UNIVERSIDADE ESTADUAL
DE CAMPINAS

INSTITUTO DE MATEMÁTICA, ESTATÍSTICA
E COMPUTAÇÃO CIENTÍFICA

CLAUDIO MICHAEL QURESHI VALDEZ

CÓDIGOS PERFEITOS NAS MÉTRICAS DE LEE E CHEBYSHEV E ITERAÇÕES DE FUNÇÕES DE RÉDEI

PERFECT CODES IN THE LEE AND CHEBYSHEV METRICS AND ITERATING RÉDEI FUNCTIONS

CAMPINAS
2015

CLAUDIO MICHAEL QURESHI VALDEZ

PERFECT CODES IN THE LEE AND CHEBYSHEV METRICS AND ITERATING RÉDEI FUNCTIONS

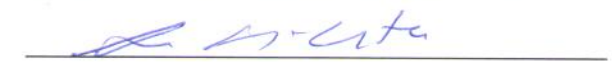
CÓDIGOS PERFEITOS NAS MÉTRICAS DE LEE E CHEBYSHEV E ITERAÇÕES DE FUNÇÕES DE RÉDEI

Thesis presented to the Institute of Mathematics, Statistics and Scientific Computing of the University of Campinas in partial fulfillment of the requirements for the degree of Doctor in Applied Mathematics.

Orientadora: SUELI IRENE RODRIGUES COSTA

Coorientador: DANIEL NELSON PANARIO RODRIGUEZ

O ARQUIVO DIGITAL CORRESPONDE À VERSÃO FINAL DA TESE DEFENDIDA PELO ALUNO CLAUDIO MICHAEL QURESHI VALDEZ, E ORIENTADA PELA PROFA. DRA. SUELI IRENE RODRIGUES COSTA.



CAMPINAS
2015

Agência(s) de fomento e nº(s) de processo(s): FAPESP, 2012/10600-2; CAPES

Ficha catalográfica
Universidade Estadual de Campinas
Biblioteca do Instituto de Matemática, Estatística e Computação Científica
Maria Fabiana Bezerra Muller - CRB 8/6162

Q62p

Qureshi Valdez, Claudio Michael, 1980-
Perfect codes in the Lee and Chebyshev metrics and iterating Rédei functions / Claudio Michael Qureshi Valdez. – Campinas, SP : [s.n.], 2015.

Orientador: Sueli Irene Rodrigues Costa.
Coorientador: Daniel Nelson Panario Rodriguez.
Tese (doutorado) – Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Códigos corretores de erros (Teoria da informação). 2. Teoria da codificação. 3. Teoria dos reticulados. 4. Geometria discreta. 5. Corpos finitos (Álgebra). I. Costa, Sueli Irene Rodrigues,1949-. II. Panario, Daniel,1959-. III. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. IV. Título.

Informações para Biblioteca Digital

Título em outro idioma: Códigos perfeitos nas métricas de Lee e Chebyshev e iterações de funções de Rédei
Palavras-chave em inglês:
Error-correcting codes (Information theory)
Codes theory
Lattice theory
Discrete geometry
Finite fields (Algebra)
Área de concentração: Matemática Aplicada
Titulação: Doutor em Matemática Aplicada
Banca examinadora:
Sueli Irene Rodrigues Costa [Orientador]
Michel Marie Deza
Marcelo Muniz Silva Alves
Emerson Luiz do Monte Carmelo
José Plínio de Oliveira Santos
Data de defesa: 28-08-2015
Programa de Pós-Graduação: Matemática Aplicada

Tese de Doutorado defendida em 28 de agosto de 2015 e aprovada

Pela Banca Examinadora composta pelos Profs. Drs.

Prof(a). Dr(a). SUELI IRENE RODRIGUES COSTA

Prof(a). Dr(a). MICHEL MARIE DEZA

Prof(a). Dr(a). MARCELO MUNIZ SILVA ALVES

Prof(a). Dr(a). EMERSON LUIZ DO MONTE CARMELO

Prof(a). Dr(a). JOSÉ PLÍNIO DE OLIVEIRA SANTOS

ACKNOWLEDGEMENT

I would like to thank God for getting up in the moments that it seems everything was uphill, for helping me achieve this goal which marks the beginning of a new stage. To all the pastors of the Universal Church who prayed for me when the situation became difficult.

Special thanks to my wife Rosanna, who always accompanies me and encouraged me to keep going during this PhD, for her love and patience which helped me get through this stage. Also to my daughter Yasmin that despite the bad sleeping nights, always gives me joy and a new reason to work hard every day. To my parents Susana and Jorge who always go along with me, striving to bring me good values, encouraging me to keep going and give me their trust and love. To my brothers Caro and Titi for all the support. To the Delgado family, especially the people of nona's house for their support in my travels to mathematical Olympiads during high school and to the Valdez family of the town of Rivera, Uruguay.

I greatly thank my supervisor Sueli Costa and my co-supervisor Daniel Panario for all your great support throughout this period. I am very fortunate to be working with them and thanks for all their advices and readiness, for their professional support and also for the human support. To the committee members of this PhD thesis for their attentive reading and valuable comments and suggestions. To professor Fernando Torres for their friendly discussions about codes and algebraic geometry during my PhD at University of Campinas. To the professors of UdelaR, who somehow helped me to reach this goal, especially Alfredo Jones, José Vieitez, Lanzilotta for recommended me to Unicamp, Gonzalo Tornaría for his guidance during mi master degree and the several useful discussion on number theory, Jana, Raul and Federico for their teaching on ergodic theory and to help me obtain financial support to make my stay at IMPA during my master degree. Also thanks to professor Ariel Affonso (president of the Uruguayan mathematical olympiad) for giving the opportunity to know how amazing is to solve math problems and help me to find my vocation. Thanks to the "Consejo de Educación Secundaria" of Uruguay and all staff and alumni of the high school institution "Liceo 10" for providing during my high school, all the support to my participation in international mathematical olympiads and a special thanks to the librarian Maria Pia.

To all institutions at which I have had the opportunity to teach allowing me to continue studying mathematics during my graduation and master degree: Universidad de la República (UdelaR), Universidad de Montevideo and the Universitario Autónomo del Sur.

To all institutions at which I have had an internship during my PhD: Mathematical Institute of Carleton University (Canada), Johann Radom institute for computational and applied mathematics (Austrian Academy of Sciences) and the department of computation of UFSC, Brazil.

To my friend Carlos Eduardo for his great help during my stay in Campinas, especially when I returned from my internship in Canada. To Junior and Luiz Fernando for helping me to find accommodation when I arrived to Campinas in the beginning of my PhD and to all my friends who accompanied me during my PhD. To my lab partners, for their friendship and helpful discussions in the blackboard, especially to Campello for his useful discussion about coding theory and Grasielle who presented to me a beautiful open problem, namely the Golomb-Welch conjecture. To Guillermo, Ariel, Viviana, Stefanie and all my friends from Uruguay who always supported me throughout this journey. To the "Boca Junior's barra brava" who came to São Paulo for cheering their team in the final of Libertadores cup in 2012 and helped me to get a return trip to Uruguay when Pluna airlines bankrupted so I could be on time for my wedding.

To the Dalipaj family who have greatly supported me during my staying in Canada and for their friendship, also to the family of Daniel Panario.

To all of them I dedicate this thesis.

Special thanks:

This work was supported by FAPESP foundation, through scholarship grants 2012/10600-2, BEPE 2014/04096-5 and the thematic project 2013/25977-7 "Security and reliability of informtaion: theory and practice", and also by CAPES (PhD scholarship from 01/03/2012 to 31/10/2012). Without this support this thesis would not have been possible.

RESUMO

O conteúdo desta tese insere-se dentro de duas áreas de pesquisa muito ativas: a teoria de códigos corretores de erros e sistemas dinâmicos sobre corpos finitos. Para abordar problemas em ambos os tópicos introduzimos um tipo de sequência finita que chamamos v-séries. No conjunto destas definimos uma métrica que induz uma estrutura de poset usada no estudo das possíveis estruturas de grupo abeliano representadas por códigos perfeitos na métrica de Chebyshev. Por outro lado, cada v-série é associada a uma árvore com raiz, a qual terá um papel importante em resultados relacionados à estrutura dinâmica de iterações de funções de Rédei. Na teoria de códigos corretores de erros, estudamos códigos perfeitos na métrica de Lee e na métrica de Chebyshev (correspondentes à métrica ℓ_p para $p = 1$ e $p = \infty$, respetivamente). Os principais resultados obtidos estão relacionados com a descrição dos códigos q-ários n-dimensionais com raio de empacotamento e, que sejam perfeitos nestas métricas, a obtenção de suas matrizes geradoras e a classificação destes, a menos de isometrias e a menos de isomorfismos. Várias construções de códigos perfeitos e famílias interessantes destes códigos com respeito à métrica de Chebyshev são apresentadas. Em sistemas dinâmicos sobre corpos finitos centramos nossa atenção em iterações de funções de Rédei, sendo o principal resultado um teorema estrutural para estas funções, o qual permite estender vários resultados sobre funções de Rédei. Este teorema pode também ser aplicado para outras classes de funções permitindo obter provas alternativas mais simples de alguns resultados conhecidos como o número de componentes conexas, o número de pontos periódicos e o valor esperado para o período e preperíodo da aplicação exponencial sobre corpos finitos.

Palavras-chave: Códigos perfeitos, métrica de Lee, conjectura de Minkowski, ladrilhamento por cubos, funções de Rédei.

ABSTRACT

The content of this thesis is inserted in two very active research areas: the theory of error correcting codes and dynamical systems over finite fields. To approach problems in both topics we introduce a type of finite sequence called ν-series. A metric is introduced in the set of such sequences inducing a poset structure used to determine all possible abelian group structures represented by perfect codes in the Chebyshev metric. Moreover, each ν-serie is associated with a rooted tree, which has an important role in results related to the cycle structure of iterating Rédei functions. Regarding the theory of error correcting codes, we study perfect codes in the Lee metric and Chebyshev metric (corresponding to the ℓ_p metric for $p = 1$ and $p = \infty$, respectively). The main results obtained are related to the description of n-dimensional q-ary codes with packing radius e which are perfect in these metrics, obtaining their generator matrices and their classification up to isometry and up to isomorphism. Several constructions of perfect codes in the Chebyshev metric are given and interesting families of such codes are presented. Regarding dynamical system over finite fields we focus on iterating Rédei functions, where our main result is a structural theorem, which allows us to extend several results on Rédei functions. The above theorem can also be applied to other maps, allowing simpler proofs of some known results related to the number of components, the number of periodic points and the expected value for the period and preperiod for iterating exponentiations over finite fields.

Keywords: Perfect codes, Lee metric, Minkowski's conjecture, cube tiling, Rédei functions.

CONTENTS

Chapter 1
INTRODUCTION

The Lee metric for n-dimensional codes over $\mathbb{Z}_q$, which coincides with the Hamming metric for $q = 2, 3$, was introduced in 1957-1958 [Lee58, Ulr57] for signal transmission over certain noisy channels. Since then, problems related to this metric have been approached in several works due to their applications [RS94, BM10, BBV98, Sch07, EY09], having many of them emerged in the last decade. Linear codes over $\mathbb{Z}_q$ are associated with lattices and have been used in the proposal of cryptographic schemes. One of the most important problems regarding the Lee metric is about the existence or non-existence of perfect codes which has been discussed in several papers [Ast82, Hor09, AHM09]. At first, only codes in the Lee metric over an alphabet $\mathbb{Z}_p$ with p a prime number were considered; then, in 1970 this approach was generalized by Golomb and Welch [GW70] for alphabet $\mathbb{Z}_q$ with arbitrary values of q. In that work, the authors presented their famous conjecture which in terms of codes over $\mathbb{Z}_q$ can be written as: for $n > 2$ and $q \geq 2e + 1$, the only n-dimensional perfect codes over $\mathbb{Z}_q$ are those with packing radius equal to 1.

The Lee metric is part of a family of more general metrics called the p-Lee metric (for $1 \leq p \leq \infty$). The use of these metrics in applications to coding and cryptography is relatively recent. For example, in [Pei08] it is studied the complexity of various computational problems related to codes in the ℓ_p norm such as the closest vector problem (CVP) and the shortest vector problem (SVP). In [JCC13] are presented some decoding algorithms for codes in the ℓ_p metric and some results there generalize known results in the Lee metric. In addition to the mentioned above, there are not many references in the literature on p-Lee metrics concerning error correcting codes, except for the specific values of p: $p = 1$ (Lee metric), $p = 2$ (Euclidean metric) and for $p = \infty$ (Chebyshev metric). In this work we focus mainly on the case $p = 1$ and $p = \infty$.

One motivation to the study of the Chebyshev metric is because it captures much of the essence of perfect codes in other p-Lee metrics since any perfect code in the ∞-Lee metric is also perfect in the p-Lee metric for large enough p [CCJ+14]. Other motivation is that for some specific values of p it is possible to prove that the only perfect codes in the p-Lee metric are also perfect codes either in the Lee metric or in the ∞-Lee metric. This is the case, for example, for the two-dimensional 2-Lee perfect codes [CJC+15].

Another motivation is the fact that q-ary perfect codes in the Chebyshev metric are associated with certain tilings by cubes of $\mathbb{R}^n$ which have intrinsic interest by themselves. In 1906, an interesting conjecture was proposed by Minkowski [Min07] while he was considering a problem in diophantine approximation. The Minkowski's conjecture states that in every tiling of $\mathbb{R}^n$ by cubes of the same length, where the centers of the cubes form a lattice, there exists two cubes that meet at an $(n-1)$-dimensional face. This conjecture was proved in 1942 by Hajós [Haj42]. A similar conjecture was proposed by Keller [Kel30] removing the restriction that the centers of the cubes have to form a lattice. However, this stronger version was shown to be true in dimensions $n \leq 6$ [Per40], false in dimensions $n \geq 8$ [LS92, Mac02] and it remains open in dimension $n = 7$. A lot of variants and related problems with cube tilings have been considered [KP08, KP12b, KP12a, SI10, SIP07] as well as application to other areas such as combinatorics and graph theory [CS90], coding theory [LS94], algebra [Sza04], harmonic analysis [Kol98], music theory [And04], among others.

Other topic covered in this thesis is regarding finite dynamics. Particularly dynamics of iterations of polynomials and rational functions over finite fields have attracted much attention in recent years. This is in part due to their applications in cryptography and integer factorization methods like *Pollard rho algorithm*; see for example [GLV00, JMV01, WZ99] for some applications in elliptic curve cryptography

In general, let $\mathcal{F}_n$ be the set of mappings from the set $\{1, 2, \ldots, n\}$ to itself. With any $\varphi \in \mathcal{F}_n$ it is associated a *functional graph* on n nodes, with a directed edge from vertex u to vertex v if and only if $\varphi(u) = v$. Functional graphs of mappings are sets of connected components; the components are directed cycles of nodes and each of those nodes is the root of a tree.

We are interested here in functions over finite fields. Iterations of functions over finite fields have centered on studies such as

- period and preperiod of an element;
- (average) "rho length" (number of iterations until we cycle back);
- number of connected components;
- length of cycles (largest, smallest, average);
- number of fixed points and conditions to have a permutation;
- isomorphism of graphs; and so on.

Iterations of some functions over finite fields have strong symmetries that can be mathematically explained. In that sense, previous results for several quadratic functions are in

[PMMnY01, Rog96, VS04]; iterations of $x+x^{-1}$ have been dealt in [Ugo14] and iterations of Chebyshev polynomials over finite fields have been treated in [Gas14]. An estimate for the number of non-isomorphic graphs of degree d polynomials is given in [KLM$^+$13]; in [MP12] some results on the asymptotic behavior for the tail and cycle length of random mappings with restricted preimages are provided. Algebraic dynamical systems generated by several rational functions on many variables over finite fields have also been considered; see Section 10.5 of [MP13].

The contributions of this thesis constitute Chapters 3, 4 and 5. In Chapter 3 we introduce a special type of finite sequences (called ν-series) with a metric (called multiplicative) which induces a poset structure in the set of such sequences. This poset structure allows us to introduce the relation "be more cyclic" between two abelian group which will be used in Chapter 4 to prove that the set of group structures represented by Chebyshev perfect codes with packing radius e and fixed cardinality is an ideal in this poset. On the other hand, every ν-series is associated with a rooted tree which will play a fundamental role in Chapter 5, in results related to the dynamic structure of iterating Rédei functions. The ν-series were introduced in [QP15] and they were also used in [QC15b].

Chapter 4 deals with error-correcting codes. We study q-ary perfect codes in the Lee metric and in the Chebyshev metric (corresponding to the ℓ_p metric for $p = 1$ and $p = \infty$). We consider admissible parameters (n, e, q) for which there exists n-dimensional q-ary perfect codes with packing radius e. The results obtained in this chapter are focused on the description of (n, e, q)-perfect codes, providing generator matrices and studying their isometry classes and isomorphism classes. For two dimensional codes this problem is solved completely, including the non-linear case, for both metrics. These results also can be used to characterize two-dimensional perfect codes with respect to the ℓ_p metrics for other values of p. Constructions of perfect codes from codes in smaller dimensions and via sections are introduced for the Chebyshev metric. Through these constructions it can be obtained families of cyclic perfect codes in all dimensions and the characterization of generator matrices for perfect codes in the Chebyshev metric. We introduce a subfamily of perfect codes (called maximal) for which we obtain a complete description of their isometry classes and isomorphism classes. Some results of this chapter were presented in [QC13, QC15a, QC15b, CCJ$^+$14].

Chapter 5 centers on dynamical system over finite fields. Many cryptographic algorithms and constructions of pseudorandom number generators are based on the iteration of certain functions defined over finite fields. Here our main result is a theorem which describes the dynamic of Rédei functions over finite fields. Some of the corollaries obtained are the description into disjoint cycles of Rédei functions when they are permu-

tation functions (extending known results), some formulas for the number of fixed points or periodic points as well as an algorithm to construct Rédei functions with prescribed length cycles. The refereed theorem can be applied to other maps, allowing to obtain alternative and simpler proofs of known results such as the number of connected components, number of fixed points and the expected value for the period and preperiod of the exponential map over finite fields. Most of the results of this chapter are collected in [QP15]. In Chapter 6 we list further interesting research problems.

Chapter 2
BACKGROUND

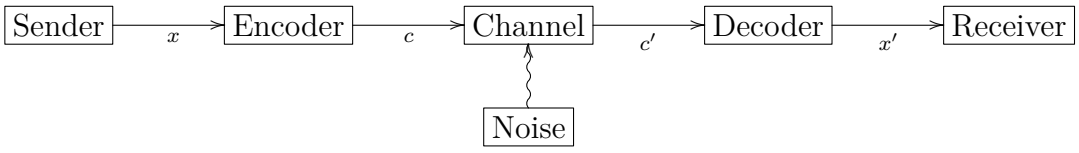
Coding theory involves the study of the properties of codes. It can be considered as part of information theory, where two main aspects are considered: reliability (error correcting codes) and security (cryptography). Codes are used for data compression, data storage and data transmission. The topics studied in this thesis are mostly related to information theory and more specifically with error correction.

The situation is roughly the following. Let us suppose that a message is to be sent through a communication channel. The characteristics of the channel depend on the nature of the message to be sent (i.e. sound, image, data). In general we have to transform our original message x into a message c which can be sent through the channel. This process is called codification. This coded message c can be distorted while it pass through the channel due to noise and interference, obtaining a message c', which may be different from c. Then the received message c' is decoded into original terms and what the receiver obtain, x', may be different from x (see picture below). The goal is to detect this error and correct it, if it is possible. Error-correcting codes focus on the second and fourth step of the scheme above, that is, coding and decoding the sent message and the problem of detection and correction of the received message.

This is a branch of information theory, which has as an important landmark, the work of Claude Shannon [Sha48] in 1948. In this field the whole process is considered as well as others related problems such as channel design, entropy, signal processing, compressing data, storing, etc.

In this work we consider a theoretical approach of channel codes, restricting our attention to the part concerned with detection and correction of error (i.e. to determine if $c = c'$ and to recover c from c' in the scheme above).

Associated with a noisy channel we have an error probability distribution.



Maximum likelihood decoding is the way to decode choosing the message (word) which has the greatest probability of having been sent. This process in general is very expensive and we have to adopt an alternative strategy. Let us suppose that the set X of all possible received words contain the set of all possible sent words C. In some cases it is possible to obtain a metric d in X which matches with the channel, in the sense that maximizing this probability is equivalent to minimizing the distance. This is the case for important types of channels such as the binary symmetric channel which matches with the Hamming metric, the most used metric in coding theory [MR91, Chapter 5].

If we denote by C the set of all the possible words to be sent, we say that C is a code in X and its elements are the codewords. Let us consider $X = \mathbb{Z}_q^n$ (in this case we say that C is an n-dimensional q-ary code) and let d be a metric invariant by translation (we will consider only this type of metrics) which matches with a noisy channel. Suppose that we transmit a word $c \in C$ and a word c' is received, if $d(c, c') = e_0$ we say that an error of distance e_0 with respect to the metric d has occurred in the transmission. An important parameter of a code is the packing radius which is defined as the smallest real number e which verify the following conditions:

(i) $B(c, e) \cap B(c', e) = \emptyset$ if $c, c' \in C$ and $c \neq c'$.

(ii) If $e' > e$ is such that $B(0, e) \subsetneq B(0, e')$ then there exists two codewords $c, c' \in C$ such that $B(c, e) \cap B(c', e) \neq \emptyset$.

The balls above are with respect to the metric d. We observe that if C is a code with packing radius e then if an error with distance $e' < e$ has occurred, then we obtain the original word when we decode by minimum distance (which in this case is the same that maximum likelihood decoding since we suppose that the metric matches with the channel). In this case we say that the code C is e-corrector or that C corrects up to distance e. So, the larger is a packing radius of a code the more its capacity of error-correction. Related to the packing radius we have the following result whose proof is straightforward [MR91, Chapter 5].

Proposition 2.0.1 (Sphere packing bound)**.** *If $C \subseteq \mathbb{Z}_q^n$ is a q-ary code with packing radius e (with respect some metric d) then $\#B(0, e) \leq q^n/\#C$.*

When the equality holds we say that C is a perfect code. Perfect codes are of special interest in coding theory and one of our main object of study in this thesis.

Remark 2.0.2. *In practice it is not enough to construct codes with large distance because we also need to have good algorithms to obtain the nearest codeword for the received word. In fact random codes are specially good in term of packing radius [Sha48] but they are not good in practice to be used for error-correction. Usually codes with certain algebraic*

structure (for example linear codes) are considered, due to they advantages in the coding-decoding processes.

Apart from the Hamming metric, one of the most used metric in error-correcting codes is the Lee metric which coincides with the first one for $q = 2$ and $q = 3$. This metric was introduced by Lee [Lee58] when he studied certain type of channels and it is defined as follows.

Definition 2.0.3 (Lee metric)**.** *Let $\mathbb{Z}_q = \{0, 1, 2, \ldots, q-1\}$ the set of integers modulo q. The Lee metric in $\mathbb{Z}_q$ is given by $d(x, y) = \min\{|x - y|, q - |x - y|\}$. This metric is extended to $\mathbb{Z}_q^n$ (for $n > 1$) as follows: if $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ belong to $\mathbb{Z}_q^n$ then $d_1(x, y) = \sum_{i=1}^n d(x_i, y_i)$ where d is the Lee metric in $\mathbb{Z}_q$.*

Golomb [Gol69] in 1969 already remarked that the most often used metrics in error-correcting codes such as the Hamming metric and the Lee metric among others come from the Lebesgue norm ℓ_p in $\mathbb{R}^n$. The p-norm in $\mathbb{R}^n$ is defined as follows: for $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$ we have

$$\begin{cases} |x|_p = \sum_{i=1}^n |x_i|^p & \text{if } 0 < p < 1, \\ |x|_p = (\sum_{i=1}^n |x_i|^p)^{\frac{1}{p}} & \text{if } 1 \leq p < \infty, \\ |x|_\infty = \max\{|x_i| : 1 \leq i \leq n\}. \end{cases} \tag{2.0.1}$$

If we consider the space $X = \mathbb{Z}_q^n$ (instead of $\mathbb{R}^n$) and we replace $|x|$ in Equation (2.0.1) by $|x|_1 = d(x, 0)$ (the Lee distance between $x \in \mathbb{Z}_q^n$ and 0) we obtain the p-Lee norm $|x|_{p,\text{Lee}}$ which induces the p-Lee metric $d_p(x, y) = |x - y|_{p,\text{Lee}}$ in $\mathbb{Z}_q^n$. When p approaches 0 the p-Lee metric is just the Hamming metric, when $p = 1$ we obtain the Lee metric and when $p = \infty$ this is the Chebyshev metric.

Next we present some notations and definitions related to error-correcting codes. We assume that a metric d in $\mathbb{Z}_q^n$ is given.

Definition 2.0.4. *An n-dimensional q-ary code is a subset $C \subseteq \mathbb{Z}_q^n$ (we assume here $\#C > 1$). An (n, e, q)-code is an n-dimensional q-ary code with packing radius e. A perfect (n, e, q)-code is also called a (n, e, q)-perfect code. A linear code is a code which is a subgroup of $\mathbb{Z}_q^n$. The minimum distance of C is $d_{min}(C) = \min\{d(x, y) : x, y \in \mathbb{Z}_q^n, x \neq y\}$. The covering radius is the smallest real number r such that for every $x \in \mathbb{Z}_q^n$ there exists $c \in C$ with $d(x, c) \leq r$.*

We consider in this work $d = d_p$ for $p \in [1, \infty]$ (and specially when $p = 1$ or $p = \infty$), so it is convenient to introduce the following notation.

Notation 2.0.5. *$PL^p(n, e, q)$ denotes the set consisting of all (n, e, q)-perfect codes. The subset of linear codes is denoted by $LPL^p(n, e, q)$.*

Definition 2.0.6. *Let $C \in PL^p(n,e,q)$. The error-correcting function of C is the function $f_C : \mathbb{Z}_q^n \to C$ given by the property $d_p(x, f_C(x)) \leq e$.*

Remark 2.0.7. *From here on we will use the same notation d_p to denote the p-Lee metric in $\mathbb{Z}_q^n$ and the ℓ_p metric in $\mathbb{Z}^n$ (i.e. the metric induced by the ℓ_p norm).*

There is a strong relation between n-dimensional q-ary codes and q-periodic sets of $\mathbb{R}^n$, that is, subsets Λ such that $q\mathbb{Z}^n + \Lambda = \Lambda$ (here the sum is the Minkowski sum of the two sets, namely $A + B = \{a + b : a \in A, b \in B\}$).

We consider the map $\pi : \mathbb{Z}^n \to \mathbb{Z}_q^n$ taking modulo q in each coordinate which establishes a correspondence between q-ary codes and q-periodic sets known in the literature as Construction A [CS13]. For $C \subseteq \mathbb{Z}_q^n$ we denote by $\Lambda_C = \pi^{-1}(C)$ the corresponding q-periodic set given by Construction A. This correspondence preserve linearity, so every q-ary linear code $C \subseteq \mathbb{Z}_q^n$ correspond with a q-periodic full-rank lattice $\Lambda_C \subseteq \mathbb{Z}^n$, that is, a subgroup of $\mathbb{R}^n$ of the form $v_1\mathbb{Z} + \cdots + v_n\mathbb{Z}$ where $\{v_1, \ldots, v_n\}$ is a basis of $\mathbb{R}^n$ as $\mathbb{R}$-vector space (see [Zam09] for more about lattices and coding theory and [Mar03] for algebraic background about lattices). An n-dimensional full-rank lattice of $\mathbb{R}^n$ is also called an n-dimensional lattice.

Linear codes - isometry and isomorphism

Now we focus on the linear case and we consider only isometries of $\mathbb{Z}_q^n$ with respect to the p-Lee metric that preserve linearity, that is, homomorphisms $f : \mathbb{Z}_q^n \to \mathbb{Z}_q^n$ such that $|f(x)|_p = |x|_p$.

