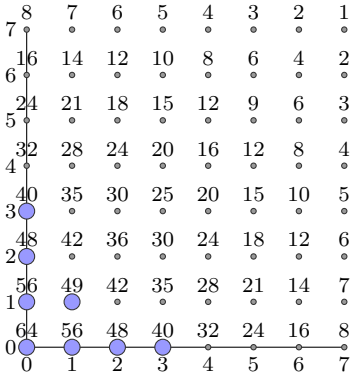
and

$$\Delta_5' := \Delta_5 + (1,1)$$

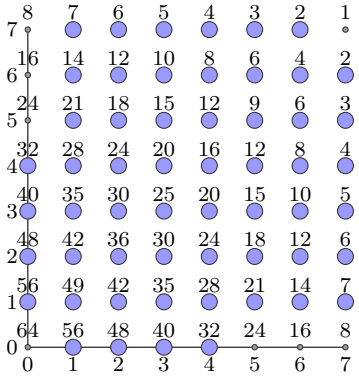
(see Definition 1.3.5). Then, $\mathcal{C}_{\mathbf{1},\Delta_5}(\mathbf{1}') = \mathcal{C}_{\mathbf{1},\Delta_5'}$. Moreover, the codes $\mathcal{C}_{\mathbf{1},\Delta_5}$ and $\mathcal{C}_{\mathbf{1},\Delta_5}(\mathbf{1}')$ are isometric (see Remark 1.3.6). Indeed, since no point in P has a vanishing coordinate, the codewords in $\mathcal{C}_{\mathbf{1},\Delta_5}(\mathbf{1}')$ are obtained by multiplying coordinate-wise the codewords

in $\mathcal{C}_{\mathbf{1},\Delta_5}$ by a non-zero element. In addition, by McWilliams identities $(\mathcal{C}_{\mathbf{1},\Delta_5})^{\perp_e}$ and $(\mathcal{C}_{\mathbf{1},\Delta_5}(\mathbf{1}'))^{\perp_e}$ are also isometric. Figure 4.4 (3) and (4) show Δ_5' and $(\Delta_5')^{\perp_e}$, respectively. The set $(\Delta_5')^{\perp_e}$ is decreasing (see Definition 1.3.12), and therefore

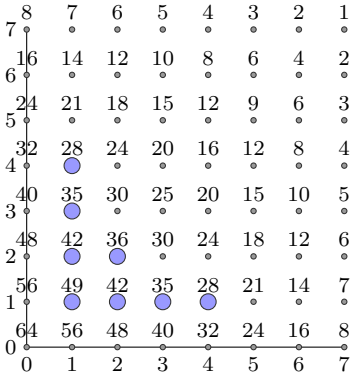
$$\mathrm{d}\left((\mathcal{C}_{\boldsymbol{v},\Delta_5})^{\perp_h}\right) = \mathrm{d}\left((\mathcal{C}_{\mathbf{1},\Delta_5})^{\perp_e}\right) = \mathrm{d}\left(\left(\mathcal{C}_{\mathbf{1},\Delta_5}(\mathbf{1}')\right)^{\perp_e}\right) = d_0\left(\left(\mathcal{C}_{\mathbf{1},\Delta_5}(\mathbf{1}')\right)^{\perp_e}\right) = 5.$$



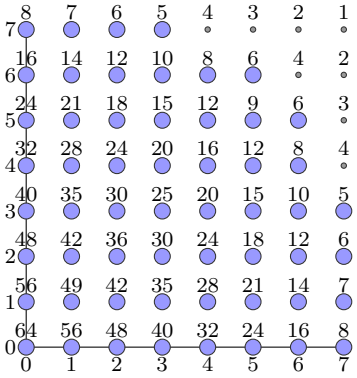
(1) Δ_5



(2) $(\Delta_5)^{\perp_e}$



(3) Δ_5'



(4) $(\Delta_5')^{\perp_e}$

Figure 4.4: Sets Δ_5, $(\Delta_5)^{\perp_e}$, Δ_5' and $(\Delta_5')^{\perp_e}$ in Example 4.2.8

4.2.4. The dimension

We state a recursive formula for the dimension of the stabilizer quantum code which was shown in [53].

Let $a, b \in \mathbb{N}$. Consider the case when $n_j = b$ for all $j = 1, \ldots, m$. We define

$$V_b(m,a) := \#\left\{(l_1,\ldots,l_m) \;\middle|\; l_j \in \mathbb{N},\ 1 \le l_j \le b,\ j = 1,\ldots m,\ \prod_{j=1}^{m} l_j \le a\right\}.$$

By [53]

$$V_b(m,a) = \sum_{s=1}^{b} V\left(m-1, \left\lfloor \frac{a}{s} \right\rfloor\right),$$

where $V_b(1,a) = \min\{a,b\}$.

Note that $\#\Delta_t = V_{\lambda(q+1)}(m,t-1)$, where all of $n_1,\dots,n_m$ are equal to $\lambda(q+1)$. Therefore we can use the recursive formula above described to compute $\#\Delta_t$, and hence the dimension of the stabilizer quantum code in Theorem 4.2.7.

For example, when $m = 2$

$$\#\Delta_t = V_{\lambda(q+1)}(2,t-1) = t-1+\left\lfloor\frac{t-1}{2}\right\rfloor+\left\lfloor\frac{t-1}{3}\right\rfloor+\cdots+\left\lfloor\frac{t-1}{t-2}\right\rfloor+\left\lfloor\frac{t-1}{t-1}\right\rfloor, \tag{4.2.5}$$

and when $m = 3$

$$\#\Delta_t = V_{\lambda(q+1)}(3,t-1) = \sum_{\beta=1}^{t-1}\sum_{\gamma=1}^{\left\lfloor\frac{t-1}{\beta}\right\rfloor}\left\lfloor\frac{t-1}{\beta\gamma}\right\rfloor.$$

4.3. MDS and Hermitian almost MDS quantum codes

In this section we give quantum codes whose parameters satisfy or are close to satisfy equality in the quantum Singleton bound (see Theorem 2.3.9). Recall that quantum codes attaining equality are said to be (quantum) MDS. First we provide quantum codes of this type.

Theorem 4.3.1. *The stabilizer quantum codes obtained from Theorem 4.2.7 with $m = 1$ are quantum MDS codes.*

Proof. For any given bound for the minimum distance $t \in \{2,\dots,\frac{q+3}{2}\}$, we have $\Delta_t = \{0,1,2,\dots,t-2\}$. The parameters of the stabilizer quantum code constructed from Theorem 4.2.7 are

$$[[n,k,d]]_q = [[\lambda(q+1), \lambda(q+1)-2(t-1), \geq t]]_q.$$

It is easily verified that the above parameters provide a quantum MDS code. Indeed, $k+2d \geq \lambda(q+1)-2(t-1)+2t = \lambda(q+1)+2 = n+2$ and the quantum Singleton bound gives an equality. □

Some sample parameters are given in Tables 4.3 to 4.7. For example, we obtain quantum MDS codes with parameters $[[12,8,3]]_5$ in Table 4.4, $[[8,4,3]]_7$ and $[[16,8,5]]_7$ in Table 4.5 and $[[20,12,5]]_9$ in Table 4.6. We do not claim that these examples are new.

The article [126] constructs MDS codes with lengths $r(q^2-1)/h$, where h is an even divisor of $q-1$ and $r \leq h/2$ (their Theorems 3, 4 and 5). This article does not provide an explicit twist vector (only its existence is proved). Our construction uses an explicit twist vector and (in the $m = 1$ case) gives codes with the same parameters as in [126].

Next we provide the other type of quantum codes we announced, whose parameters are close to satisfy equality in the quantum Singleton bound. The quantum Singleton defect of a parameter set $[[n,k,d]]$ is defined to be $n-(k+2d-2)$. MDS codes have quantum Singleton defect 0, by definition. Codes with quantum Singleton defect 1 are called quantum almost MDS (QAMDS) codes. However, from the statement of Corollary 2.3.8

one can see that the quantum Singleton defect of any code constructed using that result must be even, and thus a quantum Singleton defect of 1 cannot be achieved. The smallest nonzero Singleton defect of a code constructed using Corollary 2.3.8 is therefore 2. This motivates the following definition.

Definition 4.3.2. A quantum code constructed from Corollary 2.3.8 with parameters $[[n,k,d]]_q$ such that $n = k+2d$ is called a *quantum Hermitian almost MDS* (*QHAMDS*) code.

In Theorem 4.3.1 we showed that we can construct stabilizer quantum MDS codes. Recall that the quantum MDS conjecture (Conjecture 2.3.10) states that $n \leq q^2+1$ for a stabilizer quantum MDS code with parameters $[[n,k,d]]_q$ and q odd. Now we are going to show that we can also construct stabilizer quantum codes with $n > q^2+1$ that are at least QHAMDS. That is, they are either QHAMDS or MDS. If the quantum MDS conjecture is true, they cannot be MDS, and therefore they would have the best possible parameters.

Theorem 4.3.3. *The stabilizer quantum codes obtained from Theorem 4.2.7 with $m = 2$, $n > q^2+1$ and $t = 3$ are at least QHAMDS.*

Proof. Let $m = 2$, $t = 3$ and λ and n_2 be as defined in Theorem 4.2.7 such that $n > q^2+1$. We have $\Delta_3 = \{(0,0),(1,0),(0,1)\}$ (see Figure 4.2). The parameters of the stabilizer quantum code constructed from Theorem 4.2.7 are

$$[[n,k,d]]_q = [[\lambda(q+1)n_2, \lambda(q+1)n_2 - 6, \geq 3]]_q.$$

It is easily verified that the above parameters provide a code which is at least QHAMDS. This is because $k+2d \geq \lambda(q+1)n_2 - 6 + 2\cdot 3 = \lambda(q+1)n_2 = n$. □

Some examples will be given in Tables 4.3 to 4.7. In [30] the authors study ternary quantum codes of minimum distance three. In that paper (their Theorem 4.4) quantum codes with parameters $[[n, n-7, 3]]_3$ are shown for certain lengths n. For those lengths which are a multiple of 4 and less than 64 we can improve the dimension by 1, using the codes in Theorem 4.3.3. See also Table 4.3.

4.4. Beating Gilbert-Varshamov bound

In this section we set an infinite family of codes obtained from our construction for $m = 2$ that beat the quantum Gilbert-Varshamov bound, stated in Theorem 2.3.11. We remark that some codes with $m > 2$ also beat the Gilbert-Varshamov bound. Several examples for $m = 3$ are presented in Tables 4.3, 4.4 and 4.6. Explicit constructions better than the Gilbert-Varshamov bound have also been considered before, see for instance [84].

Recall that a parameter set $[[n,k,d]]_q$ beats the quantum Gilbert-Varhsamov (QGV) bound if the inequality in Theorem 2.3.11 for $Q = q$ is not satisfied.

In the $m = 2$ case we have the following statement, using the codes constructed in this chapter. In this statement we are using Formula (4.2.5).

Theorem 4.4.1. *Given an odd prime power q, and given d in the range $5 \le d \le \frac{q+3}{2}$, let n be in the interval*

$$\left((d-1)^{d-1}\frac{q^2}{(q^2-1)^{d-1}}q^{2(d-1)(0.7+\ln(d-1))}\right)^{\frac{1}{d-1}} \le n \le (q^2-1)^2$$

and have the form $\lambda(q+1)n_2$ where $\lambda \mid (q-1)$ and $2 \le n_2 \le q^2-1$. Then there exists a stabilizer quantum code with parameters

$$\left[\left[n, n-2\sum_{j=1}^{d-1}\left\lfloor\frac{d-1}{j}\right\rfloor, \ge d\right]\right]_q$$

and this code beats the quantum Gilbert-Varshamov bound.

Proof. We use the codes whose existence is proved in Theorem 4.2.7 in the case $m = 2$. The upper bounds $d \le \frac{q+3}{2}$ and $n \le (q^2-1)^2$ follow from the construction in Theorem 4.2.7.

Let

$$A = \sum_{i=1}^{d-1}(q^2-1)^{i-1}\binom{n}{i} \quad \text{and} \quad D = \frac{q^{n-k+2}-1}{q^2-1},$$

where $k = n-2\sum_{j=1}^{d-1}\left\lfloor\frac{d-1}{j}\right\rfloor$ (this dimension formula comes from Formula (4.2.5) which uses our construction with $m = 2$). We wish to prove that $A > D$ under the stated hypotheses. To prove this, we are going to let

$$B = \frac{1}{(d-1)^{d-1}}n^{d-1}(q^2-1)^{d-2} \quad \text{and} \quad C = \left(\frac{q^2}{q^2-1}\right)q^{2(d-1)(0.7+\ln(d-1))},$$

and we will prove three things: that $A > B$, that $B \ge C$, and that $C > D$. This will complete the proof that $A > D$.

To show that $A > B$, we use the estimate for binomial coefficients $\binom{n}{k} > (\frac{n}{k})^k$. Then

$$\begin{aligned} A &= \sum_{i=1}^{d-1}(q^2-1)^{i-1}\binom{n}{i} > \binom{n}{d-1}(q^2-1)^{d-2} \\ &> \left(\frac{n}{d-1}\right)^{d-1}(q^2-1)^{d-2} = \frac{1}{(d-1)^{d-1}}n^{d-1}(q^2-1)^{d-2} = B. \end{aligned}$$

To prove that $B \ge C$, rearranging the hypothesis

$$\left((d-1)^{d-1}\frac{q^2}{(q^2-1)^{d-1}}q^{2(d-1)(0.7+\ln(d-1))}\right)^{\frac{1}{d-1}} \le n$$

yields precisely that $B \ge C$.

To prove that $C > D$, we use the fact that if $r \ge 4$ then $H_r < 0.7 + \ln r$, where H_r is the r-th harmonic number defined by $H_r = \sum_{j=1}^{r}\frac{1}{j}$. Then

$$\sum_{j=1}^{d-1}\left\lfloor\frac{d-1}{j}\right\rfloor < \sum_{j=1}^{d-1}\frac{d-1}{j} = (d-1)H_{d-1} < (d-1)(0.7+\ln(d-1)),$$

since $d-1 \ge 4$. Lastly, it follows that

$$\begin{aligned} D &= \frac{q^{n-k+2}-1}{q^2-1} < \frac{q^{n-k+2}}{q^2-1} = \left(\frac{q^2}{q^2-1}\right)q^{n-k} \\ &= \left(\frac{q^2}{q^2-1}\right)q^{2\sum_{j=1}^{d-1}\left\lfloor\frac{d-1}{j}\right\rfloor} < \left(\frac{q^2}{q^2-1}\right)q^{2(d-1)(0.7+\ln(d-1))} = C. \end{aligned}$$

□

Theorem 4.4.1 assumes that $d \geq 5$ because of the constant 0.7, which is a choice. The cases $d = 3$ and $d = 4$ can be proved separately. They could be included in the proof above but the constant 0.7 would have to be larger. Similarly, we could have stated the theorem for $d \geq 6$ and the constant would be smaller, it would be 0.68. Then the $d = 5$ case would need to be handled separately. As d gets larger, the constant gets smaller and approaches the Euler-Mascheroni constant.

For each q between 7 and 17 and $d = 5, 6, 7$, Table 4.1 gives the range of values of n for which the quantum Gilbert-Varshamov bound is beaten, as stated in Theorem 4.4.1.

d \ q	7	9	11	13	17
5	742-2304	1438-6400	2450-14400	3818-28224	7800-82944
6	$d > \frac{q+3}{2}$	3848-6400	7022-14400	11600-28224	26006-82944
7	$d > \frac{q+3}{2}$	$d > \frac{q+3}{2}$	None	None	72590-82944

Table 4.1: Some instances of the range of lengths of stabilizer quantum codes (from Theorem 4.4.1 only) that beat the quantum Gilbert-Varshamov bound

A separate special analysis for each d, or using better estimates in the proof, or using a computer, will give a better range of values for n than the statement of Theorem 4.4.1. For example, when $q = 7$ and $d = 5$, computer calculations show that the Gilbert-Varshamov bound is beaten by our codes as soon as $n > 295$, whereas the proof of Theorem 4.4.1 gives $n \geq 742$. As another example, when $q = 11$ and $d = 7$, the range of values of n as given by the statement of Theorem 4.4.1 is empty (in Table 4.1 we wrote "None"). However, there are in fact values of n that beat the Gilbert-Varshamov bound. We state one example $[[7200, 7172, 7]]_{11}$ in Table 4.7.

We also remark that Theorem 4.4.1 is for $m = 2$. A similar result will hold for $m > 2$.

4.4.1. The case $d = 3$

Theorem 4.4.1 assumes that $d \geq 5$ to obtain a slightly stronger statement. We treat the case that $d = 3$ (and $m = 2$) separately, and we complete the analysis in detail now. We omit the $d = 4$ case, which is similar.

Suppose $d = 3$. By Formula (4.2.5) we have that Δ_3 has 3 elements, see also Figure 4.2. The two sides of the Gilbert-Varshamov bound become

$$\frac{q^{n-k+2} - 1}{q^2 - 1} = \frac{q^8 - 1}{q^2 - 1} = q^6 + q^4 + q^2 + 1$$

and

$$\sum_{i=1}^{d-1} (q^2 - 1)^{i-1} \binom{n}{i} = n + \binom{n}{2}(q^2 - 1).$$

To beat the QGV bound we obtain a condition which is a quadratic polynomial in n, namely we require that

$$n + \binom{n}{2}(q^2 - 1) - (q^6 + q^4 + q^2 + 1) > 0.$$

Solving the quadratic yields that the QGV bound is beaten when

$$n > \frac{q^2 - 3 + \sqrt{8q^8 + q^4 - 6q^2 + 1}}{2(q^2 - 1)}.$$

For $m = 2$ the largest possible n is $(q-1)(q+1)(q^2-1)$. Therefore, for each valid n which is a multiple of $q+1$ between $\frac{q^2-3+\sqrt{8q^8+q^4-6q^2+1}}{2(q^2-1)}$ and $(q^2-1)^2$, we obtain a code of that length that beats the QGV bound.

We show Table 4.2 where for each q, $3 \leq q \leq 11$, and $d = 3$ we state the range of values of n for which Gilbert-Varshamov bound is beaten.

q	3	5	7	9	11
Range of lengths	15-64	38-576	72-2304	117-6400	174-14400

Table 4.2: Some instances of the range of lengths of quantum stabilizer codes from Theorem 4.2.7 with $d = 3$ that beat the quantum Gilbert-Varshamov bound

In the $d = 4$ case (details omitted) the polynomial in n would be cubic instead of quadratic.

4.5. Examples

Tables 4.3 to 4.7 show some samples of small values of the parameters of the stabilizer quantum codes constructed with Theorem 4.2.7. For their minimum distance, we give the lower bound t provided by Theorem 4.2.7. We remind the reader of our notation: q is an odd prime power, n_1 can be any $\lambda(q+1)$ where λ is a divisor of $\frac{q-1}{2}$, and n_2 and n_3 can take any value between 2 and q^2-1. Note that for codes $[[n,k,d]]_q = [[n,k,\geq t]]_q$, constructed from Theorem 4.2.7, we must have $t \leq \frac{q+3}{2} = 3$ when $q = 3$, and $t \leq \frac{q+3}{2} = 4$ when $q = 5$.

Recall also codes with $n+2 = k+2d$ are called MDS codes and codes with $n = k+2d$ are called QHAMDS codes. We also say in the sixth column if that code beats the quantum Gilbert-Varshamov bound in the sense explained before Theorem 4.4.1.

In order to compare different quantum codes, one may use the propagation rules, see two paragraphs above Proposition 2.2.8.

In the tables below, we give some examples of codes that result from our construction and compare them to the best known codes in the literature. In some cases we improve on the best known. It is possible to have more than one improvement. For example, a $[[78,72,3]]_5$ code beats a $[[80,68,3]]_5$ code in two ways, because it has a smaller n and also has a larger k.