Notation 2.0.8. *We denote by $[n] = \{1, 2, \ldots, n\}$. We let S_n be the permutation group of $[n]$ and let e_i represents a vector (in $\mathbb{Z}_q^n$ or $\mathbb{R}^n$) which has 1 in the i-th coordinate and 0 otherwise. If x is a vector (in $\mathbb{Z}_q^n$ or $\mathbb{R}^n$) we denote by x_i for $i = 1, 2, \ldots, n$ its coordinates, that is, $x = \sum_{i=1}^n x_i e_i$. We denote by $\mathcal{G}(n,q,p)$ the group of isometries of $\mathbb{Z}_q^n$ with respect to the p-Lee metric (or simply by $\mathcal{G}$ when n, q and p are understood by the context).*

For $a \in \mathbb{Z}_2^n$ we define $\eta_a : \mathbb{Z}_q^n \to \mathbb{Z}_q^n$ such that $\eta_a(x) = \sum_{i=1}^n (-1)^{a_i} x_i e_i$ and for $\theta \in S_n$ we define $\xi_\theta : \mathbb{Z}_q^n \to \mathbb{Z}_q^n$ such that $\xi_\theta(x) = \sum_{i=1}^n x_i e_{\theta(i)}$. It is easy to see that these maps are isometries of $\mathbb{Z}_q^n$ which verify $\eta_a\eta_b = \eta_{a+b}$ for all $a, b \in \mathbb{Z}^2$ and $\xi_\theta\eta_a = \eta_b\xi_\theta$ where $b_i = a_{\theta^{-1}(i)}$ for all $a \in \mathbb{Z}_2^n$ and $\theta \in S_n$. This implies that the group generated by these maps is $\{\eta_a\xi_\theta : a \in \mathbb{Z}_2^n, \theta \in S_n\}$.

p-Lee isometries, the case $p \in [1, \infty)$

Let f be an isometry of $\mathbb{Z}_q^n$ with respect to the p-Lee metric with $p \in [1, \infty)$. For each $i \in [n]$, we have $|f(e_i)|_p = 1$ so $f(e_i) = (-1)^{a_i} e_{\theta(i)}$ for some $a_i \in \mathbb{Z}_2$ and $\theta(i) \in [n]$. Since isometries are injective functions then $\theta(i) \neq \theta(j)$ for $i \neq j$ so $f = \eta_a\xi_\theta$ with $a = (a_1, \ldots, a_n) \in \mathbb{Z}_2^n$ and $\theta \in S_n$. So, in this case $\mathcal{G} = \{\eta_a\xi_\theta : a \in \mathbb{Z}_2^n, \theta \in S_n\}$.

p-Lee isometries, the case $p = \infty$

We observe that if $q \leq 3$ and $p = \infty$ every non-zero vector has norm 1. Hence, the group of isometries coincides with the group of injective homomorphisms. Let f be an isometry of $\mathbb{Z}_q^n$ where $q > 3$, with respect to the Chebyshev metric (i.e. ∞-Lee metric). Since $|f(e_i)|_\infty = 1$ then every non-zero coordinate of e_i is ± 1. Consider the set $A(i) = \{j \in [n] : \text{the } j\text{-th coordinate of } f(e_i) \text{ is } \pm 1\}$. If $k \in A(i) \cap A(j)$ with $i \neq j$ then either $f(e_i) + f(e_j)$ or $f(e_i) - f(e_j)$ has it k-th coordinate ± 2 which is a contradiction if $q > 3$ because $|e_i \pm e_j|_\infty = 1$. Thus, the $A(i)$ are disjoints for $1 \leq i \leq n$ and non-empty (since f is injective) thus $\#A(i) = 1$ and we obtain the same conclusion that in the case $p \in [1, \infty)$, namely $\mathcal{G} = \{\eta_a \xi_\theta : a \in \mathbb{Z}_2^n, \theta \in S_n\}$.

Except for the cases $(p, q) = (\infty, 2)$ and $(p, q) = (\infty, 3)$ the group of isometries of $\mathbb{Z}_q^n$ is given by $\mathcal{G} = \{\eta_a \xi_\theta : a \in \mathbb{Z}_2^n, \theta \in S_n\}$. Moreover, if we consider the action $\varphi : S_n \times \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ given by $\theta a = (a_{\theta^{-1}(1)}, \ldots, a_{\theta^{-1}(n)})$ we have $\xi_\theta \eta_a = \eta_{\theta a} \xi_\theta$ so $\mathcal{G} \simeq \mathbb{Z}_2^n \rtimes S_n$ (the semidirect product with respect to this action). In summary, we have the following proposition.

Proposition 2.0.9. *If $(p, q) = (\infty, 2)$ or $(p, q) = (\infty, 3)$ every injective homomorphism of $\mathbb{Z}_q^n$ is also a isometry. Otherwise, the group of isometries of $\mathbb{Z}_q^n$ with respect to the p-Lee metric is given by $\mathcal{G} = \{\eta_a \xi_\theta : a \in \mathbb{Z}_2^n, \theta \in S_n\}$ (with the notation above) and we have the isomorphism $\mathcal{G} \simeq \mathbb{Z}_2^n \rtimes S_n$ with respect to this action given above.*

Remark 2.0.10. *With the notation above, we have an action $\phi : S_n \times \mathbb{Z}_q^n \to \mathbb{Z}_q^n$ given by $(\theta, x) \mapsto \xi_\theta(x)$. When we write θx for $\theta \in S_n$ and $x \in \mathbb{Z}_q^n$ we refer to this action (i.e. $\theta x = \xi_\theta(x)$).*

Isomorphism class of codes

Definition 2.0.11. *Let Λ be an n-dimensional lattice. A generator matrix for Λ is an $n \times n$ matrix (with real coefficients) such that its lines generate the lattice Λ as $\mathbb{Z}$-module. In this thesis, when we write that M is a generator matrix for a q-ary linear code C we mean that M is a generator matrix for its associate lattice Λ_C. An n-dimensional integer lattice is a lattice contained in $\mathbb{Z}^n$.*

Notation 2.0.12. *If M is an $n \times n$ matrix with coefficients in $\mathbb{Z}_q$ or $\mathbb{R}$, we denote by span(M) the $\mathbb{Z}$-module generated by this lines (i.e. linear combination of the lines with integer coefficients).*

Remark 2.0.13. *Let C be a q-ary linear code, Λ_C be its associated lattice and $M \in \mathcal{M}_n(\mathbb{Z})$ (integer $n \times n$ matrix) such that the lines of M generates C when they are considered modulo q. In this case Λ_C is generated by the lines of M and the vectors qe_i for $1 \leq i \leq n$, so M is a generator matrix for Λ_C if and only if $q\mathbb{Z}^n \subseteq$ span(M) which*

is equivalent to $AM = qI$ for some $A \in \mathcal{M}_n(\mathbb{Z})$ (where I denote the identity matrix). Therefore M is a generator matrix for C if and only if the matrix qM^{-1} has integer coefficients.

Next, we prove that if C is a linear q-ary code with generator matrix M then its cardinality is given by $q^n/\det(M)$ and its group isomorphism class is determined by the Smith normal form of A. Considering the natural projection $\pi : \Lambda_C \to \mathbb{Z}_q^n$ (taking modulo q in each coordinate) which verifies $\ker(\pi) = q\mathbb{Z}^n$ and $\mathrm{Im}(\pi) = C$, we obtain the following result as consequence of the first group isomorphism theorem [Fra13, p. 307].

Proposition 2.0.14. *If M is a generator matrix for a linear code $C \subseteq \mathbb{Z}_q^n$ (i.e. a generator matrix for Λ_C), then $C \simeq \Lambda_C/q\mathbb{Z}^n$.*

For $\alpha = \{v_1, \ldots, v_n\}$ a basis of $\mathbb{R}^n$ and $v = \sum_{i=1}^n \alpha_i v_i$ we denote by $\mathrm{coord}_\alpha(v) = (\alpha_1, \ldots, \alpha_n) \in \mathbb{R}^n$ the coordinates of v with respect to the basis α. If β is other basis of $\mathbb{R}^n$ we denote by ${}_\alpha(I)_\beta = \begin{pmatrix} \mathrm{coord}_\beta(v_1) \\ \vdots \\ \mathrm{coord}_\beta(v_n) \end{pmatrix}$ the change of basis matrix, from the basis α to the basis β. We remark that when the lattices associated with α and β verify $\Lambda_\alpha \subseteq \Lambda_\beta$, the change of basis matrix ${}_\alpha(I)_\beta$ is an $n \times n$ matrix with integer coefficients. We identify the set $\mathbb{Z}^n$ with the set of matrices $\mathcal{M}_{1\times n}(\mathbb{Z})$.

Proposition 2.0.15. *Let $\alpha = \{v_1, \ldots, v_n\}, \beta = \{w_1, \ldots, w_n\}$ be two basis of $\mathbb{R}^n$ and $\Lambda_\alpha, \Lambda_\beta$ be their associated lattices. We assume that $\Lambda_\alpha \subseteq \Lambda_\beta$. If $A =_\alpha (I)_\beta$ is the change of basis matrix from the basis α to the basis β and $D = diag(d_1, \ldots, d_n)$ is its Smith normal form (i.e. the only diagonal matrix verifying $D = PAQ$ with P and Q unimodular matrices), then $\frac{\Lambda_\beta}{\Lambda_\alpha} \simeq \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_m}$.*

Proof. The change of basis matrix verifies $\mathrm{coord}_\alpha(v)A = \mathrm{coord}_\beta(v)$ and consequently $A \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$. If $D = PAQ$ is the Smith normal form of A (where $\det(P) = \pm 1, \det(Q) = \pm 1$) then:

$$DQ^{-1} \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} = PA \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} = P \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}. \tag{2.0.2}$$

Denoting by $\begin{pmatrix} w'_1 \\ \vdots \\ w'_n \end{pmatrix} = Q^{-1} \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix}$ and substituting in Equation (2.0.2) we have:

$$P \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = D \begin{pmatrix} w'_1 \\ \vdots \\ w'_n \end{pmatrix} = \begin{pmatrix} d_1 w'_1 \\ \vdots \\ d_n w'_n \end{pmatrix}.$$

Since P and Q are unimodular matrices, then $\{d_1 w'_1, \ldots, d_n w'_n\}$ and $\{w'_1, \ldots, w'_n\}$ are also $\mathbb{Z}$-basis of α and β, respectively. The epimorphism $\phi : \mathbb{Z}^n \twoheadrightarrow \frac{\Lambda_\beta}{\Lambda_\alpha}$ given by $\phi(e_i) = w'_i + \Lambda_\alpha$ verifies $\phi \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$ if and only if $\sum_{i=1}^n m_i w'_i \in \Lambda_\alpha = d_1 w'_1 \mathbb{Z} + \ldots + d_n w'_n \mathbb{Z}$ which is equivalent to $m_i = 0 \pmod{d_i}, \forall i : 1 \leq i \leq n$. Thus, the kernel of ϕ is given by $\ker(\phi) = d_1\mathbb{Z} + \cdots + d_n\mathbb{Z}$, therefore

$$\frac{\Lambda_\beta}{\Lambda_\alpha} \simeq \frac{\mathbb{Z}^m}{d_1\mathbb{Z} + \cdots + d_n\mathbb{Z}} \simeq \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_n}$$

as claimed. □

If the generator matrix of the $C \subseteq \mathbb{Z}_q^n$ is given by $M = \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} \in \mathcal{M}_n(\mathbb{Z})$, using Proposition 2.0.15 respect to the basis $\alpha = \{qe_1, \ldots, qe_n\}$ (so $\Lambda_\alpha = q\mathbb{Z}^n$) and $\beta = \{w_1, \ldots, w_n\}$ (so $\Lambda_\beta = \Lambda_C = w_1\mathbb{Z} + \cdots + w_n\mathbb{Z}$), the matrix $A = \alpha(I)\beta$ whose Smith normal form determines the structure of $\Lambda_C/qZ^n = \Lambda_\beta/\Lambda_\alpha = C$ verifies $AM = qI$ so $A = qM^{-1}$. In summary we have the following proposition.

Proposition 2.0.16. *Let $D = diag(d_1, \ldots, d_n)$ be the Smith normal form of $qM^{-1} \in \mathcal{M}_n(\mathbb{Z})$ where M is the generator matrix for Λ_C. Then, $C \simeq \mathbb{Z}_{d_1} \times \ldots \times \mathbb{Z}_{d_n}$.*

Since $d_1 \ldots d_n = \det(A) = \det(qM^{-1}) = q^n / \det(M)$ we obtain the following corollary.

Corollary 2.0.17. *If M is a generator matrix for C, then $\#C = \frac{q^n}{\det(M)}$.*

Torus, polyominoes and polycubes

In the seminal paper of Golomb and Welch [GW70], the authors use an approach based on polyominoes and polycubes to settle several results in perfect Lee codes over large alphabets. We use a similar approach to settle results about perfect codes in the Chebyshev metric.

Definition 2.0.18. *A polycube P in $\mathbb{R}^n$ is a connected set formed by the union of a finite number of unitary cubes centered at integers points, in such a way that given two centers of cubes c and c' there exists a sequence of centers of cubes $c_0 = c, c_1, \ldots, c_k = c'$ such that $|c_i - c_{i-1}|_2 = 1$ for $1 \leq i \leq k$. When $n = 2$ a polycube is also called polyominoe.*

The n-dimensional q-ary flat torus $\mathcal{T}_q^n$ is obtained from the cube $[0, q]^n$ by identifying its opposite faces $H_i^- = [0, q]^n \cap \{x_i = 0\}$ and $H_i^+ = [0, q]^n \cap \{x_i = q\}$ via $f_i : H_i^- \to H_i^+$, $f_i(x) = x + qe_i$ (see Figure 2.1). It can also be obtained through the quotient $\mathcal{T}_q^n = \mathbb{R}^n/q\mathbb{Z}^n$, inheriting a natural group structure induced by this quotient. Given a invariant-by-translation metric d in $\mathbb{R}^n$, every ball $B = B(0, r)$ in this metric have an associated polycube $P_B \subseteq \mathbb{R}^n$ given by $P_B = \biguplus_{x \in B \cap \mathbb{Z}^n} x + [-1/2, 1/2]^n$ (see Figure 2.2).

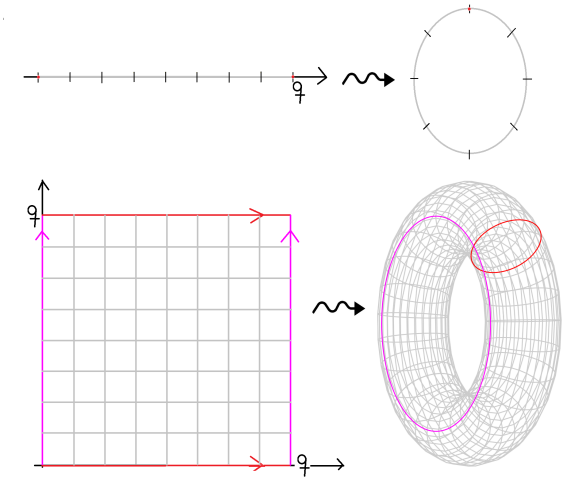


Figure 2.1: The torus in dimension one and two, obtained identifying opposite faces of the n-cube for $n = 1, 2$.

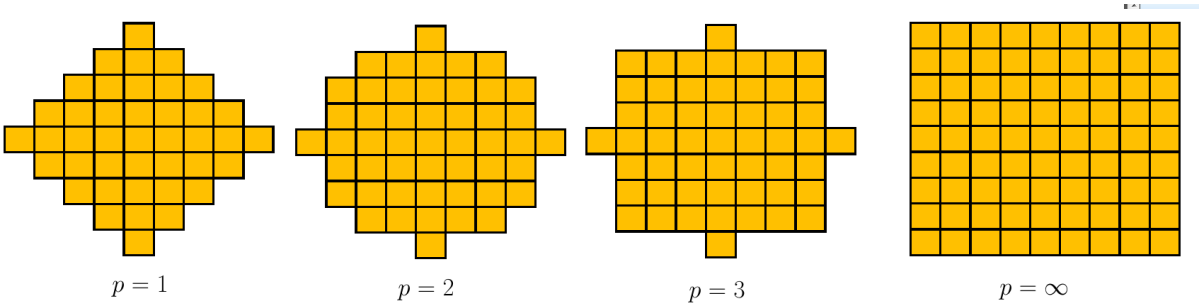


Figure 2.2: Polyominoes associated with two-dimensional p-balls of radius 4.

In this way, tiling $\mathbb{Z}^n$ by translated copies of B is equivalent to tiling $\mathbb{R}^n$ by translated copies of its associated polycube P_B. When there exists a translated copy of

this polycube inside the q-ary cube (i.e. if there exists $t \in \mathbb{R}^n$ such that $t + P_B \subseteq [0, q]^n$), tiling $\mathbb{R}^n$ by translated copies of P_B is in turn equivalent to tiling the q-ary n-torus $\mathcal{T}_q^n$ by copies of $\overline{P_B}$. This association gives us an important geometric tool to study perfect codes over $\mathbb{Z}$.

Cube tilings

Since we consider the Chebyshev metric, the polyominoes associated with balls in this metric correspond to cubes of odd length centered at an integer point $x \in \mathbb{Z}^n$ (only this type of cubes will be considered in this paper). The condition $q = (2e+1)t$ guarantees the equivalence above, so there is a correspondence between tiling of the torus $\mathcal{T}_q^n$ by cubes and perfect codes in $LPL^\infty(n, e, q)$.

Definition 2.0.19. *An n-dimensional cartesian q-ary code is a code of the form $(2e+1)\mathbb{Z}_q^n$ for some $e \in \mathbb{N}$ such that $2e+1 \mid q$. A linear q-ary code is a subgroup of $(\mathbb{Z}_q^n, +)$ (example in Figure 2.3). A cyclic q-ary code is a linear q-ary code which is cyclic as abelian group. The code $C = \mathbb{Z}_q^n$ is always a perfect code and we refer to this code as the trivial code.*

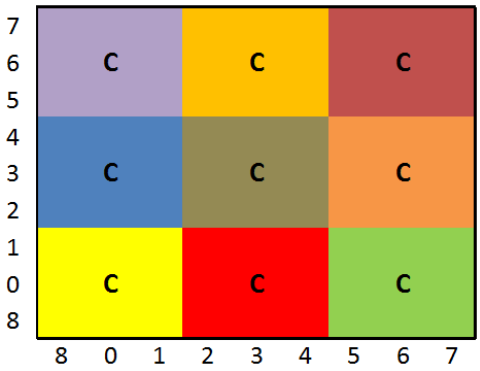


Figure 2.3: The cartesian code $3\mathbb{Z}_9^2 \in LPL^\infty(2, 1, 9)$ (codewords are marked with C).

Definition 2.0.20. *A code $C \in PL^\infty(n, e, q)$ is standard if there exist a canonical vector e_i (i.e. a vector with an 1 in the i-th coordinate and 0 in the other coordinates) for some $i : 1 \leq i \leq n$ such that $C + (2e+1)e_i \subseteq C$. In this case we also say that C is of type i; see Figure 2.4.*

As we will see later (see Remark 4.2.29), a code can have no type or it can have more than one type (for example n-dimensional cartesian codes are of type i for $1 \leq i \leq n$).

The following theorem of Hajos [Sza04], known also as Minkowski Conjecture, is of fundamental importance when we approach perfect codes in arbitrary dimension.

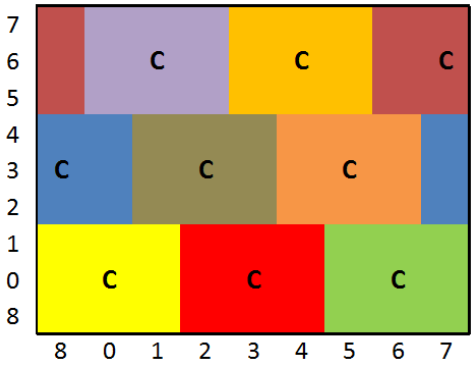


Figure 2.4: The cyclic perfect code $C = \langle (2,3) \rangle \in \mathbb{Z}_9^2 \in CPL^\infty(2,1,9)$ is a type 1 code but is not a type 2 code (codewords are marked with C).

Theorem 2.0.21 (Minkowski-Hajos)**.** *Every tiling of $\mathbb{R}^n$ by cubes of the same length whose centers form a lattice contains two cubes that meet at an $n-1$ dimensional face.*

Corollary 2.0.22. *Every linear perfect code $C \in LPL^\infty(n,e,q)$ is standard.*

Some notation and definitions

In Section 4.2 we will parametrize isomorphism classes of perfect codes through certain generalized cosets of $\mathbb{Z}_d$ that we introduce in the next definition.

Definition 2.0.23. *Let A be an abelian ring with unit and A^* the multiplicative group of its invertible elements. A generalized coset is a set of the form xC where C is a subgroup of A^* (i.e. $C < A^*$). We denote by $A/C = \{xC : x \in A\}$.*

Remark 2.0.24. *Let $C < A^*$ and $x, y \in A$. If $xC \cap yC \neq \emptyset$ then $xC = yC$, so C induce an equivalence relation in A whose equivalence classes are given by xC with $x \in A$. In this way A/C is just the quotient set with respect to this equivalence relation.*

Next we introduce some notations that will be used later.

Notation 2.0.25. *Let A be a ring (in particular a $\mathbb{Z}$-module) and $a \in A$.*
- *$\mathcal{M}_{m\times n}(A)$ denotes the set of rectangular matrices $m \times n$ with coefficients in A. In particular we identify A^n with $\mathcal{M}_{1\times n}(A)$. When $m = n$, we set $\mathcal{M}_n(A) = \mathcal{M}_{n\times n}(A)$.*
- *$\nabla_n(A)$ denotes the set of upper triangular matrices in $\mathcal{M}_n(A)$ and $\nabla_n(a, A)$ is the subset of $\nabla_n(A)$ whose elements in the principal diagonal are all equals to a. For $A = \mathbb{Z}$, we set $\nabla_n(a) = \nabla_n(a, \mathbb{Z})$.*
- *For $x \in \mathbb{Z}^n$ we denote by $\overline{x} = x + q\mathbb{Z}^n \in \mathbb{Z}_q^n$. If $M \in \mathcal{M}_n(\mathbb{Z})$ we denote by $\overline{M}$ the matrix obtained from M taking modulo q in each coordinate.*

Chapter 3
THE V-SERIES

In this chapter we introduce the concept of ν-series that plays an important role in the next chapters. In Chapter 4 they will be used in Section 4.5 in order to obtain structural information about the group isomorphism classes represented by Chebyshev perfect codes and in Chapter 5 they help to describe isomorphism classes of the function graph associated with Rédei functions and n-maps.

3.1 Definition and examples

Definition 3.1.1. *Let $\nu > 1$ be an integer. A ν-series is a finite sequence of positive integers $V = (\nu_1, \nu_2, \ldots, \nu_n)$ such that*

i) $\nu_{i+1} \mid \nu_i$ for $1 \leq i \leq n-1$;

ii) $\nu = \prod_{i=1}^{D} \nu_i$.

The numbers ν_i for $1 \leq i \leq n$ are the components of V and n is its length. The number $D = \max\{i : \nu_i > 1, 1 \leq i \leq n\}$ is the depth of V (where $D = 0$ when this set is empty) that is denoted by depth(V). We say that V is reduced if $\nu_n > 1$ or $V = (1)$.

Example 3.1.2. *$V = (24, 24, 6, 2, 2)$ is a 13824-series with depth$(V) = 5$.*

The radical of a positive integer n is the product of the distinct prime divisors of n and is denoted by $\mathrm{rad}(n)$; by convention $\mathrm{rad}(1) = 1$. If ν and n are positive integers with $\mathrm{rad}(\nu) \mid \mathrm{rad}(n)$, we have a particular way, to be given next, to construct ν-series in which each component is a divisor of n.

Definition 3.1.3. *If $\nu > 1$ and n are positive integers with rad$(\nu) \mid$ rad(n) the ν-series generated by n, denoted by $\nu(n)$ is defined as*

$$\begin{cases} \nu_1 = \gcd(\nu, n), \\ \nu_{i+1} = \gcd\left(\frac{\nu}{\nu_1 \nu_2 \ldots \nu_i}, n\right) & \text{for } i \geq 1. \end{cases}$$

If $D = \max\{i \geq 1 : \nu_i > 1\}$, we define $\nu(n) = (\nu_1, \nu_2, \ldots, \nu_D)$. By convention, for $\nu = 1$ we define $\nu(n) = (1)$ for all n.

Proposition 3.1.4. *The ν-series generated by n with $rad(\nu) \mid rad(n)$ is well defined. Moreover, if $D = \max\{\lceil e_p(\nu)/e_p(n)\rceil : p \mid n,\ p \text{ prime}\}$ where $e_p(n)$ denotes the exponent of the prime p in n, then D is the depth of $\nu(n)$.*

Proof. We observe first that if p is a prime number that does not divide n, then $e_p(\nu_i) = 0$ for all $i \geq 1$. On the other hand, if p is a prime divisor of n and $e_p(\nu) = qe_p(n) + r$ with $0 \leq r < e_p(n)$, one can prove by induction that

$$e_p(\nu_i) = \begin{cases} e_p(n) & \text{if } 1 \leq i \leq q, \\ r & \text{if } i = q+1, \\ 0 & \text{if } i > q+1. \end{cases}$$

From this, we have that $\nu(n)$ is a ν'-series with depth $D = \max\{\lceil e_p(\nu)/e_p(n)\rceil : p \mid n,\ p \text{ prime}\}$, where

$$\nu' = \prod_{i=1}^{D} \nu_i = \prod_{p|n} p^{e_p(\nu)}.$$

Now, as $\mathrm{rad}(\nu) \mid \mathrm{rad}(n)$ the last equation implies $\nu' = \nu$. □

We observe that with the notation above

$$D = \min\{\lambda \in \mathbb{Z}^+ : \nu \mid n^\lambda\}.$$

Example 3.1.5. *If we take $\nu = 360, n = 30$, the 360-series V associated with $n = 30$ is*

$$\begin{cases} \nu_1 = \gcd(360, 30) = 30, & \nu/\nu_1 = 360/30 = 12; \\ \nu_2 = \gcd(12, 30) = 6, & \nu/(\nu_1\nu_2) = 12/6 = 2; \\ \nu_3 = \gcd(2, 30) = 2, & \nu/(\nu_1\nu_2\nu_3) = 2/2 = 1. \end{cases}$$

Therefore $V = 360(30) = (30, 6, 2)$. The depth of this 360-series is 3.

3.2 Posets associated with ν-series

In this section we introduce a graph whose vertices are t^n-series (for some positive integer t) of length n, which will be used in Section 4.5 to describe structural information about the group isomorphism classes represented by perfect codes in the Chebyshev metric.

Notation 3.2.1. *We denote by $\mathcal{S}_n(\nu)$ the set consisting of ν-series of length n. For $a = (a_1, \ldots, a_n) \in \mathcal{S}_n(\nu)$ we denote by $\mathbb{Z}_a = \mathbb{Z}_{a_1} \times \cdots \times \mathbb{Z}_{a_n}$.*

Sometimes we use this correspondence and we identify the set $\mathcal{S}_n(\nu)$ with the corresponding set of abelian groups.

Definition 3.2.2. *Let $\mathbb{N}^\infty$ be the set of non-negative integer sequences which are zero for all but a finite number of terms and $\ell : \mathbb{Z}^+ \to \mathbb{N}^\infty$ given by $\ell(p_1^{\alpha_1} p_2^{\alpha_2} \ldots) = (\alpha_1, \alpha_2, \ldots)$ where $(p_n)_{n\geq 1}$ is the sequence of prime numbers. We define the multiplicative distance in $(\mathbb{Z}^+)^n$ as following:*

$$mdist(x, y) := \sum_{i=1}^{n} ||\ell(x_i) - \ell(y_i)||_1.$$

Denoting by $e_p(m)$ the exponent of the prime p in the factorial decomposition of m, we observe that for $x, y \in \mathbb{Z}^+$ we have $||\ell(x) - \ell(y)||_1 = \sum_{i=1}^{\infty} |e_{p_i}(x) - e_{p_i}(y)|$ where p_n denotes the n-th prime number.

Definition 3.2.3. *For $t \in \mathbb{Z}^+$ the t-energy is the function $E_t : (\mathbb{Z}^+)^n \to \mathbb{N}$ given by*

$$E_t(x) := \sum_{i=1}^{n} mdist(x_i, t) = mdist(x, (t, t, \ldots, t)).$$

The t-energy is defined in $\mathcal{S}_n(\nu)$ by identifying this set with the corresponding subset of $(\mathbb{Z}^+)^n$. We also remark that the set $\mathcal{S}_n(\nu)$ is in correspondence with isomorphism classes of abelian groups of order ν and in some cases we will use this identification.

Definition 3.2.4. *For $\nu = t^n$ we define the (directed) graph associated with $\mathcal{S}_n(\nu)$, which we denote by $\mathcal{G}_n(t)$, as the graph whose vertices set is $V = \mathcal{S}_n(\nu)$ and $\overrightarrow{xy}$ is a directed edge for this graph if $mdist(x, y) = 2$ and $E_t(x) > E_t(y)$.*

It is interesting to remark that for two distinct elements $x, y \in \mathcal{S}_n(\nu)$ we have $\mathrm{mdist}(x, y) \geq 2$.

Proposition 3.2.5. *If we define the relation in $\mathcal{S}_n(t^n)$ given by $x \geq y$ if $x = y$ or there exists a directed path in $\mathcal{G}_n(t)$ from x to y, then $(\mathcal{S}_n(t^n), \geq)$ is a poset.*

Proof. Reflexivity and transitivity follow directly from definition. It is easy to see from definition that the directed graph $\mathcal{G}_n(t)$ has no directed cycles and this implies the anti-symmetry of $\geq$. □

Next, we prove that the poset $\mathcal{S}_n(t^n)$ has a minimum element and a maximum element.

Proposition 3.2.6. *The poset $\mathcal{S}_n(t^n)$ has minimum element $m = (t, t, \ldots, t)$ and maximum element $M = (t^n, 1, \ldots, 1)$.*

Proof. Let $\nu = (\nu_1, \ldots, \nu_n) \in \mathcal{S}_n(t^n)$. On the one hand, if $\nu \neq m$ then there exists a prime $p \mid t$ such that $e_p(\nu_1) > e_p(t) > e_p(\nu_n)$ (where $e_p(a)$ denotes the exponent of p in a). Considering i maximum and j minimum such that $e_p(\nu_i) > e_p(t) > e_p(\nu_j)$ and $w \in \mathcal{S}_n(t^n)$ such that $w_i = \nu_i/p, w_j = p\nu_j$ and $w_k = \nu_k$ for $1 \leq k \leq n, k \notin \{i, j\}$ we have that $w < \nu$. On the other hand, if $\nu \neq M$ then $\mathrm{depth}(\nu) = D > 1$. Considering a prime $p \mid \nu_D$ and

$w \in \mathcal{S}_n(t^n)$ such that $w_1 = p\nu_1, w_D = \nu_D/p$ and $w_k = \nu_k$ for $1 \leq k \leq n, k \notin \{i, j\}$ we have that $w > \nu$. Hence, for all $\nu \in \mathcal{S}_n(t^n)$ we have $m \leq \nu \leq M$, so m is minimum and M is maximum. □

Remark 3.2.7. *By the association between t^n-series and group isomorphism classes of abelian group of order t^n, the previous proposition implies that the cyclic group $\mathbb{Z}_{t^n}$ is the biggest element and the cartesian group $\mathbb{Z}_t^n$ is the smallest element between all group isomorphism classes of abelian group of order t^n.*

3.3 Trees associated with ν-series

In this section we associate a rooted tree to each ν-series. This tree plays an important role in the description of the non-periodic part of some functional graphs that are studied in Chapter 5.

Let $G = (V, E)$ be a directed graph and $G_i = (V_i, E_i)$ be subgraphs of G for $1 \leq i \leq m$. The notation $G = \bigoplus_{i=1}^m G_i$ means that $V = \biguplus_{i=1}^m V_i$, the disjoint union of the sets V_i, and $E = \biguplus_{i=1}^m E_i$, the disjoint union of the edges in E_i. We denote by $\bullet$ any graph consisting of a unique vertex and by $\simeq$ the isomorphism relation. If H denotes a directed graph (or the isomorphism class of some directed graph) and $n \in \mathbb{Z}^+$, then $G \simeq n \times H$ means $G = \bigoplus_{i=1}^n G_i$ with each $G_i \simeq H$. We also consider the graph $\emptyset$ as a graph without vertices and edges. As our goal is to describe some functional graph, it is convenient to introduce the following definition.

Definition 3.3.1. *Let T be a rooted tree and $f \in \mathbb{Z}^+$. We denote by $Cyc(f, T)$ a directed graph with a unique cycle of length f such that each node in that cycle is the root of a tree isomorphic to T. When $T = \bullet$, that is, it consists of only one vertex, we denote $Cyc(f, \bullet)$ by $Cyc(f)$.*

Functional graphs associated with Rédei function have special symmetries: each connected component is of the form $Cyc(f, T)$ for some $f \in \mathbb{Z}^+$ and some rooted tree T (the same T for all connected components). Describing the trees T require a bit of work, so we start by introducing some operations and notations on trees.

Notation 3.3.2. *If T is a rooted tree and x is a vertex (or node) in T, we denote by $\rho_T(x)$ the set of directed predecessors of x in T. In this way, $\#\rho_T(x) = indeg(x)$ is the in-degree of x. By definition each vertex in T has out-degree equal to 1 except for the root which has out-degree equal to 0. The vertices x with $\rho_T(x) = \emptyset$ are called leaves; the set of all leaves in T is denoted by $\mathcal{H}_T$. We consider the empty graph $\emptyset$ as a rooted tree.*

Definition 3.3.3. *Let $T_1, T_2, \ldots, T_k$ be rooted trees with roots $t_1, t_2, \ldots, t_k$, respectively. If $G = \bigoplus_{i=1}^k T_i$ is the graph whose connected components are the rooted trees T_i for $1 \leq i \leq k$, then $\langle G \rangle$ denotes a rooted tree where its root has directed predecessors $t_1, t_2, \ldots, t_k$. The*

empty graph verifies $G \oplus \emptyset = G$ *for every graph* G *and* $\langle \emptyset \rangle = \bullet$ *(the tree consisting of a unique point).*

Now, we define a special type of trees associated with ν-series. These trees play an important role in the description of the Rédei functional graphs.

Definition 3.3.4. *If* $V = (\nu_1, \nu_2, \ldots, \nu_D)$ *is a* ν*-series, we define recursively the tree* T_V *associated with* V *as follows:*

$$\begin{cases} T_V^0 = \bullet, \\ T_V^k = \langle \nu_k \times T_V^{k-1} \oplus \bigoplus_{i=1}^{k-1} (\nu_i - \nu_{i+1}) \times T_V^{i-1} \rangle \text{ for } 1 \leq k \leq D, \end{cases} \tag{3.3.1}$$

and

$$T_V = \langle (\nu_D - 1) \times T_V^{D-1} \oplus \bigoplus_{i=1}^{D-1} (\nu_i - \nu_{i+1}) \times T_V^{i-1} \rangle. \tag{3.3.2}$$

For $V = (1)$ *we define* $T_V = \bullet$.

Example 3.3.5. *In Figure 3.1 we show the inductive construction of* T_V *when the* ν*-series* $V = (\nu_1, \nu_2, \nu_3, \nu_4)$ *has four components.*

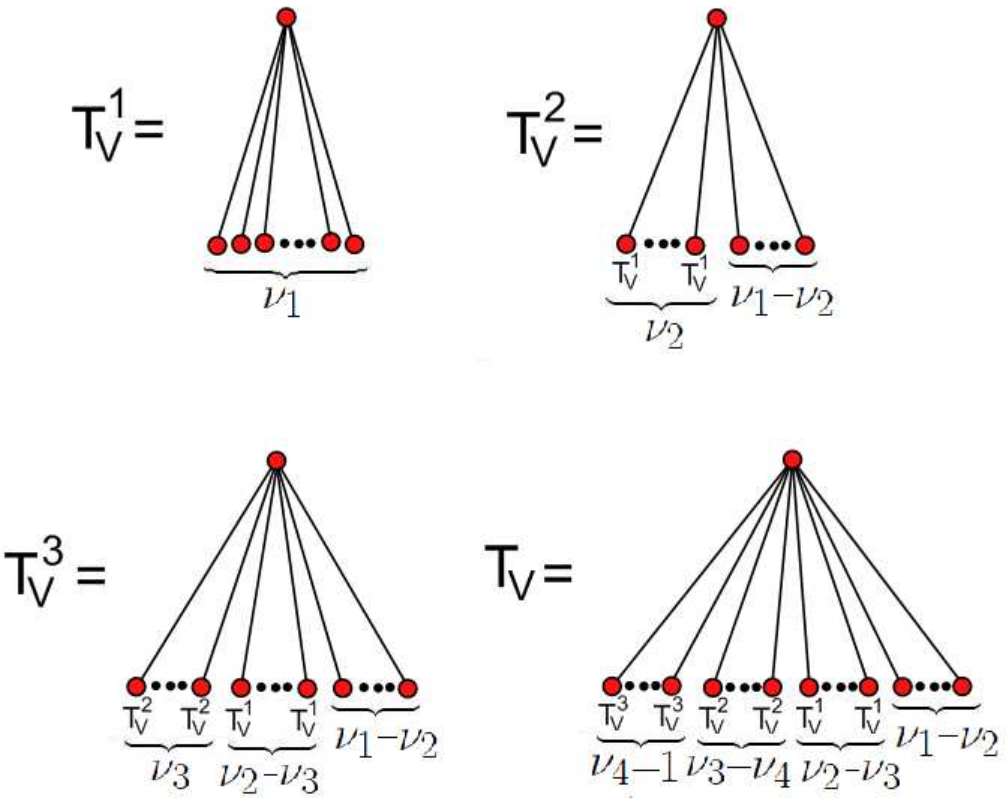


Figure 3.1: Inductive definition of T_V for $V = (\nu_1, \nu_2, \nu_3, \nu_4)$.

Example 3.3.6. *We consider the* 360*-series associated with* 30*, that is* $V = 360(30) = (30, 6, 2)$*. In Figure 3.2 we show the inductive construction of* T_V *for this* 360*-series.*

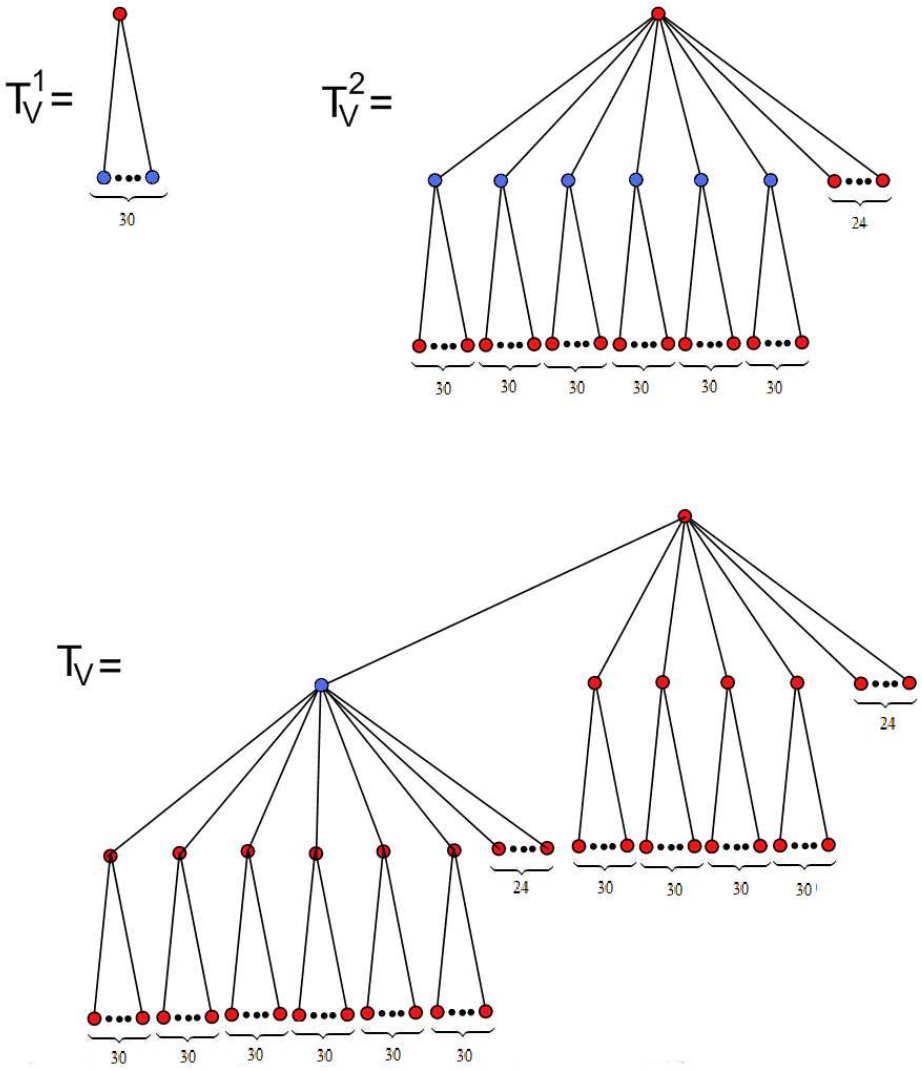


Figure 3.2: The tree associate with the 360-series $V = 360(30)$.

Proposition 3.3.7. *If* $rad(\nu) \mid rad(n)$ *the tree associated with the* ν*-series generated by* n *has exactly* ν *vertices.*

Proof. If we denote by n_k the number of vertices of $T^k_{\nu(n)}$ for $0 \leq k \leq D$, the number of vertices of $T_{\nu(n)}$ is $n_D - n_{D-1}$, where the sequence $(n_k)_{0 \leq k \leq D}$ verifies

$$\begin{cases} n_0 = 1, \\ n_k = \nu_k n_{k-1} + \sum_{i=1}^{k-1} (\nu_i - \nu_{i+1}) n_{i-1} + 1 \text{ for } 1 \leq k \leq D. \end{cases}$$

We can rewrite this last recurrence relation as

$$n_k = \sum_{i=2}^{k}(n_{i-1} - n_{i-2})\nu_i + \nu_1 n_0 + 1, \text{ for } 1 \leq k \leq D.$$

Clearly, $n_k - n_{k-1} = \nu_k(n_{k-1} - n_{k-2})$ for $2 \leq k \leq D$, which implies that the number of vertices of $T_{\nu(n)}$ is $n_D - n_{D-1} = \prod_{j=1}^{D} \nu_j = \nu$. □

The proof of the following lemma is immediate.

Lemma 3.3.8. *If $T = \langle T_1 \oplus T_2 \oplus \ldots \oplus T_k \rangle$ then*

$$depth(T) = \max_{1 \leq i \leq k} depth(T_i) + 1.$$

Proposition 3.3.9. *If $T_{\nu(n)}$ is the tree associated with $\nu(n)$ then*

$$depth(T_{\nu(n)}) = depth(\nu(n))$$

Proof. Let $D = depth(\nu(n))$. Using (3.3.1) and Lemma 3.3.8, we can prove by induction that $depth(T^k_{\nu(n)}) = k$. Using again Lemma 3.3.8 and (3.3.2) we have

$$depth(T_{\nu(n)}) = depth(T^{D-1}_{\nu(n)}) + 1 = (D-1) + 1 = D = depth(\nu(n)).$$

□

Definition 3.3.10. *Let $n \geq 2$ and $f \geq 1$ be integers and $\lambda \in \mathbb{R}$ such that $n^\lambda = \nu \in \mathbb{Z}^+$. We define*

$$H_n(f, \lambda) = Cyc(f, T_{\nu(n)}).$$

Remark 3.3.11. *The following are some properties of the parameter λ that are not difficult to check:*

- *$H_n(f, \lambda)$ is a cycle if and only if $\lambda = 0$.*
- *When $\lambda \in \mathbb{N}$ this parameter represents the depth of the tree attached to the cyclic points in $H_n(f, \lambda)$.*
- *In general, the depth of the tree is given by the number of components of the ν-series $\nu(n)$ which is the least integer D such that $\nu \mid n^D$.*
- *$H_n(f, \lambda)$ has exactly fn^λ vertices.*

Chapter 4

CODES IN THE LEE METRIC AND IN THE CHEBYSHEV METRIC

In this chapter we study perfect codes in the Lee metric and in the Chebyshev metric. We start with a brief discussion on how Construction A behaves with respect to the p-Lee norm in general and consider some particularities of the Lee ($p = 1$) and Chebyshev ($p = \infty$) metrics. In Section 2 we study two-dimensional perfect codes with respect to these two metrics and in Section 3 we discuss on similarities and differences regarding these two metrics as well as on some facts about p-Lee metrics in general. In Section 4 we present several constructions of Chebyshev perfect codes from sections and also from codes in smaller dimensions which allow us to extend some results from dimension 2 to higher dimensions. In Section 5 we introduce a special class of matrices (perfect matrices) which is in correspondence with Chebyshev perfect codes in arbitrary dimension and also study isomorphism classes of such codes. In Section 6 structural properties of the isomorphism classes that can be represented by perfect codes in the Chebyshev metric are discussed.

4.1 Codes in Lebesgue spaces

Let d_p be the p-Lee metric in $\mathbb{Z}_q^n$ and we denote by $B_p(x, e) = \{y \in \mathbb{Z}^n : d_p(x, y) \leq e\}$ the ball with center $x \in \mathbb{Z}^n$ and radius $e \geq 0$ with respect to this metric. In [CJC+15], the authors show that for every p, $1 < p < \infty$ there exists perfect codes in the p-Lee metric with the same minimum distance but different packing radius. For $p = 1$ it is a well known fact that the minimum distance d and the packing radius e for perfect codes verify $e = \lfloor \frac{d-1}{2} \rfloor$ (see [EVY13]). We prove here that this is also the case for $p = \infty$. The idea is, given two points $x, y \in \mathbb{Z}^n$ with $d_\infty(x, y) = d$, to find a point $m = m(x, y) \in \mathbb{Z}^n$ such that the distance $d_\infty(x, m)$ and $d_\infty(y, m)$ are as close as possible to $\frac{d}{2}$. We find such m that also works well for $p = 1$, in the sense that the same proof for the case $p = \infty$ (using $m = m(x, y)$) holds for $p = 1$.

Notation 4.1.1. *Let $x, y \in \mathbb{Z}^n$, $P = \{i \in [n] : x_i \equiv y_i \pmod 2\}$, $m = \frac{x+y}{2}$ and $I = [n] \setminus P$. We decompose $I = I_1 \uplus I_2$ where $\max I_1 < \min I_2$ and $\#I_1 - \#I_2 \in \{0, 1\}$ (if $\#I \leq 1$ we*

define $I_1 = I$ and $I_2 = \emptyset$). We denote by $m(x, y) = z$ the point in $\mathbb{Z}^n$ given by

$$z_k = \begin{cases} m_i & \text{if } i \in P, \\ m_i - sgn(x_i - y_i)/2 & \text{if } i \in I_1, \\ m_i - sgn(y_i - x_i)/2 & \text{if } i \in I_2. \end{cases},$$

where sgn denotes the sign function.

Remark 4.1.2. *With the notation above we have $\#I_1 - \#I_2 \equiv d_1(x, y) \pmod 2$ and by direct calculation, it is easy to check that for $x, y \in \mathbb{Z}^n$ and $z = m(x, y)$ we have:*

- *$d_1(x, z) = \lfloor \frac{d+1}{2} \rfloor$ and $d_1(y, z) = \lfloor \frac{d}{2} \rfloor$ if $d = d_1(x, y)$, or*
- *$d_\infty(x, z) \leq \lfloor \frac{d+1}{2} \rfloor$ and $d_\infty(y, z) \leq \lfloor \frac{d+1}{2} \rfloor$ if $d = d_\infty(x, y)$.*

Proposition 4.1.3. *For the Lee metric and for the Chebyshev metric, the minimum distance d and the packing radius e for a code C in $\mathbb{Z}^n$ are related by $e = \lfloor \frac{d-1}{2} \rfloor$. Moreover, if C is perfect with respect to one of these metrics, then $d = 2e + 1$.*

Proof. By triangular inequality $e \geq \lfloor \frac{d-1}{2} \rfloor$. Let p be 1 or ∞ and $d = d_p(x, y)$ with $x, y \in C$. By Remark 4.1.2, the point $z = m(x, y)$ is in $B_p\left(x, \lfloor \frac{d+1}{2} \rfloor\right) \cap B_p\left(y, \lfloor \frac{d+1}{2} \rfloor\right)$ so $e = \lfloor \frac{d-1}{2} \rfloor$. Now we suppose that C is perfect and let $x' \in C$ such that $d_p(z, x') \leq e$. If d is odd, then $d = 2e + 2$ and $d_p(x, x') \leq (e + 1) + e < d$ which is a contradiction, so $d = 2e + 1$. □

As it was seen in Chapter 2, Construction A establishes a correspondence between q-ary codes $C \subseteq \mathbb{Z}_q^n$ and q-periodic sets in $\mathbb{Z}^n$. On the other hand, for all $p \in [1, \infty]$, the ℓ_p metric in $\mathbb{Z}^n$ induces the p-Lee metric in the quotient $\mathbb{Z}^n/q\mathbb{Z}^n = \mathbb{Z}_q^n$ [CJC+15] and a natural question is how this construction behaves with respect to these metrics.

It is clear that if $\Lambda \subseteq \mathbb{Z}^n$ is a q-periodic set with packing radius $e(\Lambda)$, then the corresponding code $C = \overline{\Lambda}$ has packing radius $e(C) \geq e(\Lambda)$. In fact the strict inequality is possible, for example the binary code $C = \{(0, 0, 0), (1, 1, 1)\} \subseteq \mathbb{Z}_2^3$ is 1-perfect (i.e. $e(C) = 1$) in the Lee metric but the packing radius of its corresponding lattice Λ is 0 (since $(0, 0, 0)$ and $(2, 0, 0)$ are in Λ). This correspondence works well when the ball $B_p(0, e) \subseteq \mathbb{Z}^n$ does not contain points which are congruent modulo q and for this it is sufficient that this property holds for the horizontal segment $\{(-\lfloor e \rfloor, 0), \ldots, (\lfloor e \rfloor, 0)\}$ (since $B_p(0, e) \subseteq B_\infty(0, \lfloor e \rfloor)$). In summary, we have the following proposition.

Proposition 4.1.4. *Let $C \subseteq \mathbb{Z}_q^n$ be a code with packing radius e in the p-Lee metric. If $2\lfloor e \rfloor + 1 \leq q$, then $\Lambda_C \subseteq \mathbb{Z}^n$ is a code with packing radius e in the ℓ_p metric.*

Corollary 4.1.5. *If $C \subseteq \mathbb{Z}_q^n$ is a linear perfect code with packing radius e such that $q \geq 2\lfloor e \rfloor + 1$, then $\Lambda_C \subseteq \mathbb{Z}^n$ is a e-perfect code in the ℓ_p metric.*

The condition $q \geq 2\lfloor e \rfloor + 1$ which guarantees preservation of packing radius by Construction A is almost the same one that appears in Proposition 3.14 of [CJC+15] (with the difference that when the fractional part of e belongs to (1/2,1) they obtain $q \geq 2\lfloor e \rfloor + 2$). In the case of the Lee metric this condition is well known in the literature and we say that the code is defined over a large alphabet [Pos75]. An interesting problem is, given $n, e \in \mathbb{Z}^+$ and $p \in (1, \infty)$, to determine $q_0(n, e, p)$, the minimum value of $q \geq 2$ such that Construction A preserves the packing radius for every (n, e, q)-code in the p-Lee metric. Proposition 4.1.4 implies $q_0(n, e, q) \leq 2\lfloor e \rfloor + 1$.

We observe that Lee codes have integer packing radius so in this case large alphabet is equivalent to $q \geq 2e + 1$. In the Chebyshev metric the distance is bounded by q so every code is defined over large alphabet, in other words the condition $q \geq 2e + 1$ is always satisfied and we have:

$$\{\text{Perfect } q\text{-periodic codes in } (\mathbb{Z}^n, \ell^\infty)\} \underset{\pi^{-1}}{\overset{\pi}{\rightleftarrows}} \{\infty\text{-Lee Perfect codes in } \mathbb{Z}_q^n\}\ .$$

4.2 Two-dimensional perfect codes

In this section we study two-dimensional codes in the Lee metric and in the Chebyshev metric. In both metrics we characterize the set of $(2, e, q)$-perfect codes providing generator matrix for these codes. We also study isometry and isomorphism classes of such codes.

4.2.1 Lee two-dimensional perfect codes

In this part we use "perfect code" as synonym of "perfect code with respect to the Lee metric". We observe that the minimum distance of every two-dimensional q-ary code verifies $d \leq q$ therefore in this case every code is defined over a large alphabet. If C is a two-dimensional q-ary code with packing radius e we have $\#B_1(0, e) = 2e^2 + 2e + 1$. We denote by $q_e = 2e^2 + 2e + 1$. For each positive integer e, Golomb and Welch presented in [GW70] a $(2, e, q_e)$-perfect code C_e. This code is given by $C_e = \langle (\overline{e}, \overline{e+1}) \rangle$ in $\mathbb{Z}_{q_e}$. By Construction A these codes correspond to perfect lattices with respect to the ℓ_1 metric.

Proposition 4.2.1. *The lattice Λ_{C_e} that corresponds to the q_e-ary perfect code C_e via Construction A is given by $\Lambda_{C_a} = \nu_1\mathbb{Z} + \nu_2\mathbb{Z}$ where $\nu_1 = (e, e+1)$ and $\nu_2 = (-(e+1), e)$.*

Proof. Since $q_e = 2e^2 + 2e + 1$ we have $(2e+1) \cdot (\overline{e}, \overline{e+1}) = (\overline{2e^2 + e}, \overline{2e^2 + 3e + 1}) = (\overline{-(e+1)}, \overline{e}) \in C_e$, therefore if $M = \begin{pmatrix} e & e+1 \\ -(e+1) & e \end{pmatrix}$ then the lines of $\overline{M}$ generate the code C_e. Since $q_e M^{-1} = \begin{pmatrix} e & -(e+1) \\ e+1 & e \end{pmatrix}$ has integer entries, the matrix M is in fact, a generator matrix for Λ_{C_a}. □

Since every q_e-periodic integer lattice is also a hq_e-periodic integer lattice for every positive integer h we have the following corollary.

Corollary 4.2.2. *If $q = q_e h$ with $h \in \mathbb{Z}^+$ then the q-ary code $C_{e,h}$ with generator matrix $M = \begin{pmatrix} e & e+1 \\ -(e+1) & e \end{pmatrix}$ is a $(2, e, q)$-perfect code.*

In order to simplify notation we will omit the overline when we consider modular classes if there is no danger of confusion.

Definition 4.2.3. *Let C a q-ary code with packing radius e. We say that C is of Lee-type 1 if $(e, e+1) + C = C$ and C is of Lee-type 2 if $(e+1, e) + C = C$. If C is a code of Lee-type 1 or of Lee-type 2 we say that C is Lee-standard.*

Our next goal is to prove that every two-dimensional perfect code in the Lee metric is Lee-standard. We observe that for linear codes with packing radius e, C is of Lee-type 1 if $(e, e+1) \in C$ and it is of Lee-type 2 if $(e+1, e)$. We also observe that the permutation $\sigma(x, y) = (y, x)$ establish a correspondence between Lee-type 1 codes and Lee-type 2 code, this map is an isometry and so it preserves perfection and packing radius.

Notation 4.2.4. *We denote by $e_1 = (1, 0)$ and $e_2 = (0, 1)$ the unitary vectors of $\mathbb{Z}_q^2$ and the horizontal and vertical lines by $h_i = \mathbb{Z}_q \times \{i\}$ and $v_j = \{j\} \times \mathbb{Z}_q$ for $i, j \in \mathbb{Z}_q$. For $x \in \mathbb{Z}_q^2$ we define the following sets:*

- *up*$(x) = x + \{(-1, 1), (0, 1), (1, 1)\}$,
- *down*$(x) = x + \{(-1, -1), (0, -1), (1, -1)\}$,
- *right*$(x) = x + \{(1, -1), (1, 0), (1, 1)\}$,
- *left*$(x) = x + \{(-1, -1), (-1, 0), (-1, 1)\}$.

The following geometric lemmas can be verified easily.

Lemma 4.2.5. *If a horizontal line r cuts a Lee-ball $B = B(c, e)$ then $\#(B \cap r) = 2\ell + 1$ for some integer ℓ with $0 \leq \ell \leq e$. If $B \cap r = \{c' + (i, 0) : -\ell \leq i \leq \ell\}$ then $c = c' + (e - \ell)e_2$ or $c = c' - (e - \ell)e_2$. In particular, when $\ell = e$ we have that c is the midpoint of the segment $B \cap r$.*

Lemma 4.2.6. *Let B be a Lee-ball of radius e with $1 \leq e \leq \frac{q-1}{2}$.*

(i) If $\#(h_{i+1} \cap B) > \#(h_i \cap B) \Rightarrow \forall x \in h_i \cap B : up(x) \subseteq B$,

(ii) if $\#(h_{i-1} \cap B) > \#(h_i \cap B) \Rightarrow \forall x \in h_i \cap B : down(x) \subseteq B$,

(iii) if $\#(h_i \cap B) > \max\{\#(h_{i+1} \cap B), \#(h_{i-1} \cap B)\} \Rightarrow \#(h_i \cap B) = 2e + 1$.