Finally, the article [126] has a construction of MDS codes with lengths of the form $r(q^2-1)/h$, where h is an even divisor of $q-1$ and $r \leq h/2$ (see Theorems 3, 4 and 5 in [126]). Some of the MDS codes appearing in our tables may also be obtained with the construction in [126].

m	n_1	n_2	n_3	$[[n,k,(d\geq)\,t]]_q$	Beats QGV	Comment
1	4			$[[4,0,3]]_3$	No	MDS
1	8			$[[8,4,3]]_3$	Yes	MDS
2	4	5		$[[20,14,3]]_3$	Yes	QHAMDS
2	4	6		$[[24,18,3]]_3$	Yes	QHAMDS
2	4	7		$[[28,22,3]]_3$	Yes	QHAMDS
2	4	8		$[[32,26,3]]_3$	Yes	QHAMDS, equals $[[32,26,3]]_3$ in [30]
2	8	5		$[[40,34,3]]_3$	Yes	QHAMDS, beats $[[40,33,3]]_3$ in [30]
2	8	6		$[[48,42,3]]_3$	Yes	QHAMDS, equals $[[48,42,3]]_3$ in [30]
2	8	7		$[[56,50,3]]_3$	Yes	QHAMDS, beats $[[56,49,3]]_3$ in [30]
2	8	8		$[[64,58,3]]_3$	Yes	QHAMDS , beats $[[64,57,3]]_3$ in [30]
3	8	3	3	$[[72,64,3]]_3$	Yes	Beats $[[72,62,3]]_3$ in [78]
3	4	8	4	$[[128,120,3]]_3$	Yes	Length not obtained with $m=1,2$

Table 4.3: A $q=3$ sample of stabilizer quantum codes

m	n_1	n_2	n_3	$[[n,k,(d\geq)\,t]]_q$	Beats QGV	Comment
1	6			$[[6,2,3]]_5$	No	MDS
1	12			$[[12,8,3]]_5$	Yes	MDS
1	12			$[[12,6,4]]_5$	Yes	MDS
2	6	5		$[[30,24,3]]_5$	No	QHAMDS, beats $[[33,13,3]]_5$ in [15]
2	6	6		$[[36,30,3]]_5$	No	QHAMDS
2	6	6		$[[36,26,4]]_5$	No	Length not obtained with $m=1$
2	6	7		$[[42,36,3]]_5$	Yes	QHAMDS
2	6	13		$[[78,72,3]]_5$	Yes	QHAMDS, beats $[[80,68,3]]_5$ in [15]
2	6	13		$[[78,68,4]]_5$	Yes	Beats $[[78,60,4]]_5$ in [88]
2	6	16		$[[96,86,4]]_5$	Yes	Same as in [88]
2	6	19		$[[114,104,4]]_5$	Yes	Length not obtained with $m=1$
2	6	22		$[[132,122,4]]_5$	Yes	Beats $[[132,118,4]]_5$ in [127]
2	12	24		$[[288,282,3]]_5$	Yes	QHAMDS
2	12	24		$[[288,278,4]]_5$	Yes	Beats $[[288,275,4]]_5$ in [48]
3	24	13	2	$[[624,612,4]]_5$	Yes	Same as in [48]
3	24	24	2	$[[1152,1144,3]]_5$	Yes	Length not obtained with $m=1,2$

Table 4.4: A $q=5$ sample of stabilizer quantum codes

m	n_1	n_2	n_3	$[[n,k,(d \geq) t]]_q$	Beats QGV	Comment
1	8			$[[8,4,3]]_7$	No	MDS
1	16			$[[16,12,3]]_7$	Yes	MDS
1	16			$[[16,10,4]]_7$	Yes	MDS
1	16			$[[16,8,5]]_7$	Yes	MDS
1	24			$[[24,20,3]]_7$	Yes	MDS, same as [126]
1	48			$[[48,44,3]]_7$	Yes	MDS
2	8	7		$[[56,50,3]]_7$	No	QHAMDS
2	8	8		$[[64,58,3]]_7$	No	QHAMDS, beats $[[65,53,3]]_7$ in [77]
2	8	8		$[[64,54,4]]_7$	No	Length not obtained with $m=1$
2	8	8		$[[64,48,5]]_7$	No	Beats $[[65,41,5]]_7$ in [77]
2	8	9		$[[72,66,3]]_7$	Yes	QHAMDS, beats $[[75,63,3]]_7$ in [88]
2	8	9		$[[72,56,5]]_7$	No	Beats $[[75,51,5]]_7$ in [88]
2	8	15		$[[120,114,3]]_7$	Yes	QHAMDS, beats $[[126,114,3]]_7$ in [15]
2	8	21		$[[168,162,3]]_7$	Yes	QHAMDS, beats $[[168,158,3]]_7$ in [15]
2	8	21		$[[168,158,4]]_7$	Yes	Beats $[[168,152,4]]_7$ in [15]
2	8	25		$[[200,190,4]]_7$	Yes	Same as in [88]
2	8	48		$[[384,378,3]]_7$	Yes	QHAMDS, same as in [23]
2	8	48		$[[384,374,4]]_7$	Yes	Same as in [23]
2	8	48		$[[384,368,5]]_7$	Yes	Same as in [23]
2	16	27		$[[432,422,4]]_7$	Yes	Beats $[[432,419,4]]_7$ in [48]
3	16	48	2	$[[768,760,3]]_7$	Yes	Length not obtained with $m=1,2$

Table 4.5: A $q=7$ sample of stabilizer quantum codes

m	n_1	n_2	n_3	$[[n,k,(d \geq) t]]_q$	Beats QGV	Comment
1	10			$[[10,6,3]]_9$	No	MDS
1	20			$[[20,16,3]]_9$	Yes	MDS
1	20			$[[20,14,4]]_9$	Yes	MDS
1	20			$[[20,12,5]]_9$	Yes	MDS
1	40			$[[40,36,3]]_9$	Yes	MDS
2	10	10		$[[100,80,6]]_9$	Yes	Length not obtained with $m=1$
2	10	24		$[[240,230,4]]_9$	Yes	Beats $[[246,228,4]]_9$ in [88]
2	10	55		$[[550,534,5]]_9$	Yes	Length not obtained with $m=1$
3	80	80	2	$[[12800,12792,3]]_9$	Yes	Length not obtained with $m=1,2$

Table 4.6: A $q=9$ sample of stabilizer quantum codes

m	n_1	n_2	$[[n, k, (d \geq) t]]_q$	Beats QGV	Comment
1	12		$[[12, 8, 3]]_{11}$	No	MDS
1	12		$[[12, 6, 4]]_{11}$	Yes	MDS
1	12		$[[12, 4, 5]]_{11}$	Yes	MDS
1	60		$[[60, 56, 3]]_{11}$	Yes	MDS
1	60		$[[60, 54, 4]]_{11}$	Yes	MDS
1	60		$[[60, 52, 5]]_{11}$	Yes	MDS
2	12	15	$[[180, 174, 3]]_{11}$	Yes	QHAMDS, beats $[[183, 171, 3]]_{11}$ in [88]
2	12	15	$[[180, 164, 5]]_{11}$	No	Beats $[[183, 159, 5]]_{11}$ in [88]
2	60	120	$[[7200, 7172, 7]]_{11}$	Yes	Length not obtained with $m = 1$

Table 4.7: A $q = 11$ sample of stabilizer quantum codes

Chapter 5

Stabilizer quantum codes from evaluation codes at the roots of trace-depending polynomials

The purpose of the present chapter is the same as the preceding one: to construct classical linear codes that satisfy the hypotheses of Corollary 2.3.8, that is, to be Hermitian self-orthogonal, and thereby obtain stabilizer quantum codes. We also aim for these quantum codes to have good parameters. However, instead of considering MCCs over relatively small fields, we use our other strategy, that is to use evaluation codes over large fields $\mathbb{F}_{q^{2\mu}}$, q being a prime power and μ a positive integer, and then reduce the field by considering their subfield-subcodes.

Recall from Definition 1.3.1 that given a set $P = \{\alpha_1, \ldots, \alpha_n\}$ of n distinct points of some set $\mathcal{X}$ and a vector space of functions on the finite field $\mathbb{F}_{q^{2\mu}}$, $V = \{f : \mathcal{X} \to \mathbb{F}_{q^{2\mu}}\}$, an evaluation code over $\mathbb{F}_{q^{2\mu}}$ is a linear code of the form $\mathcal{C}_V^P = \mathrm{ev}_P(V)$ for some linear map

$$\mathrm{ev}_P : V \to \mathbb{F}_{q^{2\mu}}^n, \quad \mathrm{ev}_P(f) = (f(\alpha_1), \ldots, f(\alpha_n)).$$

The research in this chapter is motivated from the fact that quantum error-correcting codes with good parameters can be constructed by evaluating univariate polynomials at the roots of the trace polynomial $\mathrm{tr}_{2\mu}(X) = X + X^q + \cdots + X^{q^{2\mu-1}}$ [50]. Then, we propose to evaluate polynomials at the roots of trace-depending polynomials $\gamma + \mathrm{tr}_{2\mu}(h(X))$, where $\gamma \in \mathbb{F}_{q^{2\mu}}$ and $h(X) \in \mathbb{F}_{q^{2\mu}}[X]$, with the aim of obtaining quantum codes with new lengths and excellent parameters.

We refer the reader to pages 12 to 14 of the introduction of this PhD thesis for more details of the work carried out in this chapter. We start from the end by stating that binary code records according to [62] using the above procedure are provided in Section 5.4. However, for completely general cases we had to use the computational system Magma to ensure self-orthogonality. To avoid the use of Magma in Section 5.1 we perform a theoretical analysis to construct Hermitian self-orthogonal linear codes by restricting ourselves to a specific family of trace-depending polynomials, see Definition 5.1.1. Theorem 5.1.9

determines when the sum of some powers of the roots of these polynomials vanishes, which is crucial for determining the self-orthogonality of the constituent linear codes. This last property is studied in Theorem 5.1.14, giving rise to q^μ-ary stabilizer quantum codes in Corollary 5.1.15. Later in Section 5.2, we provide stabilizer codes over smaller fields using subfield-subcodes. Finally in Section 5.3 we provide new binary records according to [62] and non-binary codes improving the ones available in the literature, all of them with parameters exceeding the quantum Gilbert-Varshamov bound.

The entire contents in this chapter were carried out with D. Ruano and published in the journal *Finite Fields and Their Applications*, see [46]. The notation has been adapted to ease the reading of this thesis.

5.1. Evaluation codes and b-th trace-depending polynomials

In this section, we introduce a particular family of trace-depending polynomials and consider linear codes that evaluate at the roots of the polynomials in this family. We study their parameters and self-orthogonality conditions. Later, we will see that good stabilizer quantum codes can be derived from them and their subfield-subcodes.

5.1.1. The b-th trace-depending polynomials

Let q be a prime power. Since in the future we will be interested in subfield-subcodes and Hermitian duality, our initial results are stated over the field $\mathbb{F}_{q^{2\mu}}$ with μ a positive integer.

For defining the trace-depending polynomials we are interested in, we consider the trace polynomials $\mathrm{tr}_{2\mu}(X)$ and $\mathrm{tr}_\mu(X)$ defined as follows:

$$\mathrm{tr}_j(X) := X + X^q + X^{q^2} + \cdots + X^{q^{j-1}},$$

where j equals either 2μ or μ. Notice that they give rise to a trace map as that given in Section 1.5, where q was equal to p^h and $q^j = p^l$. Next, set $b = b(t) = 1 + q^t$ for some integer number $0 < t \leq \mu$ and introduce the polynomial

$$P_b(X) := \begin{cases} 1 + \mathrm{tr}_{2\mu}(X^b) & \text{if } 0 < t < \mu, \\ 1 + \mathrm{tr}_\mu(X^b) & \text{otherwise } (t = \mu). \end{cases}$$

Now, consider the quotient ring $\mathcal{R}_0 := \mathbb{F}_{q^{2\mu}}[X]/\langle X^{q^{2\mu}-1} - 1\rangle$ and we are ready for introducing the concept of b-th trace-depending polynomial.

Definition 5.1.1. With the above notation, we denote by $\mathrm{Tr}_b(X)$ the representative with minimum degree of the class of $P_b(X)$ in $\mathcal{R}_0$. We name $\mathrm{Tr}_b(X)$ the *b-th trace-depending polynomial*.

Remark 5.1.2. Later in Subsection 5.1.2 we will introduce codes obtained by evaluating at the roots of the polynomial $\mathrm{Tr}_b(X)$. When $t = \mu$, Definition 5.1.1 uses the polynomial

$\mathrm{tr}_\mu(X)$ instead of $\mathrm{tr}_{2\mu}(X)$ because, when the characteristic of the field $\mathbb{F}_{q^{2\mu}}$ is 2, otherwise $\mathrm{Tr}_b(X) = 1$ and $\mathrm{Tr}_b(X)$ has no roots. Indeed, when $t = \mu$, the following computation

$$\mathrm{tr}_{2\mu}(X^b) = X^{1+q^\mu} + X^{q(1+q^\mu)} + X^{q^2(1+q^\mu)} + \cdots + X^{q^{\mu-1}(1+q^\mu)} + X^{q^\mu(1+q^\mu)} + X^{q^{\mu+1}(1+q^\mu)} + \cdots + X^{q^{2\mu-1}(1+q^\mu)}$$

shows the equality

$$\mathrm{tr}_{2\mu}(X^b) + \langle X^{q^{2\mu}-1} - 1\rangle = 2\Big[\mathrm{tr}_\mu(X^b) + \langle X^{q^{2\mu}-1} - 1\rangle\Big],$$

which also proves that, in this case ($t = \mu$), when the characteristic of the field $\mathbb{F}_{q^{2\mu}}$ is not even, the trace maps $\mathrm{tr}_{2\mu}$ and tr_μ play an analogue role.

Next, we determine the degree of the polynomial $\mathrm{Tr}_b(X)$.

Proposition 5.1.3. *The degree of the b-th trace-depending polynomial* $\mathrm{Tr}_b(X)$, $b = 1+q^t$, $1 \le t \le \mu$, *is* $n = n(t) = q^{2\mu-1-t} + q^{2\mu-1}$.

Proof. The case when $t = \mu$ is clear. Assume $0 < t < \mu$ and write

$$\mathrm{Tr}_b(X) = \sum_{z=0}^{n} c_z X^z.$$

Since $P_b(X)$ has no term involving a power of $X^{q^{2\mu}-1}$ and $\mathrm{Tr}_b(X)$ is the representative with minimum degree of its class in $\mathcal{R}_0$, $c_0 = 1$. Write $z = \sum_{\ell=0}^{2\mu-1} \kappa_\ell q^\ell$, with $0 \le \kappa_\ell < q$, the q-adic expansion of the exponents $z > 0$ such that $c_z \neq 0$. Sometimes, for the sake of simplicity and easiness, this q-adic expansion will be represented with a 2μ-tuple $(z)_q$ as in Table 5.1. The q-adic expansion of b is displayed in Table 5.2, and the q-adic expansion

q^ℓ	q^0	q^1	$\cdots$	q^{t-1}	q^t	$\cdots$	$q^{2\mu-t}$	$\cdots$	$q^{2\mu-1}$
$(z)_q$	κ_0	κ_1	$\ldots$	κ_{t-1}	κ_t	$\ldots$	$\kappa_{2\mu-t}$	$\ldots$	$\kappa_{2\mu-1}$

Table 5.1: q-adic expansion of z, any exponent of $\mathrm{Tr}_b(X) = \sum_{z=0}^{n} c_z X^z$

q^ℓ	q^0	q^1	$\cdots$	q^{t-1}	q^t	q^{t+1}	$\cdots$	$q^{2\mu-t}$	$\cdots$	$q^{2\mu-1}$
$(b)_q$	1	0	$\ldots$	0	1	0	$\ldots$	0	$\ldots$	0

Table 5.2: q-adic expansion of b

of the elements $z > 0$ such that $c_z \neq 0$ can be obtained by successively shifting the values in Table 5.2. Indeed, each shift corresponds to an exponent $z = q^s b$, $0 \le s \le 2\mu - 1$, where $q^{2\mu}$ is identified with 1. As a consequence, $c_z = 1$ whenever $c_z \neq 0$, and the degree of the b-th trace-depending polynomial $\mathrm{Tr}_b(X)$ is given by the sequence of shifts which gives the largest positive integer; it is $n = q^{2\mu-1-t} + q^{2\mu-1}$. Notice that, for simplicity, $b = q^0 b$ is considered a shift of b. □

Along this chapter and with the above notation, we only consider triples (q, μ, b) satisfying the following property:

The polynomial $\mathrm{Tr}_b(X)$ has $n := n(t) := q^{2\mu-1-t} + q^{2\mu-1}$ different roots in the field $\mathbb{F}_{q^{2\mu}}$. (5.1.1)

We denote these roots by $\{\beta_1, \beta_2, \ldots, \beta_n\} =: T$.

The following result proves that the triples $(q, \mu, b(\mu))$ always satisfy Property (5.1.1). For $0 < t < \mu$, by explicit computation, we have found a number of triples (q, μ, b) satisfying Property (5.1.1). Some examples can be seen in Table 5.3. With some of these values we have obtained good stabilizer quantum codes, as we will show in Section 5.3. We do not know a general result characterizing the before mentioned triples.

q	μ	t	b	n = degree
2	2	1	3	12
2	4	2	5	160
2	4	3	9	144
2	6	3	9	2304
2	6	5	33	2112
3	2	1	4	36
3	4	2	10	2430
3	4	3	28	2268
5	2	1	6	150
5	4	2	26	81250
5	4	3	126	78750
7	2	1	8	392
11	2	1	12	1452

Table 5.3: Triples (q, μ, b), $b = 1 + q^t$, satisfying Property (5.1.1)

Proposition 5.1.4. *Assume $b = b(\mu)$. The b-th trace-depending polynomial $\mathrm{Tr}_b(X) \in \mathbb{F}_{q^{2\mu}}[X]$ has $n = n(\mu) = q^{\mu-1} + q^{2\mu-1}$ different roots in the field $\mathbb{F}_{q^{2\mu}}$.*

Proof. The polynomial $\mathrm{tr}_\mu(X)$ gives the trace map $\mathrm{tr}_\mu : \mathbb{F}_{q^\mu} \to \mathbb{F}_q$. The map $g : \mathbb{F}_{q^{2\mu}} \to \mathbb{F}_{q^\mu}$ defined as $g(x) = x^b$ is well-defined and it is surjective; with the exception of $0 \in \mathbb{F}_{q^\mu}$, each element in $\mathbb{F}_{q^\mu}$ has $q^\mu + 1$ counter-images. The map $P_b - 1$ defined by $P_b(X) - 1$ satisfies $P_b - 1 = \mathrm{tr}_\mu \circ g$, therefore the set of roots of $\mathrm{Tr}_b(X)$ is

$$(\mathrm{tr}_\mu \circ g)^{-1}(-1) = g^{-1}[\mathrm{tr}_\mu^{-1}(-1)].$$

Since tr_μ is a trace map, $\mathrm{tr}_\mu^{-1}(-1)$ has $q^{\mu-1}$ different elements and the cardinality of $(\mathrm{tr}_\mu \circ g)^{-1}(-1)$ is $(q^\mu + 1)q^{\mu-1} = q^{2\mu-1} + q^{\mu-1}$, which concludes the proof. □

5.1.2. Evaluation codes at the roots of trace-depending polynomials

Now we are going to define the family of codes we are interested in. These codes are evaluation codes as introduced in Section 1.3. We only consider triples (q, μ, b) satisfying Property (5.1.1). We fix any of them, set $\mathrm{Tr}(X) := \mathrm{Tr}_b(X)$ and define the evaluation map ev_T at the roots of $\mathrm{Tr}(X)$, $T = \{\beta_1, \beta_2, \ldots, \beta_n\}$, as:

$$\mathrm{ev}_T : \mathcal{R} := \mathbb{F}_{q^{2\mu}}[X]/\langle \mathrm{Tr}(X)\rangle \to \mathbb{F}_{q^{2\mu}}^n, \quad \mathrm{ev}_T(f) = (f(\beta_1), f(\beta_2), \ldots, f(\beta_n)), \tag{5.1.2}$$

where f stands for the class of a polynomial $f \in \mathbb{F}_{q^{2\mu}}[X]$ in $\mathcal{R}$ and its corresponding polynomial function.

Definition 5.1.5. Let $E = \{0, 1, \ldots, n-1\}$ and consider a non-empty subset $\Delta \subseteq E$. We define the evaluation code, $\mathcal{C}_\Delta^T$, of Δ at the roots of the trace-depending polynomial $\mathrm{Tr}(X)$ (given by a triple (q, μ, b)) as the linear code of length n over the field $\mathbb{F}_{q^{2\mu}}$ generated by the set $\{\mathrm{ev}_T(X^e) \mid e \in \Delta\}$, that is,

$$\mathcal{C}_\Delta^T = \langle \mathrm{ev}_T(X^e) \mid e \in \Delta\rangle_{\mathbb{F}_{q^{2\mu}}} = \mathrm{ev}_T(\langle X^e \mid e \in \Delta\rangle)_{\mathbb{F}_{q^{2\mu}}}.$$

Notice that these codes can also be thought as univariate MCCs as defined in Subsection 1.3.1.

Our next result describes the polynomial $\mathrm{Tr}(X)$. Recall that $b = 1 + q^t$ with $0 < t \leq \mu$.

Proposition 5.1.6. *Let $\mathrm{Tr}(X) = \sum_{z=0}^n c_z X^z$. One has that $c_z = 0$ for all indices z, with the exception of:*

- *$z = 0$;*
- *$z = q^j b$, where $0 \leq j \leq 2\mu - t - 1$;*
- *and, when $t < \mu$, $z = z_j := q^{j-1}(1 + q^{2\mu - t})$ for $1 \leq j \leq t$.*

Thus, $\mathrm{Tr}(X)$ has $2\mu + 1$ non-zero coefficients c_z when $t < \mu$ and it has $\mu + 1$ otherwise ($t = \mu$). All the non-vanishing coefficients are equal to 1.

Proof. It is clear that $c_0 = 1$. The monomials in the second item of the statement: $X^{q^j b}$, $0 \leq j \leq 2\mu - t - 1$, are terms with coefficient 1 in the polynomial $\mathrm{Tr}(X)$ by the construction of $P_b(X)$, and they are the only terms with non-vanishing coefficient when $t = \mu$ because taking classes modulo the ideal $\langle X^{q^{2\mu}-1} - 1\rangle$ does not produce any modification of $P_b(X)$.

When $t < \mu$, apart from the above monomials, there are new terms with coefficient 1 in the expression of $P_b(X)$ which are $X^{q^j b}$, $2\mu - t \leq j \leq 2\mu - 1$. Recall that $\mathrm{Tr}(X)$ is the representative of minimum degree of the class of $P_b(X)$ modulo $\langle X^{q^{2\mu}-1} - 1\rangle$. As we explained in the proof of Proposition 5.1.3, the representatives of the classes modulo $\langle X^{q^{2\mu}-1} - 1\rangle$ of the monomials $X^{q^j b}$, $0 \leq j \leq 2\mu - 1$, are monomials X^z where z is an integer whose q-adic expansion (see Table 5.1) is given by a sequence of shifts of the q-adic expansion of b (see Table 5.2). Clearly the monomials $X^{q^j b}$, with $0 \leq j \leq 2\mu - t - 1$, correspond to the first shifts and those where $2\mu - t \leq j \leq 2\mu - 1$ correspond to the values z_j in the last item of the statement. □

Remark 5.1.7. Table 5.4 shows the q-adic expansions of the indices $z \neq 0$ in the expression of $\mathrm{Tr}(X) = \sum_{z=0}^{n} c_z X^z$ such that $c_z \neq 0$. Recall that the values z_j introduced in Proposition 5.1.6 do not appear when $t = \mu$ and notice that b and z_1 are the unique indices which are not a multiple of q. The q-adic expansions show how the indices z are ordered as natural numbers, for instance $n > z_t$ and both are larger than the remaining ones.

$(z)_q$ \ q^ℓ	q^0	q^1	$\cdots$	q^{t-1}	q^t	q^{t+1}	$\cdots$	$q^{2\mu-t-1}$	$q^{2\mu-t}$	$\cdots$	$q^{2\mu-1}$
$(b)_q$	1	0	$\ldots$	0	1	0	$\ldots$	0	0	$\ldots$	0
$(qb)_q$	0	1	$\ldots$	0	0	1	$\ldots$	0	0	$\ldots$	0
$\vdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$
$(n)_q = (q^{2\mu-t-1}b)_q$	0	0	$\ldots$	0	0	0	$\ldots$	1	0	$\ldots$	1
$(z_1)_q$	1	0	$\ldots$	0	0	0	$\ldots$	0	1	$\ldots$	0
$\vdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$
$(z_t)_q$	0	0	$\ldots$	1	0	0	$\ldots$	0	0	$\ldots$	1

Table 5.4: q-adic expansions of the indices $z \neq 0$ such that $c_z \neq 0$ in the expression of $\mathrm{Tr}(X) = \sum_{z=0}^{n} c_z X^z$

We are interested in codes $\mathcal{C}_\Delta^T \subseteq \mathbb{F}_{q^{2\mu}}^n$ which are self-orthogonal with respect to the Hermitian inner product. This is because under that condition, Corollary 2.3.8 allows us to construct quantum stabilizer codes. For this reason (see the proof of the forthcoming Theorem 5.1.14), we introduce the following values:

$$s_i := \sum_{j=1}^{n} \beta_j^i; \quad 1 \leq i \leq q^{2\mu} - 1.$$

Now we state a result involving the above values s_i in the fashion of [50, Lemma 4], which can be proved similarly. Notice that the reason why we only consider polynomials $\mathrm{Tr}_b(X)$ which completely factorize in $\mathbb{F}_{q^{2\mu}}$ is to be able to use this result.

Lemma 5.1.8. *With the above notation, for every index r such that $1 \leq r \leq n$, the following equality*

$$\left(\sum_{j=0}^{r-1} c_{n-j} s_{r-j} \right) + r c_{n-r} = 0$$

holds.