Applying the symmetry $\theta(x, y) = (y, x)$ we can obtain analogous results for vertical lines instead of horizontal lines.

Lemma 4.2.7 (Slingshot lemma)**.** *Let $C \in PL^1(2, e, q)$ and $f : \mathbb{Z}_q^2 \to C$ its associated error-correcting-function . Let $B = B(c, e)$ with $c \in C$ and $P \in B$.*

1. *If up$(P) \not\subseteq B$ and down$(P) \not\subseteq B$ then:*

   (i) $f(P) \neq f(P - e_1) \Rightarrow f(P) = P + e \cdot e_1$.

   (ii) $f(P) \neq f(P + e_1) \Rightarrow f(P) = P - e \cdot e_1$.

2. *If right$(P) \not\subseteq B$ and left$(P) \not\subseteq B$ then:*

   (i) $f(P) \neq f(P - e_2) \Rightarrow f(P) = P + e \cdot e_2$.

   (ii) $f(P) \neq f(P + e_2) \Rightarrow f(P) = P - e \cdot e_2$.

Proof. It suffices to prove part (i) of 1 (the others are analogous). Let $i = y(P)$ (the second coordinate of P). By Lemma 4.2.6 we have that $\#(h_i \cap B) = 2e + 1$, then by Lemma 4.2.5 $h_i \cap B = \{P + (j, 0) : -t \leq j \leq k\}$ with $t, k \geq 0$ e $t + k + 1 = 2e + 1$. Since $f(P) \in B$ (since $P \in B$) and $f(P - e_1) \neq f(P)$ we have $P - e_1 \notin B$. In particular $P - e_1 \notin h_i \cap B$, thus $t = 0, k = 2e$ and $h_i \cap B = \{P, \ldots, P + (2e, 0)\}$, so by Lemma 4.2.5 the center of the Lee-Ball B is $f(P) = P + (e, 0)$ (see Figure 4.1 which justify the name of the lemma). □

Definition 4.2.8. *We denote by $\mathscr{C} \subseteq \mathbb{Z}_q^2$ the set given by $\mathscr{C} = \{(-1, i) : -1 \leq i \leq 2\} \cup \{(0, -1), (0, 2)\}$.*

Definition 4.2.9. *Let B_1 and B_2 be two Lee-balls of radius e. We say that B_1 and B_2 are adjacent if they are disjoint and there exists $c_1 \in B_1$ and $c_2 \in B_2$ with $d_1(c_1, c_2) = 1$.*

Definition 4.2.10. *Let B_1 and B_2 be two adjacent Lee-balls of radius e. We say that they fit well if $x + \mathscr{C} \subseteq B_1 \cup B_2 \Rightarrow x \in B_1 \cup B_2$ or $x + e_2 \in B_1$ and we say that they do not fit otherwise (see Figure 4.2).*

Lemma 4.2.11. *If $C \in PL^1(2, e, q)$ then in the covering $\biguplus_{c \in C} B(c, e) = \mathbb{Z}_q^2$, any two adjacent balls fit.*

Proof. We suppose on the contrary that there are two adjacent Lee-balls $B_1 = B(c_1, e)$ and $B_2 = B(c_2, e)$ which do not fit and let $x \in \mathbb{Z}_q^2$ such that $x + \mathscr{C} \subseteq B_1 \cup B_2$, $x \notin B_1 \cup B_2$ and $y = x + e_2 \notin B_1 \cup B_2$ (see Figure 4.3). If $f : \mathbb{Z}_q^2 \to C$ is the error-correcting function associated with C, we can apply the slingshot Lemma (Lemma 4.2.7) to x and y obtaining two codewords $c_3 = f(x) = x + e \cdot e_1$ and $c_4 = f(y) = y + e \cdot e_1$ with $d(c_3, c_4) = \| e_2 \|_{1,Lee} = 1 < 2e + 1 = d_{min}(C)$, which is a contradiction (see Figure 4.3). □

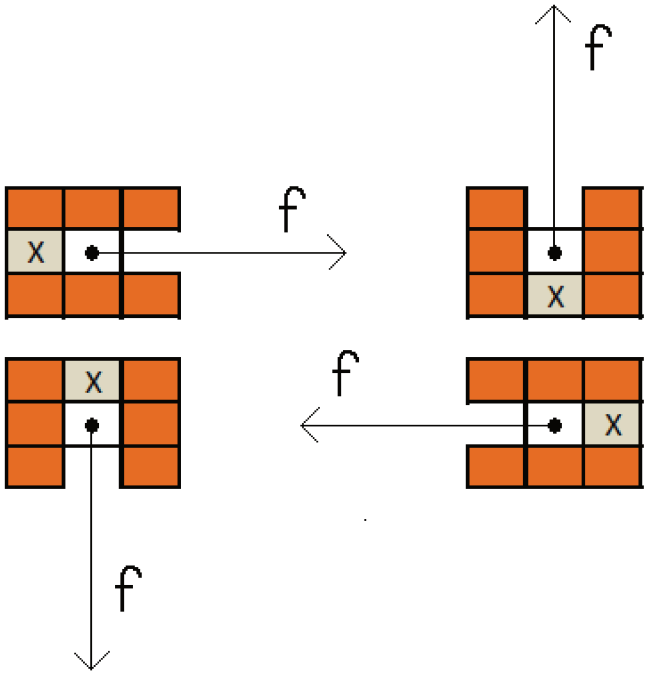


Figure 4.1: The four possibilities for the slingshot Lemma.

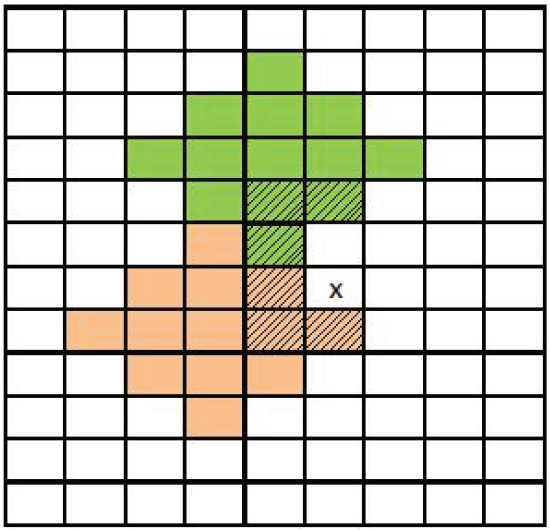


Figure 4.2: Example of two adjacent balls that do not fit.

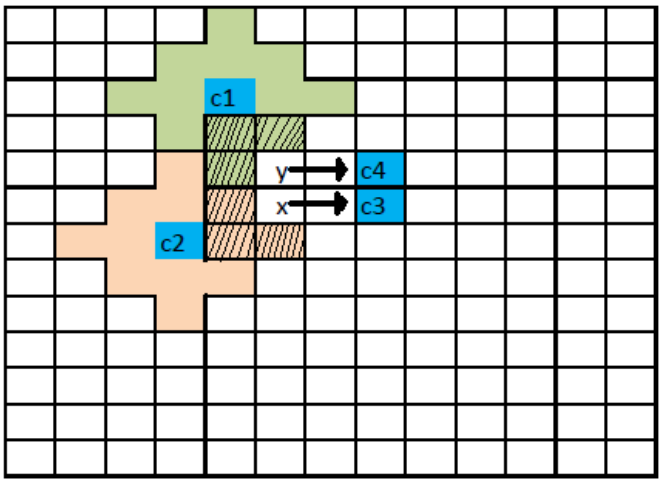


Figure 4.3: Contradiction obtained by applying slingshot Lemma (c_1, c_2, c_3, c_4, x and y are as in the proof of Lemma 4.2.11).

Lemma 4.2.12. *Let $C \in PL^1(2, e, q)$, $\biguplus_{c \in C} B(c, e) = \mathbb{Z}_q^2$ and $f : \mathbb{Z}_q^2 \to C$ be its associated error-correcting function. We have $f(c + (e+1)e_2) \neq f(c + (e+2)e_2)$ for all $c \in C$.*

Proof. Let $c' = f(c + (e+1)e_2)$ and r be the vertical line through c. Since $c + (e+1)e_2 \in r \cap B(c', e) \Rightarrow \#(r \cap B(c', e)) = 2\ell + 1$ with $0 \leq \ell \leq e$. We note that $f(c + (e+1)e_2) = f(c + (e+2)e_2) \Leftrightarrow \ell = 0$. We assume on the contrary that $\ell > 0$. By Lemma 4.2.5 we have $c' = x_0 \pm (e - \ell)e_1$ where $r \cap B(c', e) = \{x_0 + ie_2 : -\ell \leq i \leq \ell\}$. Applying an axial symmetry around the axis r if necessary, we can suppose that $c' = x_0 - (e - \ell)e_1$. It is not difficult to prove that $x := c + (1, e)$ verifies:

- $x \notin B(c, e) \cup B(c', e)$,
- $x + \mathscr{C} \subseteq B(c, e) \cup B(c', e)$, and
- $x + (0, 1) \notin B(c, e) \cup B(c', e)$ (since $\ell > 0$).

Hence $B(c, e)$ and $B(c', e)$ are adjacent balls which do not fit, contradicting Lemma 4.2.11 (see Figure 4.4). □

Definition 4.2.13. *Let $C \in PL^1(2, e, q)$. For each codeword $c \in C$ we define the ω-set of c as $\omega(c) = \{\nu_1, \ldots, \nu_\tau\}$ where the adjacent balls to $B(c, e)$ are exactly the balls $B(c + \nu_i, e)$ for $1 \leq i \leq \tau$.*

Lemma 4.2.14. *If $C \in PL^1(2, e, q)$ then the set $\omega(c)$ does not depend on c. Moreover, denoting by $v' = \sigma(v)$ where $\sigma(x, y) = (y, x)$, we have only two possibilities:*

i) $\omega(c) = \{\pm\nu_1, \pm\nu_2\}$ or

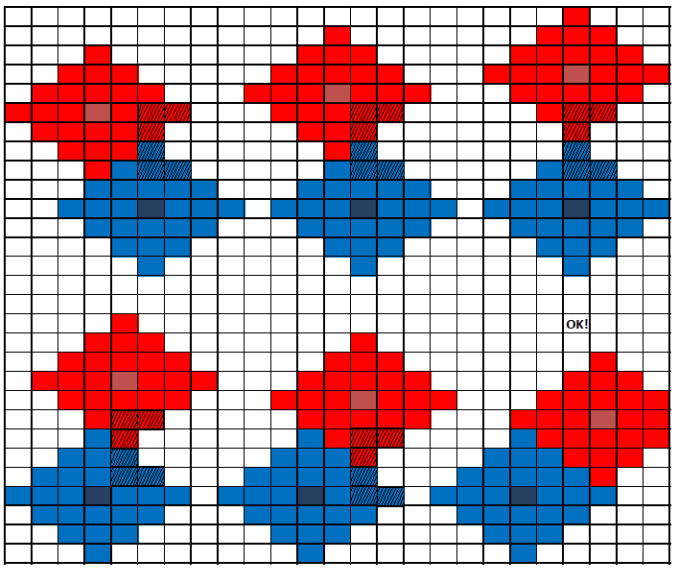


Figure 4.4: There is a unique way to fit two adjacent balls up to symmetry.

ii) $\omega(c) = \{\pm\nu_1', \pm\nu_2'\}$,

where $\nu_1 = (e, e+1)$ *and* $\nu_2 = (-(e+1), e)$.

Proof. Let $c \in C$ and $B = B(c, e)$ with respect to the Lee metric, we want to determine the center of the adjacent Lee-balls to B with radius e. If r is the vertical line through c and $c_1 = f_C(c + (e+1)e_2)$ we obtain $B_1 = B(c_1, e)$ which is adjacent to B. By Lemma 4.2.12 $\#(r \cap B_1) = 1$, then by Lemma 4.2.5 we have that $c_1 = c + \nu_1$ or $c_1 = c + \overline{\nu_1}$. First, we study the case $c_1 = c + \nu_1$. Applying slingshot lemma (Lemma 4.2.7) to the point $P_1 = c + (-1, e)$ we obtain a new codeword $c_2 = f(P) = c + \nu_2$ such that the ball $B_2 = B(c_2, e)$ is adjacent to B. Applying again the same lemma to the point $P_2 = c + (-e, -1)$ we obtain a third ball $B_3 = B(c - \nu_1, e)$ which is adjacent to B and to the point $P_3 = c + (1, -e)$ we obtain a fourth ball $B(c - \nu_2, e)$ which is also adjacent to B. Hence $\omega := \{\pm\nu_1, \pm\nu_2\} \subset \omega(c)$. To prove that in fact these sets coincide it suffices to prove that $c + \{P \in \mathbb{Z}_q^2 : d_1(P, c) = e+1\} \subseteq \bigcup_{i=1}^4 B_i$. We consider the partition $\{P \in \mathbb{Z}_q^2 : d_1(P, c) = e+1\} = c + \bigcup_{i=1}^4 \ell_i$ where $\ell_1 = \{(x, e+1-x) : 0 \leq x \leq e\}, \ell_2 = \{(y-(e+1), y) : 0 \leq y \leq e\}, \ell_3 = \{(x, -x-(e+1)) : 0 \leq x \leq e\}$ and $\ell_4 = \{(y + (e+1), y) : 0 \leq y \leq e\}$. By direct calculation we can check that $c + \ell_i \subseteq B_i$ for $1 \leq i \leq 4$, thus $\omega(c) = \{\pm\nu_1, \pm\nu_2\}$. To the case $c_1 = c - \nu_1$ we can use a similar argument obtaining $\omega(c) = \{\pm\nu_1', \pm\nu_2'\}$. Finally, to prove that $\omega(c)$ does not depend on c it suffices to prove that for adjacent codewords $c, c' \in C$ (i.e. for codewords such that their respective balls are adjacent) we have $\omega(c) = \omega(c')$. Since c and c' are adjacent codewords we have that $0 \in \omega(c) + \omega(c')$. On the contrary, if $\omega(c) \neq \omega(c')$ then $0 \notin \omega(c) + \omega(c') = \{\pm\nu_1 \pm \overline{\nu_1}, \pm\nu_2 \pm \overline{\nu_2}\}$ (since $q \geq 2e+1$) which is a contradiction, so $\omega(c) = \omega(c')$. □

Corollary 4.2.15. *Every two-dimensional q-ary perfect code C in the Lee metric is Lee-standard. With the same notation used in the previous lemma, if C is of Lee-type 1 then $\omega(c) = \{\pm\nu_1, \pm\nu_2\}$ for all $c \in C$ and if C is of Lee type 2 then $\omega(c) = \{\pm\nu_1', \pm\nu_2'\}$ for all $c \in C$.*

Proposition 4.2.16. *If $PL^1(2, e, q) \neq \emptyset$ then $q = hq_e$ for some $h \in \mathbb{Z}^+$.*

Proof. Let $\nu = \nu_1$ if C is of Lee-type 1 or $\nu = \nu_1'$ if C is of Lee-type 2. Since $C + \nu = C$, then $q = \#\nu\mathbb{Z} \mid \#C$, so by the sphere packing condition $q_e \mid q$. □

Theorem 4.2.17. *Let $PL^1(2, e, q)$ be the set of all $(2, e, q)$-perfect codes in the Lee metric (linear and non-linear) and $\nu_1 = (e, e+1), \nu_2 = (-(e+1), e), \eta_1 = (1, -(2e+1)), \eta_2 = (0, q_e)$ be vectors in $\mathbb{Z}_q^2$ where $q_e = 2e^2+2e+1$. For $q = hq_e$ we denote by $D_{e,h} = \nu_1\mathbb{Z}+\nu_2\mathbb{Z}$ and $D'_{e,h} = \nu_1'\mathbb{Z} + \nu_2'\mathbb{Z}$ where $(x, y)' = (y, x)$.*
1) (Existence) $PL^1(2, e, q) \neq \emptyset \Leftrightarrow q = hq_e$ for some positive integer h.
2) (Description) Let $q = hq_e$. Then, $C \in PL^1(2, e, q) \Leftrightarrow C = c + D_{e,h}$ or $C = c + D'_{e,h}$ for any $c \in C$ (in particular $C - c$ is a group).
3) (Structure) If $C \in PL^1(2, e, q)$ and $G_C = C - c$ its associated group (where $c \in C$), then:

- *(i) G_C is cyclic if and only if $q = q_e$. In this case $G_C \simeq \mathbb{Z}_q$ with generator $\nu = (e, e+1)$ if $G_C = D_e$ or $\nu' = (e+1, e)$ if $G_C = D'_e$, where $D_e = D_{e,1}$ and $D_{e'} = D'_{e,1}$ are the codes introduced by Golomb and Welch [GW70].*
- *(ii) If $q = hq_e$ with $h > 1$ then $G_C \simeq \mathbb{Z}_q \times \mathbb{Z}_h$. Moreover, $G_C = \eta_1\mathbb{Z} \oplus \eta_2\mathbb{Z}$ or $G_C = \eta_1'\mathbb{Z} \oplus \eta_2'\mathbb{Z}$ according to either $G_C = D_{e,h}$ or $G_C = D'_{e,h}$ respectively.*

Proof. The existence follows from Corollary 4.2.2 and Proposition 4.2.16. By Corollary 4.2.15 if $c \in C$ then $c + D_{e,h} \subseteq C$ or $c + D'_{e,h} \subseteq C$. Since $c + D_{e,h}$ and $c + D'_{e,h}$ are in $PL^1(2, e, q)$ (Corollary 4.2.2) then $C = c + D_{e,h}$ or $C = c + D'_{e,h}$ which proves the second part. To prove part 3, we can suppose that C is a linear Lee-type 1 perfect code, so $C = \nu_1\mathbb{Z} + \nu_2\mathbb{Z}$. Let $A = \begin{pmatrix} -1 & -1 \\ e+1 & e \end{pmatrix}$. Since $A \begin{pmatrix} \nu_1 \\ \nu_2 \end{pmatrix} = \begin{pmatrix} \eta_1 \\ \eta_2 \end{pmatrix}$ and $\det(A) = 1$, we have $C = \eta_1\mathbb{Z} + \eta_2\mathbb{Z}$ where $\eta_1 = (1, -(2e+1))$ and $\eta_2 = (0, q_e)$ (in $\mathbb{Z}_q^2$). Clearly, $\eta_1\mathbb{Z} \cap \eta_2\mathbb{Z} = (0), |\eta_1\mathbb{Z}| = q$ e $|\eta_2\mathbb{Z}| = \frac{q}{q_e} = h$, thus $C = \eta_1\mathbb{Z} \oplus \eta_2\mathbb{Z} \simeq \mathbb{Z}_q \times \mathbb{Z}_h$. Since $h|q$ it is clear that C is cyclic if and only if $h = 1$. □

Corollary 4.2.18. *There are exactly $2q_e = 4e^2+4e+2$ perfect codes in $PL^1(2, e, q)$ where $q \equiv 0 \pmod{q_e}$, two of them are linear and the others can be obtained from these two via translation. The two linear codes can be obtained one from the other via the symmetry $(x, y) \mapsto (y, x)$. Therefore, there is a unique $(2, e, q)$-perfect code in the Lee metric up to isometry (including translation).*

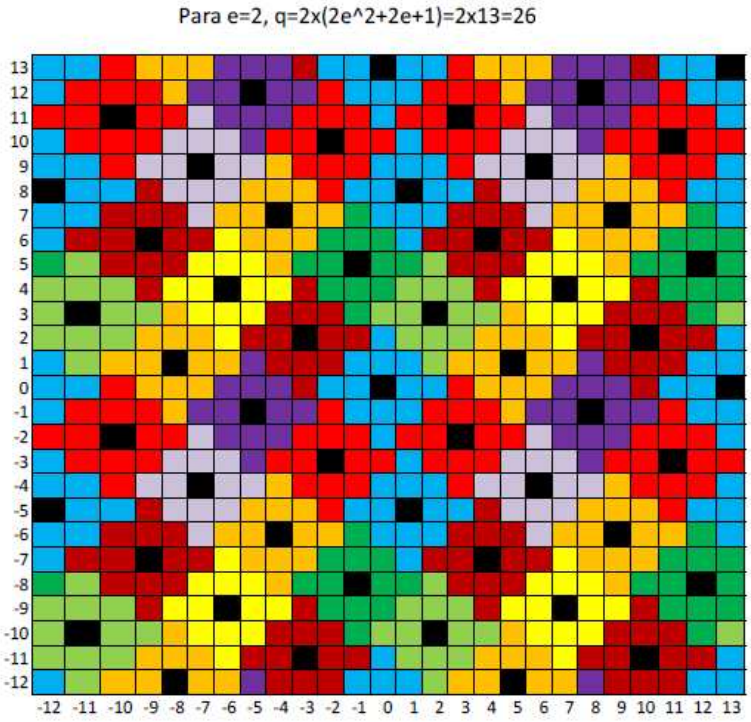


Figure 4.5: Non-cyclic perfect Lee-code generated by the vectors $(1, 21)$ and $(0, 13)$ (the black squares represent the codewords).

Corollary 4.2.19. *$PL^1(2, e, q)$ contain a cyclic code if and only if $q = q_e$. In this case, the unique code up to isometry is the cyclic code $D_e = \langle (e, e + 1) \rangle \subseteq \mathbb{Z}_q^2$ introduced by Golomb and Welch [GW70].*

Corollary 4.2.20. *There are non-cyclic perfect codes in the Lee metric (when $q = hq_e$, $h > 1$).*

Example 4.2.21. *If $q = 26$ and $e = 2$ we have the perfect code $C = (1, 21)\mathbb{Z}_{26} + (0, 13)\mathbb{Z}_{26}$ in $\mathbb{Z}_{26} \times \mathbb{Z}_{26}$ (see Figure 4.5).*

Example 4.2.22. *Since $1105 = 5 \cdot 13 \cdot 17$, there are exactly 5 perfect codes in the Lee metric in $\mathbb{Z}_{1105}^2$ up to translation and change of coordinate (that is, application of $\sigma(x, y) = (y, x)$). One of them is cyclic and the others are non-cyclic. These codes are given by:*

- $C_1 = (1, -3)\mathbb{Z}_{1105} \oplus (0, 5)\mathbb{Z}_{1105}$ *($e = 1$),*
- $C_2 = (1, -5)\mathbb{Z}_{1105} \oplus (0, 13)\mathbb{Z}_{1105}$ *($e = 2$),*
- $C_3 = (1, -13)\mathbb{Z}_{1105} \oplus (0, 85)\mathbb{Z}_{1105}$ *($e = 6$),*
- $C_4 = (1, -21)\mathbb{Z}_{1105} \oplus (0, 221)\mathbb{Z}_{1105}$ *($e = 10$),*

- $C_5 = (23, 24)\mathbb{Z}_{1105}$ *(*$e = 23$*).*

4.2.2 Chebyshev two-dimensional perfect codes

In this part we study two-dimensional perfect codes with respect to the Chebyshev metric. First we describe the set of all (non-necessarily linear) $(2, e, q)$-perfect codes and how they can be obtained from a one-dimensional perfect code using horizontal and vertical construction. In particular we obtain that every two-dimensional perfect code is standard, which is not true in higher dimensions. This result in dimension 2 is known and is mentioned in [Kis13], but we found no formal proof for it in the literature. The proof presented here illustrates well the coding theory approach to be used in further results. Then we focus on the linear case providing generator matrices for perfect codes and describing isometry classes and isomorphism classes of the $(2, e, q)$-perfect codes. In this part we use "perfect code" as synonym of "perfect code with respect to the Chebyshev metric". The following result (whose proof is straightforward) characterizes the parameters for which there exists perfect codes with these parameters.

Proposition 4.2.23. *A necessary and sufficient condition for the existence of an n-dimensional q-ary e-perfect code in the Chebyshev metric is that $q = (2e + 1)t$ for some integer $t > 1$. Moreover, if this condition is satisfied there exist a code in $LPL^{\infty}(n, q, e)$.*

Corollary 4.2.24. *There exists a non trivial perfect code over $\mathbb{Z}_q$ if and only if q is neither a power of 2 nor a prime number.*

These results led us restrict to the case $q = (2e + 1)t$ where $e \geq 0$ and $t > 1$ are integers and we will maintain this notation while we deal with the Chebyshev metric.

Linear and non-linear two-dimensional perfect codes in the Chebyshev metric

It is immediate to see that the only perfect codes C in $PL^{\infty}(1, e, q)$ are of the form $a + (2e + 1)\mathbb{Z}_q$ where $q = (2e + 1)t$. If we fix a map $h : \mathbb{Z}_t \to \mathbb{Z}_q$ we can construct a two-dimensional q-ary perfect code as follows:
• (Horizontal construction) $C_1(a, h) = \{(h(k) + (2e + 1)s, a + (2e + 1)k) : k, s \in \mathbb{Z}_t\}$.
• (Vertical construction) $C_2(a, h) = \{(a + (2e + 1)k, h(k) + (2e + 1)s) : k, s \in \mathbb{Z}_t\}$.

It is not difficult to see that the above construction gives us $(2, e, q)$-codes of cardinality t^2 and minimum distance $d \geq 2e + 1$ from which is easy to deduce perfection. In fact we obtain $(2, e, q)$-perfect codes of type 1 (if horizontal construction is used) or of type 2 (if vertical construction is used). Moreover, every two-dimensional perfect code can be obtained in this way as we will see next.

The following geometric lemma is an analogous of the slingshot Lemma (Lemma 4.2.7) and it is used in a similar way to prove the next proposition.

Lemma 4.2.25. *Let $\pi_i : \mathbb{Z}_q^n \to \mathbb{Z}_q$ be the canonical projection (i.e. $\pi(x_1, \ldots, x_n) = x_i$), $C \in PL^\infty(n, e, q)$, f_C be its error-correcting function and x be an element of $\mathbb{Z}_q^n$.*

- *If $f_C(x) \neq f_C(x - e_i)$ then $\pi_i \circ f_C(x) = \pi_i(x) + e \cdot e_i$.*
- *If $f_C(x) \neq f_C(x + e_i)$ then $\pi_i \circ f_C(x) = \pi_i(x) - e \cdot e_i$.*

Proof. Let $f_C(x) = c$ and d be the Lee metric in $\mathbb{Z}_q$. We denote by $x_i = \pi_i(x)$ and $c_i = \pi_i(c)$. The equation $f_C(x) = c$ implies that $M_i = \max\{d(x_j, c_j) : 1 \leq j \leq n, j \neq i\} \leq e$ and $d(x_i, c_i) \leq e$. But $f_C(x - e_i) \neq c$ implies that $d(x - e_i, c) = \max\{M_i, d(x_i - 1, c_i)\} \geq e + 1$, therefore $d(x_i - 1, c_i) \geq e + 1$. We have $\|(c_i - x_i)\| \leq e$ and $\|(c_i - x_i) - 1\| \geq e + 1$ then $c_i - x_i = e$ and $c_i = x_i + e$. The other case can be obtained from this considering the isometry η_i of $\mathbb{Z}_q^n$ given by $\eta_i(x_1, \ldots, x_i, \ldots, x_n) = (x_1, \ldots, -x_i, \ldots, x_n)$. □

Lemma 4.2.26. *If $C \in PL^\infty(2, e, q)$ verifies $(2e + 1)\mathbb{Z}_q \times \{0\} \subseteq C$ then C is a standard code of type* 1.

Proof. Assume, on the contrary, that there is a codeword $c = (c_1, c_2) \in C$ such that $c + (2e + 1)e_1 = (c_1 + 2e + 1, c_2) \notin C$, and we take c with this property such that c_2 is minimum. We claim that $c_2 \geq 2e + 1$. Indeed, if $0 \leq c_2 < 2e + 1$ and we express $c_1 = (2e + 1)k + r$ with $|r| \leq e$, then $((2e + 1)k, e)$ belongs to both balls $B_\infty((2e + 1)k, e)$ and $B_\infty(c, e)$ which is a contradiction, so $c_2 \geq 2e+1$. We consider now $p = (c_1, c_2-(e+1))$, then $f_C(p + e_2) = c \neq f_C(p)$ and by Lemma 4.2.25 we have $f_C(p) = (a, c_2 - (2e + 1))$ for some $a \in \mathbb{Z}_q$. We observe that $c_2 - (2e+1) \geq 0$ and by the minimality of c_2 we have that $(a + (2e + 1)k, c_2 - (2e + 1)) \in C$ for $0 \leq k < t$. Consider now $p' = (c_1 + e + 1, c_2 - e)$ and express $c_1 + e + 1 - a = (2e + 1)v + w$ with $v, w \in \mathbb{Z}_q$ and $|w| \leq e$. Clearly, $f_C(p' - e_1) = c \neq f_C(p')$ and $f_C(p' - e_2) = (a + (2e+1)v, c_2 - (2e+1)) \neq f_C(p')$, thus, by Lemma 4.2.25 we have $f_C(p') = p' + (e, e) = c + (2e + 1)e_1$ which is a contradiction. □

Proposition 4.2.27. *Every two-dimensional perfect code in the Chebyshev metric is standard.*

Proof. Let $C \in PL^\infty(2, e, q)$ with $q = (2e + 1)t$ and $t > 1$ an integer. Let we suppose that C is not of type 2, so there exists a codeword $c \in C$ such that $c + (2e + 1)e_2 \notin C$. Composing with a translation, if necessary, we can assume $c = 0$. Consider $p = (0, e+1)$, by Lemma 4.2.25 we have $f_C(p) = (a, 2e + 1)$ with $|a| \leq e$ and $a \neq 0$. Composing with the isometry $(x, y) \mapsto (-x, y)$, if necessary, we can assume $0 < a \leq e$. We consider the following statement: $\{(p_h = (2e + 1)h, 2e + 1), q_h = (a + (2e + 1)h, 2e + 1)\} \subseteq C$, which is valid for $h = 0$ (from above). Assume that this property holds for a fixed h, $0 \leq h < t$ and consider $p = ((2e + 1)h + e + 1, e)$. This point verifies $f_C(p - e_1) = p_h \neq f_C(p)$

and $f_C(p+e_2) = q_h \neq f_C(p)$, so by Lemma 4.2.25 we have $f_C(p) = p + (e,-e) = ((2e+1)(h+1),0) = p_{h+1} \in C$. Now consider $p' = (a+(2e+1)h+e+1, e+1)$ which verifies $f_C(p'-e_1) = q_h \neq f_C(p')$ and $f_C(p'-e_2) = p_{h+1} \neq f_C(p')$, so by Lemma 4.2.25 we have $f_C(p') = p' + (e,e) = (a+(2e+1)(h+1), 2e+1) = q_{h+1} \in C$. By induction we have that $(2e+1)\mathbb{Z}_q \times \{0\} \subseteq C$ and by Lemma 4.2.26 our code C is standard. □

Corollary 4.2.28. *Every two-dimensional perfect code C in the Chebyshev metric is of the form $C = C_1(a,h)$ or $C = C_2(a,h)$ for some $a \in \mathbb{Z}_q$ and some function $h : \mathbb{Z}_t \to \mathbb{Z}_q$.*

Remark 4.2.29. *Proposition 4.2.27 cannot be generalized to higher dimensions. For example the code $C = \{(0,0,0),(5,0,0),(1,0,5),(6,0,5),(1,5,0),(6,5,1),(1,5,5),(6,5,6)\} \in PL^\infty(3,2,10)$ is a three-dimensional non-standard perfect code.*

Corollary 4.2.30. *The number of $(2,e,q)$-perfect codes is $(2e+1)^2\,(2(2e+1)^t - 1)$.*

Proof. We consider the set $L = PL^\infty(2,e,q)$, $L^0 = \{C \in L : 0 \in C\}$ and $L_i^0 = \{C \in L^0 : C \text{ is of type } i\}$ for $i = 1,2$. The map $L \twoheadrightarrow L^0$ given by $C \mapsto C - f_C(0)$ is $(2e+1)^2$ to 1, so $\#L = (2e+1)^2 \# L^0$. By Proposition 4.2.27, $L^0 = L_1^0 \cup L_2^0$ and considering the involution $L_1^0 \to L_2^0$ given by $C \mapsto \theta(C)$ where $\theta(x,y) = (y,x)$, which has exactly one fixed point (given by $(2e+1)\mathbb{Z}_q^n$) we have $\#L^0 = 2\#L_2^0 - 1$. Finally, codes in L_2^0 are univocally determined by $h : \mathbb{Z}_t \to \mathbb{Z}_{2e+1}$, thus $\#L_2^0 = (2e+1)^t$ and so $\#L = (2e+1)^2\,(2(2e+1)^t - 1)$. □

Generator matrices and admissible structures for two-dimensional perfect codes in the Chebyshev metric

In this part we provide generator matrices for linear perfect codes and we describe all two-dimensional cyclic perfect codes in the Chebyshev metric. A description of which group structure can be represented by two-dimensional linear perfect codes is given.

Notation 4.2.31. *We denote by $LPL^\infty(2,e,q)_o$ the set of $(2,e,q)$-perfect codes of type 2.*

Remark 4.2.32. *By Proposition 4.2.27, every two-dimensional perfect code is of type 1 or is of type 2. In addition, the isometry $\pi(x,y) = (y,x)$ induces a correspondence between the codes of type 1 and codes of type 2. So, without loss of generality we can restrict our study to type 2 perfect codes.*

Theorem 4.2.33. *Let $q = (2e+1)t$ with $t > 1$, $d_1 = \gcd(2e+1,t)$ and $h_1 = \frac{2e+1}{d_1}$. Every integer matrix of the form $M = \begin{pmatrix} 2e+1 & kh_1 \\ 0 & 2e+1 \end{pmatrix}$ with $k \in \mathbb{Z}$ is the generator matrix of some type 2 perfect code $C \in LPL^\infty(2,e,q)_o$. Conversely, every type 2 perfect code $C \in LPL^\infty(2,e,q)_o$ has a generator matrix of this form.*

Proof. Let $M = \begin{pmatrix} 2e+1 & kh_1 \\ 0 & 2e+1 \end{pmatrix}$ with $k \in \mathbb{Z}$. Since $qM^{-1} = \begin{pmatrix} t & -k\frac{t}{d_1} \\ 0 & t \end{pmatrix}$ has integer coefficient, M is the generator matrix of the q-ary code $C = \langle \overline{c_1}, \overline{c_2} \rangle \subseteq \mathbb{Z}_q^2$ where $c_1 = (2e+1, kh1)$ and $c_2 = (0, 2e+1)$. Every codeword is of the form $\overline{c} = x\overline{c_1} + y\overline{c_2}$ with $x, y \in \mathbb{Z}$. Since $||\overline{c}||_\infty = \max\{|\overline{(2e+1)x}|_1, |\overline{kh_1x + (2e+1)y}|_1\}$, the inequality $||\overline{c}||_\infty < 2e+1$ implies $\overline{c} = 0$, thus the minimum distance of C is $\text{dist}(C) \geq 2e+1$. In addition, the cardinality of C is $\#C = q^2/\det(M) = t^2$, so by the sphere packing condition the code C is perfect with packing radius e and it is of type 2 because is linear and $\overline{c_2} = (2e+1)\overline{e_2} \in C$. To prove the converse we consider a code $C \in LPL^\infty(2, e, q)_o$, since C is linear then $0 \in C$ and $C = C_2(0, h)$ for some $h : \mathbb{Z}_t \to \mathbb{Z}_q$. In particular, C has two codewords $c_1 = (\overline{2e+1}, \overline{y_1})$ and $c_2 = (\overline{0}, \overline{2e+1})$ where $y_1 \in \mathbb{Z}$ is such that $\overline{y_1} = h(1) \in \mathbb{Z}_q$. Let $ty_1 = (2e+1)s + r$ with $s, r \in \mathbb{Z}$ and $0 \leq r < 2e+1$. By linearity $tc_1 - sc_2 = (\overline{0}, \overline{r}) \in C$ which has minimum distance $2e+1$, so $r = 0$ and $y_1 = h_1k$ for some integer k. The code C' generated by c_1 and c_2 has generator matrix $M = \begin{pmatrix} 2e+1 & kh_1 \\ 0 & 2e+1 \end{pmatrix}$, therefore by the first part, the code C' generated by c_1 and c_2 is a $(2, e, q)$-perfect code which is contained in C, so $C' = C$. □

Notation 4.2.34. *We denote by $LC_q(e, k)$ the q-ary perfect code whose generator matrix is given by* $\begin{pmatrix} 2e+1 & kh_1 \\ 0 & 2e+1 \end{pmatrix}$.

Remark 4.2.35. *Replacing the first row by the sum of that row and an integer multiple of the second row if necessary, we can always suppose that the number k in the statement of Theorem 4.2.33 verify $0 \leq k < d_1$. In fact, it is possible replace k by any integer congruent to k modulo d_1 with this elementary operation in rows, so $LC_q(e, k) = LC_q(e, k_0)$ if $k \equiv k_0 \pmod{d_1}$.*

Now we approach the problem of what group isomorphism classes are represented by $(2, e, q)$-perfect codes (admissible structures). By the sphere packing condition, if $C \in LPL^\infty(2, e, q)$ then $\#C = t^2$. The structure theorem for finitely generated abealian groups [Fra13, p. 338] in this case, take the following spacial form.

Lemma 4.2.36. *If C is an abelian group of order t^2 then there is an unique divisor $d|t$ such that $C \simeq \mathbb{Z}_{t/d} \times \mathbb{Z}_{dt}$.*

The question of what isomorphism classes are represented by two-dimensional perfect codes in the Chebyshev metric is equivalent to determining for what values of $d|t$ there exists $C \in LPL^\infty(2, e, q)$ such that $C \simeq \mathbb{Z}_{t/d} \times \mathbb{Z}_{dt}$.

Lemma 4.2.37. *Let $q = (2e+1)t, d_1 = \gcd(2e+1, t), h_1 = \frac{2e+1}{d_1}, d_2 = \gcd(d_1, k), h_2 = \frac{d_1}{d_2}, k_1 = \frac{k}{d_2}$ and $k' \in \mathbb{Z}$ such that $k_1k \equiv 1 \pmod{h_2}$. Then $N = \begin{pmatrix} (2e+1)h_2 & 0 \\ (2e+1)k' & h_1d_2 \end{pmatrix}$ is a generator matrix for $LC_q(e, k)$.*

Proof. Let M be the generator matrix for $LC_q(e,k)$ given in Theorem 4.2.33 and $U = \begin{pmatrix} h_2 & -k_1 \\ k' & \frac{1-k_1k'}{h_2} \end{pmatrix}$. Since $\det(U) = 1$ and $UM = N$ we have that N is also a generator matrix for $LC_q(e,k)$. □

Theorem 4.2.38. *Let $q = (2e+1)t$, k be an integer and $h_2 = \frac{\gcd(2e+1,t)}{\gcd(2e+1,t,k)}$.*

(i) $LC_q(e,k) \simeq \mathbb{Z}_{t/h_2} \times \mathbb{Z}_{th_2}$ (isomorphic as groups).

(ii) There exists $C \in LPL^{\infty}(2,e,q)$ such that $C \simeq \mathbb{Z}_{t/d} \times \mathbb{Z}_{td}$ if and only if $d \mid \gcd(2e+1,t)$.

Proof. To prove (i) we consider the homomorphism $T : \mathbb{Z}^2 \to \mathbb{Z}_q^2$ given by $T(x) = x\overline{N}$, where N is as in Lemma 4.2.37. We have that $\ker(T) = \frac{t}{h_2}\mathbb{Z} \times th_2\mathbb{Z}$ and by the referred lemma $\mathrm{Im}(T) = LC_q(e,k)$, so (i) follows from the First group isomorphism theorem [Fra13, p. 307]. To prove (ii) we observe that for every k we have $h_2 \mid \gcd(2e+1,t)$ and for $d \mid d_1$ where $d_1 = \gcd(2e+1,t)$, then $LC_q(e, \frac{d_1}{d}) \simeq \mathbb{Z}_{t/d} \times \mathbb{Z}_{td}$. □

Corollary 4.2.39. *There exists a two-dimensional perfect code $C \simeq \mathbb{Z}_a \times \mathbb{Z}_b$ and $a \mid b$ if and only if ab is a perfect square and b/a is an odd number.*

Proof. ($\Rightarrow$) By Theorems 4.2.33 and 4.2.38 if $\mathbb{Z}_a \times \mathbb{Z}_b \simeq C$ with $a|b$ for some perfect code C, then there exists integers t, h_2 and e such that $a = \frac{t}{h_2}, b = th_2$ and $h_2 \mid 2e+1$ (in particular h_2 is odd), thus $ab = t^2$ is a perfect square and $\frac{b}{a} = h_2^2$ is odd.
($\Leftarrow$) Let $ab = t^2$ and $b = as$ with s odd. Since $a^2s = t^2$ we have $s = (2e+1)^2$ and $(2e+1)a = t$. Defining $q = (2e+1)t$, by Theorem 4.2.38 we have $LC_q(e,1) \simeq \mathbb{Z}_a \times \mathbb{Z}_b$. □

Corollary 4.2.40. *Let $C \in LPL^{\infty}(2,e,q)$ with $q = (2e+1)t$. Then, $C \simeq \mathbb{Z}_t \times \mathbb{Z}_t \Leftrightarrow C$ is the cartesian code $C = (2e+1)\mathbb{Z}_q^2$.*

Proof. By Theorem 4.2.33 and Remark 4.2.35 every code is of the form $C = LC_q(e,k)$ for some k with $0 \leq k < d_1$ and by Theorem 4.2.38 we have $C \simeq \mathbb{Z}_t \times \mathbb{Z}_t \Leftrightarrow h_2 = 1 \Leftrightarrow d_1 = d_2 \Leftrightarrow d_1 \mid k \Leftrightarrow 2e+1 \mid kh_1 \Leftrightarrow k = 0 \Leftrightarrow C = (2e+1)\mathbb{Z}_q^2$. □

Corollary 4.2.41. *There exists a linear two-dimensional q-ary perfect code C that is non-cartesian if and only if $q = p^2a$ where p is an odd prime number and a is a positive integer.*

Proof. By Theorem 4.2.38 part (ii), there exists a q-ary non-cartesian perfect code if and only if $q = (2e+1)t$ for some integers e and t such that $\gcd(2e+1,t) > 1$. This last condition is equivalent to $2e+1 = pm$ and $t = pn$ for some odd prime p and $m, n \in Z^+$, thus $q = p^2a$ where p is an odd prime and a is a positive integer. □

Example 4.2.42. *The first value of q for which there exists a two-dimensional q-ary perfect code that is neither cartesian nor cyclic is for $q = 3^2 \cdot 2$. An example of such code has generators $\{(0,9),(1,3)\} \subseteq \mathbb{Z}_{18}^2$, see Figure 4.6.*

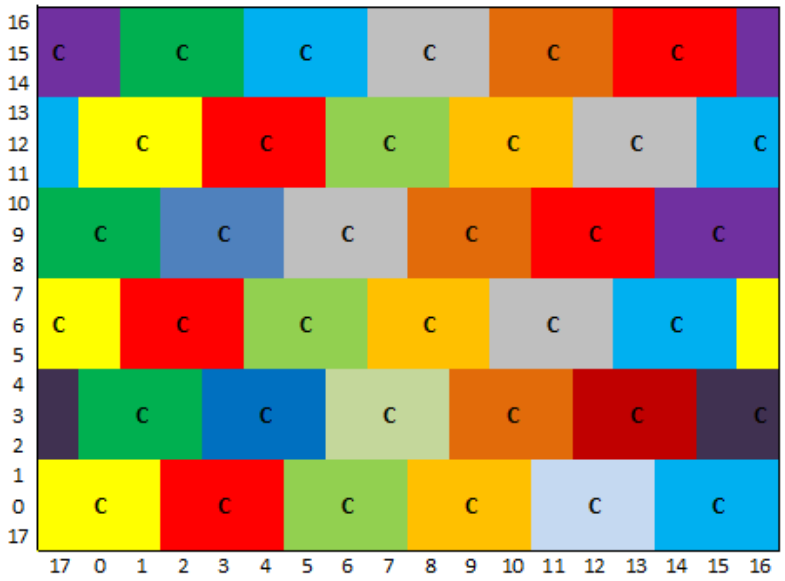


Figure 4.6: For $q = 3^2 \cdot 2$, the perfect code $C = \langle (0,9), (1,3) \rangle \subseteq \mathbb{Z}_{18}^2$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_{18}$.

Corollary 4.2.43. *There exists a two-dimensional cyclic q-ary perfect code if and only if $q = p^2 a$ where p is an odd prime number and a is an odd positive integer.*

Proof. By Theorem 4.2.38 part (ii), there exists a q-ary cyclic perfect code if and only if $q = (2e+1)t$ for some integers e and t such that $\gcd(2e+1, t) = t > 1$. This last condition is equivalent to $2e + 1 = mt$ for some odd integer m, thus $q = mt^2$ where a is an odd integer and $t > 1$ which is equivalent to $q = ap^2$ where a is an odd integer and p is an odd prime number. □

Corollary 4.2.44. *Let $q = (2e+1)t$. There exists a cyclic code in $LPL^\infty(2, e, q)$ if and only if $t \mid 2e+1$. In this case $LC_q(e, k)$ is cyclic if and only if* $\gcd(k, t) = 1$.

Proof. By Theorem 4.2.38 part (ii), there exists a cyclic code in $LPL^\infty(2, e, q)$ if and only if $\gcd(2e+1, t) = t$ if and only if $t \mid 2e+1$. In this case, by Theorem 4.2.38 part (i), we have $LP_q(e, k) \equiv \mathbb{Z}_{t^2} \Leftrightarrow h_2 = t \Leftrightarrow$ and $\gcd(2e+1, t, k) = \gcd(t, k) = 1$. □

Isometry and isomorphism classes of two-dimensional perfect codes in the Chebyshev metric

Since the cardinality of a perfect q-ary code is determined by its packing radius, it suffices to classify isometry classes and isomorphism classes in the set $LPL^\infty(2, e, q)$ for a fixed value of e. Moreover, since every $(2, e, q)$-perfect code is isometric to an type 2 perfect code we can restrict to $LPL^\infty(2, e, q)_o$. Our main result here is a parametrization of the set $LPL^\infty(2, e, q)_o$ by the ring $\mathbb{Z}_{d_1}$ (where $d_1 = \gcd(2e+1, t)$) in such a way that isometry classes and isomorphism classes correspond to certain generalized cosets.

Lemma 4.2.45. *There exists $u \in \mathbb{Z}_d^*$ such that $a \equiv ub \pmod{d} \Leftrightarrow \gcd(a,d) = \gcd(b,d)$.*

Proof. If $a \equiv ub \pmod{d}$ with $\gcd(u,d) = 1$ clearly $\gcd(a,d) = \gcd(b.d)$. Now suppose that $\gcd(a,d) = \gcd(b,d)$ and consider $d = p_1^{\alpha_1} \cdots p_t^{\alpha_t} q_1^{\beta_1} \cdots q_s^{\beta_s}$ and $a = p_1^{\gamma_1} \cdots p_t^{\gamma_t} q_1^{\delta_1} \cdots q_s^{\delta_s}$ the factorial decomposition of d and a where $\alpha_i > \gamma_i \geq 0$ for $1 \leq i \leq t$ and $0 < \beta_j \leq \delta_j$ for $1 \leq j \leq s$. Since $\gcd(a,d) = \gcd(b,d)$ we have $p_i^{\gamma_i} \parallel b$ (since $\min\{\nu_{p_i}(a) = \gamma_i, \alpha_i\} = \min\{\nu_{p_i}(b), \alpha_i\}$). Let $a_i = \frac{a}{p_i^{\gamma_i}}$ and $b_i = \frac{b}{p_i^{\gamma_i}}$ for $i = 1, 2, \ldots, t$. The congruence $a \equiv bx \pmod{p_i^{\alpha_i}}$ is equivalent to $a_i \equiv b_i x \pmod{p_i^{\alpha_i - \gamma_i}}$ which is equivalent to $x \equiv a_i c_i \pmod{p_i^{\alpha_i - \gamma_i}}$ where $b_i c_i \equiv 1 \pmod{p_i^{\alpha_i - \gamma_i}}$ (we observe that $p \nmid b_i$). Consider the system of congruences

$$\begin{cases} x \equiv a_1 c_1 & (\text{mod } p_1^{\alpha_1 - \gamma_1}) \\ x \equiv a_2 c_2 & (\text{mod } p_2^{\alpha_2 - \gamma_2}) \\ \vdots & \\ x \equiv a_t c_t & (\text{mod } p_t^{\alpha_t - \gamma_t}) \\ x \equiv 1 & (\text{mod } q_1 q_2 \ldots q_s) \end{cases}$$

By the Chinese remainder theorem there exists a solution $u \in \mathbb{Z}$ for this system. Since $p_i \nmid a_i c_i$ and $\alpha_i > \gamma_i$ we have $\gcd(u,d) = 1$. For $j, 1 \leq j \leq s$ we have $q_j^{\delta_j} \mid b$ (since $\gcd(a,d) = \gcd(b.d)$) and therefore $a \equiv bu \pmod{q_j^{\gamma_j}}$ because both sides are congruent to 0 modulo $q_j^{\gamma_j}$. By the Chinese remainder theorem again, we have $a \equiv bu \pmod{d}$. □

Theorem 4.2.46. *Let $q = (2e+1)t, d_1 = \gcd(2e+1, t)$ and $h_1 = \frac{2e+1}{d_1}$. We have the parametrization (bijection):*

$$\psi : \mathbb{Z}_{d_1} \to LPL^{\infty}(2, e, q)_o$$

$$k + d_1\mathbb{Z} \mapsto LC_q(e, k),$$

which induces the parametrizations:

$$\psi_{\mathcal{G}} : \frac{\mathbb{Z}_{d_1}}{\{1, -1\}} \to LPL^{\infty}(2, e, q)_o / \mathcal{G}$$

$$k \cdot \{1, -1\} \mapsto [\psi(k)]_{\mathcal{G}},$$

and

$$\psi_{\mathcal{A}} : \frac{\mathbb{Z}_{d_1}}{\mathbb{Z}_{d_1}^*} \to LPL^{\infty}(2, e, q)_o / \mathcal{A}$$

$$k \cdot \mathbb{Z}_{d_1}^* \mapsto [\psi(k)]_{\mathcal{A}},$$

Proof. By Theorem 4.2.33 and Remark 4.2.35 the map ψ is well defined and is a surjection, so it remains to prove that $LC_q(e, k_1) = LC_q(e, k_2) \Leftrightarrow k_1 \equiv k_2 \pmod{d_1}$. Since both codes have the same cardinality t^2, we have

$$LC_q(e, k_1) = LC_q(e, k_2) \Leftrightarrow LC_q(e, k_1) \subseteq LC_q(e, k_2) \Leftrightarrow (h_1 k_1, 2e+1) \in LC_q(e, k_2)$$

$$\Leftrightarrow \exists x, y, \in \mathbb{Z} : \begin{cases} (2e+1)x + h_1k_2y \equiv h_1k_1 \pmod{q} \\ (2e+1)y \equiv 2e+1 \pmod{q} \end{cases}$$

$$\Leftrightarrow \exists x, y, \in \mathbb{Z} : \begin{cases} y \equiv 1 \pmod{t} \\ d_1x + k_2y \equiv k_1 \pmod{td_1} \end{cases} \Rightarrow \exists y \in \mathbb{Z} : \begin{cases} y \equiv 1 \pmod{d_1} \\ k_2y \equiv k_1 \pmod{d_1} \end{cases}$$

which implies $k_1 \equiv k_2 \pmod{d_1}$.

Let $\eta_i : \mathbb{Z}_q^2 \to \mathbb{Z}_q^2$ for $i = 1, 2$ given by $\eta_1(x, y) = (-x, y)$ and $\eta_2(x, y) = (x, -y)$. We have that $\eta_1(LC_q(e, k)) = \langle(-(2e+1), 0), (-kh_1, 2e+1)\rangle = LC_q(e, -k)$ and the same is valid for η_2, thus $[\psi(k)]_{\mathcal{G}} = \{\psi(-k), \psi(k)\}$ and so $\psi_{\mathcal{G}}$ is well defined and is a bijection. By Theorem 4.2.38 we have $\psi(k) = LC_q(e, k) \simeq \mathbb{Z}_{t/h_2} \times \mathbb{Z}_{th_2}$ where $h_2 = \frac{d_1}{\gcd(d_1,k)}$, therefore $[\psi(k_1)]_{\mathcal{A}} = [\psi(k_2)]_{\mathcal{A}} \Leftrightarrow \gcd(k_1, d_1) = \gcd(k_2, d_1)$ and so $k_1 \equiv uk_2 \pmod{d_1}$ for some $u \in \mathbb{Z}$ with $gcd(u, d_1) = 1$ (Lemma 4.2.45), which is equivalent to $k_1\mathbb{Z}_{d_1}^* = k_2\mathbb{Z}_{d_1}^*$. □

Example 4.2.47. *Let $p > 2$ be a prime number and we take $q = p^2$ and $e \geq 1$ such that $2e + 1 = p$. In this case $d_1 = p$ and we have exactly p codes in $LPL^\infty(2, p, p^2)$ given by $LC_{p^2}(p, k)$ for $0 \leq k < p$, where the code $LC_{p^2}(p, k)$ has generator matrix $M_k = \begin{pmatrix} p & 0 \\ k & p \end{pmatrix} \in \mathcal{M}_{2\times 2}(\mathbb{Z}_{p^2})$. There exist exactly $\frac{p+1}{2}$ of such perfect codes up to isometry, given by $LC_{p^2}(p, k)$ for $0 \leq k \leq \frac{p-1}{2}$. Since p is prime, we have $\mathbb{Z}_p = \{0\} \uplus \mathbb{Z}_p^*$, so there exist exactly 2 perfect codes in $LPL^\infty(2, p^2, p)$ up to isomorphism, one of which is the cartesian code (which corresponds to $k = 0$) and the other is $LC_{p^2}(p, 1)$ (which is isomorphic to $LC_{p^2}(p, k)$ for $1 < k < p$).*

Corollary 4.2.48. *The set $\{LC_q(e, k) : 0 \leq k \leq \frac{d_1-1}{2}\}$ is a set of representative of $LPL^\infty(2, e, q)/\mathcal{G}$ and $\{LC_q(e, k) : k \mid d_1\}$ is a set of representative of $LPL^\infty(2, e, q)/\mathcal{A}$.*

Corollary 4.2.49. *There exist exactly $d_1 = \gcd(2e + 1, t)$ codes in $LPL^\infty(2, e, q)$ where $q = (2e+1)t$. There exist exactly $\frac{d_1+1}{2}$ of such codes up to isometry and there exist exactly $\sigma_0(d_1)$ of such codes up to isomorphism where σ_0, as usual, denotes the number-of-divisors function.*

Proof. The first two assertion are immediate. For the third assertion we observe that $\mathbb{Z}_{d_1} = \biguplus_{d|d_1} d\mathbb{Z}_{d_1}^*$ and use Theorem 4.2.46. □

4.2.3 Some remarks on p-Lee two-dimensional perfect codes

In what follows we point out some similarities and differences between perfect codes in the Lee metric ($p = 1$) and in the Chebyshev metric ($p = \infty$) and also comment on connections with perfect p-Lee codes for other values of p.

On the one hand the characterization of the values $(2, e, q)$ for which there exist a perfect code (admissible parameters) is trivial in the case of the Chebyshev metric

but is not so trivial in the case of the Lee metric. On the other hand, for a given admissible parameter $(2, e, q)$ there is only one perfect code up to symmetry in the Lee metric while in the case of Chebyshev codes this number can be arbitrary large (depend on the choice of e and q) even if we are restricted to linear codes. For this reason the problem of determining the isometry and isomorphism classes only have sense in the second case. One remarkable similarity in both cases is that it is possible to define the type of a code, that is, there exists exactly two vector $v_1(e) = (a, b) \in \mathbb{Z}^n$ and $v_2(e) = (b, a) \in \mathbb{Z}^n$ such that if C is a $(2, e, q)$-perfect code then $\overline{v_1} + C = C$ or $\overline{v_2} + C = C$. This property plays an important role in the description of the perfect q-ary code with a given packing radius e. Another remarkable property is related to the ω-set of codewords (Definition 4.2.13). For general p, we say that two p-Lee balls $B_p(c, e)$ and $B_p(c', e)$ are adjacent if they are disjoint and there exists $x \in B_p(c, e)$ and $y \in B_p(c', e)$ such that $d_p(x, y) = 1$. Then, for a given codeword $c \in C$ we define its ω-set with respect to the p-metric by the property $v \in \omega_p(c) \Leftrightarrow B_p(c + v, e)$ is adjacent to $B_p(c, e)$ and $c + v \in C$. In the case of Lee and Chebyshev metrics, we have that for every perfect code $\bigcap_{c \in C} \omega_p(c) \neq \emptyset$, which geometrically means that these codes present certain regularity.