In addition, when $r > n$, one gets

$$\sum_{j=0}^{n} c_{n-j} s_{r-j} = 0.$$

The following result determines the indices $i \leq n$ for which the value s_i does not vanish and, therefore, it helps to show when Hermitian orthogonality of vectors $\mathrm{ev}_T(X^e)$

does not hold (see, again, the proof of Theorem 5.1.14). For that purpose, consider the values:

$$j_{2,\ell} := 1 + (2+\ell)q^{t-1} + (q-(2+\ell))q^{2\mu-t-1},$$

where $0 \le \ell \le q-1$.

Theorem 5.1.9. *Keep the notation as in Proposition 5.1.6.*

– *When $1 < t < \mu$, there are exactly q indices $i \le n$ such that $s_i \neq 0$. We denote these indices in increasing order as $i_0 < i_1$ whenever $q = 2$. Otherwise, we denote them as*

$$i_0 < i_1 < i_{2,0} < i_{2,1} < \cdots < i_{2,q-3}.$$

Then,

a) *It holds that $i_0 = n - z_1$, $i_1 = n - (z_1 + z_t - n)$, and $i_{2,\ell} = n - j_{2,\ell}$ for $0 \le \ell \le q-3$.*

b) *$s_{i_0} = s_{i_{2,\ell}} = 1$ for $\ell = 0$ and for ℓ even.*

c) *$s_{i_1} = s_{i_{2,\ell}} = -1$ for ℓ odd.*

– *When $t = 1$, there exist exactly $q+1$ indices $i \le n$ such that $s_i \neq 0$. With the above notation, these indices are*

$$i_0 < i_1 < i_{2,0} < i_{2,1} < \cdots < i_{2,q-3} < i_{2,q-2} := i_{2,q-3} + q^{2\mu-2} - q^{2\mu-3} + q - 1,$$

and they satisfy Property **a)**, *and properties* **b)** *and* **c)** *for $0 \le \ell \le q-2$. The case $q = 2$, $\mu = 2$ and $t = 1$ should be treated separately; here there are four indices $i_0 < i_1 < i_{2,0} < i_{2,1}$ satisfying the above mentioned properties* **a)**, **b)** *and* **c)**.

– *When $t = \mu$, there is only one index $i_0 = q^{2\mu-1} - q^{\mu} + q^{\mu-1} - 1$ lower than n such that $s_{i_0} \neq 0$. Here we also find an exception in the case $q = t = \mu = 2$ where there are two indices $i_0 = 5$ and $i_1 = 10$ satisfying $s_i \neq 0$.*

Proof. Lemma 5.1.8 and q-adic expansions are the main tools of our proof. We divide it in two cases: *Case A*, where we study the case $t \neq 1$ and *Case B* that corresponds to the situation $t = 1$. Within each case, we consider several steps and state and prove some lemmas. *Step A.1* computes i_0 and s_{i_0} proving the first equalities in **a)** and **b)** and also the first statement in the case $t = \mu$. *Step A.2* determines i_1 and s_{i_1} showing the second equality in **a)** and the first one in **c)**. Here we also conclude the proof of the case $t = \mu$. *Step A.3* (respectively, *A.4*) computes $i_{2,0}$ and $s_{i_{2,0}}$ (respectively, $i_{2,\ell}$ and $s_{i_{2,\ell}}$ for $\ell \neq 0$). The treatment of *Case B* is a bit different because distinct q-adic expansions appear. We consider here three steps corresponding to results which will prove the statement of Theorem 5.1.9 in this case $t = 1$.

Our strategy mainly consists of noticing that fixed an index h such that $s_h \neq 0$, the next index $h' > h$ such that $s_{h'} \neq 0$ occurs when the coefficient of s_h in the sum provided by Lemma 5.1.8 that starts with $c_n s_{h'}$ is different from zero. To reach this conclusion, we also prove that the mentioned coefficient is zero for those indices h'' such

that $h < h'' < h'$ and, in this case, $s_{h''} = 0$.

Case A. $t \neq 1$. *Step A.1.* We start by proving the first equality in Items **a)** and **b)** of the statement. Thus, we assume $1 < t < \mu$. As before, we set $\mathrm{Tr}_b(X) = \sum_{z=0}^{n} c_z X^z$. Denoting $\mathrm{Supp} := \mathrm{Supp}_{\mathrm{Tr}_b(X)} := \{z \neq 0 \mid c_z \neq 0\}$, we have proved that

$$\mathrm{Supp} = \{z \mid (z)_q \text{ is obtained by iteratively applying shifts to } (b)_q\}$$

and this set has cardinality 2μ.

From our notation $i_0 := \min\{i \mid 1 \leq i \leq n \text{ and } s_i \neq 0\}$. Setting $r = i_0$ in the first equality of Lemma 5.1.8, we get

$$c_n s_{i_0} + c_{n-1} s_{i_0-1} + \cdots + c_{n-(i_0-1)} s_1 = -i_0 c_{n-i_0}.$$

The definition of i_0 shows that $0 \neq s_{i_0} = -i_0 c_{n-i_0}$. Since our supporting field is $\mathbb{F}_{q^{2\mu}}$, this implies that $-i_0$ is not a multiple of q and $c_{n-i_0} \neq 0$. Taking into account that $n = q^{2\mu-1-t} + q^{2\mu-1}$, $n - i_0$ has to be of the form $1 + \lambda q$ because otherwise i_0 would be a multiple of q and thus $i_0 c_{n-i_0}$ would be 0. The index i_0 is a minimum and therefore $n - i_0$ equals the value

$$\max\{n - z = n - \sum_{\ell=0}^{2\mu-1} \kappa_\ell q^\ell \mid n - z \in \mathrm{Supp} \text{ and its } q\text{-adic expansion starts with } 1\}.$$

Inspecting the set of q-adic expansions that are obtained as (successive) shifts of $(b)_q$ –see Table 5.4– one deduces that, with the notation in Proposition 5.1.6, the following equality holds:

$$n - i_0 = z_1 = 1 + q^{2\mu-t}$$

and hence $s_{i_0} = -(-1) = 1$. Therefore the first equality in Items **a)** and **b)** of the statement follows for $1 < t < \mu$.

When $t = \mu$, noticing that the cardinality of Supp is μ and reasoning analogously, we obtain $n - i_0 = b = 1 + q^\mu$ and therefore $i_0 = q^{2\mu-1} - q^\mu + q^{\mu-1} - 1$. This proves our last statement with the exception of the uniqueness of i_0 that will be proved later.

Step A.2. Let us prove the first equality in Item **c)** of the statement. Assume $1 < t < \mu$ and, as in the statement of the theorem, set

$$i_1 := \min\{i \mid i_0 < i \leq n \text{ and } s_i \neq 0\}.$$

Again by Lemma 5.1.8, one gets:

$$c_n s_{i_1} + c_{n-1} s_{i_i-1} + \cdots + c_{n+i_0-i_1} s_{i_0} + c_{n+i_0-i_1-1} s_{i_0-1} + \cdots + c_{n-(i_1-1)} s_1 = -i_1 c_{n-i_1},$$

which, from the definition of i_1, implies

$$s_{i_1} + c_{n+i_0-i_1} s_{i_0} = -i_1 c_{n-i_1}. \tag{5.1.3}$$

The inequalities $i_0 < i \leq n$ prove $0 \leq n - i < n - i_0 = z_1$ and thus $i_0 \leq n + i_0 - i < i_0 + z_1$. We look for i_1 such that $c_{n+i_0-i_1} \neq 0$ (later we will see that this is the only possibility) and then $n + i_0 - i_1$ must be equal to the value

$$\max\{n + i_0 - i \in \mathrm{Supp} \mid i_0 \leq n + i_0 - i < n\}.$$

Considering the q-adic expansions of the values in Supp (see Table 5.4), that maximum is attained when $n+i_0-i_1 = z_t$, because z_t is the larger value in Supp lower than n. Then, $i_1 = n+i_0-z_t = n-(z_1+z_t-n)$ as stated in **a)**. The index i_1 is a multiple of q if and only if $n - i_1$ is, thus looking at the q-adic expansions of the shifts of $(b)_q$, $i_1 c_{n-i_1}$ equals 0 except when $n-i_1$ equals b or z_1. Now $n-i_1$ is neither b nor z_1 and therefore, by Equality (5.1.3), $s_{i_1} = -1$ as said in Item **c)** of our theorem. Indeed, reasoning by contradiction, if $n - i_1 = b$ then $z_t - i_0 = b$ and thus $z_t + z_1 = n + b$, which means $q^{t-1} + q^{2\mu-t} = q^t + q^{2\mu-t-1}$, a contradiction. In addition, $n - i_1 = z_1$ implies $z_t - i_0 = z_1$ and therefore $z_t = n$, again a contradiction.

Notice that in the searching of i_1, one could consider Equality (5.1.3) with some index i, $i_0 < i < i_1$ instead of i_1, $s_i \neq 0$ and $c_{n+i_0-i} = 0$, but then $n - i$ should be either z_1 or b. In the first case $i = n - z_1 = i_0$ which contradicts the fact that $i_0 < i$; and in the second one, the inequality $q^{2\mu-1} + q^{2\mu-t-1} + 1 + q^t < q^{2\mu-1} + q^{t-1} + 1 + q^{2\mu-t}$ proves $n + b < z_t + z_1$, which implies $i_1 = 2n - z_1 - z_t < n - b = i$ and i would not be the required minimum value with $s_i \neq 0$.

Now we conclude the proof of our last statement concerning the case $t = \mu$. Reasoning as in the previous paragraphs, one gets two possibilities.

The first one is that Equality (5.1.3) holds for some index i_1 such that $c_{n+i_0-i_1} = 0$, then $n - i_1 = b$ and, since we proved before that in this case $n - i_0 = b$, then $i_1 = i_0$, which contradicts the fact $i_1 > i_0$.

Otherwise, $n + i_0 - i_1$ should be an element in Supp of the form $(1 + q^\mu)q^j$, for some $0 < j \leq \mu - 2$, because Equality (5.1.3) makes no sense for $j = 0$ -except when $q = \mu = 2$- nor for $j = \mu - 1$ (since it would imply that $i_0 = i_1$). Then

$$i_1 = (1+q^\mu)q^{\mu-1} + (1+q^\mu)q^{\mu-1} - (1+q^\mu) - (1+q^\mu)q^j = (1+q^\mu)(2q^{\mu-1} - q^j - 1),$$

and thus $i_1 > n$, proving that there is no such $i_1 \leq n$. As a consequence, we conclude that i_0 is the only index satisfying $s_{i_0} \neq 0$ when $t = \mu$ and the case $q = \mu = 2$ does not hold.

Notice that $n + i_0 - i_1 = 1 + q^\mu = b$ if and only if $n + i_0 - i_1 = n - i_0$, which is equivalent to $i_1 = 2i_0$ and then $2i_0 \leq n$. This inequality happens if and only if $q^{2\mu-1} + q^{\mu-1} \leq 2q^\mu + 2$, which holds only when $q = \mu = 2$. Therefore, only in this case, we get a new index i_1 such that $s_{i_1} = -1 = 1$ as stated.

Step A.3. Assume $1 < t < \mu$. Iterating our reasoning, define

$$i_2 := \min\{i \mid i_1 < i \leq n \text{ and } s_i \neq 0\}.$$

By Lemma 5.1.8 one gets

$$c_n s_{i_2} + \cdots + c_{n+i_1-i_2} s_{i_1} + \cdots + c_{n+i_0-i_2} s_{i_0} + \cdots + c_{n-(i_2-1)} s_1 = -i_2 c_{n-i_2}, \tag{5.1.4}$$

where the main novelty is that one might have three non-vanishing summands on the left hand side of the equality.

Let us study Equality (5.1.4). First we determine the q-adic expansion of the value i_1.

Lemma 5.1.10. *With the above notation, the q-adic expansion of i_1 is that displayed in Table 5.5.*

q^ℓ	q^0	$\cdots$	q^{t-2}	q^{t-1}	q^t	$\cdots$	$q^{2\mu-t-2}$	$q^{2\mu-t-1}$	$q^{2\mu-t}$	$\cdots$	$q^{2\mu-2}$	$q^{2\mu-1}$
$(i_1)_q$	$q-1$	$\ldots$	$q-1$	$q-2$	$q-1$	$\ldots$	$q-1$	1	$q-1$	$\ldots$	$q-1$	0

Table 5.5: q-adic expansion of i_1 in the proof of Theorem 5.1.9

Proof. We start with the following chain of equalities

$$\begin{aligned} i_1 = (n-z_1)+(n-z_t) &= q^{2\mu-1}+q^{2\mu-1-t}-\left(1+q^{2\mu-t}\right)+q^{2\mu-1}+q^{2\mu-1-t}-\left(q^{2\mu-1}+q^{t-1}\right) \\ &= q^{2\mu-1}+q^{2\mu-1-t}-\left(1+q^{2\mu-t}\right)+q^{2\mu-1-t}-q^{t-1} =: w. \end{aligned} \tag{5.1.5}$$

Noticing that $q^{2\mu-1} = (q-1)q^{2\mu-2}+(q-1)q^{2\mu-3}+\cdots+(q-1)q+q$, one gets that the value w in (5.1.5) equals

$$\begin{aligned} &(q-1)q^{2\mu-2}+\cdots+(q-2)q^{2\mu-t}+(q+1)q^{2\mu-t-1} \\ &\qquad +(q-1)q^{2\mu-t-2}+\cdots+(q-1)q^t+(q-2)q^{t-1}+\cdots+(q-1), \end{aligned}$$

which ends the proof. □

Next we study the index i_2 involved in Equality (5.1.4).

Lemma 5.1.11. *There is only an index $i_2' > i_1$ such that $c_{n+i_1-i_2'} \neq 0$. With the notation as before Theorem 5.1.9, this index satisfies $n-i_2' = j_{2,0}$.*

Proof. Since $i_2' > i_1$, there exists a positive integer $j_2' < z_1+z_t-n$ such that $i_2' = n-j_2'$. Then $n+i_1-i_2' = i_1+j_2' < n$. By Lemma 5.1.10, $z = z_t$ is the unique value $z = n+i_1-i_2' < n$ as in Proposition 5.1.6 that can be obtained with indices $j_2' < z_1+z_t-n$. This is because the last coordinate of the q-adic expansion $(z)_q$ of the remaining values z in Proposition 5.1.6 vanishes. By inspection, we deduce that the q-adic expansion of j_2' is that given in Table 5.6 and thus, with the notation as before the statement of Theorem 5.1.9, $j_2' = j_{2,0}$. □

q^ℓ	q^0	q^1	$\cdots$	q^{t-2}	q^{t-1}	q^t	$\cdots$	$q^{2\mu-t-2}$	$q^{2\mu-t-1}$	$q^{2\mu-t}$	$\cdots$	$q^{2\mu-1}$
$(j_2')_q$	1	0	$\ldots$	0	2	0	$\ldots$	0	$q-2$	0	$\ldots$	0

Table 5.6: q-adic expansion of j_2' in the proof of Theorem 5.1.9

Lemma 5.1.12. *The above introduced index $i_2 = \min\{i \mid i_1 < i \leq n \text{ and } s_i \neq 0\}$ equals $n-j_{2,0} := i_{2,0}$. In addition, $s_{i_{2,0}} = 1$.*

Proof. Assume first that $q > 2$. Define $j_2 = n - i_2$, then

$$j_2 < n - i_1 = z_1 + z_t - n = 1 + (q-1)q^{2\mu-1-t} + q^{t-1} =: \theta. \tag{5.1.6}$$

The q-adic expansion of θ in the above equality proves that there is no index j, $j_{2,0} < j < z_1 + z_t - n$ such that $s_{n-j} \neq 0$. In fact, write $i = n - j$, by Lemma 5.1.11, we have that $c_{n+i_1-i} = 0$; in addition $ic_{n-i} = 0$ because either i is a multiple of q or, otherwise, $c_{n-i} = 0$. This is because inspecting the q-adic expansion of $j_{2,0}$ and the expression (5.1.6), we notice that there is no j as required with a q-adic expansion having only two ones; in fact j should have a q-adic expansion of the form $1 + (q-2)q^{2\mu-t-1} +$ other terms. Finally, $c_{n+i_0-i} = c_{n-z_1+j} = 0$ since all the coefficients of the q-adic expansion of $n - z_1$ are $q-1$ except those of $q^{2\mu-1}$ and $q^{2\mu-1-t}$. Therefore, considering Equality (5.1.4) with i instead of i_2, we get $s_{n-j} = 0$. As a consequence, $i_2 = n - j_{2,0} := i_{2,0}$ is our candidate for satisfying $s_{i_2} \neq 0$. Let us show that, indeed, $s_{i_{2,0}} \neq 0$.

Equality (5.1.4) reads

$$s_{n-j_{2,0}} + \cdots + c_{z_t} s_{i_1} + \cdots + c_{n-z_1+j_{2,0}} s_{i_0} = -(n - j_{2,0}) c_{j_{2,0}}$$

and we know that $c_{z_t} = 1$, $s_{i_1} = -1$. Now,

$$\begin{aligned} n - z_1 + j_{2,0} &= q^{2\mu-1} + q^{2\mu-1-t} - q^{2\mu-t} - 1 + (q-2)q^{2\mu-1-t} + 2q^{t-1} + 1 \\ &= q^{2\mu-1} + q^{2\mu-1-t} - q^{2\mu-t} - 1 + q^{2\mu-t} - 2q^{2\mu-t-1} + 2q^{t-1} + 1 \\ &= q^{2\mu-1} - q^{2\mu-t-1} + 2q^{t-1} \\ &= (q-1)q^{2\mu-2} + (q-1)q^{2\mu-3} + \cdots + (q-1)q + q - q^{2\mu-t-1} + 2q^{t-1}, \end{aligned}$$

getting a q-adic expansion as in Table 5.7.

q^ℓ	q^0	$\cdots$	q^{t-2}	q^{t-1}	q^t	$\cdots$	$q^{2\mu-t-2}$	$q^{2\mu-t-1}$	$\cdots$	$q^{2\mu-2}$	$q^{2\mu-1}$
$(n - z_1 + j_{2,0})_q$	0	$\ldots$	0	2	0	$\ldots$	0	$q-1$	$\ldots$	$q-1$	0

Table 5.7: q-adic expansion of $n - z_1 + j_{2,0}$ in the proof of Theorem 5.1.9

Therefore the q-adic expansion of $n - z_1 + j_{2,0}$ has more than two non-vanishing entries and then, it cannot be one of the values z described in Proposition 5.1.6. Thus $c_{n-z_1+j_{2,0}} = 0$. Similarly, the q-adic expansion of $j_{2,0}$ has three nonvanishing entries and therefore $c_{j_{2,0}} = 0$. This concludes the proof of the case $q > 2$ and $s_{i_{2,0}} = s_{n-j_{2,0}} = -s_{i_1} = 1$.

When $q = 2$, the only indices i such that $s_i \neq 0$ are i_0 and i_1. This fact can be proved by noticing that, reasoning as above, the unique candidate $j_2 := n - i_2 < n - i_1$ such that $s_{i_2} \neq 0$ is $j_{2,0} = 1 + q^t = b$. Using again Equality (5.1.4) one gets

$$s_{n-b} + \cdots + c_{z_t} s_{i_1} + \cdots + c_{i_0+b} s_{i_0} = -(n-b)c_b.$$

The only unknown value is c_{i_0+b}, and

$$i_0 + b = q^{2\mu-1} + q^{2\mu-1-t} - (q^{2\mu-t} + 1) + q^t + 1 = q^{2\mu-1} - q^{2\mu-t} + q^{2\mu-t-1} + q^t.$$

Now writing again $q^{2\mu-1} = \sum_{i=1}^{2\mu-2}(q-1)q^{2\mu-1-i}+q$, one deduces that the value i_0+b equals

$$(q-1)q^{2\mu-2}+\cdots+(q-1)q^{2\mu-t+1}+(q-2)q^{2\mu-t} \\ +[(q-1)q^{2\mu-t-1}+\cdots+(q-1)q+q]+q^{2\mu-t-1}+q^t.$$

The value given in square brackets is $q^{2\mu-t}$ and therefore the q-adic expansion of i_0+b has more than two non-vanishing entries, which means that $c_{i_0+b}=0$. Thus $s_{i_1}=1$ and $-(n-b)c_b=1$ proving that $s_{n-b}=0$. Notice that in this case the characteristic of the supporting field is two. □

Step A.4. To finish the proof of our Theorem 5.1.9 when $t\neq 1$, it suffices to reason as before. That is to say, in the next step define $i_{2,1} := \min\{i \mid i_{2,0} < i \leq n \text{ and } s_i \neq 0\}$; again one gets an equality similar to Equality (5.1.4) and, as we will see later, $c_{n+i_{2,0}-i_{2,1}} \neq 0$ is the only feasible possibility, then $n+i_{2,0}-i_{2,1}=z_t$ and thus,

$$i_{2,1} = n-(z_t-n+j_{2,0}) = n-j_{2,1} = n-(1+3q^{t-1}+(q-3)q^{2\mu-t-1}).$$

Iterating the reasoning, one obtains candidates $i_{2,\ell}$, $0\leq\ell\leq q-2$, as in the statement (note that these indices satisfy $i_{2,\ell}\leq n$, which is equivalent to $j_{2,\ell}\geq 0$).

We start by computing the values $s_{i_{2,\ell}}$, $1\leq\ell\leq q-3$. Recall that $s_{i_{2,0}}=1$ and note that we assume $q\geq 3$ since we have obtained all the indices i with $s_i\neq 0$ (and the values s_i) in the case $q=2$. By Lemma 5.1.8, the following equality holds:

$$c_n s_{i_{2,\ell}} + c_{n+i_{2,\ell-1}-i_{2,\ell}} s_{i_{2,\ell-1}} + \cdots + c_{n+i_{2,0}-i_{2,\ell}} s_{i_{2,0}} + c_{n+i_1-i_{2,\ell}} s_{i_1} + c_{n+i_0-i_{2,\ell}} s_{i_0} = -i_{2,\ell} c_{n-i_{2,\ell}}. \tag{5.1.7}$$

Consider an index $0\leq\ell'<\ell$. Then, one gets the chain of equalities

$$n+i_{2,\ell'}-i_{2,\ell} = n+(\ell-\ell')q^{t-1}-(\ell-\ell')q^{2\mu-t-1} = (\ell-\ell')q^{t-1}-(\ell-\ell'-1)q^{2\mu-t-1}+q^{2\mu-1},$$

which proves that $c_{n+i_{2,\ell-1}-i_{2,\ell}} = c_{z_t}$.

The right hand side of Equality (5.1.7) vanishes because $c_{n-i_{2,\ell}} = c_{j_{2,\ell}} = 0$, which holds since the q-adic expansion of $j_{2,\ell}$ does not coincide with any element in Table 5.4.

Next we are going to show that, with the exception of the first two summands, every summand in the left hand side of Equality (5.1.7) vanishes. *In this case* $s_{i_{2,\ell}} + s_{i_{2,\ell-1}} = 0$ *and we obtain the values of the indices* s_i *as in the statement.*

We start by proving that $c_{n+i_{2,\ell'}-i_{2,\ell}} = 0$ whenever $0\leq\ell'<\ell$ and $\ell'\neq\ell-1$. In this case, $1<\ell-\ell'\leq q-3$ and the q-adic expansion of $n+i_{2,\ell'}-i_{2,\ell}$ is

$$(\ell-\ell')q^{t-1}-(\ell-\ell'-1)q^{2\mu-t-1}+q^{2\mu-1},$$

which has an expansion with a summand $(q-1)q^{2\mu-2}$. This implies that $n+i_{2,\ell'}-i_{2,\ell}$ is not an element in Table 5.4 and thus $c_{n+i_{2,\ell'}-i_{2,\ell}}=0$.

We prove now that $c_{n+i_1-i_{2,\ell}}=0$. Notice that $n+i_1-i_{2,\ell} = i_1+j_{2,\ell}$. Table 5.5 shows the q-adic expansion of i_1 and then, the summand corresponding to the least power of

q in the q-adic expansion of $i_1 + j_{2,\ell}$ is $(\ell+1)q^{t-1}$. Since $1 \le \ell \le q-3$, this last q-adic expansion does not coincide with any expansion in Table 5.4, proving that $c_{n+i_1-i_{2,\ell}} = 0$.

To conclude the proof of the computation of $s_{i_{2,\ell}}$, $1 \le \ell \le q-3$, it only remains to check whether $c_{n+i_0-i_{2,\ell}}$ vanishes. Indeed,

$$\begin{aligned} n + i_0 - i_{2,\ell} &= i_0 + j_{2,\ell} = i_0 + 1 + (2+\ell)q^{t-1} + (q-2-\ell)q^{2\mu-t-1} \\ &= q^{2\mu-1} + q^{2\mu-t-1} - 1 - q^{2\mu-t} + 1 + (2+\ell)q^{t-1} + (q-2-\ell)q^{2\mu-t-1} \\ &= q + (q-1)q + \cdots + (q-1)q^{2\mu-2} + (2+\ell)q^{t-1} + (q-\ell-1)q^{2\mu-t-1} - q^{2\mu-t} \\ &= (2+\ell)q^{t-1} + (q-\ell-1)q^{2\mu-t-1} + (q-1)q^{2\mu-t} + \cdots + (q-1)q^{2\mu-2}. \end{aligned}$$

Then, the first summand in the q-adic expansion of $i_0 + j_{2,\ell}$ is $(2+\ell)q^{t-1}$ showing that $c_{n+i_0-i_{2,\ell}} = 0$ by Table 5.4.

To finish, we determine the value $s_{i_{2,q-2}}$. Then, again by Lemma 5.1.8, one has

$$c_n s_{i_{2,q-2}} + c_{n+i_{2,q-3}-i_{2,q-2}} s_{i_{2,q-3}} + \cdots + c_{n+i_0-i_{2,q-2}} s_{i_0} = -i_{2,q-2} c_{n-i_{2,q-2}}, \tag{5.1.8}$$

where $n - i_{2,q-2} = j_{2,q-2} = b$. Then $-i_{2,q-2}c_{n-i_{2,q-2}} = 1$ and, as we proved before, only the first two summands in the left hand side of Equality (5.1.8) do not vanish. Then when the characteristic of the supporting field is odd, one gets $s_{i_{2,q-2}} + 1 = 1$ and thus $s_{i_{2,q-2}} = 0$. Otherwise (the characteristic of the supporting field is 2), $s_{i_{2,q-2}} - 1 = 1$ and, as well, $s_{i_{2,q-2}} = 0$.

Then, we have proved that $q-3$ is the largest index ℓ such that $s_{i_{2,\ell}} \neq 0$.

It remains to prove that that $s_i = 0$ whenever $n \ge i \ge i_{2,0}$ and $i \neq i_{2,\ell}$, $0 \le \ell \le q-3$.

We start by proving that for any ℓ as above, $s_{i_{2,\ell}+j} = 0$ whenever $0 < j < q^{2\mu-t-1} - q^{t-1}$. Set $f := i_{2,\ell} - i_{2,\ell-1} = q^{2\mu-t-1} - q^{t-1}$. By Lemma 5.1.8, the following equality holds:

$$\begin{aligned} c_n s_{i_{2,\ell}+j} + c_{n-j} s_{i_{2,\ell}} + c_{n-j-f} s_{i_{2,\ell-1}} + c_{n-j-2f} s_{i_{2,\ell-2}} + \cdots + c_{n-j-\ell f} s_{i_{2,0}} \\ + c_{n+i_1-i_{2,\ell}-j} s_{i_1} + c_{n+i_0-i_{2,\ell}-j} s_{i_0} = -(i_{2,\ell}+j) c_{n-i_{2,\ell}-j}. \end{aligned} \tag{5.1.9}$$

Consider an integer α such that $0 \le \alpha \le \ell \le q-3$, then

$$n - j - \alpha f = q^{2\mu-t-1} + q^{2\mu-1} - \alpha(q^{2\mu-t-1} - q^{t-1}) - j = q^{2\mu-1} + (1-\alpha)q^{2\mu-t-1} + \alpha q^{t-1} - j.$$

Since $0 < j < q^{2\mu-t-1} - q^{t-1}$, one gets

$$q^{2\mu-1} - \alpha q^{2\mu-t-1} + (\alpha+1)q^{t-1} < n - j - \alpha f < q^{2\mu-1} + (1-\alpha)q^{2\mu-t-1} + \alpha q^{t-1},$$

and the q-adic expansion of $n-j-\alpha f$ contains either the summand $(q-1)q^{2\mu-2}$ or $q^{2\mu-1}$. Then, it can be neither n nor z_t. This proves that, for all α and j as before, $c_{n-j-\alpha f} = 0$ by Table 5.4.

Next we prove that $c_{n+i_1-i_{2,\ell}-j}$ vanishes. Indeed,

$$\begin{aligned} n + i_1 - i_{2,\ell} - j &= n + 2n - z_1 - z_t - (n - j_{2,\ell}) - j = 2n + j_{2,\ell} - z_1 - z_t - j \\ &= 2(q^{2\mu-1} + q^{2\mu-1-t}) + (1 + (2+\ell)q^{t-1} + (q-2-\ell)q^{2\mu-t-1}) \\ &\quad - (1 + q^{2\mu-t}) - (q^{t-1} + q^{2\mu-1}) - j \\ &= q^{2\mu-1} - q^{2\mu-t} + (q-\ell)q^{2\mu-t-1} + (1+\ell)q^{t-1} - j. \end{aligned}$$

Since $0 < j < q^{2\mu-t-1} - q^{t-1}$, one gets that

$$q^{2\mu-1} - q^{2\mu-t} + (q-\ell-1)q^{2\mu-t-1} + (2+\ell)q^{t-1}$$

and

$$q^{2\mu-1} - q^{2\mu-t} + (q-\ell)q^{2\mu-t-1} + (1+\ell)q^{t-1}$$

are a lower and an upper bound on the values $n+i_1-i_{2,\ell}-j$. Then, the q-adic expansion of $n+i_1-i_{2,\ell}-j$ has a summand $(q-1)q^{2\mu-2}$ if $\ell \neq 0$. When $\ell = 0$, the above mentioned q-adic expansion has a summand $q^{2\mu-1}$ and it must be lower than z_t. In any case, $c_{n+i_1-i_{2,\ell}-j} = 0$ for all j.

The value $c_{n+i_0-i_{2,\ell}-j}$ is also zero. In fact,

$$\begin{aligned} n + i_0 - i_{2,\ell} - j &= n + (n - z_1) - (n - j_{2,\ell}) - j = n + j_{2,\ell} - z_1 - j \\ &= q^{2\mu-1} - q^{2\mu-t} + (q-\ell-1)q^{2\mu-1-t} + (2+\ell)q^{t-1} - j. \end{aligned}$$

Using again that $0 < j < q^{2\mu-t-1} - q^{t-1}$, we see that

$$q^{2\mu-1} - q^{2\mu-t} + (q-\ell-1)q^{2\mu-1-t} + (2+\ell)q^{t-1}$$

and $q^{2\mu-1} - q^{2\mu-t} + (q-\ell-2)q^{2\mu-1-t} + (3+\ell)q^{t-1}$ are an upper and a lower bound on the values $n + i_0 - i_{2,\ell} - j$. Then, computing the q-adic expansions of both bounds, we deduce that the q-adic expansion of $n + i_0 - i_{2,\ell} - j$ has a summand $(q-1)q^{2\mu-2}$ and thus $c_{n+i_0-i_{2,\ell}-j} = 0$. Moreover, $-(i_{2,\ell}+j)c_{n-i_{2,\ell}-j} = 0$, because when $n - i_{2,\ell} - j$ is not a multiple of q, $n - i_{2,\ell} - j$ can be neither b nor z_1. Then by Equality (5.1.9), it holds that $s_{i_{2,\ell}+j} = 0$ whenever $0 < j < q^{2\mu-t-1} - q^{t-1}$ and $0 \leq \ell \leq q-3$.

In an analogue manner, it can be shown that $s_{i_{2,q-2}+j} = 0$ for $0 < j \leq 1 + q^t$ and *Theorem 5.1.9 is proved when* $t \neq 1$.

Case B. $t = 1$. In this case, $t = 1$, $z_t = z_1$ and an ordered set of indices i candidates to satisfy $s_i \neq 0$ is

$$n - z_1 < 2(n - z_1) < \cdots < q(n - z_1).$$

Notice that these are the indices given in the statement because $i_0 = n - z_1$, $i_1 = (n - z_1) + (n - z_1) = 2(n - z_1)$ and for $0 \leq \ell \leq q-3$,

$$(\ell+3)(n - z_1) = n - j_{2,\ell}.$$

Indeed, $(\ell+3)n - (\ell+3)z_1 = n - j_{2,\ell}$ if and only if $(\ell+3)z_1 = (\ell+2)n + j_{2,\ell}$ if and only if

$$(\ell+3)\left(1 + q^{2\mu-1}\right) = (\ell+2)\left(q^{2\mu-2} + q^{2\mu-1}\right) + (\ell+3) + (q - (2+\ell))\, q^{2\mu-2}.$$

With this new notation, one has to successively apply Lemma 5.1.8 obtaining equalities as follows for $1 \leq \beta \leq q$:

$$\begin{aligned} c_n s_{\beta(n-z_1)} + c_{z_1} s_{(\beta-1)(n-z_1)} + c_{2z_1-n} s_{(\beta-2)(n-z_1)} + \cdots + c_{(\beta-1)z_1-(\beta-2)n} s_{n-z_1} \\ = -\beta(n - z_1) c_{n-\beta(n-z_1)}. \end{aligned} \quad (5.1.10)$$

The following lemma will be useful to conclude our proof.

Lemma 5.1.13. *For $1 \le \alpha \le q$, the values $\alpha z_1 - (\alpha-1)n$ are equal to $q^{2\mu-2}(q-\alpha+1)+\alpha$. In addition, the q-adic expansion of $\alpha z_1 - (\alpha-1)n$ coincides with that of some element in Table 5.4 if and only if either $\alpha = 1$ or $\mu = 2$ and $\alpha = q$.*

Proof. The proof follows from the chain of equalities:

$$\begin{aligned}\alpha z_1 - (\alpha-1)n &= \alpha(1+q^{2\mu-1}) - (\alpha-1)(q^{2\mu-2}+q^{2\mu-1}) \\ &= q^{2\mu-1} - (\alpha-1)q^{2\mu-2} + \alpha = q^{2\mu-2}(q-\alpha+1)+\alpha.\end{aligned}$$

Moreover, $q^{2\mu-2}(q-\alpha+1)+\alpha = z_1$ when $\alpha = 1$ and it equals q^2+q whenever $\mu = 2$ and $\alpha = q$. Otherwise, the value $q^{2\mu-2}(q-\alpha+1)+\alpha$ cannot be expressed as $q^i + q^{i+1}$, $0 \le i \le 2\mu-2$. □

Step B.1. First we assume that

$$s_{\beta(n-z_1)+j} = 0 \quad \text{for } 0 \le \beta \le q-1 \text{ and } 0 < j < n - z_1. \tag{5.1.11}$$

In a few lines we will prove that this assumption is true.

Now, from Lemma 5.1.13, we deduce that every summand (with the exception of the first two ones) in the left hand side of Equality (5.1.10) vanishes. In addition, $n - \beta(n-z_1) = n - \beta n + \beta z_1 = \beta z_1 - (\beta-1)n$. Again by Lemma 5.1.13, the right hand side of Equality (5.1.10) is zero for $\beta \neq 1$ and 1 for $\beta = 1$. This proves that, *whenever $1 \le \beta \le q$, the value $s_{\beta(n-z_1)} = 1$ if β is odd and it equals -1, otherwise.*

Step B.2. Let us prove our Assertion (5.1.11). Also that $s_{q(n-z_1)+j} = 0$ for every j such that $0 < j < j_1 := q^{2\mu-2} - q^{2\mu-3} + q - 1$ and $s_{q(n-z_1)+j_1} \neq 0$. Note that $j_1 \le n - z_1 \le n - q(n-z_1)$ and that the first inequality is an equality when $\mu = 2$.

Let us prove Assertion (5.1.11). Take $0 < j < n - z_1 = q^{2\mu-2} - 1$ and $0 \le \beta \le q-1$. By Lemma 5.1.8, one has

$$\begin{aligned}&c_n s_{\beta(n-z_1)+j} + c_{n-j} s_{\beta(n-z_1)} + c_{z_1-j} s_{(\beta-1)(n-z_1)} \\ &\quad + c_{2z_1-n-j} s_{(\beta-2)(n-z_1)} + \cdots + c_{(\beta-1)z_1-(\beta-2)n-j} s_{n-z_1} = -(\beta(n-z_1)+j) c_{\beta z_1-(\beta-1)n-j}.\end{aligned} \tag{5.1.12}$$

The values $c_{\alpha z_1-(\alpha-1)n-j}$, $0 \le \alpha \le q-1$, satisfy:

$$c_{\alpha z_1-(\alpha-1)n-j} = \begin{cases} 0 & \text{if } 0 \le \alpha \le q-2 \text{ or } \alpha = q-1 \text{ and } j \neq j_1 \\ 1 & \text{if } \alpha = q-1,\ j = j_1 \text{ and } \mu \neq 2. \end{cases}$$

Indeed, for $\alpha = 0$ the value c_{n-j} vanishes because $z_1 < n - j < n$ and n and z_1 are the largest indices i such that $c_i \neq 0$. For $1 \le \alpha \le q-1$, from the fact $0 < j < q^{2\mu-2} - 1$ and by Lemma 5.1.13, the following chain of inequalities holds:

$$(q-\alpha)q^{2\mu-2} + \alpha + 1 < \alpha z_1 - (\alpha-1)n - j < (q-\alpha+1)q^{2\mu-2} + \alpha.$$

Then, looking at the q-adic expansions of the bounds on $\alpha z_1 - (\alpha-1)n - j$ given by the above inequalities, the result is true for every α such that $1 \le \alpha < q-1$. When $\alpha = q-1$, $\alpha z_1 - (\alpha-1)n - j$ appears in Table 5.4 only when $\mu \neq 2$ and $\alpha z_1 - (\alpha-1)n - j = q^{2\mu-2} + q^{2\mu-3}$, that is, $j = j_1$.

Hence, from Equality (5.1.12) we have $s_{\beta(n-z_1)+j} = 0$ for $0 \le \beta \le q-1$ and $0 < j < n - z_1$, except when $\beta = q-1$, $j = j_1$ and $\mu \neq 2$. In such a case, Equality (5.1.12) is

$$s_{(q-1)(n-z_1)+j_1} = -((q-1)(n-z_1) + j_1)c_{(q-1)z_1-(q-2)n-j_1},$$

and the right hand side vanishes because of the characteristic of the field. This proves Assertion (5.1.11).

Now, when $0 < j < j_1$, it holds that

$$q^{2\mu-3} + 1 < qz_1 - (q-1)n - j < q^{2\mu-2} + q,$$

and again $qz_1 - (q-1)n - j$ appears in Table 5.4 only when $\mu \neq 2$ and $qz_1 - (q-1)n - j = q^{2\mu-3} + q^{2\mu-4}$, that is, $j = j_1 - q^{2\mu-4} + 1$. Reasoning as before, we get $s_{q(n-z_1)+j} = 0$ for all $0 < j < j_1$.

Finally, when $j = j_1$, then $qz_1 - (q-1)n - j_1 = q^{2\mu-3} + 1$ and

$$c_{qz_1-(q-1)n-j_1} = \begin{cases} 0 & \text{if } \mu \neq 2 \\ 1 & \text{if } \mu = 2. \end{cases}$$

If $\mu \neq 2$, then $j_1 < n - z_1$ and we can apply the results above. From Equality (5.1.12) we get

$$s_{q(n-z_1)+j_1} + c_{(q-1)z_1-(q-2)n-j_1} s_{n-z_1} = 0,$$

giving rise to the equality $s_{q(n-z_1)+j_1} = -1$ (note that when q is even, $1 = -1$). Otherwise, when $\mu = 2$, $j_1 = n - z_1$ and $q(n-z_1) + j_1 = (q+1)(n-z_1)$. Then, Lemma 5.1.13 proves

$$s_{(q+1)(n-z_1)} + c_{z_1} s_{q(n-z_1)} + c_{qz_1-(q-1)n} s_{n-z_1} = -(n-b)c_b. \tag{5.1.13}$$

Here, the last summand of the left hand side of Equality (5.1.13) equals one and the right hand side is also equal to one. Therefore, in this case,

$$s_{(q+1)(n-z_1)} = -s_{q(n-z_1)} = \begin{cases} -1 & \text{if } q \text{ is odd} \\ 1 & \text{if } q \text{ is even.} \end{cases}$$

We have proved that the set $\Gamma = \{\ell(n-z_1)\}_{\ell=1}^{q} \cup \{q(n-z_1) + j_1\}$ *is the set of indices* $r \le q(n-z_1) + j_1$ *such that* $s_r \neq 0$.

Step B.3. To conclude, we show that if $q(n-z_1) + j_1 < r \le n$, *then* $s_r = 0$ *except when* $q = \mu = 2$, *in which case* $s_n \neq 0$.

Suppose that $q = \mu = 2$ does not hold. In this case, $r = q(n-z_1) + j$ where

$$q^{2\mu-2} - q^{2\mu-3} + q - 1 = j_1 < j \le n - q(n-z_1) = q^{2\mu-2} + q, \tag{5.1.14}$$

and by Lemma 5.1.8, the following equality

$$\begin{aligned} &c_n s_{q(n-z_1)+j} + c_{n-j+j_1} s_{q(n-z_1)+j_1} + c_{n-j} s_{q(n-z_1)} + c_{z_1-j} s_{(q-1)(n-z_1)} \\ &+ c_{2z_1-n-j} s_{(q-2)(n-z_1)} + \cdots + c_{(q-1)z_1-(q-2)n-j} s_{n-z_1} = -(q(n-z_1)+j) c_{n-q(n-z_1)-j} \end{aligned} \quad (5.1.15)$$

holds.

From the inequalities in (5.1.14), we deduce

$$q^{2\mu-1} + q^{2\mu-3} - q + 1 > n - j \geq q^{2\mu-1} - q,$$

and then, $c_{n-j} \neq 0$ if and only if $n - j = z_1$. Moreover,

$$q^{2\mu-1} + q^{2\mu-2} > n - j + j_1 \geq q^{2\mu-1} + q^{2\mu-2} - (q^{2\mu-3} + 1) > z_1,$$

which proves $c_{n-j+j_1} = 0$.

Recalling Lemma 5.1.13, for $1 \leq \alpha \leq q$, the following chain of inequalities holds:

$$(q-\alpha)q^{2\mu-2} + q^{2\mu-3} - q + (\alpha+1) > \alpha z_1 - (\alpha-1)n - j \geq (q-\alpha)q^{2\mu-2} - q + \alpha.$$

Looking at the q-adic expansions of the bounds on $\alpha z_1 - (\alpha-1)n - j$ given by the above inequalities, one deduces that, when $1 \leq \alpha < q$, the coefficient of $q^{2\mu-2}$ in the q-adic expansion of $\alpha z_1 - (\alpha-1)n - j$ admits three possibilities: it is different from 0 and 1, it is 0 in which case the coefficient $q-1$ appears in the before mentioned q-adic expansion, or it is 1 but its contiguous term in the q-adic expansion is not 1. This proves that $c_{\alpha z_1-(\alpha-1)n-j} = 0$ for all $1 \leq \alpha < q$.

If $n - j \neq z_1$, then the left hand side of Equality (5.1.15) is equal to $s_{q(n-z_1)n+j}$. If the right hand side of Equality (5.1.15) is not a multiple of q, then neither $n - q(n-z_1) - j$ is and one could get $c_{n-q(n-z_1)-j} \neq 0$ only when $n - q(n-z_1) - j$ equals z_1 or b. The first situation cannot hold because $n - q(n-z_1) - j < q^{2\mu-3} + 1 < z_1$ and the second one contradicts the fact $n - j \neq z_1$. Therefore, $s_{q(n-z_1)n+j}$ vanishes for all index j as above.

Otherwise, if $n - j = z_1$, one gets

$$s_{(q+1)(n-z_1)} + c_{z_1} s_{q(n-z_1)} = -(n-b)c_b$$

and then, $s_{(q+1)(n-z_1)} = 0$.

The only remaining case is $q = \mu = 2$. Then, $n = 12$, $z_1 = 9$, $j_1 = 3$ and $\Gamma = \{\ell(n-z_1)\}_{\ell=1}^{q+1} = \{3, 6, 9\}$ is the set of indices $r \leq q(n-z_1) + j_1 = 9$ such that $s_r \neq 0$. Now, Equality (5.1.15) is

$$s_{6+j} + c_{15-j} s_9 + c_{12-j} s_6 + c_{9-j} s_3 = -(6+j)c_{6-j},$$

and, then, one deduces the equalities $s_{10} = s_{11} = 0$ and $s_{12} = 1$.

This concludes the proof of this case $t = 1$ and that of Theorem 5.1.9. □

With the above ingredients, we are ready to provide the parameters of Hermitian self-orthogonal codes of the type $\mathcal{C}_\Delta^T$, defined in the previous Subsection 5.1.2.