In [CJC+15], the authors prove that every two-dimensional perfect code C in the 2-Lee metric, has packing radius $e \in \{1, \sqrt{2}, 2, \sqrt{8}\}$ and for each of these value either C is a perfect code in the Lee metric or C is a perfect code in the Chebyshev metric. Moreover, we have:

- $PL^2(2, 1, q) = PL^1(2, 1, q)$,
- $PL^2(2, \sqrt{2}, q) = PL^\infty(2, 1, q)$,
- $PL^2(2, 2, q) = PL^1(2, 2, q)$,
- $PL^2(2, \sqrt{8}, q) = PL^\infty(2, 2, q)$.

Using our results on Lee perfect codes and Chebyshev perfect codes we can describe completely two-dimensional perfect codes in the 2-Lee metric. In fact, checking for several values of e and p, we did not find other p-Lee ball different from the Lee-ball and Chebyshev-ball capable of tiling the plane. We also observe the inclusion of p-Lee balls over $\mathbb{Z}^2$:

$$B_1(0, [e]) = B_1(0, e) \subseteq B_p(0, e) \subseteq B_\infty(0, e) = B_\infty(0, [e])$$

and we make the following conjecture.

Conjecture 4.2.50. *For every $p \geq 1$,$e \geq 1$ and $q \geq 2[e] + 1$, if $PL^p(2.e, q) \neq \emptyset$ then either $PL^p(2, e, q) = PL^1(2, [e], q)$ or $PL^\infty(2, [e], q)$.*

4.3 Some constructions for the Chebyshev metric

In this section we give some constructions of perfect codes in the maximum metric from perfect codes in smaller dimensions. We also present a section construction which plays an important role in the next section. In this section and in the following section of this chapter we deal only with perfect codes in the Chebyshev metric, and use d to denote the Chebyshev metric in $\mathbb{Z}_q^n$ and B for the ball with respect to this metric.

The simplest way to obtain perfect codes is using cartesian product. Using the sphere packing condition we obtain the following proposition.

Proposition 4.3.1 (Cartesian product construction)**.** *If $C_1 \in PL^\infty(n_1, e, q)$ and $C_2 \in PL^\infty(n_1, e, q)$ then $C_1 \times C_2 \in PL^\infty(n_1 + n_2, e, q)$. This construction preserves linearity.*

Proof. Let $c_{11}, c_{12} \in C_1$ and $c_{21}, c_{22} \in C_2$, we observe that

$$d_\infty((c_{11}, c_{21}), (c_{12}, c_{22})) = \max\{d_\infty(c_{11}, c_{12}), d_\infty(c_{21}, c_{22})\}.$$

If $(c_{11}, c_{21}) \neq (c_{12}, c_{22})$ then $c_{11} \neq c_{12}$ or $c_{21} \neq c_{22}$, thus $d_\infty(c_{11}, c_{12}) \geq 2e+1$ or $d_\infty(c_{12}, c_{22}) \geq 2e+1$ (since C_1 and C_2 have packing radius e), therefore $d_\infty((c_{11}, c_{21}), (c_{12}, c_{22})) \geq 2e+1$ and we conclude that the packing radius of $C_1 \times C_2$ is at least e. Calculating the cardinality $C_1 \times C_2 = \#C_1 \cdot \#C_2 = t^{n_1} \cdot t^{n_2} = t^{n_1+n_2}$, where t is such that $q = (2e+1)t$. By the sphere packing condition we conclude that the packing radius of $C_1 \times C_2$ is e and that $C_1 \times C_2$ is a perfect code. The fact that this construction preserve linearity is clear. □

Corollary 4.3.2. *There exists a linear non-cartesian n-dimensional q-ary perfect code if and only if $q = p^2a$ where p is an odd prime number and a is a positive integer.*

Proof. By Corollary 4.2.41, there exists a perfect code $C \in LPL^\infty(2, e, q)$ for some e that is neither trivial nor standard cartesian. By Proposition 4.3.1, $C \times (2e+1)\mathbb{Z}_q^{n-2} \in LPL^\infty(n, e, q)$ is neither trivial nor standard cartesian. □

Corollary 4.3.3. *If $q = (2e+1)t$ and $d_1, d_2, \ldots, d_k$ are divisors (not necessarily distinct) of $\gcd(2e+1, t)$, there exists a code $C \in LPL^\infty(2k, e, q)$ such that*

$$C \simeq \mathbb{Z}_{\frac{t}{d_1}} \times \mathbb{Z}_{\frac{t}{d_2}} \times \ldots \mathbb{Z}_{\frac{t}{d_k}} \times \mathbb{Z}_{d_1 t} \times \mathbb{Z}_{d_2 t} \times \ldots \mathbb{Z}_{d_k t}$$

and a code $C \in LPL^\infty(2k+1, e, q)$ such that

$$C \simeq \mathbb{Z}_{\frac{t}{d_1}} \times \mathbb{Z}_{\frac{t}{d_2}} \times \ldots \mathbb{Z}_{\frac{t}{d_k}} \times \mathbb{Z}_t \times \mathbb{Z}_{d_1 t} \times \mathbb{Z}_{d_2 t} \times \ldots \mathbb{Z}_{d_k t}.$$

Proof. By Theorem 4.2.38, we have a code $C_i \in LPL^\infty(2, e, q)$ such that $C_i \simeq \mathbb{Z}_{\frac{t}{d_i}} \times \mathbb{Z}_{d_i}$ for $1 \leq i \leq k$ and the code $(2e+1)\mathbb{Z}_q \in LPL^\infty(1, e, q)$ is isomorphic to $\mathbb{Z}_t$. So we can construct a perfect code as claimed using the above construction. □

Remark 4.3.4. *There are others linear perfect codes whose group structure is not of the form given in Corollary 4.3.3 (for example those in Corollary 4.3.8).*

The next construction is exclusively for linear codes, this allows us to construct a linear perfect q-ary code from other codes of smaller dimension.

Notation 4.3.5. *If H is a subgroup of an abelian group G and $t \in \mathbb{Z}^+$, we denote by $t^{-1}H = \{g \in G : tg \in H\}$.*

Remark 4.3.6. *With the notation above, $t^{-1}H$ is a subgroup of G that contain H.*

Proposition 4.3.7 (Linear construction)**.** *If $C \in LPL^{\infty}(n, e, q)$ with $q = (2e+1)t$ and $x \in t^{-1}C$, then $\widetilde{C} = C \times \{0\} + (x, 2e+1)\mathbb{Z} \in LPL^{\infty}(n+1, e, q)$.*

Proof. Since $tx \in C$ every codeword $v \in \widetilde{C}$ can be written as $v = (c + xk, (2e+1)k)$ with $c \in C$ and $0 \leq k < t$ and we have

$$\|(c + xk, (2e+1)k)\|_{\infty} = \max\{\|c + xk\|_{\infty}, \|(2e+1)k\|_{\infty}\}. \tag{4.3.1}$$

If $k = 0$, then $\|(c + xk, (2e+1)k)\|_{\infty} = \|c\|_{\infty} \geq 2e+1$ if $c \neq 0$ (since C has packing radius e). If $0 < k < t$, then $\|(2e+1)k\|_{\infty} \geq 2e+1$ and by Equation (4.3.1) we have $\|(c + xk, (2e+1)k)\|_{\infty} \geq 2e+1$. We conclude that C has packing radius at least e. We want to calculate the cardinality of C, that is

$$\#C = \frac{\#C \times \{0\} \cdot \#(x, 2e+1)\mathbb{Z}}{\#C \times \{0\} \cap (x, 2e+1)\mathbb{Z}}. \tag{4.3.2}$$

We have $\#C \times \{0\} = \#C = t^n$. Let θ the additive order of tx in $\mathbb{Z}_q^n$ (i.e. the least positive integer θ such that $\theta tx = 0$). It is straightforward to check that the order of $(x, 2e+1)$ in $\mathbb{Z}_q^{n+1}$ is $t\theta$ and that $C \times \{0\} \cap (x, 2e+1)\mathbb{Z} = (tx, 0)\mathbb{Z}$. Using Equation (4.3.2) we have $\#C = \frac{t^n \cdot t\theta}{\theta} = t^{n+1}$ and by the sphere packing condition the code $\widetilde{C} \subseteq \mathbb{Z}_q^{n+1}$ is perfect with packing radius e. □

Corollary 4.3.8. *If $q = (2e+1)t$ with $t^{n-1} \mid 2e+1$ and $n \geq 1$, then the q-ary cyclic code*

$$\mathcal{C}_{n,e,q} = \left\langle \left(\frac{2e+1}{t^{n-1}}, \frac{2e+1}{t^{n-2}}, \ldots, \frac{2e+1}{t}, 2e+1 \right) \right\rangle \in LPL^{\infty}(n, e, q).$$

Proof. We denote by $p_n = \left(\frac{2e+1}{t^{n-1}}, \frac{2e+1}{t^{n-2}}, \ldots, \frac{2e+1}{t}, 2e+1 \right) \in \mathbb{Z}_q^n$ and proceed by induction. For $n = 1$ it is clear. If $C_{n,e,q} \in LPL^{\infty}(n, e, q)$ holds for some $n \geq 1$, we apply the linear construction with $x = \left(\frac{2e+1}{t^n}, \frac{2e+1}{t^{n-2}}, \ldots, \frac{2e+1}{t} \right)$. Since $tx = p_n \in C_{n,e,q}$ then $\widetilde{C} = \langle (p_n, 0), (x, 2e+1) = p_{n+1} \rangle \in LPL^{\infty}(n+1, e, q)$. We observe that $tp_{n+1} = (p_n, 0)$ (since $(2e+1)t \equiv 0 \pmod{q}$), so $\widetilde{C} = \langle p_{n+1} \rangle$. □

In particular, if $2e + 1 = t^{n-1}$ we obtain the following family of cyclic perfect codes.

Corollary 4.3.9. *If $q = t^n$ where t is an odd number, then the q-ary code $C = \langle (1, t, t^2, \ldots, t^{n-1}) \rangle \in LPL^{\infty}(n, e, q)$, for the packing radius $e = (t^{n-1} - 1)/2$.*

Proposition 4.3.10. *Let $q = (2e + 1)t$. There exists a cyclic code in $LPL^{\infty}(n, e, q)$ if and only if $t^{n-1} \mid 2e + 1$.*

Proof. If $C \in LPL^{\infty}(n, e, q)$ is cyclic, there exists $c \in C$ with order $t^n = |C|$. Since $qc = 0$ we have $t^n \mid q$, and so $t^{n-1} \mid 2e + 1$. The converse follows from Corollary 4.3.8. □

The next construction generalize horizontal and vertical construction for two-dimensional perfect code in the maximum metric presented in the previous section.

Proposition 4.3.11 (Non linear construction)**.** *Let $C \in PL^{\infty}(n, e, q)$ and $h : C \to \mathbb{Z}_q$ be a map (called height function). If $\widehat{C} = \{(c, h(c) + (2e + 1)k) : c \in C, k \in \mathbb{Z}\}$, then $\widehat{C} \in PL^{\infty}(n + 1, e, q)$.*

Proof. Since $(2e + 1)t = q$ we have $\#\widehat{C} = \#C \cdot t = t^{n+1}$, thus it suffices to prove that the minimum distance of $\widehat{C}$ is at least $2e + 1$. Let $\widehat{c}_i = (c_i, h(c_i) + (2e + 1)k_i) \in \widehat{C}$ with $c_i \in C$ for $i = 1, 2$ and suppose that $\| \widehat{c_1} - \widehat{c_2} \|_{\infty} < 2e + 1$. The relation

$$\| \widehat{c_1} - \widehat{c_2} \|_{\infty} = \| c_1 - c_2 \|_{\infty} + \| (h(c_1) - h(c_2)) + (2e + 1)(k_1 - k_2) \|_{\infty}$$

implies $\| c_1 - c_2 \|_{\infty} < 2e$ and $\| (h(c_1) - h(c_2)) + (2e + 1)(k_1 - k_2) \|_{\infty} < 2e + 1$ and so $c_1 = c_2$ (since the minimum distance of C is $2e + 1$) and $k_1 = k_2$. Therefore the minimum distance of $\widehat{C}$ is also $2e + 1$ and $\widehat{C} \in PL^{\infty}(n + 1, e, q)$. □

Remark 4.3.12. *The non linear construction generalize horizontal and vertical constructions. Indeed, let $NL(C, h)$ be the code obtained from the non-linear construction from the code C and the height function h. Considering $C_a = a + (2e + 1) \in PL^{\infty}(1, e, q)$ and $h_a(k) = h(a + (2e + 1)k)$ then $C_2(a, h_a) = NL(C_a, h)$ and $C_1(a, h_a) = \sigma NL(C_a, h)$ where $\sigma = (1\ 2)$.*

Remark 4.3.13. *If C is linear, it is possible to choose the height function in such a way that $\widetilde{C}$ is also linear, but for arbitrary choice of h this is not true.*

Remark 4.3.14. *Every code constructed from the non linear construction is standard. Consequently, there are codes that cannot be constructed from the non-linear construction (for example the code given in the Remark 4.2.29). On the other hand, by Corollary 2.0.22 we can obtain every linear perfect code using this construction (with good choices for the height functions) in a finite number of steps.*

The next construction allows us to obtain perfect codes in lower dimension from a given perfect code via cartesian sections. This construction plays a fundamental role in the next section, when we introduce the concept of ordered code.

Definition 4.3.15. *Let $S \subseteq \mathbb{Z}_q^n$. A perfect code over S is a subset $C \subseteq S$ for which there exists $e \in \mathbb{N}$ such that $S = \biguplus_{c \in C} (B(c,e) \cap S)$. In this case, e is determined by C (by the packing sphere condition) and is called the packing radius of C.*

Notation 4.3.16. *Let $[n] = \{1, 2, \ldots, n\}$. If $I \subseteq [n]$, we denote by $H_I = \{x \in \mathbb{Z}_q^n : x_i = 0, \forall i \in I\}$ (these sets are called cartesian subgroups). We define its dimension as $\dim(H_I) = n - \#I$.*

Definition 4.3.17. *Let $I \subseteq [n]$. The orthogonal projection over H_I is the unique morphism $\pi_I : \mathbb{Z}_q^n \to \mathbb{Z}_q^n$ verifying $\pi_I(e_i) = \begin{cases} 0 & \forall i \in I \\ e_i & \forall i \in I^c \end{cases}$.*

The following lemma is a direct consequence of this definition.

Lemma 4.3.18. *Let $I \subseteq [n]$. For $h \in H_I$ and $x \in \mathbb{Z}_q^n$ we have $d(x,h) \geq d(\pi_I(x), h)$.*

Notation 4.3.19 (Generalized balls)**.** *If $H \subseteq \mathbb{Z}_q^n$ and $e \in \mathbb{N}$, we denote by*

$$B(H,e) = \{x \in \mathbb{Z}_q^n : d(x,h) \leq e \text{ for some } h \in H\} = \bigcup_{h \in H} B(h,e).$$

Lemma 4.3.20. *If $x \in \mathbb{Z}_q^n$ and $H = H_I$ is a cartesian subgroup, then $x \in B(H,e)$ if and only if $|x_i|_1 \leq e$ for all $i \in I$.*

Proof. If $x \in B(H,e)$ then exists $y \in H$ such that $d(x,y) \leq e$, so $|x_i - y_i|_1 \leq e$ for all $i \in [n]$. In particular $|x_i - 0|_1 \leq e$, for all $i \in I$. Reciprocally, if $x \in \mathbb{Z}_q^n$ verifies $|x_i|_1 \leq e$ for all $i \in I$ we consider the point $y \in \mathbb{Z}_q^n$ such that $y_i = \begin{cases} y_i = 0 & \text{for } i \in I \\ y_i = x_i & \text{for } i \in I^c \end{cases}$, then $x \in B(y,e) \subseteq B(H,e)$. □

Remark 4.3.21. *If $C \in LPL^\infty(n,e,q)$ and $f_C : \mathbb{Z}_q^n \to C$ is the associated error correcting function, then $B(H,e) \cap C = f_C(H)$.*

Definition 4.3.22. *Let $C \subseteq \mathbb{Z}_q^n$ and $I \subseteq [n]$. The cartesian section of C (respect to the cartesian subgroup H_I) is given by $C\langle I \rangle = \pi_I(B(H_I,e) \cap C) = \pi_I \circ f_C(H_I)$.*

We remark that if $m = \#I$, then H_I can be identified with $\mathbb{Z}_q^{n-m}$, consequently codes over H_I are in correspondence with codes over $\mathbb{Z}_q^{n-m}$.

Proposition 4.3.23 (Section construction)**.** *If $C \in PL^\infty(n,e,q)$ and $I \subseteq [n]$, then $C\langle I \rangle$ is a perfect code over H_I with packing radius e.*

Proof. Let $h \in H_I$ and $c = \pi_I(f_C(h)) \in C\langle I \rangle$. By Lemma 4.3.18 $d(c,h) \leq d(f_C(h), h) \leq e$ and we have that $h \in B(c,e)$, so $H \subseteq \bigcup_{c \in C\langle I \rangle} B(c,e)$. Since $H = \bigcup_{c \in C\langle I \rangle} (B(c,e) \cap H)$ the

covering radius of $C\langle I\rangle$ is at most e (as code over H_I). On the other hand, if $\widehat{c}_1, \widehat{c}_2 \in C\langle I\rangle$ verify $d(\widehat{c}_1, \widehat{c}_2) \leq 2e$ and let $\widehat{c}_i = \pi_I(c_i)$ for $i = 1, 2$ where $c_i \in B(H, e) \cap C$, we have

$$|c_1(i) - c_2(i)|_1 = |\widehat{c}_1(i) - \widehat{c}_2(i)|_1 \leq 2e, \ \forall i \in I^c, \tag{4.3.3}$$

and by Lemma 4.3.20 we have

$$|c_1(i) - c_2(i)|_1 \leq |c_1(i)|_1 + |c_2(i)|_1 \leq 2e \ \forall i \in I. \tag{4.3.4}$$

Equations (4.3.3) and (4.3.4) imply $d(c_1, c_2) \leq 2e$, since C has packing radius e we have $c_1 = c_2$ so $\widehat{c}_1 = \widehat{c}_2$. Therefore $C\langle I\rangle$ has minimum distance $d \geq 2e + 1$ and its packing radius is at least e. We conclude that $C\langle I\rangle$ is a perfect code in H_I with packing radius e. □

In the linear case, under some conditions we can prove that the resulting code is also linear.

Lemma 4.3.24. *If $C \in LPL^{\infty}(n, e, q)$ is of type i for all $i \in I$, then $C\langle I\rangle$ is a linear perfect code of H_I with packing radius e. Moreover, $C\langle I\rangle = \pi_I(C)$.*

Proof. We just need to check linearity and for this it suffices to prove that $\pi_I(C) = C\langle I\rangle$. It is clear that $C\langle I\rangle = \pi_I(C \cap B(H_I, e)) \subseteq \pi_I(C)$. For the other inclusion, let $c \in C$ and for each $i \in I$ we consider $k_i \in \mathbb{Z}$ such that $|c + (2e + 1)k_i|_1 \leq e$. Since C is of type i for all $i \in I$, then $(2e + 1)k_i e_i \in C$ and also the vector $v = \sum_{i \in I}(2e + 1)k_i e_i \in C$. By Lemma 4.3.20 $c + v \in C \cap B(H_I, e)$ and $(c + v)_j = c_j$ for all $j \in I^c$, therefore $\pi_I(c) = \pi_I(c + v) \in \pi_I(B(H_I, e) \cap C) = C\langle I\rangle$ and we have $\pi_I(C) \subseteq C\langle I\rangle$. □

4.4 Perfect codes in the Chebyshev metric in arbitrary dimensions

4.4.1 Permutation associated with perfect codes

The type of a code is an important concept when we deal with two-dimensional perfect codes, in part because every two-dimensional perfect code is isometric to a one of type 2 which have a generator matrix with a simple form (upper triangular in this case). This last property is false in greater dimensions so we need a more general concept in order to describe all perfect codes with given parameters (n, e, q).

Notation 4.4.1. *For $C \in LPL^{\infty}(n, e, q)$ we denote by*

$$\tau(C) = \max\{i : 1 \leq i \leq n, C \text{ is of type } i\}.$$

Definition 4.4.2. *Let $C \in LPL^{\infty}(n,e,q)$ with $q=(2e+1)t$ and $t>1$. We consider the following sequence:*

$$\begin{cases} \wp_1 = \tau(C),\ J_1 = \{\wp_1\},\ C_1 = C\langle J_1\rangle \\ \wp_{i+1} = \tau(C_i),\ J_{i+1} = J_i \cup \{\wp_{i+1}\},\ C_{i+1} = C\langle J_{i+1}\rangle \quad \text{for } 1 \leq i < n \end{cases}$$

The permutation of $[n]$ associated with C is $\wp(C) = (\wp_1, \wp_2, \ldots, \wp_n)$.

Remark 4.4.3. *Minkowski-Hajos Theorem (Theorem 2.0.21) and Lemma 4.3.24 guarantee the existence of $\wp_i$ in each step and the linearity of the corresponding code C_i (because we start from a linear code C). Since $(2e+1)e_k \notin H_I$ for $k \in I$, we have that the numbers $\wp_i$ are pairwise different, so $\wp \in S_n$.*

Example 4.4.4. *We consider the code $C = span\begin{pmatrix} 1 & 3 & 0 & 0 \\ 0 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 0 & 0 & 3 & 0 \end{pmatrix}$ over $\mathbb{Z}_{81}^4$. This code is a perfect code with parameters $(n,e,q) = (4,1,81)$, let us calculate its associated permutation. In the first step we have:*

- $\wp_1 = \tau(C) = 3, J_1 = \{3\}, C_1 = C\langle 3\rangle = span\begin{pmatrix} 1 & 3 & 0 & 0 \\ 0 & 0 & 0 & 3 \\ 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$,

in the second step we have:

- $\wp_2 = \tau(C_1) = 4, J_2 = \{3,4\}, C_2 = C\langle 3,4\rangle = span\begin{pmatrix} 1 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$,

in the third step we have:

- $\wp_3 = \mathcal{I}(C_2) = 1, J_2 = \{1,3,4\}, C_3 = C\langle 1,3,4\rangle = span\begin{pmatrix} 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$,

and in the last step we have $\wp_4 = \tau(C_3) = 2$ so, the permutation associated with C is $\wp(C) = (3,4,1,2)$.

Definition 4.4.5. *We say that a perfect code $C \in LPL^{\infty}(n,e,q)$ is ordered if its associated partition is given by $\wp(C) = (n, n-1, \ldots, 2, 1)$.*

Proposition 4.4.6. *For all $C \in LPL^{\infty}(n,e,q)$ there exists $\theta = \theta_C \in S_n$ such that $\theta(C)$ is ordered.*

Proof. Let $C \in LPL^{\infty}(n,e,q)$ with $\wp(C) = (\wp_1, \wp_2, \ldots, \wp_n)$ and θ be the permutation given by $\theta(\wp_i) = n+1-i$. For all i with $1 \leq i < n$ we have $(2e+1)e_{\wp_{i+1}} \in C\langle \wp_1, \ldots, \wp_i \rangle = \pi_{H_I}(C)$ where $I = \{\wp_1, \ldots, \wp_i\}$, so there exists $c \in C \cap \pi_{H_I}^{-1}((2e+1)e_{\wp_{i+1}})$. We have $c_{\wp_{i+1}} = 2e+1$ and $c_k = 0$ for $k \notin \{\wp_1, \wp_2, \ldots, \wp_{i+1}\}$. Since $\theta(c)_i = c_{\theta^{-1}(i)}$ we have $\theta(c)_{n-i} = 2e+1$ and $\theta(c)_k = 0$ for $k : n \geq k \geq n-i$, so

$$(2e+1)e_{n-i} = \pi_{H_{\theta(I)}}(\theta(c)) \in \theta(C)\langle n, n-1, \ldots, n+1-i \rangle$$

for $1 \leq i < n$. This last condition together with the fact that $(2e+1)e_n = \theta((2e+1)e_{\wp_1}) \in \theta(C)$ imply $\wp(\theta(C)) = (n, n-1, \ldots, 1)$. □

Notation 4.4.7. *We denote by $LPL^{\infty}(n,e,q)_o = \{C \in LPL^{\infty}(n,e,q) : C \text{ is ordered}\}$.*

Example 4.4.8. *Let C be the code defined in Example 4.4.4. The permutation $\theta = (1\ 2)(3\ 4)$ verify $\theta(\wp_i) = 5-i$, so the resulting code $\theta(C) \in LPL^{\infty}(4,1,81)_o$. We remark that this permutation is not unique, for example if we take $\tau = (1\ 3\ 4\ 2)$ we have $\tau(C) \in LPL^{\infty}(4,1,81)_o$ and $\tau(C) \neq \theta(C)$.*

4.4.2 Perfect matrices

In this section we characterize matrices associated with perfect codes in the Chebyshev metric.

Definition 4.4.9. *Let $q = (2e+1)t$. A matrix $M \in \nabla_n(2e+1)$ is a (e,q)-perfect matrix if there exists matrices $A \in \nabla_n(t)$ and $B \in \nabla_n(1)$ such that $AM = qB$.*

Remark 4.4.10. *For $n = 2$ a matrix $M = \begin{pmatrix} 2e+1 & a \\ 0 & 2e+1 \end{pmatrix}$ is (e,q)-perfect if only if there exists $x, y \in \mathbb{Z}$ satisfying $\begin{pmatrix} t & x \\ 0 & t \end{pmatrix}\begin{pmatrix} 2e+1 & a \\ 0 & 2e+1 \end{pmatrix} = \begin{pmatrix} q & qz \\ 0 & q \end{pmatrix}$ and this is equivalent to $ta + (2e+1)x = qz$ or $qz - (2e+1)x = ta$. This last diophantine equation has solution if and only if $\gcd(q, 2e+1) = 2e+1 \mid ta$ which is equivalent to $a = kh_1$ for some $k \in \mathbb{Z}$ (where $h_1 = \frac{2e+1}{\gcd(2e+1,t)}$). Is summary, a 2×2 matrix is a (e,q)-perfect matrix if and only if is the generating matrix of a type 2 perfect code in $LPL^{\infty}(2,e,q)$.*

Proposition 4.4.11. *If $q = (2e+1)t$ and M is a $n \times n$ integer matrix with rows $M_1, M_2, \ldots, M_n$, then M is a (e,q)-perfect matrix if and only if the following condition are satisfied:*

1. *M is upper triangular,*

2. $M_{ii} = 2e + 1$,

3. $t\overline{M_i} \in span(\overline{M_{i+1}}, \ldots, \overline{M_n})$ *for* $1 \leq i < n$,

where for $x \in \mathbb{Z}^n$ *we denote by* $\overline{x} = x + q\mathbb{Z}^n \in \mathbb{Z}_q^n$ *the residual class of* x *modulo* q.

Proof. Conditions (1) and (2) are equivalent to $M \in \nabla_n(2e + 1)$ and condition (3) is equivalent to the existence of integers $\alpha_{ij} \in \mathbb{Z}$ for $1 \leq i < j \leq n$ and vectors $B_i \in \mathbb{Z}^n$ for $1 \leq i \leq n$ verifying $tM_i = \sum_{j=i+1}^{n} \alpha_{ij} M_j + qN_i$ for $1 \leq i < j \leq n$ and these equations can be expressed in matricial form $AM = qB$ where the matrix A is upper triangular with $A_{ij} = \begin{cases} t & \text{for } i = j \\ -\alpha_{ij} & \text{for } i < j \end{cases}$ and B has rows $B_1, B_2, \ldots, B_n$. □

Lemma 4.4.12. *Let* $q = (2e+1)t$, $C \in LPL^{\infty}(n, e, q)$ *and* H *be a* k*-dimensional cartesian subgroup of* $\mathbb{Z}_q^n$. *If* $S \subseteq C \cap H$ *and* $\#S = t^k$, *then* $S = C \cap H$ *and the code* S *is a perfect code over* H *with packing radius* e.