Theorem 5.1.14. *Let q be a prime power. Consider the polynomial $\mathrm{Tr}(X) = \mathrm{Tr}_b(X)$, where $b = 1 + q^t$ with $0 < t \le \mu$, μ being a positive integer. Assume that $(q, \mu, b) \neq (2, 2, 3)$ is a triple satisfying Property (5.1.1). Define $A(q,t)$ as follows:*

$$A(q,t) := \begin{cases} q^\mu - \lceil \frac{q-1}{2} \rceil q^{\mu-1} - \lceil \frac{q-1}{2} \rceil q^{\mu-t-1} - 2 & \text{if } 0 < t \le \frac{\mu}{2}, \\ q^\mu - \lceil \frac{q-1}{2} \rceil q^{\mu-1} - \lceil \frac{q-1}{2} \rceil q^{t-1} - 2 & \text{if } \frac{\mu}{2} < t < \mu, \\ q^{\mu-1} - 2 & \text{if } t = \mu, \end{cases}$$

whenever $q \neq 2$, and

$$A(q,t) := \begin{cases} 2^\mu - 2^{t-1} - 2 & \text{when } q = 2 \text{ and } t < \mu, \\ 2^{\mu-1} - 2 & \text{when } q = 2 \text{ and } t = \mu. \end{cases}$$

For any nonnegative integer τ, define $\Delta(\tau) := \{e \in \mathbb{Z} \mid 0 \le e \le \tau\}$. Then, if $\tau \le A(q,t)$, the linear code $\mathcal{C}^T_{\Delta(\tau)}$, over $\mathbb{F}_{q^{2\mu}}$, has length $n = q^{2\mu-t-1} + q^{2\mu-1}$ and satisfies:

i) *It is Hermitian self-orthogonal, that is*

$$\mathcal{C}^T_{\Delta(\tau)} \subseteq \left(\mathcal{C}^T_{\Delta(\tau)}\right)^{\perp_h}.$$

ii) *Its dimension is $\tau + 1$ and the minimum distance of $\left(\mathcal{C}^T_{\Delta(\tau)}\right)^{\perp_h}$ is larger than or equal to $\tau + 2$.*

Proof. We first carry out the proof in the case $t \neq \mu$.

By Proposition 5.1.3, $n = q^{2\mu-t-1} + q^{2\mu-1}$ is the length of the code $\mathcal{C}^T_{\Delta(\tau)}$. With the above notation, to show Item **i)**, we have to prove that $\mathrm{ev}_T(X^e) \cdot_h \mathrm{ev}_T(X^{e'}) = 0$ whenever $e, e' \le A(q,t)$. Now

$$\mathrm{ev}_T(X^e) \cdot_h \mathrm{ev}_T(X^{e'}) = \sum_{j=1}^{n} \beta_j^{e+q^\mu e'} = s_{e+q^\mu e'}.$$

Define $\mathcal{I} := \{i \mid 1 \le i < q^{2\mu} \text{ and } s_i \neq 0\}$. With the notation as in Theorem 5.1.9, set

$$\mathcal{I}_1 = \{i_0, i_1\} \cup \{i_{2,0}, i_{2,1}, \ldots, i_{2,q^*}\},$$

where $q^* = q - 3$ if $t \neq 1$ and $q^* = q - 2$ otherwise. Theorem 5.1.9 shows that

$$\mathcal{I}_1 = \{i \mid 1 \le i \le n \text{ and } s_i \neq 0\}$$

and, clearly, $\mathcal{I}_1 \subseteq \mathcal{I}$.

To prove Item **i)**, we are going to determine a set $\mathcal{J} \supseteq \mathcal{I}$ of candidates i to satisfy $s_i \neq 0$. Since we have obtained the indices $r \le n$ such that $s_r \neq 0$, we look for indices $r > n$ with this last property. Applying the second part of Lemma 5.1.8, we get

$$c_n s_r + c_{n-1} s_{r-1} + \cdots + c_0 s_{r-n} = 0,$$

so the indices $r > n$ such that $s_r \neq 0$ fulfill $r - n = \beta - \alpha$ for some α and β such that $c_\alpha \neq 0$ and $s_\beta \neq 0$. Otherwise, $s_r = 0$ by the above formula. Therefore, for obtaining our

set of candidates $\mathcal{J}$, we have to consider the elements in $\mathcal{I}_1$ and append those indices r iteratively obtained by the formula $\beta-\alpha+n$, where β is some previously obtained element in $\mathcal{J}$ (i.e., β is in $\mathcal{I}_1$ or it is a new candidate given by the procedure we are describing) and α is one of the indices (different from n) appearing in Table 5.4.

The q-adic expansion of the indices in $\mathcal{I}_1$ (with the exception of the last one when $t = 1$) can be obtained as follows: $i_0 = (q^{2\mu-1} - 1) - (q-1)q^{2\mu-1-t}$ and then, all the coefficients in its q-adic expansion are $q-1$ with the exception of those of $q^{2\mu-1}$ and $q^{2\mu-1-t}$, which are zero. The remaining values $i_1, i_{2,0}, \ldots, i_{2,q-3}$ are obtained from the previous one by adding $q^{2\mu-1-t} - q^{t-1}$. Thus the coefficients in the q-adic expansion of the elements in $\mathcal{I}_1$ successively decrease one unit with respect to q^{t-1} and increase one unit with respect to $q^{2\mu-1-t}$. See the forthcoming Table 5.8, where we give the q-adic expansions of the above indices and of an index j_0 which will be used later. Each q-adic expansion starts in the first part of the table and continues in the corresponding line of the second one.

Now we consider the q^μ-adic expansion of each index $i \in \mathcal{J}$. It is expressed as

$$i = i(0) + i(1)q^\mu,$$

with $i(0)$ and $i(1)$ nonnegative integers lower than q^μ.

We only need to prove that

$$\text{if } e, e' \le A(q,t), \text{ then } e + e'q^\mu \notin \mathcal{J}. \tag{5.1.16}$$

For the following reasoning, see Table 5.8. *Assume $t \neq \mu$ and $q \neq 2$.*

$(z)_q$ \ q^ℓ	q^0	q^1	$\cdots$	q^{t-1}	q^t	$\cdots$	$q^{\mu-t-1}$	$q^{\mu-t}$	$\cdots$	$q^{\mu-2}$	$q^{\mu-1}$	$\to$
$(i_0)_q$	$q-1$	$q-1$	$\ldots$	$q-1$	$q-1$	$\ldots$	$q-1$	$q-1$	$\ldots$	$q-1$	$q-1$	
$(i_1)_q$	$q-1$	$q-1$	$\ldots$	$q-2$	$q-1$	$\ldots$	$q-1$	$q-1$	$\ldots$	$q-1$	$q-1$	
$\vdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$	$\vdots$	
$(i_{2,q-3})_q$	$q-1$	$q-1$	$\ldots$	0	$q-1$	$\ldots$	$q-1$	$q-1$	$\ldots$	$q-1$	$q-1$	
$(j_0)_q$	$q-1$	$q-1$	$\ldots$	$q-1$	$q-1$	$\ldots$	$\lfloor\frac{q-1}{2}\rfloor$	$q-1$	$\ldots$	$q-1$	$\lfloor\frac{q-1}{2}\rfloor$	

$\to$	q^μ	$q^{\mu+1}$	$\cdots$	$q^{\mu+t-1}$	$q^{\mu+t}$	$\cdots$	$q^{2\mu-t-1}$	$q^{2\mu-t}$	$\cdots$	$q^{2\mu-2}$	$q^{2\mu-1}$
	$q-1$	$q-1$	$\ldots$	$q-1$	$q-1$	$\ldots$	0	$q-1$	$\ldots$	$q-1$	0
	$q-1$	$q-1$	$\ldots$	$q-1$	$q-1$	$\ldots$	1	$q-1$	$\ldots$	$q-1$	0
	$\vdots$	$\vdots$	$\cdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$	$\vdots$
	$q-1$	$q-1$	$\ldots$	$q-1$	$q-1$	$\ldots$	$q-1$	$q-1$	$\ldots$	$q-1$	0
	$q-1$	$q-1$	$\ldots$	$q-1$	$q-1$	$\ldots$	$\lfloor\frac{q-1}{2}\rfloor$	$q-1$	$\ldots$	$q-1$	$\lfloor\frac{q-1}{2}\rfloor$

Table 5.8: q-adic expansions of the candidates in $\mathcal{I}_1$ and j_0 when $1 < t \le \frac{\mu}{2}$ within the proof of Theorem 5.1.14

Notice that, as said, $i_0(1), i_1(1)$ and $i_{2,\ell}(1)$, $0 \le \ell \le q-3$, are positive integers lower than $q^{\mu-1}$. To obtain the values in $\mathcal{J}$, we have to add $n = q^{2\mu-1} + q^{2\mu-1-t}$ to every previous

value in $\mathcal{J}$ and subtract an index different from n appearing in Table 5.4. In addition, in each step, we start with an index β with q^μ-adic expansion $i(0)+i(1)q^\mu$ to get the q^μ-adic expansion of the next one: $j(0)+j(1)q^\mu = \beta-\alpha+n$, where $j(1) > i(1)$ and $j(0) \le i(0)$.

Suppose now that $1 \le t \le \frac{\mu}{2}$. Our first step is to define a bound $A'(q,t) \ge A(q,t)$, that eases the understanding of the definition of $A(q,t)$. We desire that every $i \in \mathcal{J}$ fulfills the following statement:

$$\text{if } \min\{i(0),i(1)\} \le A'(q,t), \text{ then } \max\{i(0),i(1)\} > A'(q,t),$$

because then Statement (5.1.16) is proved for $A'(q,t)$ instead of $A(q,t)$ (and therefore for $A(q,t)$) and thus Theorem 5.1.14 i) holds. The reason for choosing $A(q,t)$ is that, as we will see next, the expression of $A'(q,t)$ differs depending on whether or not $q-1$ is even.

The bound $A'(q,t) = \sum_{v=0}^{q^{\mu-1}} A'_v q^v$ is given by $\min\{\max\{i(0),i(1) \mid i \in \mathcal{J}\}-1$. To get this minimum, the elements $i \in \mathcal{J}$ to be considered are of the form:

$$i = i' + xn - x\alpha, \tag{5.1.17}$$

$i' \in \mathcal{J}$, $\alpha = q^{\mu-1}+q^{\mu-t-1}$ or $\alpha = q^{\mu-1}+q^{\mu+t-1}$ and $x < q$ is a positive integer such that, in the expression $|i(0)-i(1)| = \sum_{v=0}^{q^{\mu-1}} h_v q^v$, $h_{q^{\mu-1}}$ is either 0 (if $q-1$ is even) or 1 (if $q-1$ is odd). When looking for such a bound, one should not consider candidates given by values $i' \in \mathcal{J}\backslash\mathcal{I}_1 \cup \{i_{2,q-2}\}$; this is because the coefficient of $q^{2\mu-1}$ in its q-adic expansion is positive and increases if one adds n, giving rise to a greater value $\max\{i(0),i(1)\}$ than when starting with elements i' in $\mathcal{I}_1\backslash\{i_{2,q-2}\}$.

Then, to get the bound $A'(q,t)$, one must keep in mind those elements $i \in \mathcal{J}$ described in Equality (5.1.17) with $i' \in \mathcal{I}_1\backslash\{i_{2,q-2}\}$ and consider the element i whose value $\max\{i(0),i(1)\}$ is a minimum. Taking into account that the coefficients of $q^{\mu-1}$ and $q^{2\mu-1}$ in the q-adic expansion of every element in $\mathcal{I}_1\backslash\{i_{2,q-2}\}$ are, respectively, $q-1$ and 0, we get $A'_{q^{\mu-1}} = \frac{q-1}{2}$ when $q-1$ is even and $A'_{q^{\mu-1}} = \lceil \frac{q-1}{2} \rceil$, otherwise.

As a consequence, the inclusion in our Item **i)** holds if one considers the value $A(q,t) := \min S - 1$, where

$$S = \Bigg\{ j(0) \mid j(0) = j(1),\ j(0) = \sum_{v=0}^{q^{\mu-1}-1} j(0)_v q^v + \left\lfloor \frac{q-1}{2} \right\rfloor q^{\mu-1},$$
$$j = i + xn - y(q^{\mu-1}+q^{\mu-t-1}) \text{ or } j = i + xn - y(q^{\mu-1}+q^{\mu+t-1}),$$
$$i \in \mathcal{I}_1\backslash\{i_{2,q-2}\},\ x,y \text{ positive integers} \Bigg\}.$$

Then, $A(q,t) = j_0(0) - 1$, where

$$j_0 = i_0 + \left\lfloor \frac{q-1}{2} \right\rfloor n - \left\lceil \frac{q-1}{2} \right\rceil \left(q^{\mu-t-1}+q^{\mu-1}\right),$$

see Table 5.8, and notice that we need $i = i_0$ to obtain $j(0) = j(1)$. This proves the corresponding case in the statement. It is worthwile to add that $A'(q,t) = A(q,t)$ only when $q-1$ is even.

When $\frac{\mu}{2} < t < \mu$, then $\mu - t - 1 < t - 1$ and we can reason similarly, but to get the value j_0' playing the same role as j_0, instead of i_0, we have to use the value i_0' in $\mathcal{I}_1$ whose q-adic expansion has $\lceil \frac{q-1}{2} \rceil$ as a coefficient for $q^{2\mu-t-1}$. That is, i_0' is $i_{2,\lceil \frac{q-1}{2} \rceil - 2}$ when $q \geq 4$ and $i_0' = i_1$ otherwise ($q = 3$). Then we have to consider

$$j_0' = i_0' + \left\lfloor \frac{q-1}{2} \right\rfloor n - \left\lceil \frac{q-1}{2} \right\rceil \left(q^{\mu-1} + q^{\mu+t-1}\right)$$

to deduce that $A(q,t) = j_0'(0) - 1$.

The cases $t = \mu$ *and* $q = 2$ follow by computing

$$A(q,t) = \min\{\max\{i(0), i(1)\}, i \in \mathcal{J}\} - 1 = i_1(0) - 1.$$

Now, we show Item **ii)**. The dimension of $\mathcal{C}^T_{\Delta(\tau)}$ is $\tau + 1$ because ev_T is injective; in fact it is given by a Vandermonde matrix over $\mathbb{F}_{q^{2\mu}}$ of rank $\tau + 1$. Finally, the assertion about the minimum distance of $\left(\mathcal{C}^T_{\Delta(\tau)}\right)^{\perp_h}$ follows from the following two facts: The above mentioned matrix is also a parity-check matrix of the code $\left(\mathcal{C}^T_{\Delta(\tau)}\right)^{\perp_e}$, and then its minimum distance is at least $\tau + 2$, and this last code is isometric to $\left(\mathcal{C}^T_{\Delta(\tau)}\right)^{\perp_h}$, since $\left(\mathcal{C}^T_{\Delta(\tau)}\right)^{\perp_h} = \left(\left(\mathcal{C}^T_{\Delta(\tau)}\right)^{\perp_e}\right)^{q^\mu}$. □

By Corollary 2.3.8, we get the following immediate consequence of Theorem 5.1.14.

Corollary 5.1.15. *Let* q *be a prime power. Assume that* (q, μ, b) *is a triple satisfying Property (5.1.1). With notation as in Theorem 5.1.14, for each non-negative integer* $\tau \leq A(q,t)$*, there is a stabilizer quantum code with parameters*

$$[[q^{2\mu-1-t} + q^{2\mu-1}, q^{2\mu-1-t} + q^{2\mu-1} - 2\tau - 2, \geq \tau + 2]]_{q^\mu}.$$

5.2. Subfield-subcodes of evaluation codes at the roots of trace-depending polynomials

In this section we show that, considering subfield-subcodes of the above described codes, one obtains $q^{\mu'}$-ary stabilizer codes, where $\mu' < \mu$ and μ' divides μ. Some of these codes have excellent parameters as we will explain in Section 5.3.

For a start and in order to bound the parameters of the codes we are interested in, we need to define another family of related evaluation codes which will be useful in the forthcoming Proposition 5.2.2. Denote by $U = \mathbb{F}_{q^{2\mu}} \backslash \{0\} = \left\{\alpha_1, \alpha_2, \ldots, \alpha_{q^{2\mu}-1}\right\}$ the set of non-zero elements of the finite field $\mathbb{F}_{q^{2\mu}}$. Consider the map

$$\mathrm{ev}_U : \mathcal{R}_0 \left(= \mathbb{F}_{q^{2\mu}}[X]/\langle X^{q^{2\mu}-1} - 1\rangle\right) \to \mathbb{F}_{q^{2\mu}}^{q^{2\mu}-1}, \quad \mathrm{ev}_U(f) = (f(\alpha_1), \ldots, f(\alpha_{q^{2\mu}-1})),$$

f being the polynomial function defined by the class of a polynomial (also named f) of $\mathbb{F}_{q^{2\mu}}[X]$ in $\mathcal{R}_0$. It is similar to the map ev_T given in Subsection 5.1.2.

Fix a positive integer $\mu' < \mu$ such that μ' divides μ. Following Subsection 1.5.1, write $E_0 := \{0, 1, \ldots, q^{2\mu} - 2\}$ regarded as a set of representatives of the quotient ring

$\mathbb{Z}/\left(q^{2\mu}-1\right)\mathbb{Z}$, where we consider minimal closed sets with respect to $q^{2\mu'}$. Recall that these sets are denoted by $\Lambda_a := \{q^{2\mu' i}a \mid i \geq 0\}$, where $a \in \mathcal{A} := \{a_0 < a_1 < \cdots < a_\nu\} \subseteq E_0$, $\mathcal{A}$ being the ordered set of minimum elements of minimal closed sets.

Let Γ be a nonempty subset of E_0, using the map ev_U, we define the evaluation code $\mathcal{C}_\Gamma^U$ as the linear code, over the field $\mathbb{F}_{q^{2\mu}}$, generated by the set $\{\mathrm{ev}_U(X^e) \mid e \in \Gamma\}$. Notice that it is a univariate $\{1\}$-affine variety code. Within this framework, the subfield-subcode of $\mathcal{C}_\Gamma^U$ over the field $\mathbb{F}_{q^{2\mu'}}$ is

$$\mathcal{S}_\Gamma^U := \mathcal{C}_\Gamma^U \cap \left(\mathbb{F}_{q^{2\mu'}}\right)^{q^{2\mu}-1}.$$

In order to bound the minimum distance by considering the BCH approach, we are only interested in sets Γ which are union of minimal closed sets whose minimum elements start at a_0 and are consecutive. That is, fix a positive integer $\tau < \nu$ and set

$$\Gamma(\tau) := \Lambda_{a_0} \cup \Lambda_{a_1} \cup \cdots \cup \Lambda_{a_\tau}.$$

Then, by Proposition 1.5.9 and the fact that Euclidean and Hermitian dual of our codes are isometric (see the end of the proof of Theorem 5.1.14), one gets the following result:

Proposition 5.2.1. *With the above notation, the following BCH-type bound holds:*

$$\mathrm{d}\left(\left(\mathcal{S}_{\Gamma(\tau)}^U\right)^{\perp_h}\right) \geq a_{\tau+1}+1.$$

Now we return to consider the family of evaluation codes defined in Subsection 5.1.2, where the map ev_T is used. Keeping the notation as in that subsection, we define the subfield-subcode over the field $\mathbb{F}_{q^{2\mu'}}$ of the code $\mathcal{C}_\Delta^T$ as

$$\mathcal{S}_\Delta^T := \mathcal{C}_\Delta^T \cap \mathbb{F}_{q^{2\mu'}}^n.$$

Recall that $E = \{0, 1, \ldots, n-1\}$ and pick a_τ. Consider the set $\Gamma(\tau)$; these values are initially regarded as powers of monomials generating a linear space of elements in the quotient ring $\mathcal{R}_0$, but, since we desire to use the map ev_T, we must consider their classes modulo the ideal $\langle \mathrm{Tr}(X)\rangle$ and, when considered as elements in $\mathcal{R} = \mathbb{F}_{q^{2\mu}}[X]/\langle \mathrm{Tr}(X)\rangle$, they provide generators of the form X^e, $e \in \Gamma(\tau)^E$, of a linear space which can be evaluated by ev_T. Notice that $\Gamma(\tau)^E$ is a suitable set of indices included in E. Then, reasoning as in the proof of [50, Theorem 13], the following result follows. It is a remarkable fact that the bound given in Proposition 5.2.1 is inherited by $\left(\mathcal{S}_{\Gamma(\tau)^E}^T\right)^{\perp_h}$, although it is not a direct consequence of the relation between both codes.

Proposition 5.2.2. *The dimension and minimum distance of the subfield-subcode $\mathcal{S}_{\Gamma(\tau)^E}^T$ over the field $\mathbb{F}_{q^{2\mu'}}$ and its Hermitian dual satisfy:*

1. $\dim\left(\mathcal{S}_{\Gamma(\tau)^E}^T\right) \leq \sum_{\ell=0}^{\tau} \#\Lambda_{a_\ell}$.
2. $\mathrm{d}\left(\left(\mathcal{S}_{\Gamma(\tau)^E}^T\right)^{\perp_h}\right) \geq a_{\tau+1}+1$.

We conclude this subsection by providing parameters of $q^{\mu'}$-ary stabilizer quantum codes, derived from the codes in Proposition 5.2.2.

Theorem 5.2.3. *Let q be a prime power and $(q,\mu,b) \neq (2,2,3)$, $b = 1+q^t$ and $0 < t \leq \mu$, a triple satisfying Property (5.1.1). Fix a positive integer $\mu' < \mu$ such that μ' divides μ. Set $\mathcal{A} := \{a_0 < a_1 < \cdots < a_\nu\} \subset E_0 := \{0,1,\ldots,q^{2\mu}-2\}$ the ordered set of minimum elements of minimal closed sets, corresponding to the quotient ring $\mathbb{Z}/\left(q^{2\mu}-1\right)\mathbb{Z}$, with respect to $q^{2\mu'}$. Consider the value $A(q,t)$ introduced in Theorem 5.1.14 and the following values:*

$$B(q,t) := q^\mu - (q-1)q^{\mu-t} - q, \quad B^1(q,t) := q^\mu - (q-1)q^{\mu-t} - 2$$

and $C(q,t) := (q^{2\mu-2}-1)/(q^{\mu-2}+1)$.

Define $D(q,t)$ as follows:

- *When $t > 1$,*
  - *$D(q,t) := A(q,t)$, whenever $\mu' \neq 1$.*
  - *Otherwise ($\mu' = 1$):*

$$D(Q,t) := \begin{cases} B(Q,t) & \text{if } \mu \text{ is even,} \\ \min\{A(Q,t), B(Q,t)\} & \text{otherwise.} \end{cases}$$

- *When $t = 1$ and $\mu \neq 2$,*
  - *$D(q,t) := A(q,t)$, whenever $\mu' > 2$,*
  - *$D(q,t) := C(q,t)$, whenever $\mu' = 2$,*
  - *$D(q,t) := B^1(q,t)$, otherwise ($\mu' = 1$).*
- *When $t = 1$ and $\mu = 2$, $D(q,t) := q-2$.*

Then, for each element $a_\tau \in \mathcal{A}$ such that $a_\tau \leq D(q,t)$, the subfield-subcode $\mathcal{S}^T_{\Gamma(\tau)^E}$ over the field $\mathbb{F}_{q^{2\mu'}}$ is Hermitian self-orthogonal and, as a consequence, there exists a stabilizer quantum code with parameters

$$\left[\left[q^{2\mu-1-t}+q^{2\mu-1}, \geq q^{2\mu-1-t}+q^{2\mu-1}-2\sum_{\ell=0}^{\tau}\#\Lambda_{a_\ell}, \geq a_{\tau+1}+1\right]\right]_{q^{\mu'}}.$$

Proof. Our proof follows a close reasoning to that used when proving [50, Theorem 15], although we consider subfield-subcodes over $\mathbb{F}_{q^{2\mu'}}$ instead of over $\mathbb{F}_{q^2}$. Consider the basis $\mathcal{B}$ of $\mathcal{C}^U_{\Gamma(\tau)}$ introduced in the proof of [50, Proposition 11] and, reasoning as at the beginning of the proof of [50, Theorem 15], it suffices to prove that

$$\mathrm{ev}_T\left(X^{eq^{2\mu'\ell}+e'q^{\mu'}q^{2\mu'm}}\right) \cdot_e \mathrm{ev}_T\left(X^0\right) = 0,$$

for values $\ell, m \in \{0,1,\ldots,\frac{\mu}{\mu'}-1\}$, $m \geq \ell$ and $e, e' \in \{a_0, a_1, \ldots, a_\tau\}$.

When $\mu'(2m-2\ell+1) \leq \mu$, it holds that

$$\mathrm{ev}_T\left(X^{eq^{2\mu'\ell}+e'q^{\mu'}q^{2\mu'm}}\right) \cdot_e \mathrm{ev}_T\left(X^0\right) = \left[\mathrm{ev}_T\left(X^{e+e'q^{\mu'(2m-2\ell+1)}}\right) \cdot_e \mathrm{ev}_T\left(X^0\right)\right]^{q^{2\mu'\ell}}.$$

Otherwise, $\mu < \mu'(2m-2\ell+1) \leq \mu'(\frac{2\mu}{\mu'}-1) = 2\mu-\mu' < 2\mu$. Therefore, one can set $2m-2\ell+1 = \frac{\mu}{\mu'}+s$, where $1 \leq s < \frac{\mu}{\mu'}$ and then

$$\begin{aligned}\mathrm{ev}_T\left(X^{eq^{2\mu'\ell}+e'q^{\mu'}q^{2\mu'm}}\right)\cdot_e \mathrm{ev}_T\left(X^0\right) &= \left[\mathrm{ev}_T\left(X^{e+e'q^{\mu+s\mu'}}\right)\cdot_e \mathrm{ev}_T\left(X^0\right)\right]^{q^{2\mu'\ell}} \\ &= \left(\left[\mathrm{ev}_T\left(X^{eq^{\mu-s\mu'}+e'}\right)\cdot_e \mathrm{ev}_T\left(X^0\right)\right]^{q^{\mu+s\mu'}}\right)^{q^{2\mu'\ell}}.\end{aligned}$$

Thus, one concludes that it suffices to prove that both products

$$\mathrm{ev}_T\left(X^{e+e'q^{\mu'r}}\right)\cdot_e \mathrm{ev}_T\left(X^0\right) \qquad \text{and} \qquad \mathrm{ev}_T\left(X^{eq^{\mu'r}+e'}\right)\cdot_e \mathrm{ev}_T\left(X^0\right)$$

vanish for all values $e, e' \leq D(q,t)$ and $\mu' r \leq \mu$. Then, since we give a common bound for e and e', it suffices to check that

$$\mathrm{ev}_T\left(X^{e+e'q^{\mu'r}}\right)\cdot_e \mathrm{ev}_T\left(X^0\right) = 0 \tag{5.2.1}$$

for $e, e' \leq D(q,t)$ and $0 \leq r \leq \frac{\mu}{\mu'}$.

Assume first that $t > 1$. Then $e+e'q^{\mu'r} < i_0 = q^{2\mu-1}-(q-1)q^{2\mu-1-t}-1$ when $\mu' r < \mu-1$ and Equality (5.2.1) holds by Theorem 5.1.9. Thus, one only has to check Equality (5.2.1) when $\mu' r = \mu$ or $\mu' r = \mu-1$. *Suppose first that* $\mu' \neq 1$, then the case $\mu' r = \mu-1$ does not happen because μ' divides μ. Then, $\mu' r = \mu$ and therefore, if $e, e' \leq A(q,t)$, Equality (5.2.1) is true because of the proof of Theorem 5.1.14 and our result is proved in this case. *Now, if* $\mu' = 1$, it suffices that $e, e' \leq A(q,t)$ to prove Equality (5.2.1) when $\mu' r = r = \mu$. Otherwise, $\mu' r = r = \mu-1$, and $e, e' \leq B(q,t)$ implies $e + e'q^{\mu-1} < i_0$. Noticing that $(B(q,t)+1)+(B(q,t)+1)q^{\mu-1} \geq i_0$, one deduces that Equality (5.2.1) is true whenever $e, e' \leq \min\{A(q,t), B(q,t)\}$. Note that if μ is even, $r = \mu$ means $2m-2\ell+1 = \mu$ by the reasoning at the beginning of the proof and this case cannot hold. Hence, when $t > 1$, $\mu' = 1$ and μ is even, the bound $D(q,t)$ equals $B(q,t)$.

To conclude the proof, *assume that* $t = 1$. First *suppose* $\mu \neq 2$. Then $i_0 = q^{2\mu-2}-1$ and $e + e'q^{\mu'r} < i_0$ when $\mu' r < \mu-2$. As above, to prove Equality (5.2.1) when $\mu' r = \mu$ it suffices to have that $e, e' \leq A(q,t)$. But one needs $e, e' \leq B^1(q,t)$ in case $\mu' r = \mu-1$ and $e, e' \leq C(q,t)$ whenever $\mu' r = \mu-2$ (notice that $C(q,t)(1+q^{\mu-2}) = i_0$ but $\lfloor C(q,t) \rfloor \neq C(q,t)$). We also notice that

$$B^1(q,t) < C(q,t).$$

Finally, since $\mu = \mu'\alpha$ for some positive integer α, $\mu' r = \mu-2 = \mu'\alpha-2$, then $2 = \mu'(\alpha-r)$, which happens only when either $\mu' = 1$ or $\mu' = 2$. Therefore, $D(q,t)$ equals $A(q,t)$ when $\mu' > 2$, it is $C(q,t)$ when $\mu' = 2$ and $B^1(q,t)$ in case $\mu' = 1$. *When* $\mu = 2$, then $\mu' = 1$ and $B^1(q,t) = q-2$. This concludes the proof. □

Remark 5.2.4. When the set of exponents of the polynomial $\mathrm{Tr}(X)$ is contained in $\Gamma(\tau)$, then $\dim\left(\mathcal{S}^T_{\Gamma(\tau)^E}\right) \leq \sum_{\ell=0}^{\tau} \#\Lambda_{a_\ell} - 1$ (because there is a relation modulo $\mathrm{Tr}(X)$ ($\mathrm{Tr}(X) = 0$), which decreases the dimension by one). Therefore, one gets a favourable situation since the bound on the dimension of the stabilizer quantum code given in Theorem 5.2.3 is increased by two.

5.3. Examples

In this section, we present some examples of stabilizer quantum codes obtained from our previous results. We only show those codes having good parameters, in particular the parameters of all codes in this section beat the quantum Gilbert-Varshamov bound (see Subsection 2.3.4) and, some of them, either are binary records or beat the parameters of others available in the literature. See the last but one paragraph above Proposition 2.2.8 to recall how propagation rules allow us to say when a code beats another one. Recall also that, by record, we mean a binary quantum code whose parameters either improve some given in [62] or correspond to an entry in [62] whose construction was missing.

5.3.1. Binary examples

With the notation as in Theorem 5.2.3, consider the triple $(q, \mu, b) = (2, 4, 5)$. We have that $t = 2$ and $a_0 = 0$, $a_1 = 1$, $a_2 = 2$, $a_3 = 3$, $a_4 = 5$, $a_5 = 6$, $a_6 = 7$, $a_7 = 9$, $a_8 = 10$, $a_9 = 11$ are minimum elements of minimal closed sets. Moreover the cardinality of the minimal closed sets Λ_{a_ℓ}, $1 \le \ell \le 8$, is always 4. Set $\mu' = 1$ and then $D(q,t) = B(q,t) = 10$. Applying Theorem 5.2.3 with $\tau = 8$ and noticing that the condition in Remark 5.2.4 holds, we obtain a $[[160, 96, \ge 12]]_2$ binary stabilizer quantum code, which beats the $[[160, 96, \ge 11]]_2$ code given in [62]. Thus, we have obtained a record as a binary quantum code. Now, using the subcode and length extension propagation rules (see Subsection 2.2.2) we find four new records. These are $[[160, 95, \ge 12]]_2$, $[[161, 96, \ge 12]]_2$, $[[162, 96, \ge 12]]_2$ and $[[163, 96, \ge 12]]_2$.

In the remaining of this chapter, we will also use the following result to construct stabilizer codes. This result was stated in [44] and it is an easy consequence of [73, Lemma 76] (see also [6]).

Theorem 5.3.1. *Let $\mathcal{C}$ be an $\mathbb{F}_{q^{2r}}$-linear code of length n and dimension k, where r is a positive integer. Suppose $\mathcal{C} \subseteq \mathcal{C}^{\perp_h}$, where*

$$\mathcal{C}^{\perp_h} := \left\{ \boldsymbol{x} \in \left(\mathbb{F}_{q^{2r}}\right)^n \mid \boldsymbol{x} \cdot_h \boldsymbol{y} = \sum_{i=1}^{n} x_i y_i^{q^r} = 0 \text{ for all } \boldsymbol{y} \text{ in } \mathcal{C} \right\}.$$

Then, there exists an $\mathbb{F}_q$-stabilizer quantum code with parameters

$$\left[\left[rn, rn - 2rk, \ge d^{\perp_h}\right]\right]_q,$$

where $d^{\perp_h}$ is the minimum distance of the code $\mathcal{C}^{\perp_h}$.

With the same previous triple $(q, \mu, b) = (2, 4, 5)$, using Theorem 5.1.14 and sets $\Delta(i)$, $0 \le i \le 12$ ($A(q,t) = 12$), one obtains Hermitian self-orthogonal codes $\mathcal{C}^T_{\Delta(i)}$. By applying Theorem 5.3.1 to these codes, one gets binary stabilizer quantum error-correcting codes of length $n = 640$ whose parameters are displayed in Table 5.9.

We can also combine our procedures and starting from our initial linear codes over $\mathbb{F}_{2^8}$, we consider subfield-subcodes over $\mathbb{F}_{2^4}$. These codes use sets Δ which are successive union of consecutive minimal closed sets Λ'_i, $0 \le i \le 12$, with respect to 2^4. That is

k	624	616	608	600	592	584	576	568	560	552	544	536
$d \geq$	3	4	5	6	7	8	9	10	11	12	13	14

Table 5.9: Parameters of binary stabilizer quantum codes of length 640

$\Lambda_0' = \{0\}$, $\Lambda_1' = \{1, 16\}$, $\Lambda_2' = \{2, 32\}$, $\Lambda_3' = \{3, 48\}$, $\Lambda_4' = \{4, 64\}$, $\Lambda_5' = \{5, 80\}$, $\Lambda_6' = \{6, 96\}$, $\Lambda_7' = \{7, 112\}$, $\Lambda_8' = \{8, 128\}$, $\Lambda_9' = \{9, 144\}$, $\Lambda_{10}' = \{10, 160\}$, $\Lambda_{11}' = \{11, 176\}$, and $\Lambda_{12}' = \{12, 192\}$. In this way, using Theorem 5.2.3 with $\mu' = 2$, one obtains Hermitian self-orthogonal codes over $\mathbb{F}_{16}$. Note that $D(q,t) = 12$. Then, Theorem 5.3.1, applied to these codes, gives rise to binary stabilizer quantum error-correcting codes of length $n = 320$. Some of their parameters are displayed in Table 5.10.

k	308	300	292	284	276	268	260	252	244	236	228	220
$d \geq$	3	4	5	6	7	8	9	10	11	12	13	14

Table 5.10: Parameters of binary stabilizer quantum codes of length 320

Applying the last two procedures (both with $A(q,t) = 10$) to the triple $(q, \mu, b) = (2, 4, 9)$, we get binary stabilizer quantum error-correcting codes with parameters

$$[[576, 576 - 8(i+1), \geq i+2]]_2$$

with $1 \leq i \leq 10$, and of length $n = 288$ with parameters as in Table 5.11.

k	276	268	260	252	244	236	228	220	212	204
$d \geq$	3	4	5	6	7	8	9	10	11	12

Table 5.11: Parameters of binary stabilizer quantum codes of length 288

The lengths of the last four families of codes exceed those considered in [62]. We have not found binary quantum codes with these lengths in the literature, thus we may conclude that they are new.

5.3.2. Non-binary examples

We devote this subsection to provide parameters of non-binary stabilizer quantum error-correcting codes obtained with the same three procedures described in Subsection 5.3.1 for the binary case. Specifically, our codes come from applying either Theorem 5.2.3, or Theorem 5.1.14 and then Theorem 5.3.1, or Theorem 5.3.1 applied to subfield-subcodes of codes given by Theorem 5.2.3. Most of them are new and we have not found other codes for comparison, but some of them can be compared and beat some codes in the recent literature.

With the triple $(q, \mu, b) = (3, 2, 4)$, applying Theorem 5.1.14 and then Theorem 5.3.1, after noticing that $A(q,t) = 3$, we get ternary stabilizer quantum codes with parameters $[[72, 64, \geq 3]]_3$, $[[72, 60, \geq 4]]_3$ and $[[72, 56, \geq 5]]_3$.

Consider now the triple $(q,\mu,b) = (5,2,6)$ and apply Theorem 5.2.3 with $\mu' = 1$. The value $D(q,t)$ equals 3 and we obtain a 5-ary stabilizer quantum code with parameters $[[150,136,\geq 5]]_5$ beating the $[[150,134,\geq 5]]_5$ code given in [23]. With the help of Theorems 5.1.14 and 5.3.1, taking into account that $A(q,t) = 11$, we also obtain new 5-ary codes with length $n = 300$ and remaining parameters as given in Table 5.12.

k	292	288	284	280	276	272	268	264	260	256	252
$d \geq$	3	4	5	6	7	8	9	10	11	12	13

Table 5.12: Parameters of 5-ary stabilizer quantum codes of length 300

Using now the triple $(5,2,26)$ and applying Theorem 5.2.3 with $\mu' = 1$, since $B(q,t) = 16$, we get a family of stabilizer quantum codes with parameters

$$\{[[130, 130-2(2i+1), \geq 2+i]]_5\}_{i=1}^{9}.$$

Moreover, considering the triple $(q,\mu,b) = (7,2,8)$ and applying Theorem 5.2.3 with $\mu' = 1$, $D(q,t) = 5$ and we get 7-ary stabilizer quantum codes with parameters $[[392,378,\geq 5]]_7$, $[[392,374,\geq 6]]_7$ and $[[392,370,\geq 7]]_7$, beating the codes with parameters $[[392,376,\geq 5]]_7$, $[[392,372,\geq 6]]_7$ and $[[392,364,\geq 7]]_7$ given in [23] and the code with parameters $[[392,368,\geq 7]]_7$ given in [44]. With the same triple, applying Theorems 5.1.14 and 5.3.1, since $A(q,t) = 23$, we are able to obtain a family of 7-ary stabilizer quantum codes with parameters $[[784, 784-4(i+1), \geq i+2]]_7$, $1 \leq i \leq 23$.

Finally, if we take $(q,\mu,b) = (7,2,50)$ and apply Theorem 5.2.3 with $\mu' = 1$, we get $B(q,t) = 36$ and there is a family of stabilizer quantum codes with the following parameters: $\{[[350, 350-2(2i+1), \geq i+2]]_7\}_{i=1}^{15}$.

5.4. Sporadic stabilizer quantum codes from trace-depending polynomials

In this section, we show that excellent quantum codes can be obtained by evaluating at the zeros of trace-depending polynomials. We consider here trace-depending polynomials which are different from those studied in this chapter, and some of our assertions are supported in calculations made with the computational algebra system Magma [17]. It is an open question to develop a complete theory for studying this class of quantum error-correcting codes.

All the codes in this section are constructed as follows. Set $q = 2$, $\mu = 4$ and consider some new trace-depending polynomials $\mathrm{Tr}'(X)$ different from the above considered b-th trace-depending polynomials $\mathrm{Tr}_b(X)$. We have used [17] to check that our polynomials $\mathrm{Tr}'(X)$ have no multiple roots over the field $\mathbb{F}_{2^8}$. The number of roots of each $\mathrm{Tr}'(X)$, say m, is not required to be the degree of $\mathrm{Tr}'(X)$. Following the same notation and construction described in Section 5.2, we consider suitable sets $\Delta \subset E$, codes $\mathcal{C}_\Delta^{T'}$ obtained by evaluation under the map (5.1.2) -where $\mathrm{Tr}(X)$ is substituted by $\mathrm{Tr}'(X)$ and T by

the set T' of roots of $\mathrm{Tr}'(X)$- and subfield-subcodes $\mathcal{S}_\Delta^{T'} := \mathcal{C}_\Delta^{T'} \cap \mathbb{F}_{2^4}^m$ over the field $\mathbb{F}_{2^4}$. Proposition 5.2.2 determines bounds on the dimension and minimum distance of these codes. Using [17] again, we check that the codes $\mathcal{S}_\Delta^{T'}$ are Hermitian self-orthogonal. Finally, applying Theorem 5.3.1 we get binary stabilizer quantum codes.

Table 5.13 shows polynomials $\mathrm{Tr}'(X)$, sets Δ and parameters of the binary stabilizer quantum codes obtained, proving that, by selecting suitable trace-depending polynomials $\mathrm{Tr}'(X)$, the above procedure produces records with respect to [62]. Note that γ stands for a primitive element of the field $\mathbb{F}_{2^8}$ and $\mathrm{tr}_{2^\mu}(X)$ is the trace polynomial defined before Definition 5.1.1. We conclude by explaining that the sets Λ_i' that appear in Table 5.13 are some of the 16-ary minimal closed sets, over the set $E_0 = \{0, 1, \ldots, 254\}$, considered in Subsection 5.3.1.

$\mathrm{Tr}'(X)$	m	Δ	$[[n,k,d]]_2$
$1+\mathrm{tr}_{2^\mu}(\gamma^5 X^3)$	120	$\Delta_1 = \cup_{i=0}^{5}\Lambda_i'$	$[[240, 196, \geq 7]]_2$
$1+\mathrm{tr}_{2^\mu}(\gamma^5 X^3)$	120	$\Delta_2 = \cup_{i=0}^{6}\Lambda_i'$	$[[240, 188, \geq 8]]_2$
$1+\mathrm{tr}_{2^\mu}(\gamma^5 X^3)$	120	$\Delta_3 = \cup_{i=0}^{7}\Lambda_i'$	$[[240, 180, \geq 9]]_2$
$1+\mathrm{tr}_{2^\mu}(\gamma^5 X^3)$	120	$\Delta_4 = \cup_{i=0}^{8}\Lambda_i'$	$[[240, 172, \geq 10]]_2$
$1+\mathrm{tr}_{2^\mu}(\gamma^5 X^3)$	120	$\Delta_5 = \cup_{i=0}^{9}\Lambda_i'$	$[[240, 164, \geq 11]]_2$
$1+\mathrm{tr}_{2^\mu}(\gamma^5 X^3)$	120	$\Delta_6 = \cup_{i=0}^{10}\Lambda_i'$	$[[240, 156, \geq 12]]_2$
$1+\mathrm{tr}_{2^\mu}(\gamma^5 X^5)$	96	$\Delta_7 = \cup_{i=0}^{11}\Lambda_i'$	$[[192, 132, \geq 9]]_2$
$1+\mathrm{tr}_{2^\mu}(\gamma^5 X^5)$	96	$\Delta_8 = \cup_{i=0}^{8}\Lambda_i'$	$[[192, 124, \geq 10]]_2$
$1+\mathrm{tr}_{2^\mu}(\gamma X^{19}+X^{10})$	116	$\Delta_9 = \cup_{i=0}^{7}\Lambda_i'$	$[[232, 172, \geq 9]]_2$
$1+\mathrm{tr}_{2^\mu}(\gamma X^{19}+X^{10})$	116	$\Delta_{10} = \cup_{i=0}^{8}\Lambda_i'$	$[[232, 164, \geq 10]]_2$
$1+\mathrm{tr}_{2^\mu}(\gamma X^{19}+X^{10})$	116	$\Delta_{11} = \cup_{i=0}^{9}\Lambda_i'$	$[[232, 156, \geq 11]]_2$
$1+\mathrm{tr}_{2^\mu}(\gamma X^{19}+X^{10})$	116	$\Delta_{12} = \cup_{i=0}^{10}\Lambda_i'$	$[[232, 148, \geq 12]]_2$
$1+\mathrm{tr}_{2^\mu}(\gamma^3 X^9+X)$	112	$\Delta_{13} = \cup_{i=0}^{7}\Lambda_i'$	$[[224, 164, \geq 9]]_2$
$1+\mathrm{tr}_{2^\mu}(\gamma^3 X^9+X)$	112	$\Delta_{14} = \cup_{i=0}^{8}\Lambda_i'$	$[[224, 156, \geq 10]]_2$
$1+\mathrm{tr}_{2^\mu}(\gamma^3 X^9+X)$	112	$\Delta_{15} = \cup_{i=0}^{9}\Lambda_i'$	$[[224, 148, \geq 11]]_2$
$1+\mathrm{tr}_{2^\mu}(\gamma^8 X^{25}+X^{10})$	100	$\Delta_{16} = \cup_{i=0}^{7}\Lambda_i'$	$[[200, 140, \geq 9]]_2$
$1+\mathrm{tr}_{2^\mu}(\gamma^8 X^{25}+X^{10})$	112	$\Delta_{17} = \cup_{i=0}^{8}\Lambda_i'$	$[[200, 132, \geq 10]]_2$
$1+\mathrm{tr}_{2^\mu}(\gamma^{17} X^3+X^{13})$	104	$\Delta_{18} = \cup_{i=0}^{7}\Lambda_i'$	$[[208, 148, \geq 9]]_2$
$1+\mathrm{tr}_{2^\mu}(\gamma^{17} X^3+X^{13})$	104	$\Delta_{19} = \cup_{i=0}^{8}\Lambda_i'$	$[[208, 140, \geq 10]]_2$
$1+\mathrm{tr}_{2^\mu}(\gamma^{17} X^3+X^{13})$	104	$\Delta_{20} = \cup_{i=0}^{9}\Lambda_i'$	$[[208, 132, \geq 11]]_2$

Table 5.13: Sporadic binary stabilizer quantum error-correcting records

Part IV

Further research. Some advances

In this last part of the PhD thesis we provide some ideas for future research. We propose a problem and a conjectural answer from which we have some evidence; furthermore, it has been tested with a number of calculations.

Again, we desire to construct new stabilizer quantum codes from Hermitian self-orthogonal linear codes and their subfield-subcodes by using Corollary 2.3.8.