Proof. We have that $t^k = \#S \leq \#(C \cap H) \leq \frac{q^k}{(2e+1)^k} = t^k$ (the last inequality is consequence of the sphere packing condition) so $S = C \cap H$. Let e' be the packing radius of S. Since C has packing radius e we have $e' \geq e$, by the sphere packing condition $(2e' + 1)^k \leq \frac{q^k}{\#S} = (2e + 1)^k$ hence $e' = e$ and $(2e + 1)^k \cdot \#S = q^k$, therefore $S = C \cap H$ is a perfect code over H with packing radius e. □

Proposition 4.4.13. *Every ordered perfect code* $C \in LPL^{\infty}(n, e, q)$ *has a generator matrix which is a* (e, q)*-perfect matrix.*

Proof. Let $C \in LPL^{\infty}(n, e, q)$. By the Hermite normal form theorem we have a generator matrix M for C which is upper triangular. Let $M_1, M_2, \ldots, M_n$ be the rows of M and we denote by $m_i = M_{ii}$ the elements in the principal diagonal. Multiplying by -1 if it were necessary we can suppose that each $m_i > 0$ ($m_i \neq 0$ because M is non-singular). We will prove the following assertion by induction:

$$\begin{cases} t\overline{M_{n-i}} \in \text{span}\left(\overline{M_{n-(i-1)}}, \overline{M_{n-(i-2)}}, \ldots, \overline{M_n}\right) \\ m_{n-(i-1)} = m_{n-(i-2)} = \ldots = m_n = 2e + 1 \end{cases} \tag{4.4.1}$$

for $1 \leq i < n$, where as usual $\overline{X} = X + q\mathbb{Z}^n \in \mathbb{Z}_q^n$ is the residual class modulo q of $X \in \mathbb{Z}^n$. For $i = 1$ we express $m_n = (2e+1)a + r$ with a and b non-negative integer $0 \leq r < 2e+1$. Since C is of type n (since C is ordered) we have that $v = (2e + 1)e_n \in \Lambda_C$ and the same for $re_n = M_n - av \in \Lambda_C$. The packing radius of Λ_C (which is equal to the packing radius of C) is e and consequently its minimum distance is $2e + 1$, but $||re_n||_{\infty} = r$ which imply $r = 0$ and $M_n = av$. Substituting M_n by v we have another generator matrix M' for C, since $\det(M) = \det(M') = \det(\Lambda_C)$ and $\det(M) = a \det(M')$ we have $a = 1$ and $m_n = 2e + 1$. Using that C is ordered, the code $C\langle n \rangle$ is of type $n - 1$ and using that

$m_{n-1}e_{n-1} \in C\langle n\rangle$ and a similar argument used in the proof of $m_n = 2e+1$ we can prove that $m_{n-1} = 2e+1$, then $t\overline{M_{n-1}} \in H_{\{1,\ldots,n-1\}} \cap C$. On the other hand, since $M_n = (2e+1)e_n$ we have $\text{span}(\overline{M_n}) \subseteq C \cap H_{\{1,\ldots,n-1\}}$ and $\#\text{span}(\overline{M_n}) = t$, thus by Lemma 4.4.12 we have $H_{\{1,\ldots,n-1\}} \cap C = \text{span}(\overline{M_n})$ so the assertion (4.4.1) is true for $i = 1$. Now consider j with $2 \leq j < n$ and let us suppose that the assertion (4.4.1) is true for i with $1 \leq i < j$. By inductive hypotesis $t\overline{M_{n-i}} \in \text{span}\left(\overline{M_{n-(i-1)}}, \overline{M_{n-(i-2)}}, \ldots, \overline{M_n}\right)$ for $1 \leq i < j$ so linear construction (Prop. 4.3.7) guarantees that $C' = \text{span}\left(\overline{M_{n-(j-1)}}, \overline{M_{n-(j-2)}}, \ldots, \overline{M_n}\right)$ is a perfect code over $H_{\{1,2,\ldots,n-j\}}$ with packing radius e. In particular $\#C' = t^j$ and by Lemma 4.4.12 we have that $C' = C \cap H_{1,2,\ldots,n-j}$. Since C is ordered, $C\langle n-(j-1),\ldots,n\rangle$ is of type $n-j$ and using that $m_{n-j}e_{n-j} \in C\langle n-(j-1),\ldots,n\rangle$ and a similar argument used in the proof of $m_n = 2e+1$ we can prove that $m_{n-j} = 2e+1$, then $t\overline{M_{n-j}} \in H_{\{1,2,\ldots,n-j\}} \cap C = \text{span}\left(\overline{M_{n-(j-1)}}, \overline{M_{n-(j-2)}}, \ldots, \overline{M_n}\right)$, so assertion (4.4.1) is true for $i = j$. Finally, assertion (4.4.1) for $1 \leq i < n$ and Proposition 4.4.11 imply that M is an (e,q)-perfect matrix. □

Remark 4.4.14. *In order to obtain a (e,q)-perfect generator matrix for an ordered perfect code $C \in LPL^{\infty}(n,e,q)$ from a given generator matrix we can apply the same algorithm of the Hermite normal form and multiply some rows by -1 if it were necessary.*

Definition 4.4.15. *We say that a matrix $M \in \nabla_n(2e+1)$ is reduced if $|M_{ij}| \leq e$ for $1 \leq i < j \leq n$.*

Notation 4.4.16. *We denote by $\mathcal{P}_n(e,q) = \{M \in \nabla_n(2e+1) : M \text{ is } (e,q) - \text{perfect}\}$. The subset of reduced matrices in $\nabla_n(2e+1)$ and $\mathcal{P}_n(e,q)$ is denoted by $\nabla_n(2e+1)_{red}$ and $\mathcal{P}_n(e,q)_{red}$ respectively.*

Proposition 4.4.17. *Let $M, M' \in \mathcal{P}_n(e,q)$. If $M_{ij} \equiv M'_{ij} \pmod{2e+1}$ then span(M) = span(M').*

Proof. A reduced (e,q)-perfect generator matrix for a code $C \in LPL^{\infty}(n,e,q)$ is just a modified version of the Hermite normal form, so $\text{span}(M) = \text{span}(M')$ is a consequence of the uniqueness of the Hermite normal form. □

Corollary 4.4.18. *There is a surjection $\mathcal{P}_n(e,q)_{red} \twoheadrightarrow LPL^{\infty}(n,e,q)_o$ given by $M \mapsto$ span$(M)/q\mathbb{Z}^n$.*

Proof. By Proposition 4.4.13 and Remark 4.4.14 we can obtain a (e,q)-perfect generator matrix M from the Hermite normal form of any generator matrix with the condition $0 \leq M_{ij} < 2e+1$ if $i < j$. For $i = 2,3,\ldots,n$ and for $1 \leq j < i$, if the element ji is greater than e we can substract the i-th row to the j-th row obtaining a new equivalent matrix whose element ji has absolute value at most e. Repeating this process we obtain a reduced (e,q)-perfect generator matrix for a given ordered code $C \in LPL^{\infty}(n,e,q)_o$. □

Corollary 4.4.19. *Let $q = (2e+1)t$. We have the following inequality:*

$$\log_{2e+1}\left(\#LPL^{\infty}(n,e,q)\right) \leq \binom{n}{2} \tag{4.4.2}$$

Proof. Using Lemma 4.4.18 we obtain:

$$\#LPL^{\infty}(n,e,q) \leq \#\mathcal{P}_n(e,q)_{\mathrm{red}} \leq \#\nabla_n(2e+1)_{\mathrm{red}} = (2e+1)^{\binom{n}{2}}.$$

□

Definition 4.4.20. *A perfect code C is maximal if its parameter (n,e,q) verify equality in Corollary 4.4.19. In this case we also say that the parameter (e,q) ia n-maximals.*

Remark 4.4.21. *If (e,q) is n-maximal then $\mathcal{P}_n(e,q)_{red} = \nabla_n(2e+1)_{red}$.*

4.4.3 n-maximal codes

In this part we show that there are infinitely many maximal codes in each dimension establishing conditions which guarantee maximality. We extend some results obtained for two-dimensional code to maximal codes including a parametrization theorem for such codes and for their isometry and isomorphism classes.

Lemma 4.4.22. *If (e,q) is n-maximal, then (e,q) is i-maximal for all $i, 1 \leq i \leq n$.*

Proof. Let (e,q) be an n-maximal pair and $M_0 \in \nabla_i(2e+1)$ with $1 \leq i < n$. We consider the matrix $M = \begin{pmatrix} (2e+1)I_{n-i} & 0 \\ 0 & M_0 \end{pmatrix} \in \nabla_n(2e+1)$, since (e,q) is n-maximal there exists $A \in \nabla_n(t), B \in \nabla_n(1)$ such that $AM = qB$. If we denote by A_0 and B_0 the submatrices consisting of the last i rows and the last i columns of A and B respectively. Clearly, $A_0 \in \nabla_i(t)$ and $B_0 \in \nabla_i(1)$ and $A_0M_0 = qB_0$, therefore M_0 is (e,q)-perfect, so the pair (e,q) is i-maximal. □

Lemma 4.4.23. *Let $q = (2e+1)t$ and $\overline{X} = X + q\mathbb{Z}^n \in \mathbb{Z}_q^n$ be the residual class of $X \in \mathbb{Z}^n$ modulo q. The following assertions are equivalent:*

(i) (e,q) is n-maximal.

(ii) For all $M \in \nabla_n(2e+1)$, there exists $A \in \nabla_n(t), B \in \nabla_n(1)$ such that $AM = qB$.

(iii) $t\mathbb{Z}_q^i \subseteq span(\overline{M})$ for all $M \in \nabla_i(2e+1)$ and for all i, $1 \leq i < n$.

Proof. We have (ii) $\Leftrightarrow \nabla_n(2e+1) = \mathcal{P}_n(e,q) \Leftrightarrow (i)$. We note that if (iii) holds then condition (3) in Proposition 4.4.11 is always satisfied, thus (iii) $\Rightarrow$ (ii). In order to prove (ii) $\Rightarrow$ (iii), by Lemma 4.4.22 it suffices to prove (ii) $\Rightarrow t\mathbb{Z}_q^{n-1} \subseteq \mathrm{span}(\overline{M})$ for all $M \in \nabla_{n-1}(2e+1)$. Let $M' \in \nabla_{n-1}(2e+1)$ and $w \in \mathbb{Z}^{n-1}$, we want to prove that

$t\overline{w} \in \text{span}(\overline{M})$. We consider the matrix $M = \begin{pmatrix} 2e+1 & w \\ 0^t & M' \end{pmatrix} \in \nabla_n(2e+1)$. By (ii) there exist matrices $A \in \nabla_n(t), B \in \nabla_n(1)$ such that $AM = B$, expressing $A = \begin{pmatrix} t & v \\ 0^t & A' \end{pmatrix}$ and $B = \begin{pmatrix} 1 & u \\ 0^t & B' \end{pmatrix}$ with $A' \in \nabla_{n-1}(t)$ and $B' \in \nabla_{n-1}(1)$, from the equality $AM = qB$ we obtain $tw + vM' = qu$, thus $t\overline{w} = -v\overline{M'} \in \text{span}(\overline{M})$. □

Lemma 4.4.24. *If* $(2e+1)^n \mid q$, *then* $(2e+1)^{n-1}\mathbb{Z}_q^{n-1} \subseteq span(\overline{M})$ *for all* $M \in \nabla_{n-1}(2e+1)$.

Proof. For $n = 1$ the assertion is true because $(0) \subseteq \text{span}(\overline{M})$ and for $n = 2$ the assertion is true since $(2e+1)\mathbb{Z}_q \subseteq \text{span}(2e+1) = (2e+1)\mathbb{Z}_q$. Let us suppose that the assertion is true for $n-1$ where $n \geq 3$ and $(2e+1)^n \mid q$. Let $M \in \nabla_{n-1}(2e+1)$ and we express $M = \begin{pmatrix} 2e+1 & w \\ 0^t & M' \end{pmatrix}$ with $M' \in \nabla_{n-2}(2e+1)$ and $w \in \mathbb{Z}^{n-2}$. Since $(2e+1)^{n-2} \mid q$ we have $(2e+1)^{n-2}\mathbb{Z}_q^{n-2} \subseteq \text{span}(\overline{M})$, then $(2e+1)^{n-2}H_{\{1\}} \subseteq \text{span}\overline{(0^t, M')}$ and we obtain the following chain of inequalities:

$$(2e+1)^{n-1}H_{\{1\}} \subseteq (2e+1)^{n-2}H_{\{1\}} \subseteq \text{span}\overline{(0^t, M')} \subseteq \text{span}(\overline{M}),$$

in particular $(2e+1)^{n-1}H_{\{1\}} \subseteq \text{span}(\overline{M})$. To conclude the proof we need to show that $(2e+1)^{n-1}\overline{e_1} \in \text{span}(\overline{M})$. We have that $(2e+1)^{n-1}\overline{e_1} - (2e+1)^{n-2}(2e+1, w) = (0, -(2e+1)^{n-2}w) \in (2e+1)^{n-2}H_{\{1\}} \subseteq \text{span}(\overline{M})$, so $(2e+1)^{n-1}\overline{e_1} \in \text{span}(\overline{M})$. In conclusion, we have that

$$(2e+1)^{n-1}\mathbb{Z}_q^{n-1} = (2e+1)^{n-1}\mathbb{Z}\overline{e_1} \oplus (2e+1)^{n-1}H_{\{1\}} \subseteq \text{span}(\overline{M}).$$

□

Corollary 4.4.25. *If* $(2e+1)^n \mid q$ *then* $(2e+1)^i\mathbb{Z}_q^i \subseteq span(\overline{M})$ *for all* $M \in \nabla_i(2e+1)$ *and for all* i, $1 \leq i < n$.

Theorem 4.4.26. *Let* $q = (2e+1)t$. *The pair* (e, q) *is* n*-maximal if and only if* $(2e+1)^{n-1} \mid t$.

Proof. First, we suppose that $(2e+1)^{n-1} \mid t$ (or equivalently $(2e+1)^n \mid q$). By Corollary 4.4.25, for all $M \in \nabla(2e+1)$ and $1 \leq i < n$ we have:

$$t\mathbb{Z}_q^i \subseteq (2e+1)^{n-1}\mathbb{Z}_q^i \subseteq (2e+1)^i\mathbb{Z}_q^i \subseteq \text{span}(\overline{M}),$$

and by Lemma 4.4.23 the pair (e, q) is n-maximal. Now we suppose that (e, q) is n-maximal and consider the bidiagonal matrix $M \in \nabla_n(2e+1)$ which has 1 in the secondary diagonal (i.e. in the diagonal above the principal diagonal). Since (e, q) is n-maximal,

there exists $A \in \nabla_n(t), B \in \nabla_n(1)$ such that $AM = qB$. If we denote the first row of A by $A_1 = (a_{11}, a_{12}, \ldots, a_{1n})$ and the first row of B by B_1, we have that $qB_1 = (q, a_{11} + (2e+1)a_{12}, a_{12} + (2e+1)a_{13}, \ldots, a_{1,n-1} + (2e+1)a_{1n})$ using $a_{11} = t$ we deduce that:

$$t + (-1)^n(2e+1)^{n-1}a_{1n} = \sum_{i=1}^{n-1}(-2e-1)^{i-1}(a_{1i} + (2e+1)a_{1,i+1}) \equiv 0 \pmod{q}.$$

If $h \in \mathbb{Z}$ is such that $t+(-1)^n(2e+1)^{n-1}a_{1n} = qh$ we have $t(1-(2e+1)h) = (-1)^{n+1}(2e+1)^{n-1}a_{1n}$, since $\gcd(1-(2e+1)h, 2e+1) = 1$ we have $(2e+1)^{n-1} \mid t$. □

Since $\nabla_n(2e+1) = \mathcal{P}_n(e,q)$ holds for maximal codes, in this case we obtain the following parametrization for ordered codes which generalize the first part of Theorem 4.2.46.

Theorem 4.4.27. *Let (e,q) be an n-maximal pair. There is a parametrization*

$$\psi : \nabla_n(2e+1)_{red} \to LPL^{\infty}(n,e,q)_o$$

given by $\psi(M) = span(M)/q\mathbb{Z}^n$.

Next we study isomorphism classes of perfect codes.

Notation 4.4.28. *An unimodular integer matrix is a square matrix with determinant 1 or -1. We denote by $\Gamma_n = \{M \in M_n(\mathbb{Z}) : M \text{ is unimodular}\}$. If $A, B \in M_n(\mathbb{Z})$ we say that A and B are Γ_n-equivalent if there exists $U, V \in \Gamma_n$ such that $A = UBV$, we denote $A \underset{\Gamma}{\sim} B$ for this equivalence relation.*

We remark that two matrices A and B are Γ-equivalent if we can obtain one from the other through a finite number of elementary operations on the rows and on the columns. For $X \subseteq M_n(\mathbb{Z})$ we denote by X/Γ_n the quotient space for this equivalence relation.

Theorem 4.4.29. *Let (e,q) be an n-maximal pair. There is a parametrization*

$$\psi_{\mathcal{A}} : \frac{\nabla_n(2e+1)_{red}}{\Gamma_n} \to \frac{LPL^{\infty}(n,e,q)_o}{\mathcal{A}}$$

given by $\psi_{\mathcal{A}}(M) = [\psi(M)]_{\mathcal{A}}$ (where ψ is as in Theorem 4.4.27)

Proof. If M is the generator matrix for a linear code $C \subseteq \mathbb{Z}_q^n$ then the matrix qM^{-1} has integer coefficient and their Smith normal form determines the isomorphism class of C (as abelian group). On the other hand for $M_1, M_2 \in \nabla_n(2e+1)_{\text{red}}$ we have the following equivalences:

$$\text{span}(\overline{M_1}) \underset{\mathcal{A}}{\sim} \text{span}(\overline{M_2}) \Leftrightarrow qM_1^{-1} \underset{\Gamma}{\sim} qM_2^{-1} \Leftrightarrow \exists U, V \in \Gamma_n : UqM_1^{-1}V = qM_2^{-1}$$

$$\Leftrightarrow \exists U, V \in \Gamma_n : V^{-1} M_1 U^{-1} = M_2 \Leftrightarrow M_1 \underset{\Gamma}{\sim} M_2,$$

so $\psi_{\mathcal{A}}$ is well defined and is injective. Since ψ is surjective then $\psi_{\mathcal{A}}$ is surjective, therefore $\psi_{\mathcal{A}}$ is a bijection. □

The next goal is to characterize what are the possible group isomorphism classes that can be represented by maximal perfect codes.

Definition 4.4.30. *Let $G = \mathbb{Z}_{d_1} \times \ldots \times \mathbb{Z}_{d_m}$ with $d_1 | d_2 | \ldots | d_m$. We say that G is an (n, e, q)-admissible structure if there exist $C \in LPL^{\infty}(n, e, q)$ such that $C \simeq G$ as abelian groups.*

Lemma 4.4.31. *For a, x and y non-zero integers we have* $\begin{pmatrix} a & 0 \\ 0 & axy \end{pmatrix} \underset{\Gamma}{\sim} \begin{pmatrix} ay & a \\ 0 & ax \end{pmatrix}$.

Proof. We have the following chain of Γ-equivalence:

$$\begin{pmatrix} a & 0 \\ 0 & axy \end{pmatrix} \underset{\Gamma}{\sim} \begin{pmatrix} a & a \\ 0 & axy \end{pmatrix} \underset{\Gamma}{\sim} \begin{pmatrix} a & a \\ ax & axy + ax \end{pmatrix} \underset{\Gamma}{\sim} \begin{pmatrix} a & a - ay \\ ax & ax \end{pmatrix}$$

$$\underset{\Gamma}{\sim} \begin{pmatrix} a & a - ay \\ 0 & ax \end{pmatrix} \underset{\Gamma}{\sim} \begin{pmatrix} ay & a \\ 0 & ax \end{pmatrix}$$

□

Lemma 4.4.32. *If M is a $n \times n$ integer matrix with determinant $(2e+1)^n$, then $\Gamma_n M \Gamma_n \cap \nabla_n(2e+1)_{red} \neq \emptyset$. Moreover, M is Γ-equivalent to a bidiagonal matrix $A \in \nabla_n(2e+1)_{red}$.*

Proof. For $n = 1$, $\det(M) = 2e + 1$ implies $M = (2e + 1) \in \nabla_1(2e + 1)_{\text{red}}$. Let us suppose that the result is true for $n - 1$ and we consider a $n \times n$ integer matrix M with $\det(M) = (2e+1)^n$. By Smith normal form $M \underset{\Gamma}{\sim} D$ where $D = \text{diag}(d_1, d_2, \ldots, d_n)$ is a diagonal matrix with $d_1 \mid d_2 \mid \ldots \mid d_n$ and $d_1 d_2 \ldots d_n = (2e+1)^n$, in particular $d_n = (2e+1)x$ and $2e+1 = d_1 y$ for some integers x and y. Permuting the second and nth rows of D and then the second and nth column we have $D \underset{\Gamma}{\sim} \widetilde{D} := \text{diag}(d_1, d_n, d_3, \ldots, d_{n-1}, d_2)$. Applying Lemma 4.4.31 with $d_n = d_1 xy$ we obtain $\widetilde{D} \underset{\Gamma}{\sim} \begin{pmatrix} 2e+1 & v \\ 0^t & D_0 \end{pmatrix}$ where $v = (d_1, 0, \ldots, 0) \in \mathbb{Z}^{n-1}$ and $D_0 = \text{diag}(d_1 x, d_3, \ldots, d_{n-1}, d_2)$. By inductive hypothesis there exists unimodular matrices $U_0, V_0 \in \Gamma_{n-1}$ such that $U_0 D_0 V_0 \in \nabla_{n-1}(2e + 1)$ with $U_0 D_0 V_0$ bidiagonal, thus

$$\begin{pmatrix} 1 & 0 \\ 0^t & U_0 \end{pmatrix} \begin{pmatrix} 2e+1 & v \\ 0^t & U_0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0^t & V_0 \end{pmatrix} = \begin{pmatrix} 2e+1 & vV_0 \\ 0^t & U_0 D_0 V_0 \end{pmatrix}$$

is a bidigonal matrix in $\nabla_n(2e + 1)$. Since this matrix have $2e + 1$ in the main diagonal, we can obtain a reduced matrix from this, by applying some elementary operations on rows, thus the result holds for n. □

Corollary 4.4.33. *If we denote by $M_n(\mathbb{Z}, det = D)$ the set of matrices $M \in M_n(\mathbb{Z})$ with $\det(M) = D$, each equivalence class in $\nabla_n(2e+1)_{red}/\Gamma_n$ is contained in exactly one equivalence class in $M_n(\mathbb{Z}, det = (2e+1)^n)/\Gamma_n$. Moreover, both quotient sets have the same number of elements.*

Theorem 4.4.34. *Let (e, q) be an n-maximal pair where $q = (2e+1)t$ and $G = \mathbb{Z}_{d_1} \times \ldots \times \mathbb{Z}_{d_n}$ with $d_1|d_2|\ldots|d_n$. Then G is a (n, e, q)-admissible structure if and only if $d_1 d_2 \ldots d_n = t^n$ and $d_n|q$.*

Proof. The direct implication follows from the fact that if $C \in LPL^\infty(n, e, q)$ then $\#C = t^n$ and $qC = \{0\}$ (since $C \subseteq \mathbb{Z}_q^n$). We denote by $\mathcal{D} = \{(d_1, \ldots, d_n) \in \mathbb{N} : d_1|\ldots|d_n, d_1 \ldots d_n = t^n, d_n|q\}$. To prove the converse implication it suffices to prove that $\#\mathcal{D} = \#LPL^\infty(n, e, q)_{\text{red}}/\mathcal{A}$ (where $X/\mathcal{A}$ denotes the set of isomorphism classes of codes in X). By Theorem 4.4.29, Lemma 4.4.32 and the Smith normal form theorem we have that $\#LPL^\infty(n, e, q)_{\text{red}}/\mathcal{A} = \#\mathcal{F}$ where $\mathcal{F} = \{(f_1, \ldots, f_n) \in \mathbb{N} : f_1|\ldots|f_n, f_1 \ldots f_n = (2e+1)^n\}$, so it suffices to prove that $\#\mathcal{D} = \#\mathcal{F}$. We consider $X = \{(x_1, \ldots, x_n) \in \mathbb{N}^n : x_1 \mid \ldots \mid x_n \mid q\}$ and the involution $\psi : X \to X$ defined by $\psi(x_1, \ldots, x_n) = (y_1, \ldots, y_n)$ where $x_i y_j = q$ if $i + j = n + 1$. For $x = (x_1, \ldots, x_n) \in X$ we denote by $p(x) = x_1 \ldots x_n$. Since $(2e+1)^{n-1} \mid t$, then $\mathcal{F} \subseteq X$ and the property $p(\psi(a)) \cdot p(a) = q^n$ imply $\psi(\mathcal{F}) = \mathcal{D}$ and $\#\mathcal{F} = \#\mathcal{D}$. □

The involution argument in the above proof give us the following corollary.

Corollary 4.4.35. *Let $q = (2e+1)t$ with $(2e+1)^{n-1} \mid t$ and $C \in LPL^\infty(n, e, q)$ with generator matrix M. If the Smith normal form of M is given by $D = diag(d_1, \ldots, d_n)$, then $C \simeq \mathbb{Z}_{q/d_n} \times \mathbb{Z}_{q/d_{n-1}} \times \ldots \times \mathbb{Z}_{q/d_1}$.*

The following corollary give us the number of isomorphism classes of perfect codes in $LPL^\infty(n, e, q)$.

Corollary 4.4.36. *Let $q = (2e+1)t$ with $(2e+1)^{n-1} \mid t$ and $f(x)$ be the generating function $f(x) = \frac{1}{(1-x)(1-x^2)\ldots(1-x^n)}$. If $e_p(m)$ is the exponent of the prime p in the factorial decomposition of m, then the number of isomorphism classes of perfect codes in $LPL^\infty(n, e, q)$ is given by:*

$$\prod_{p|2e+1} [x^{ne_p(2e+1)}] f(x).$$

In particular for $n = 2$ this number is given by

$$\prod_p [x^{2e_p(2e+1)}] \frac{1}{(1-x)(1-x^2)} = \prod_p (e_p(2e+1) + 1) = \sigma_0(2e+1),$$

the number of divisor of $2e+1$ (according with Corollary 4.2.49, since $\gcd(2e+1, t) =$

$2e+1$). *For* $n=3$ *this number is given by*

$$\prod_p [x^{3e_p(2e+1)}] \frac{1}{(1-x)(1-x^2)(1-x^3)} = \prod_p \lceil 3/4 \cdot (e_p(2e+1)+1)^2 \rfloor$$

where $\lceil x \rfloor$ *denotes the nearest integer to* x. *In particular when* $2e+1$ *is square-free this number is* $3^{\omega(2e+1)}$ *where* $\omega(n)$ *is the number of distinct prime divisors of* n.

Proof. Let $X(\alpha) = \{(x_1, \ldots, x_n) \in \mathbb{N}^n : x_1 \leq \ldots \leq x_n, x_1 + \ldots + x_n = n\alpha\}$ for $\alpha \in \mathbb{Z}^+$ and $e_p(a_1, \ldots, a_n) := (e_p(a_1), \ldots, e_p(a_n))$ (where $e_p(m)$ denote the exponent of p in m). If $\mathcal{F}$ is as in the proof of Theorem 4.4.34, then for each prime divisor $p \mid 2e+1$ and for each $a \in \mathcal{F}$ we have $e_p(a) \in X(e_p(2e+1))$. In this way we have a bijection between $\mathcal{F}$ and $\prod_p X(e_p(2e+1))$ where p runs over the prime divisors of $2e+1$, in particular the number of isomorphism classes of (n,e,q)-codes (with $(2e+1)^{n-1} \mid t$) is given by $\#\mathcal{F} = \prod_{p|2e+1} \#X(e_p(2e+1))$. With the standard change of variable $x_i = y_n + \ldots + y_{n+1-i}$ for $1 \leq i \leq n$ we have $\#X(\alpha) = \#\{(y_1, \ldots, y_n) \in \mathbb{N}^n : y_1 + 2y_2 + \ldots + ny_n = n\alpha\}$ which clearly is the coefficient of $x^{n\alpha}$ in the generating function $f(x) = \frac{1}{(1-x)(1-x^2)\ldots(1-x^n)}$. For $n=2$ and $n=3$ we have the well known formulas $f(x) = \sum_{n=0}^{\infty} \lfloor \frac{n+2}{2} \rfloor x^n$ and $f(x) = \sum_{n=0}^{\infty} \left\lceil \frac{(n+3)^2}{12} \right\rfloor x^n$ respectively (see for example [Har20, p. 10]). □

4.5 The ideal of admissible structures for Chebyshev perfect codes

On the one hand the group $G = \mathbb{Z}_t \times \mathbb{Z}_t \times \ldots \times \mathbb{Z}_t = \mathbb{Z}_t^n$ (cartesian group) is always represented by a perfect code in $LPL^{\infty}(n,e,q)$ with $q = (2e+1)t$. On the other hand cyclic groups seem more difficult to be represented by perfect codes. Informally speaking is like the more cyclic is a group the more difficult is to represent it as a perfect code. We formalize this idea through the poset $\mathcal{S}_n(t^n)$ (Proposition 3.2.5). We will show that in the two-dimensional case and in the maximal case, the isomorphism classes that can be represented by perfect code is an ideal in this poset and we conjecture that this is valid in general.