Let us give a sketch of what we propose. As we stated in the introduction, J-affine variety codes are codes well suited for our purpose. As a first step, we aim for the lengths of the linear codes we consider not to be obtainable with univariate $\{1\}$-affine variety codes (BCH codes). To achieve it, we plan to enlarge these codes by evaluating at further elements of the supporting field. As we will see in Equation (5.4.1), the (Hermitian) self-orthogonality conditions of such codes allow us to focus on certain projections which are also $\{1\}$-affine variety codes. Thus, as a second step, we also desire to improve the range of dimensions of self-orthogonal univariate $\{1\}$-affine variety codes given in [41] (see also [1]). As a consequence, these improvements will be inherited to the parameters of the resulting quantum codes.

Let us introduce the codes to be studied. Keep the notation for MCCs introduced in Section 1.3.1. Let q be a prime power and consider s, n_1, n_2 and λ positive integers such that s is even, $n_1 = (q^s+1)n_2$, $n_2 \mid q^s-1$ and $\lambda \leq \frac{q^{2s}-1}{n_1}$. Let $\gamma \in \mathbb{F}_{q^{2s}}$ be a primitive element of the field $\mathbb{F}_{q^{2s}}$ and $\zeta_{n_1} \in \mathbb{F}_{q^{2s}}$ be a primitive n_1-th root of unity. Our codes (that can be thought as univariate MCCs) are defined as

$$\mathcal{C}_\Delta^P := \langle \mathrm{ev}_P(X^e) \mid e \in \Delta \rangle = \mathrm{ev}_P(\langle X^e \mid e \in \Delta \rangle) \subseteq \mathbb{F}_{q^{2s}}^n$$

obtained from the evaluation map

$$\mathrm{ev}_P : \mathcal{R} = {}^{\mathbb{F}_{q^{2s}}[X]}\!/_I \to \mathbb{F}_{q^{2s}}^n, \qquad \mathrm{ev}_P(f) = (f(\alpha_1), \ldots, f(\alpha_n)),$$

where $I = \left\langle (X^{n_1}-1)(X^{n_1}-\gamma^{n_1})\cdots(X^{n_1}-\gamma^{(\lambda-1)n_1}) \right\rangle_{\mathbb{F}_{q^{2s}}}$, Δ is some subset of the set $\{0,1,\ldots,\lambda n_1-1\}$ which contains the possibilities of exponents of any monomial reduced modulo I and

$$P = \{\alpha_1, \ldots, \alpha_n\} = \left\{1, \zeta_{n_1}, \ldots, \zeta_{n_1}^{n_1-1}, \gamma, \gamma\zeta_{n_1}, \ldots, \gamma\zeta_{n_1}^{n_1-1}, \ldots, \gamma^{\lambda-1}, \gamma^{\lambda-1}\zeta_{n_1}, \ldots, \gamma^{\lambda-1}\zeta_{n_1}^{n_1-1}\right\}$$

is the zero set of I. Notice that the length of our codes $\mathcal{C}_\Delta^P$ equals $n = \lambda n_1$. Furthermore, we impose the condition $\lambda n_1 \nmid q^{2s}-1$ for this length cannot be obtained with univariate $\{1\}$-affine variety codes.

Our goal is to give conditions so that the subfield-subcodes $\mathcal{S}_\Delta^P = \mathcal{C}_\Delta^P \cap \mathbb{F}_{q^2}^n$ give rise to q-ary stabilizer quantum codes from Corollary 2.3.8. We desire to use techniques we know to get subfield-subcodes of J-affine variety codes (see Section 1.5.1) and adapt them to our setting. Although it requires its own study, in the sequel we will use the same notation as in such section. We desire to obtain a larger range of dimensions for our self-orthogonal codes than those in literature and also to provide a bound for the minimum distance of the resulting stabilizer codes. Notice that from Corollary 2.3.8 this

minimum distance is bounded by $\mathrm{d}\left(\left(\mathcal{S}_{\Delta}^{P}\right)^{\perp_h}\right)$. Sets Δ we want to consider are union of minimal closed sets with consecutive minimum elements. That is,

$$\Delta = \Lambda_{a_0} \cup \Lambda_{a_1} \cup \cdots \cup \Lambda_{a_\tau} \subseteq \{0, 1, \ldots, \lambda n_1 - 1\},$$

where

$$\mathcal{A} = \{a_0 < a_1 < \cdots < a_\nu\} \subseteq \{0, 1, \ldots, \lambda n_1 - 1\}$$

denotes the ordered set of minimum elements of all minimal closed sets. Such a bound will be $a_{\tau+1}$, which follows from an analogue result to that of Proposition 1.5.9.

We study when the following inclusion holds $\mathcal{C}_{\Delta}^{P} \subseteq \left(\mathcal{C}_{\Delta}^{P}\right)^{\perp_h}$ because then $\mathcal{S}_{\Delta}^{P} \subseteq \mathcal{C}_{\Delta}^{P} \subseteq \left(\mathcal{C}_{\Delta}^{P}\right)^{\perp_h} \subseteq \left(\mathcal{S}_{\Delta}^{P}\right)^{\perp_h}$. Then, given $e, e' \in \{0, 1, \ldots, \lambda n_1 - 1\}$, we need to know when the following inner product vanishes:

$$\begin{aligned} \mathrm{ev}_P(X^e) \cdot_h \mathrm{ev}_P(X^{e'}) &= \sum_{i=0}^{n_1-1} \zeta^{i(e+qe')} + \gamma^{e+qe'} \sum_{i=0}^{n_1-1} \zeta^{i(e+qe')} + \cdots + \gamma^{(\lambda-1)(e+qe')} \sum_{i=0}^{n_1-1} \zeta^{i(e+qe')} \\ &= \left(\sum_{i=0}^{n_1-1} \zeta^{i(e+qe')}\right)\left(1 + \gamma^{e+qe'} + \cdots + \gamma^{(\lambda-1)(e+qe')}\right). \end{aligned} \tag{5.4.1}$$

We only study the case when the factor $\sum_{i=0}^{n_1-1} \zeta^{i(e+qe')}$ vanishes, ignoring the other factor, since it suffices in order to get zero in the above product. Then, we restrict our study of self-orthogonality conditions to the projected code in the first n_1 coordinates, $\mathcal{C}_{\Delta}^{P}[\{1, \ldots, n_1\}]$. It is a univariate $\{1\}$-affine variety code $\mathcal{C}_{\Delta'}^{P'}$, where $\Delta' \subseteq \{0, 1, \ldots, n_1 - 1\}$ and $P' = \left\{1, \zeta_{n_1}, \ldots, \zeta_{n_1}^{n_1-1}\right\}$. Notice that the set Δ' is obtained from Δ after reducing its elements modulo n_1 and thus the elements are reordered in new closed sets

$$\Delta' = \Lambda'_{a'_0} \cup \Lambda'_{a'_1} \cup \cdots \cup \Lambda'_{a'_\tau} \subseteq \{0, 1, \ldots, n_1 - 1\},$$

where $a'_0, a'_1, \ldots, a'_\tau$ are the respective minimum elements of these new minimal closed sets.

In [41] it was proved that if $a'_\tau < \frac{n_1}{q^{2(s-1)}+1}$ holds, then the code $\mathcal{C}_{\Delta'}^{P'}$ satisfies $\mathcal{C}_{\Delta'}^{P'} \subseteq \left(\mathcal{C}_{\Delta'}^{P'}\right)^{\perp_h}$. However, with our advanced work we conjecture the larger bound

$$a'_\tau \leq qn_2 - \left\lfloor \frac{(q-1)n_2 - 1}{q^{s-1}} \right\rfloor - 1.$$

By the manner we have constructed this bound we believe that it is sharp. This belief is also supported with many computer calculations. Moreover, we would achieve our goal of obtaining many more self-orthogonal $\{1\}$-affine variety codes by improving their range of dimensions. For example, taking $q = 3$, $s = 4$, $n_1 = (3^4 + 1) \cdot 16 = 82 \cdot 16$ and $n_2 = 16$, the bound in [41] is $a'_\tau \leq 1$ but our bound is $a'_\tau \leq 46$. This fact would also allow us to construct many new stabilizer quantum codes from the enlarged construction provided above.

Conclusions

This PhD thesis offers some advances on two problems in the fields of mathematics and information theory. These problems are the repair problem in distributed and cloud storage systems and the construction of better quantum error-correcting codes than the current ones. Both can be treated with the construction of suitable classical error-correcting codes.

With respect to the first problem, we focus on the setting where simultaneous multiple device failures may happen. Error-correcting codes devoted to this problem are called (r, δ)-locally recoverable codes.

After recalling the basics on classical and quantum error-correcting codes, Chapters 3 to 5 provide some suitable codes to address the former problems. We considered evaluation codes, mainly monomial-Cartesian codes and their generalized constructions. They allowed us to present new codes suited to both problems.

Chapter 3 regarded monomial-Cartesian codes as (r, δ)-locally recoverable codes and provided a recovery method. We determined those giving rise to (r, δ)-optimal locally recoverable codes for a natural bound on their minimum distance, which are in fact (r, δ)-optimal with that minimum distance. By considering a large subfamily of monomial-Cartesian codes we proposed infinitely many sets of new (r, δ)-optimal locally recoverable codes. These were a family of subfield-subcodes of J-affine variety codes that admit the same parameters of certain optimal monomial-Cartesian codes but are supported over smaller fields.

Afterwards, in Chapter 4, we used generalized (or twisted) monomial-Cartesian codes to construct new stabilizer quantum error-correcting codes. We provided an explicit twist vector and formulae for their minimum distance and dimension. We showed that when we use generalized monomial-Cartesian codes that arise from polynomials in one variable, our codes are quantum MDS, and when they arise from polynomials in two variables and our lower bound for the minimum distance is 3, the obtained codes are at least Hermitian almost MDS. Our family of codes was shown to have excellent parameters. This good quality of our quantum codes is justified because, on the one hand, when they come from polynomials in two variables, we got an infinite family that beats the Gilbert-Varshamov bound. On the other hand, because we were able to present many examples that are better than any known code in the literature.

Evaluating polynomials at the roots of the trace map gives rise to codes with very good parameters. Motivated by this fact, in Chapter 5, we constructed codes by eval-

uating polynomials at the roots of trace-depending polynomials (given by a constant plus the trace of a polynomial). These codes provided new wide ranges of lengths and also excellent parameters. In particular we obtained binary records according to Markus Grassl tables and non-binary codes improving the previous ones in the literature.

To conclude, we gave some ideas for further research. We showed in Part IV a construction (of certain Hermitian self-orthogonal linear codes and their subfield-subcodes) derived from some codes close to univariate $\{1\}$-affine variety codes. Lengths of these linear codes cannot be obtained with self-orthogonal affine variety codes as before alluded. Moreover we think they also improve the range of dimensions of self-orthogonal codes defined by univariate $\{1\}$-affine variety codes given in a previous paper.

Conclusiones

Esta tesis doctoral ofrece algunos avances en dos problemas de los campos de las matemáticas y la teoría de la información. Estos problemas son el problema de recuperación en sistemas de almacenamiento distribuido y en la nube y la construcción de códigos cuánticos correctores de errores mejores que los existentes. Ambos se pueden tratar con la construcción de ciertos códigos clásicos correctores de errores.

Con respecto al primer problema nos centramos en la situación en la que se puedan producir fallos en varios nodos simultáneamente. Los códigos correctores de errores diseñados para este problema se denominan códigos (r, δ)-localmente recuperables.

Tras introducir lo básico sobre códigos clásicos y cuánticos correctores de errores, los Capítulos 3, 4 y 5 proporcionan algunos códigos adecuados para abordar los problemas anteriores. Estos eran códigos de evaluación, principalmente códigos Cartesiano-monomiales y sus construcciones generalizadas, que nos permitieron presentar nuevos códigos aptos en ambos problemas.

El Capítulo 3 consideraba los códigos Cartesiano-monomiales como códigos (r, δ)-localmente recuperables y proporcionaba un método de recuperación. Determinamos aquellos que dan lugar a códigos (r, δ)-óptimos localmente recuperables para una cota natural en su distancia mínima, que de hecho son (r, δ)-óptimos para esa distancia mínima. Considerando una amplia subfamilia de códigos Cartesiano-monomiales propusimos un número infinito de conjuntos de nuevos códigos (r, δ)-óptimos localmente recuperables. Estos eran una familia de subcódigos-subcuerpo de códigos variedad J-afín que admiten los mismos parámetros que ciertos códigos Cartesiano-monomiales pero sobre cuerpos más pequeños.

Posteriormente, en el Capítulo 4, usamos códigos Cartesiano-monomiales generalizados (o twisteados) para construir nuevos códigos cuánticos estabilizadores correctores de errores. Proporcionamos un vector de twisteo explícito y fórmulas para su distancia mínima y dimensión. Demostramos que cuando usamos códigos Cartesiano-monomiales generalizados que se obtienen a partir de polinomios en una variable, nuestros códigos son cuánticos de máxima distancia de separación, y cuando se obtienen de polinomios en dos variables y nuestra cota para la distancia mínima es 3, los códigos obtenidos son al menos Hermitianos casi de máxima distancia de separación. Mostramos que nuestra familia de códigos posee parámetros excelentes. Esta buena calidad de nuestros códigos cuánticos viene justificada porque, por una parte, cuando provienen de polinomios en dos variables, obtuvimos una familia infinita que bate la cota Gilbert-Varshamov y, por

otra parte, porque fuimos capaces de presentar numerosos ejemplos que son mejores que los códigos conocidos en la literatura.

Evaluar polinomios en las raíces del polinomio traza da lugar a códigos con parámetros muy buenos. Motivados por este hecho, en el Capítulo 5, construimos códigos evaluando polinomios en las raíces de polinomios dependientes de la traza (dados por una constante no nula más la traza de otro polinomio). Estos códigos proporcionaban nuevos rangos de longitudes y también parámetros excelentes. En particular obtuvimos récords binarios con respecto a las tablas de Markus Grassl y códigos no binarios mejorando los obtenidos previamente en la literatura.

Para concluir dimos algunas ideas de trabajo futuro. En la Parte IV mostramos una construcción (de ciertos códigos lineales autoortogonales Hermíticos y sus subcódigos subcuerpo) derivada de unos códigos cercanos a los códigos variedad $\{1\}$-afín en una variable. Las longitudes de estos códigos lineales no se pueden obtener con códigos variedad afín autoortogonales como los anteriormente aludidos. También creemos que mejoran el rango de dimensiones de códigos autoortogonales definidos por códigos variedad $\{1\}$-afín en una variable dado en un artículo previo.

List of Figures

1.1. Information broadcasting scheme on a noisy channel [71] 23
1.2. Two Euclidean balls of radius $\left\lfloor \frac{d-1}{2} \right\rfloor$ centered in the codewords $\boldsymbol{c}$ and $\boldsymbol{c}'$. 24
1.3. Grid representation of E, where $m = 2$, $n_1 = 10$ and $n_2 = 9$ 33
1.4. Shaded region representing $\mathrm{F}(\langle \boldsymbol{X}^{\boldsymbol{e}}, X_1^{n_1}, X_2^{n_2} \rangle)$ 34
1.5. Grid representation of E, where $m = 2$, $n_1 = 8$, $n_2 = 6$. In blue, the points in $\Delta = (\{0,1,2\} \times \{0,1\}) \cup \{(0,2),(1,2)\}$ 35

2.1. Instance of the qubit as two states of an electron orbiting an atom [104] . 47
2.2. Two codes in a Hilbert space: (A) A not desired code $\mathcal{Q}$, with non-orthogonal, deformed "error" subspaces $A_i := \boldsymbol{E}_i \mathcal{Q}$; (B) A desired code, with orthogonal, undeformed subspaces [104] 52

3.1. Sets $\Delta_{i,j}$ in Proposition 3.2.1 70
3.2. Sets $\Delta_{i,s}^2$ and $\Delta_{j,s}^{2,\sigma}$ in Proposition 3.2.2 71
3.3. Sets $\Delta_{i,j}^3$ and $\Delta_{i,j}^{3,\sigma}$ in Proposition 3.2.3 72
3.4. On the right, the set obtained by removing four exponents of $\Delta_{2,5}^3$ (on the left) as described in Remark 3.2.4 74
3.5. Examples in Remark 3.2.7 76
3.6. Sets Δ_1 and Δ_2 in the proof of Lemma 3.2.8 77
3.7. Set S in the proof of Lemma 3.2.9 78
3.8. Toy example in the proof of Lemma 3.2.9 78
3.9. Set Δ_{i,n_2-1}^1 in the proof of Theorem 3.2.11 80
3.10. Sets $\Delta_{2,0}^2$ and M_2^7 in the proof of Theorem 3.2.11 81
3.11. Set M_1^2 in the proof of Theorem 3.2.11 81
3.12. Set S^7 in the proof of Theorem 3.2.11 82
3.13. Resulting set (1) (respectively, (2)) when removing 9 (respectively, 16) points from M_1^2 (respectively, S^7) in the proof of Theorem 3.2.11 83
3.14. Sets $\overline{S}^2$ and $\overline{S}^7$ in the proof of Theorem 3.2.11 84
3.15. Sets S' obtained by removing points from $\overline{S}^i$ in the proof of Theorem 3.2.11 84
3.16. Sets S'' obtained by adding points to S' in the proof of Theorem 3.2.11 . 84
3.17. Sets Δ, Δ' (and Δ'') considered in the proof of Proposition 3.3.4 for values $(i, p^h, q, P_1, z, t, u, v) = (1, 8, 64, U_9, 3, 2, 2, 1)$ 95

3.18. Sets $\Delta_2^{\perp}$, Δ_0'', Δ'' and Δ' considered in the proof of Proposition 3.3.6 for values $(i, 2^h, q, P_1, P_2, J, z) = (1, 4, 16, U_5 \cup \{0\}, U_{n_2-1} \cup \{0\}, \varnothing, 2)$ 100
3.19. Sets Δ considered in Examples 3.3.8 102

4.1. Grid representation of E, where $m = 2$, $n_1 = 8$, $n_2 = 6$, and $\Delta = (\{0,1,2\} \times \{0,1\}) \cup \{(0,2),(1,2)\}$ 115
4.2. Sets Δ_3, Δ_4 and Δ_5, where $m = 2$, $n_1 = 8$ and $n_2 = 6$. We use the same conventions as in the paragraph above Figure 1.3 119
4.3. Pairs $((i_1, i_2), (r_1, r_2))$ giving the set $S := \{((0,0),(0,0)), ((1,0),(7,0)), ((0,1),(0,7)), ((1,1),(7,7)), ((2,1),(6,7))\}$ in Example 4.2.8 120
4.4. Sets Δ_5, $(\Delta_5)^{\perp_e}$, Δ_5' and $(\Delta_5')^{\perp_e}$ in Example 4.2.8 121

List of Tables

3.1. Optimal (r, δ)-subfield-subcodes over $\mathbb{F}_{p^h}$ in the bivariate case 104
3.2. Optimal (r, δ)-subfield-subcodes over $\mathbb{F}_{p^h}$ in the multivariate case 107

4.1. Some instances of the range of lengths of stabilizer quantum codes (from Theorem 4.4.1 only) that beat the quantum Gilbert-Varshamov bound . . 125
4.2. Some instances of the range of lengths of quantum stabilizer codes from Theorem 4.2.7 with $d = 3$ that beat the quantum Gilbert-Varshamov bound 126
4.3. A $q = 3$ sample of stabilizer quantum codes 127
4.4. A $q = 5$ sample of stabilizer quantum codes 127
4.5. A $q = 7$ sample of stabilizer quantum codes 128
4.6. A $q = 9$ sample of stabilizer quantum codes 128
4.7. A $q = 11$ sample of stabilizer quantum codes 129

5.1. q-adic expansion of z, any exponent of $\mathrm{Tr}_b(X) = \sum_{z=0}^{n} c_z X^z$ 133
5.2. q-adic expansion of b 133
5.3. Triples (q, μ, b), $b = 1 + q^t$, satisfying Property (5.1.1) 134
5.4. q-adic expansions of the indices $z \neq 0$ such that $c_z \neq 0$ in the expression of $\mathrm{Tr}(X) = \sum_{z=0}^{n} c_z X^z$ 136
5.5. q-adic expansion of i_1 in the proof of Theorem 5.1.9 140
5.6. q-adic expansion of j_2' in the proof of Theorem 5.1.9 140
5.7. q-adic expansion of $n - z_1 + j_{2,0}$ in the proof of Theorem 5.1.9 141
5.8. q-adic expansions of the candidates in $\mathcal{I}_1$ and j_0 when $1 < t \leq \frac{\mu}{2}$ within the proof of Theorem 5.1.14 149
5.9. Parameters of binary stabilizer quantum codes of length 640 156
5.10. Parameters of binary stabilizer quantum codes of length 320 156
5.11. Parameters of binary stabilizer quantum codes of length 288 156
5.12. Parameters of 5-ary stabilizer quantum codes of length 300 157
5.13. Sporadic binary stabilizer quantum error-correcting records 158

References

[1] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli. On quantum and classical BCH codes. *IEEE Trans. Inf. Theory*, 53(3):1183–1188, 2007. 60, 161

[2] H. E. Andersen and O. Geil. Evaluation codes from order domain theory. *Finite Fields Appl.*, 14(1):92–123, 2008. 33

[3] B. Andrade, C. Carvalho, V. G. L. Neumann, and A. C. P. Veiga. A family of codes with locality containing optimal codes. *IEEE Access*, 10:39145–39153, 2022. 6, 69, 88

[4] A. Ashikhmin, A. Barg, E. Knill, and S. Litsyn. Quantum error-detection I: Statement of the problem. *IEEE Trans. Inf. Theory*, 46:778–788, 2000. 9

[5] A. Ashikhmin, A. Barg, E. Knill, and S. Litsyn. Quantum error-detection II: Bounds. *IEEE Trans. Inf. Theory*, 46:789–800, 2000. 9

[6] A. Ashikhmin and E. Knill. Non-binary quantum stabilizer codes. *IEEE Trans. Inf. Theory*, 47:3065–3072, 2001. 10, 45, 59, 155

[7] S. Axler. *Linear algebra done right*. Undergraduate Texts in Mathematics. Springer Cham, New York, 2015. 48

[8] S. Ball. On sets of vectors of a finite vector space in which every subset of basis size is a basis. *J. Eur. Math. Soc.*, 14(3):733–748, 2012. 29

[9] S. Ball. Some constructions of quantum MDS codes. *Des. Codes Cryptogr.*, 89:811–821, 2021. 10

[10] S. Ball, A. Centelles, and F. Huber. Quantum error-correcting codes and their geometries. *Ann. Inst. Henri Poincaré Comb. Phys. Interact.*, 10(2):337–405, 2023. 45, 51, 53

[11] B. Barbero-Lucas, F. Hernando, H. Martín-Cruz, and G. McGuire. MDS, Hermitian almost MDS, and Gilbert-Varshamov quantum codes from generalized monomial-Cartesian codes. *Quantum Inf. Process.*, 23(86), 2024. 4, 112

[12] A. Barg, K. Haymaker, E. Howe, G. Matthews, and A. Várilly-Alvarado. Locally recoverable codes from algebraic curves and surfaces. In E. W. Howe, K. E. Lauter,

and J. L. Walker, editors, *Algebraic Geometry for Coding Theory and Cryptography*, volume 9 of *Association for Women in Mathematics Series*, pages 95–126. Springer, 2017. 4

[13] A. Barg, I. Tamo, and S. Vladut. Locally recoverable codes on algebraic curves. *IEEE Trans. Inf. Theory*, 63(8):4928–4939, 2017. 4

[14] C. H. Bennett, D. P. DiVicenzo, J. A. Smolin, and W. K. Wootters. Mixed state entanglement and quantum error correction. *Phys. Rev. A*, 54(5):3824–3851, 1996. 53

[15] S. Bhardwaj, M. Goyal, and M. Raka. New quantum codes from constacyclic codes over a general non-chain ring. arXiv preprint arXiv:2212.02821, 2022. 11, 127, 128

[16] J. Bierbrauer and Y. Edel. Quantum twisted codes. *J. Comb. Designs*, 8:174–188, 2000. 10

[17] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system I: The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. 13, 157, 158

[18] M. Brooks. Quantum computers: what are they good for? *Nature*, 617:S1–S3, 2023. 2

[19] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane. Quantum error correction and orthogonal geometry. *Phys. Rev. Lett.*, 76:405–409, 1997. 9

[20] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane. Quantum error correction via codes over GF(4). *IEEE Trans. Inf. Theory*, 44(4):1369–1387, 1998. 9

[21] E. T. Campbell, B. M. Terhal, and C. Vuillot. Roads towards fault-tolerant universal quantum computation. *Nature*, 549:172–179, 2017. 10

[22] E. Camps, H. H. López, G. L. Matthews, and E. Sarmiento. Polar decreasing monomial-Cartesian codes. *IEEE Trans. Inf. Theory*, 67(6):3664–3674, 2021. 3, 21, 34

[23] M. Cao and J. Cui. Construction of new quantum codes via Hermitian dual-containing matrix-product codes. *Quantum Inf. Process.*, 19:427, 2020. 10, 11, 128, 157

[24] C. Carvalho. On the second Hamming weight of some Reed–Muller type codes. *Finite Fields Appl.*, 24:88–94, 2013. 33

[25] C. Carvalho and V. G. L. Neumann. A family of codes with variable locality and availability. arXiv preprint arXiv:2107.13487, 2021. 3

[26] D. Castelvecchi. Quantum computers ready to leap out of the lab in 2017. *Nature*, 541(7635):9–10, 2017. 2

[27] B. Chen, W. Fang, S. T. Xia, and F. W. Fu. Constructions of optimal (r, δ) locally repairable codes via constacyclic codes. *IEEE Trans. Commun.*, 67(8):5253–5263, 2019. 5, 6, 89

[28] B. Chen and J. Huang. A construction of optimal (r, δ)-locally recoverable codes. *IEEE Access*, 7:180349–180353, 2019. 5, 6, 69, 89

[29] B. Chen, S. T. Xia, J. Hao, and F. W. Fu. Constructions of optimal cyclic (r, δ) locally repairable codes. *IEEE Trans. Inf. Theory*, 64(4):2499–2511, 2018. 4, 5, 6, 89

[30] G. Chen and R. Li. Ternary self-orthogonal codes of dual distance three and ternary quantum codes of distance three. *Des. Codes Cryptogr.*, 69:53–63, 2013. 11, 123, 127

[31] H. Chen, J. Weng, W. Luo, and L. Xu. Long optimal and small-defect LRC codes with unbounded minimum distances. *IEEE Trans. Inf. Theory*, 67(5):2786–2792, 2021. 5, 6, 89

[32] D. Cox, J. Little, and D. O'Shea. *Ideals, varieties, and algorithms.* Undergraduate Texts in Mathematics. Springer, New York, 2007. 5, 33

[33] P. Delsarte. On subfield subcodes of modified Reed-Solomon codes (corresp.). *IEEE Trans. Inf. Theory*, 21(5):575–576, 1975. 21, 38

[34] D. Dieks. Communication by EPR devices. *Phys. Rev. A*, 92:271, 1982. 1

[35] W. Fang and F. W. Fu. Some new constructions of quantum MDS codes. *IEEE Trans. Inf. Theory*, 65:7840–7847, 2019. 10

[36] W. Fang and F. W. Fu. Optimal cyclic (r, δ) locally repairable codes with unbounded length. *Finite Fields Appl.*, 63, 2020. 5, 6, 89

[37] G.-L. Feng and T. R. N. Rao. Decoding algebraic-geometric codes up to the designed minimum distance. *IEEE Trans. Inf. Theory*, 39(1):37–45, 1993. 33

[38] G.-L. Feng and T. R. N. Rao. Improved geometric Goppa codes, part I: Basic theory. *IEEE Trans. Inf. Theory*, 41(6):1678–1693, 1995. 33

[39] K. Feng and Z. Ma. A finite Gilbert-Varshamov bound for pure stabilizer quantum codes. *IEEE Trans. Inf. Theory*, 50(12):3323–3325, 2004. 12, 61

[40] J. Fitzgerald and R. F. Lax. Decoding affine variety codes using Gröbner basis. *Des. Codes Cryptogr.*, 13:147–158, 1998. 2, 30

[41] C. Galindo, O. Geil, F. Hernando, and D. Ruano. On the distance of stabilizer quantum codes from J-affine variety codes. *Quantum Inf. Process.*, 16(111), 2017. 10, 12, 15, 21, 120, 161, 162

[42] C. Galindo, O. Geil, F. Hernando, and D. Ruano. Improved constructions of nested code pairs. *IEEE Trans. Inf. Theory*, 64(4):2444–2459, 2018. 119

[43] C. Galindo and F. Hernando. Quantum codes from affine variety codes and their subfield subcodes. *Des. Codes Cryptogr.*, 76:89–100, 2015. 10, 38, 40

[44] C. Galindo and F. Hernando. On the generalization of the construction of quantum codes from Hermitian self-orthogonal codes. *Des. Codes Cryptogr.*, 90:1103–1112, 2022. 155, 157

[45] C. Galindo, F. Hernando, and H. Martín-Cruz. Optimal (r, δ)-LRCs from monomial-Cartesian codes and their subfield-subcodes. *Des. Codes Cryptogr.*, 2024. DOI 10.1007/s10623-024-01403-z. 4, 66, 107

[46] C. Galindo, F. Hernando, H. Martín-Cruz, and D. Ruano. Stabilizer quantum codes defined by trace-depending polynomials. *Finite Fields Appl.*, 87:102138, 2023. 4, 132

[47] C. Galindo, F. Hernando, and C. Munuera. Locally recoverable J-affine variety codes. *Finite Fields Appl.*, 64, 2020. 5, 21, 40, 89

[48] C. Galindo, F. Hernando, and D. Ruano. New quantum codes from evaluation and matrix-product codes. *Finite Fields Appl.*, 36:98–120, 2015. 11, 127, 128

[49] C. Galindo, F. Hernando, and D. Ruano. Stabilizer quantum codes from J-affine variety codes and a new Steane-like enlargement. *Quantum Inf. Process.*, 14:3211–3231, 2015. 3, 10, 12, 21, 31, 97

[50] C. Galindo, F. Hernando, and D. Ruano. Classical and quantum evaluation codes at the trace roots. *IEEE Trans. Inf. Theory*, 65(4):2593–2602, 2019. 12, 13, 14, 131, 136, 152, 153

[51] O. Geil. Evaluation codes from an affine variety code perspective. In E. Martínez-Moro, C. Munuera, and D. Ruano, editors, *Advances in algebraic geometry codes*, volume 5 of *Coding Theory Cryptol.*, pages 153–180. World Sci. Publ., Singapore, 2008. 5, 21, 33

[52] O. Geil and T. Hoholdt. Footprints or generalized Bezout's theorem. *IEEE Trans. Inf. Theory*, 46(2):635–641, 2000. 5, 33

[53] O. Geil and T. Høholdt. On hyperbolic codes. In S. Boztas and I. E. Shparlinski, editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. AAECC 2001*, volume 2227 of *Lecture Notes in Comput. Sci.*, pages 159–171. Springer, 2001. 12, 118, 121

[54] O. Geil and C. Thomsen. Weighted Reed-Muller codes revisited. *Des. Codes Cryptogr.*, 66:195–220, 2013. 2, 30

[55] P. Gopalan, C. Huang, H. Simitci, and S. Yekhanin. On the locality of codeword symbols. *IEEE Trans. Inf. Theory*, 58(11):6925–6934, 2012. 4, 21, 35, 36

[56] S. Goparaju and R. Calderbank. Binary cyclic codes that are locally repairable. In *2014 IEEE International Symposium on Information Theory*, pages 676–680. IEEE, 2014. 4

[57] D. Gottesman. Class of quantum error-correcting codes saturating the quantum Hamming bound. *Phys. Rev. A*, 54(3):1862–1868, 1996. 9, 10, 45, 56

[58] D. Gottesman. *Stabilizer codes and quantum error correction*. PhD thesis, California Institute of Technology, 1997. PhD thesis. 45, 51

[59] D. Gottesman. Fault-tolerant computation with higher-dimensional systems. *Chaos Solitons Fractals*, 10:1749–1758, 1999. 10

[60] D. Gottesman. An introduction to quantum error correction and fault-tolerant quantum computation. In *Quantum Information Science and Its Contributions to Mathematics, Proceedings of Symposia in Applied Mathematics*, volume 68, pages 13–58, 2010. 54

[61] M. Grassl. *Searching for linear codes with large minimum distance*, volume 19 of *Algorithms Comput. Math.*, pages 287–313. Springer, Berlin, Heidelberg, 2006. 26

[62] M. Grassl. Bounds on the minimum distance of linear codes. *www.codetables.de*, accessed on 29/06/2022. 12, 14, 131, 132, 155, 156, 158

[63] M. Grassl and M. Rötteler. Quantum BCH codes. In *Proc. X Int. Symp. Theor. Elec. Eng.*, pages 207–212, 1999. 9

[64] V. Guruswami, C. Xing, and C. Yuan. How long can optimal locally repairable codes be? *IEEE Trans. Inf. Theory*, 65(6):3662–3670, 2019. 4

[65] I. Gómez-Casares. Fundamentos matemáticos de la computación cuántica. Master's thesis, Universidade de Santiago de Compostela. Facultade de Matemáticas, 2020. Bachelor's thesis. 45, 46

[66] K. Hoffman and R. Kunze. *Linear algebra*. Prentice-Hall, Second edition, 1971. 48

[67] T. Høholdt, J. H. van Lint, and G. R. Pellikaan. Algebraic geometry codes. In V. S. Pless and W. C. Huffman, editors, *Handbook of Coding Theory*, volume 1, pages 871–961, Netherlands, 1998. Elsevier. 33

[68] P. Huang, E. Yaakobi, H. Uchikawa, and P. H. Siegel. Cyclic linear binary locally repairable codes. In *2015 IEEE Information Theory Workshop (ITW)*, pages 1–5. IEEE, 2015. 4

[69] F. Huber and M. Grassl. Quantum codes of maximal distance and highly entangled subspaces. *Quantum*, 4(284), 2020. 61

[70] W. C. Huffman, J.-L. Kim, and P. Solé. *Concise encyclopedia of coding theory*. CRC Press, 2021. 21

[71] W. C. Huffman and V. Pless. *Fundamentals of error-correcting codes*. Cambridge University Press, 2003. 21, 23, 25, 37, 38, 39, 167

[72] L. Jin. Explicit construction of optimal locally recoverable codes of distance 5 and 6 via binary constant weight codes. *IEEE Trans. Inf. Theory*, 65(8):4658–4663, 2019. 4, 5, 6, 89

[73] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli. Nonbinary stabilizer codes over finite fields. *IEEE Trans. Inf. Theory*, 52(11):4892–4914, 2006. 10, 45, 54, 57, 58, 59, 60, 155

[74] E. Knill and R. Laflamme. A theory of quantum error-correcting codes. *Phys. Rev. A*, 55(2):900–911, 1997. 53

[75] E. Knill, R. Laflamme, A. Ashikhmin, H. N. Barnum, L. Viola, and W. H. Zurek. Introduction to quantum error correction. *Los Alamos Sci.*, (27):188–225, 2002. 45, 52, 53

[76] E. Knill, R. Laflamme, and W.H. Zurek. Resilient quantum computation: Error models and thresholds. *Proc. Royal Soc. London A*, 454:365–384, 1998. 10

[77] E. Kolotoğlu and M. Sarı. Quantum codes with improved minimum distance. *Bull. Korean Math. Soc.*, 56(3):609–619, 2019. 11, 128

[78] B. Kong and X. Zheng. Quantum codes from constacyclic codes over S_k. *EPJ Quantum Technol.*, 10(3), 2023. 11, 127

[79] X. Kong, X. Wang, and G. Ge. New constructions of optimal locally repairable codes with super-linear length. *IEEE Trans. Inf. Theory*, 67(10):6491–6506, 2021. 5, 6, 89, 100

[80] G. G. La Guardia. On the construction of nonbinary quantum BCH codes. *IEEE Trans. Inf. Theory*, 60(3):1528–1535, 2014. 10

[81] X. Li, L. Ma, and C. Xing. Optimal locally repairable codes via elliptic curves. *IEEE Trans. Inf. Theory*, 65(1):108–117, 2019. 5, 6, 89

[82] D. E. Lidar and T. A. Brun. *Quantum error correction*. Cambridge University Press, New York, 2013. 54

[83] R. Lidl and H. Niederreiter. *Introduction to finite fields and their applications*. Cambridge University Press, 1994. 25

[84] S. Ling, J. Luo, and C. Xing. Generalization of Steane's enlargement construction of quantum codes and applications. *IEEE Trans. Inf. Theory*, 56(8):4080–4084, 2010. 123

[85] H. Liu and X. Liu. Constructions of quantum MDS codes. *Quantum Inf. Process.*, 20(14), 2021. 10

[86] J. Liu, S. Mesnager, and L. Chen. New constructions of optimal locally recoverable codes via good polynomials. *IEEE Trans. Inf. Theory*, 64(2):889–899, 2018. 4

[87] J. Liu, S. Mesnager, and D. Tang. Constructions of optimal locally recoverable codes via Dickson polynomials. *Des. Codes Cryptogr.*, 88:1759–1780, 2020. 4

[88] X. Liu, H. Q. Dinh, H. Liu, and L. Yu. On new quantum codes from matrix product codes. *Cryptogr. Commun.*, 10:579–589, 2018. 11, 127, 128, 129

[89] G. Luo, M. F. Ezerman, M. Grassl, and S. Ling. Constructing quantum error-correcting codes that require a variable amount of entanglement. *Quantum Inf. Process.*, 23(4), 2024. 55, 56

[90] G. Luo, M. F. Ezerman, and S. Ling. Three new constructions of optimal locally repairable codes from matrix-product codes. *IEEE Trans. Inf. Theory*, 69(1):75–85, 2023. 5, 6, 69, 89

[91] L. Luo and Z. Ma. Fault-tolerant quantum computation with non-binary systems. *Quantum Inf. Process.*, 18:188, 2019. 10

[92] Y. Luo, C. Xing, and C. Yuan. Optimal locally repairable codes of distance 3 and 4 via cyclic codes. *IEEE Trans. Inf. Theory*, 65(2):1048–1053, 2019. 4, 5, 6, 89

[93] H. H. López, G. L. Matthews, and I. Soprunov. Monomial-Cartesian codes and their duals, with applications to LCD codes, quantum codes, and locally recoverable codes. *Des. Codes Cryptogr.*, 88:1673–1685, 2020. 2, 3, 21, 30, 66

[94] H. H. López, C. Rentería-Márquez, and R. H. Villarreal. Affine cartesian codes. *Des. Codes Cryptogr.*, 71:5–19, 2014. 31

[95] H. H. López, I. Soprunov, and R. H. Villarreal. The dual of an evaluation code. *Des. Codes Cryptogr.*, 89:1367–1403, 2021. 2

[96] F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes.* North-Holland Mathematical Library, 1977. 21, 25

[97] R. Matsumoto and S. Miura. On the Feng-Rao bound for the $\mathcal{L}$-construction of algebraic geometry codes. *IEICE Trans. Fundamentals*, E83-A(5):923–927, 2000. 33

[98] R. Matsumoto and T. Uyematsu. Constructing quantum error-correcting codes for p^m-state systems from classical error-correcting codes. *IEICE Trans. Fundamentals*, E83-A(10):1878–1883, 2000. 10

[99] G. Micheli. Constructions of locally recoverable codes which are optimal. *IEEE Trans. Inf. Theory*, 66(1):167–175, 2018. 4

[100] C. Munuera. Locally recoverable codes with local error detection. arXiv preprint arXiv:1812.00834, 2018. 4

[101] C. Munuera and J. Tena. *Codificación de la información*. Universidad de Valladolid, 1997. 21, 25

[102] C. Munuera and W. Tenorio. Locally recoverable codes from rational maps. *Finite Fields Appl.*, 54:80–100, 2018. 4

[103] C. Munuera, W. Tenorio, and F. Torres. Locally recoverable codes from algebraic curves with separated variables. *Adv. Math. Commun.*, 14(2):265–278, 2020. 4

[104] M. Nielsen and I. Chuang. *Quantum computation and quantum information*. Cambridge University Press, 2000. 45, 46, 47, 51, 52, 53, 57, 58, 167

[105] R. Pellikaan, X.-W. Wu, S. Bulygin, and R. Jurrius. *Codes, cryptology and curves with computer algebra*. Cambridge University Press, 2017. 36

[106] N. Prakash, G. M. Kamath, V. Lalitha, and P. V. Kumar. Optimal linear codes with a local-error-correction property. In *2012 IEEE International Symposium on Information Theory Proceedings*, pages 2776–2780. IEEE, 2012. 4, 5, 21, 36, 37

[107] J. Preskill. Reliable quantum computers. *Proc. Royal Soc. London A*, 454:385–410, 1998. 10

[108] J. Qiu, D. Zheng, and F. W. Fu. New constructions of optimal cyclic (r, δ) locally repairable codes from their zeros. *IEEE Trans. Inf. Theory*, 67(3):1596–1608, 2021. 5, 6, 89

[109] E. M. Rains. Nonbinary quantum codes. *IEEE Trans. Inf. Theory*, 45(6):1827–1832, 1999. 60

[110] C. Salgado, A. Varilly-Alvarado, and J. F. Voloch. Locally recoverable codes on surfaces. *IEEE Trans. Inf. Theory*, 67(9):5765–5777, 2021. 4

[111] B. Segre. Curve razionali normali e k-archi negli spazi finiti. *Ann. Mat. Pura Appl.*, 39:357–379, 1955. 29

[112] P. W. Shor. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A*, 52(4):2493–2496, 1995. 1, 45

[113] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997. 1, 45

[114] P.W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. In *Proc. 35th Ann. Symp. Found. Comp. Sc., IEEE Comp. Soc. Press*, pages 124–134, 1994. 1

[115] P.W. Shor. Fault-tolerant quantum computation. In *Proc. 37th Ann. Symp. Found. Comp. Sc., IEEE Comp. Soc. Press*, pages 56–65, 1996. 10

[116] H. Song, R. Li, Y. Liu, and G. Guo. New quantum codes from matrix-product codes over small fields. *Quantum Inf. Process.*, 19(226), 2020. 10

[117] W. Song, S. H. Dau, C. Yuen, and T. J. Li. Optimal locally repairable linear codes. *IEEE J. Sel. Areas Commun.*, 32(5):1019–1036, 2014. 5

[118] A. M. Steane. Error correcting codes in quantum theory. *Phys. Rev. Lett.*, 77(5):793–797, 1996. 45

[119] A. M. Steane. Simple quantum error-correcting codes. *Phys. Rev. A*, 54(6):4741–4751, 1996. 1

[120] A.M. Steane and B. Ibinson. Fault-tolerant logical gate networks for Calderbank-Shor-Steane codes. *Phys. Rev. A*, 72:052335, 2005. 10

[121] Z. Sun, S. Zhu, and L. Wang. Optimal constacyclic locally repairable codes. *IEEE Commun. Lett.*, 23(2):206–209, 2019. 5, 6, 89, 100

[122] I. Tamo and A. Barg. A family of optimal locally recoverable codes. *IEEE Trans. Inf. Theory*, 60(8):4661–4676, 2014. 4

[123] I. Tamo, A. Barg, S. Goparaju, and R. Calderbank. Cyclic LRC codes and their subfield subcodes. In *2015 IEEE International Symposium on Information Theory (ISIT)*, pages 1262–1266. IEEE, 2015. 4

[124] I. Tamo, D. S. Papailiopoulos, and A. G. Dimakis. Optimal locally repairable codes and connections to matroid theory. *IEEE Trans. Inf. Theory*, 62(12):6661–6671, 2016. 4

[125] A. Vardy. The intractability of computing the minimum distance of a code. *IEEE Trans. Inf. Theory*, 43(6):1757–1766, 1997. 26

[126] R. Wan and S. Zhu. New Quantum MDS codes from Hermitian self-orthogonal generalized Reed-Solomon codes. arXiv preprint arXiv:2302.06169, 2023. 11, 122, 126, 128

[127] Y. Wang, X. Kai, Z. Sun, and S. Zhu. Quantum codes from Hermitian dual-containing constacyclic codes over $\mathbb{F}_{q^2} + v\mathbb{F}_{q^2}$. *Quantum Inf. Process.*, 20(122), 2021. 11, 127

[128] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982. 1, 45, 51

[129] Y. Xia and B. Chen. Complete characterizations of optimal locally repairable codes with locality 1 and $k-1$. *IEEE Access*, 7:111271–111276, 2019. 5, 6, 89

[130] A. Zeh and E. Yaacobi. Bounds and constructions of codes with multiple localities. In *2016 IEEE International Symposium on Information Theory (ISIT)*, pages 640–644. IEEE, 2016. 4

[131] G. Zhang. A new construction of optimal (r, δ) locally recoverable codes. *IEEE Commun. Lett.*, 24(9):1852–1856, 2020. 5, 6, 89

[132] G. Zhang and H. Liu. Constructions of optimal codes with hierarchical locality. *IEEE Trans. Inf. Theory*, 66(12):7333–7340, 2020. 5, 6, 89

[133] Z. Zhang, J. Xu, and M. Liu. Constructions of optimal locally repairable codes over small fields. *Scientia Sinica Math.*, 47(11):1607–1614, 2017. 4

[134] K.-H. Zimmermann. *Integral Hecke modules, integral generalized Reed-Muller codes, and linear codes*, volume 96. Berichte des Forschungsschwerpunktes Informations- und Kommunikationstechnik, Techn. Univ. Hamburg-Harburg, Nov 1996. 26