We consider $\mathcal{S}_n(t^n)$ with the poset structure given in Section 3.2. Proposition 3.2.6 and Remark 3.2.7 motivate the following definition.

Definition 4.5.1. *If* G_1 *and* G_2 *are two abelian group of order* t^n *we say that* G_1 *is more cyclic that* G_2 *(or* G_2 *is more cartesian that* G_1*) with respect to* t, *if* $G_1 \simeq \mathbb{Z}_{q_1}$ *and* $G_2 \simeq \mathbb{Z}_{q_2}$ *with* $q_1, q_2 \in \mathcal{S}_n(t^n)$ *and* $q_1 \geq q_2$.

Notation 4.5.2. *We denote by* $\mathcal{A}(n,e,q)$ *the set of* (n,e,q)*-admissible structures (see Definition 4.4.30).*

Example 4.5.3. *The set* $\mathcal{A}(3,1,27) = \{\mathbb{Z}_{27} \times \mathbb{Z}_{27}, \mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_{27}, \mathbb{Z}_9 \times \mathbb{Z}_9 \times \mathbb{Z}_9\}$. *This set can be seen as a subset of the vertices of the graph* $\mathcal{G}_3(9)$ *as show in Figure 4.7.*

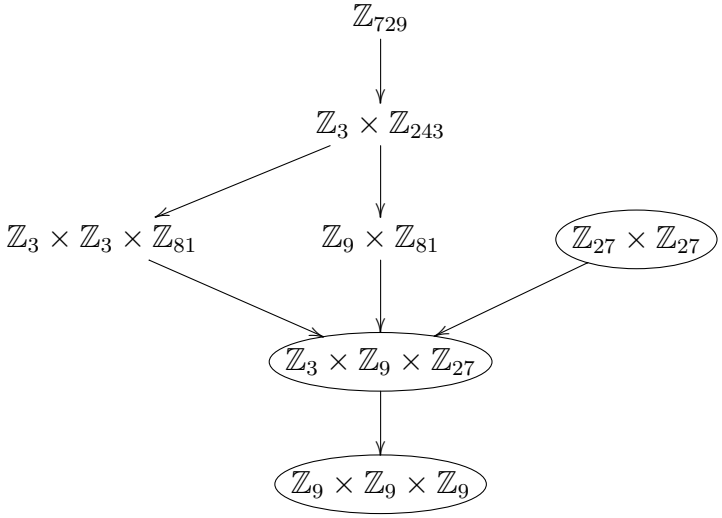


Figure 4.7: The graph $\mathcal{G}_3(9)$ and the set $\mathcal{A}(3,1,27)$ as a subset of vertices of this graph.

Example 4.5.4. *The graph $\mathcal{G}_3(15^2)$ has 49 vertices. Nine of these vertices are in $\mathcal{A}(3,7,15^3)$. Figure 4.8 show the subgraph of $\mathcal{G}_3(15^2)$ induced by the vertices in $\mathcal{A}(3,7,15^3)$.*

Theorem 4.5.5. *Let $q=(2e+1)t$. If $n=2$ or (e,q) is n-maximal then the set $\mathcal{A}(n,q,e)$ is an ideal in the poset $(\mathcal{S}_n(t^n),\geq)$*

Proof. Without loss of generality we can restrict to ordered codes. In dimension $n=2$, by Theorem 4.2.38 and Theorem 4.2.46 all perfect codes in $LPL^{\infty}(n,e,q)_o$ are of the form $C_k = \operatorname{span}\begin{pmatrix} \overline{2e+1} & k\overline{h_1} \\ \overline{0} & \overline{2e+1} \end{pmatrix} \simeq \mathbb{Z}_{t/h_2} \times \mathbb{Z}_{th_2}$ where $h_1 = \frac{2e+1}{d_1}, h_2 = \frac{d_1}{\gcd(d_1,k)}$ and $d_1 = \gcd(2e+1,t)$. So, $\mathcal{A}(2,e,q) = \{\mathbb{Z}_{t/d} \times \mathbb{Z}_{dt} : d \mid d_1\}$ which is the ball of radius $\Omega(d_1)$ (the number of prime divisors of d_1 counting with multiplicity) and center in $\mathbb{Z}_t \times \mathbb{Z}_t$ with respect to the graph metric in $\mathcal{G}_2(t)$, in particular it is a poset ideal. In the maximal case the set $\mathcal{A}(n,e,q)$ consist of $f=(f_1,\ldots,f_n) \in \mathcal{S}_n(t^n)$ such that $f_n \mid q$. If $a=(a_1,\ldots,a_n) \in \mathcal{A}(n,e,q)$ and $\overrightarrow{ab}$ is an arrow in $\mathcal{G}_n(t)$ with $b \in \mathcal{S}_n(t^n)$, then there exists a prime $p \mid t$ and $i,j \in \{2,\ldots,n\}$ such that $\nu_p(a_i) < \nu_p(t), \nu_p(a_j) > \nu_p(t)$ such that $b_i = pa_i, b_j = a_j/p$ and $b_k = a_k$ for all $k \neq i,j$, in particular $\max\{\nu_p(a_i) : 1 \leq i \leq n\} \geq \max\{\nu_p(b_i) : 1 \leq i \leq n\}$ and so $b_n \mid q$, then $b \in \mathcal{A}(n,e,q)$. □

Next we show some non-maximal examples in dimension 3.

Example 4.5.6. *We consider q-ary perfect codes in dimension 3 with $q=225$ and packing radius 7 (i.e. $e=7, t=15, q=15^2$). Using Proposition 4.4.11, we obtain that the integer matrix $M = \begin{pmatrix} 15 & a & b \\ 0 & 15 & c \\ 0 & 0 & 15 \end{pmatrix}$ is a $(7,225)$-perfect matrix if and only if $ac \equiv 0 \pmod{15}$. Applying elementary operation in rows if it were necessary we can assume that $|a| \leq 7, |b| \leq 7$ and $1 \leq b \leq 15$. For every one of these 675 matrices M we calculate the*

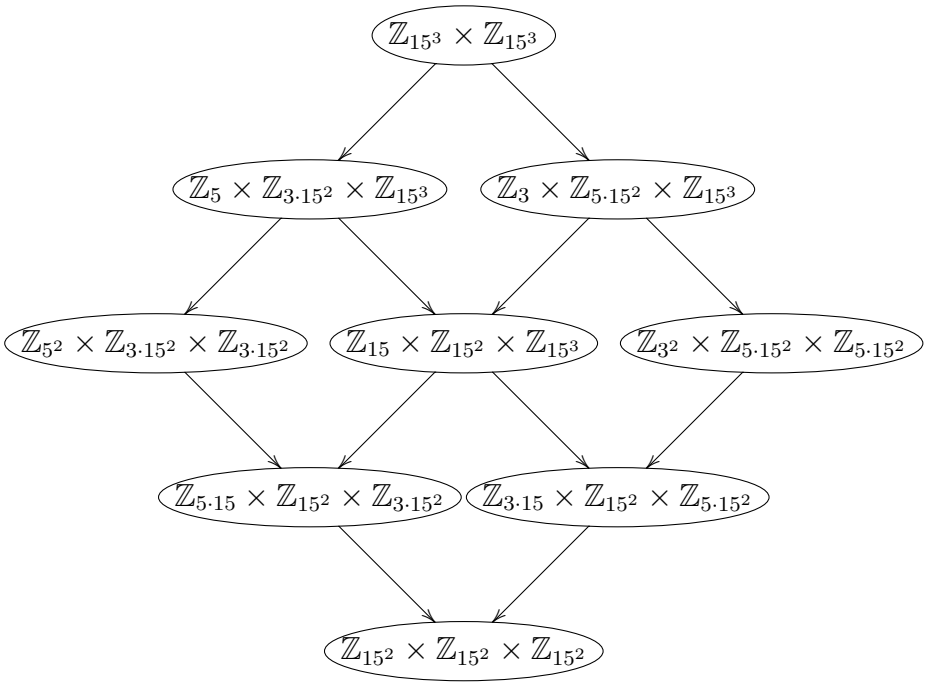


Figure 4.8: The subgraph of $\mathcal{G}_3(15^2)$ induced by $\mathcal{A}(3, 7, 15^2)$.

Smith normal form of the integer matrix qM^{-1} *to determine all possibles group structures represented in* $LPL^{\infty}(3, 7, 225)$ *obtaining* $\mathcal{A}(3, 7, 15^2) = \{\mathbb{Z}_{15} \times \mathbb{Z}_{15} \times \mathbb{Z}_{15}, \mathbb{Z}_3 \times \mathbb{Z}_{15} \times \mathbb{Z}_{5\cdot 15}, \mathbb{Z}_5 \times \mathbb{Z}_{15} \times \mathbb{Z}_{3\cdot 15}, \mathbb{Z}_{15} \times \mathbb{Z}_{15^2}\}$. *Representing by* $C_d \subseteq \mathbb{Z}_{225}^3$ *the perfect code whose generator matrix is* $\begin{pmatrix} 15 & 0 & d \\ 0 & 15 & 0 \\ 0 & 0 & 15 \end{pmatrix}$, *we have that* $\{C_d : d \mid 15\}$ *is a set of representatives. Moreover, we have:*

- $C_1 \simeq \mathbb{Z}_{15} \times \mathbb{Z}_{15^2}$,
- $C_3 \simeq \mathbb{Z}_3 \times \mathbb{Z}_{15} \times \mathbb{Z}_{5\cdot 15}$,
- $C_5 \simeq \mathbb{Z}_5 \times \mathbb{Z}_{15} \times \mathbb{Z}_{3\cdot 15}$,
- $C_{15} \simeq \mathbb{Z}_{15} \times \mathbb{Z}_{15} \times \mathbb{Z}_{15}$.

In this case we also have that $\mathcal{A}(3, 7, 15^2)$ *is a poset ideal in* $\mathcal{S}_3(15^3)$ *(see Figure 4.9).*

Example 4.5.7. *For* $e = 112, t = 15, q = (2e + 1)t = 15^3$, *using Proposition 4.4.11 we can prove that all* $(112, 15^3)$*-perfect matrix is of the form*

$$M = \begin{pmatrix} 225 & 15a + 225k_1 & ac + 15b + 225k_2 \\ 0 & 225 & 15c + 225k_3 \\ 0 & 0 & 225 \end{pmatrix}$$

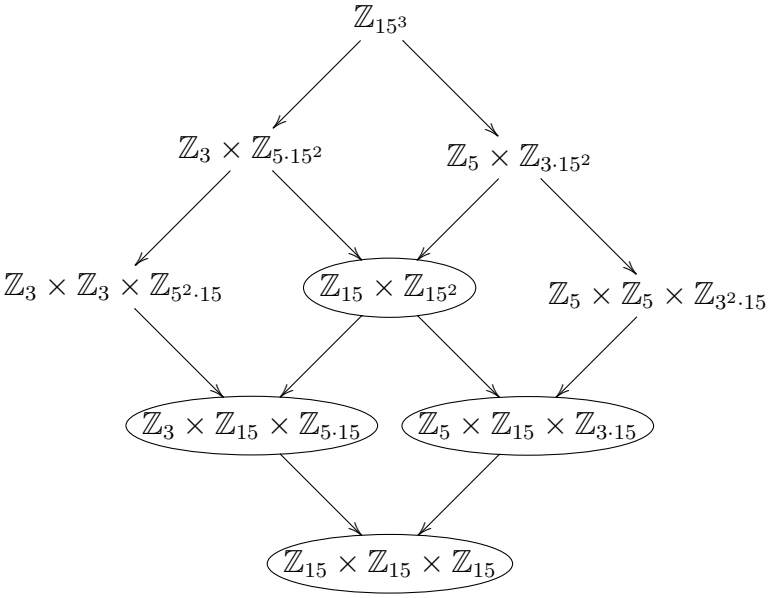


Figure 4.9: The set of admissible structures $\mathcal{A}(3, 7, 15^2)$ as subset of vertices in the graph $\mathcal{G}_3(15)$.

where a, b, c, k_1, k_2 *and* k_3 *are integers with* $0 \leq a, b, c \leq 14$. *Applying some elementary operations in rows we can restrict to matrices of the form*

$$M = \begin{pmatrix} 225 & 15a & ac + 15b \\ 0 & 225 & 15c \\ 0 & 0 & 225 \end{pmatrix}$$

with $0 \leq a, b, c \leq 14$. *After checking all the possibilities we have that each group structures in* $\mathcal{S}_3(15^3)$ *is represented by some code in* $LPL^{\infty}(3, 112, 3375)$, *in fact each group structure can be represented by a perfect code* $C(a, c)$ *with generator matrix* $\begin{pmatrix} 225 & 15a & ac \\ 0 & 225 & 15c \\ 0 & 0 & 225 \end{pmatrix}$ *as showed in following table:*

(a, c)	*Group structure of* $C(a, c)$
$(0, 0)$	$\mathbb{Z}_{15} \times \mathbb{Z}_{15} \times \mathbb{Z}_{15}$
$(0, 3)$	$\mathbb{Z}_3 \times \mathbb{Z}_{15} \times \mathbb{Z}_{5\cdot 15}$
$(0, 5)$	$\mathbb{Z}_5 \times \mathbb{Z}_{15} \times \mathbb{Z}_{3\cdot 15}$
$(3, 3)$	$\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{5^2\cdot 15}$
$(0, 1)$	$\mathbb{Z}_{15} \times \mathbb{Z}_{15^2}$
$(5, 5)$	$\mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_{3^2\cdot 15}$
$(1, 3)$	$\mathbb{Z}_3 \times \mathbb{Z}_{5\cdot 15^2}$
$(1, 5)$	$\mathbb{Z}_5 \times \mathbb{Z}_{3\cdot 15^2}$
$(1, 1)$	$\mathbb{Z}_{15^3}$

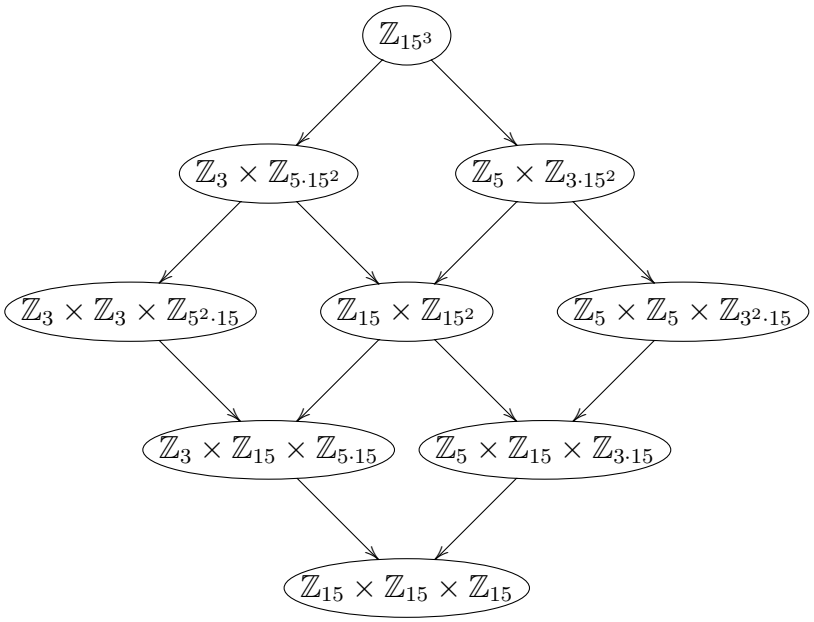


Figure 4.10: The set of admissible structures $\mathcal{A}(3, 112, 15^3)$ coincides with the set of vertices of the graph $\mathcal{G}_3(15)$.

Figure 4.10 show the set of admissible structures $\mathcal{A}(3, 112, 15^3)$ which in this case coincide with $\mathcal{S}_3(15^3)$, the whole set of vertices of $\mathcal{G}_3(15)$.

To finish we show that if the set of admissible structures $\mathcal{A}(n, e, q)$ contain a cyclic group, then $\mathcal{A}(n, e, q) = \mathcal{S}_n(t^n)$ (where $q = (2e + 1)t$). In particular, we have another case where $\mathcal{A}(n, e, q)$ is a poset ideal.

Definition 4.5.8. *We say that the pair (e, q) is n-cyclic when the set $LPL^\infty(n, e, q)$ contain a cyclic perfect code.*

Remark 4.5.9. *Let $q = (2e + 1)$. By Proposition 4.3.10 we have that (e, q) is n-cyclic if and only if $t^{n-1} \mid 2e + 1$ (or equivalently if $t^n \mid q$).*

Theorem 4.5.10. *If (e, q) is an n-cyclic pair where $q = (2e+1)t$, then every group structure associate with the elements of $\mathcal{S}_n(t^n)$ is represented by a perfect code in $LPL^\infty(n, e, q)$.*

Proof. Let $d = (d_1, \ldots, d_n)$ be a t^n-series of order n. By Lemma 4.4.32 there exists $A = (a_{ij})_{1\leq i,j\leq n} \in \nabla_n(t)$ with $A \underset{\Gamma}{\sim} \operatorname{diag}(d_1, \ldots, d_n)$. We define $M \in \nabla_n(2e + 1, \mathbb{Q})$ recursively as following:

$$\begin{cases} M_n = (2e + 1)e_n \\ M_i = (2e + 1)e_i - \sum_{k=i+1}^{n}(a_{ik}/t)M_k \quad \text{for } 1 \leq i < n, \end{cases} \tag{4.5.1}$$

where M_i denote the ith row of M. Using $t^{n-1} \mid 2e + 1$, it is not difficult to prove by induction that $M_i \in t^{i-1}\mathbb{Z}^n$ for $1 \leq i \leq n$, which implies that the matrix M has integer coefficient, hence $M \in \nabla_n(2e + 1)$. Equation (4.5.1) can be written in matricial form as

$AM = qI$, in particular $M \in \mathcal{P}_n(e,q)$ (that is, M is (e,q)-perfect) and $qM^{-1} \in M_n(\mathbb{Z})$. This last fact imply that M is the generator matrix of a code $C \in LPL^{\infty}(n,e,q)$ whose group structure is given by the Smith normal form of $qM^{-1} = A$, that is $C \simeq \mathbb{Z}_{d_1} \times \ldots \mathbb{Z}_{d_n}$. □

The property that the (n,e,q)-admissible structures are ideals was checked for other cases (in addition to the two-dimensional, the n-maximal and the n-cyclic case for $n > 2$) and we did not find a counterexample, so it is possible that a more general result than Theorem 4.5.5 holds.

Chapter 5

THE CYCLE STRUCTURE OF ITERATING RÉDEI FUNCTIONS

In this chapter we study the action of *Rédei functions over non-binary finite fields* via the action of the multiplication-by-n map over a cyclic group. These functional graphs present a strong type of symmetries. The cyclic decomposition and some properties related to the trees attached to cyclic nodes were studied in [Sha12]. We extend the description of these functional graphs giving two different characterizations for their associated trees. In Section 5.1 we focus our attention in the action of the multiplication-by-n map over the cyclic group $\mathbb{Z}_m$, describing its functional graph and relating its trees to the trees associated with ν-series. We also give in this section an alternative description of these trees. In Section 5.2 we apply the previous results to the case of Rédei functions. This section begins with a review of Rédei functions over finite fields and we briefly comment on their main properties and applications. Next, we give the structure of the functional graph associated with a Rédei function, providing period and preperiod studies. As corollaries of our main structural theorem we extend the characterization of Rédei permutations by describing its decomposition into disjoint cycles and use this to obtain a method for constructing Rédei functions with prescribed length cycles in certain geometric progression. Finally, we use our structural theorem to obtain results about tails and cycles in orbits of iterations of Rédei function.

5.1 Functional graph associated with the n-map.

If m and n are positive integers we can consider the factorization $m = \nu\omega$ with $\mathrm{rad}(\nu) \mid \mathrm{rad}(n)$ and $\gcd(n, \omega) = 1$. The n-map in $\mathbb{Z}_m$ is the application $x \mapsto nx$ which we also denote by n. The main goal of this section is to describe the functional graph of this map. Part of this was done in [Sha12] where it is proved that each connected component is of the form $Cyc(f, T)$; see also [Den13]. An explicit expression for the periodic part (that is, the length of the cycles and how many of them) and properties of the tree T are also given in [Sha12]. In this section we give another characterization of T (and therefore, of the functional graph) in terms of trees associated with ν-series and in terms of certain operators c_r that are defined below. We start by introducing some general notation and definitions.

Definition 5.1.1. *Let $g : A \to A$ be a function defined over a finite set A. If $\pi \geq 1$*

and $\rho \geq 0$ *are the least integers such that* $g^{\pi+\rho}(u) = g^{\rho}(u)$*, then* u *has* period $\pi = \mathrm{per}(u)$ *and* preperiod $\rho = \mathrm{pper}(u)$ *(with respect to* g*). Moreover* u *is a* periodic point *when* $\mathrm{pper}(u) = 0$*, and* strictly preperiodic *otherwise.*

Notation 5.1.2. *If* $g : A \to A$ *is a function defined over some finite set* A *and* $B \subseteq A$ *is such that* $g(B) \subseteq B$*, we denote by* $\mathcal{G}(g/B)$ *the functional graph of the restriction* $g|_B : B \to B$*. We also denote by* $Per(g/B) = \{x \in B : x \text{ is a periodic point}\}$*. In particular, if* $B = Per(g/A)$ *we denote by* $\mathcal{G}^{per}(g/A) = \mathcal{G}(g/B)$*. If* $x \in Per(g/A)$ *we denote by* $T_x(g/A)$ *the tree attached to* x *in the functional graph* $\mathcal{G}(g/A)$*. Sometimes when* $Per(g/A) = \{x\}$ *or the isomorphism class of* $T_x(g/A)$ *does not depend on* x *we denote* $T_x(g/A)$ *by* $T(g/A)$*. As usual, we denote by* $o_n(d)$ *the order of* d *modulo* n*.*

Lemma 5.1.3. *Let* d *be a divisor of* ω*. If* $x \in \nu\mathbb{Z}_{\nu\omega}$ *with* $\gcd(\omega, x) = \omega/d$ *then* x *is a periodic point in* $\mathcal{G}(n/\mathbb{Z}_{\nu\omega})$ *and* $per(x) = o_n(d)$*.*

Proof. If $x \in \nu\mathbb{Z}_{\nu\omega}$ with $\gcd(\omega, x) = \omega/d$ we have

$$n^{\pi}x \equiv x \,(\mathrm{mod}\ \nu\omega) \Leftrightarrow n^{\pi}x \equiv x \,(\mathrm{mod}\ \omega) \Leftrightarrow n^{\pi} \equiv 1 \,(\mathrm{mod}\ d) \Leftrightarrow \pi \equiv 0 \,(\mathrm{mod}\ o_n(d)).$$

Then x is a periodic point in $\mathcal{G}(n/\mathbb{Z}_{\nu\omega})$ and $\mathrm{per}(x) = o_n(d)$. □

Proposition 5.1.4. *We have that* $Per(n/\mathbb{Z}_{\nu\omega}) = \nu\mathbb{Z}_{\nu\omega}$ *and the following isomorphism holds:*

$$\mathcal{G}^{per}(n/\mathbb{Z}_{\nu\omega}) \simeq \bigoplus_{d|\omega} \left\{ \frac{\varphi(d)}{o_d(n)} \times Cyc(o_d(n)) \right\}.$$

Proof. By Lemma 5.1.3 we have $\mathrm{Per}(n/\mathbb{Z}_{\nu\omega}) \supseteq \nu\mathbb{Z}_{\nu\omega}$. For the other inclusion we observe that if there exists $\pi \geq 1$ such that $n^{\pi}x \equiv x \pmod{\nu\omega}$ then $(n^{\pi} - 1)x \equiv 0 \pmod{\nu}$. Therefore $x \equiv 0 \pmod{\nu}$ since $\gcd(n^{\pi} - 1, \nu) = 1$ (because $\mathrm{rad}(\nu) \mid \mathrm{rad}(n)$). This proves the first part.

For the second part we consider the partition $\nu\mathbb{Z}_{\nu\omega} = \biguplus_{d|\omega} A(d)$ where $A(d) = \{x \in \nu\mathbb{Z}_{\nu\omega} : \gcd(\omega, x) = \omega/d\}$. As $\gcd(\omega, n) = 1$ we have $nA(d) = A(d)$, and therefore

$$\mathcal{G}^{\mathrm{per}}(n/\mathbb{Z}_{\nu\omega}) = \mathcal{G}(n/\nu\mathbb{Z}_{\nu\omega}) = \bigoplus_{d|\omega} \mathcal{G}(n/A(d)). \tag{5.1.1}$$

By Lemma 5.1.3, all points in $A(d)$ have period $o_n(d)$. Hence, the graph $\mathcal{G}(n/A(d))$ is the union of $\#A(d)/o_n(d)$ cycles of length $o_n(d)$.

Finally we observe that $x \in A(d)$ if and only if $x \equiv \nu \cdot \frac{\omega}{d} \cdot u$ with $\gcd(u, d) = 1$, and for different choices of u we have different values of x. Then $\#A(d) = \varphi(d)$ and

$$\mathcal{G}(n/A(d)) \simeq \frac{\varphi(d)}{o_n(d)} \times Cyc(o_n(d)).$$

Substituting this equation in Equation (5.1.1) we have the desired isomorphism. □

Notation 5.1.5. *For $x \in \mathbb{Z}$ we denote by $\eta(x) = \min\{k \geq 0 : n^k x \equiv 0 \pmod{\nu}\}$.*

Remark 5.1.6. *We observe that $\eta(x) = depth(\nu(x))$, the depth of the ν-series generated by x.*

Proposition 5.1.7. *If $T_a(n/\mathbb{Z}_{\nu\omega})$ denotes the tree attached to the periodic point a in $\mathcal{G}(n/\mathbb{Z}_{\nu\omega})$, we have the following:*

i) The vertices of $T_a(n/\mathbb{Z}_{\nu\omega})$ are the elements $b \in \mathbb{Z}_{\nu\omega}$ such that $b \equiv w_0^{\eta(b)} a \pmod{\omega}$, where $nw_0 \equiv 1 \pmod{\omega}$.

ii) We have the isomorphism

$$T_a(n/\mathbb{Z}_{\nu\omega}) \simeq T_0(n/\mathbb{Z}_{\nu})$$

where $T_0(n/\mathbb{Z}_{\nu})$ denotes the tree attached to 0 in $\mathcal{G}(n/\mathbb{Z}_{\nu})$.

Proof. i) If $b \in T_a(n/\mathbb{Z}_{\nu\omega})$ then $a = n^k b$ where k is the least exponent such that $n^k b$ is a periodic point. By Proposition 5.1.4, this least exponent has to be equal to $\eta(b)$, therefore $n^{\eta(b)} b = a$. In particular $n^{\eta(b)} b \equiv a \pmod{\omega}$, and so $b \equiv w_0^{\eta(b)} a \pmod{\omega}$.

ii) For a periodic point $a \in \mathbb{Z}_{\nu\omega}$ we consider

$$V_a = \{b \in \mathbb{Z}_{\nu\omega} : b \equiv w_0^{\eta(b)} a \pmod{\omega}\}$$

and the function $g : V_a \to V_a$ defined by

$$g(x) = \begin{cases} nx & \text{if } x \neq a, \\ a & \text{if } x = a. \end{cases}$$

We observe that the graph $\mathcal{G}(g/V_a)$ is composed of the tree $T_a(n/\mathbb{Z}_{\nu\omega})$ together with a loop in a. On the other hand, using Proposition 5.1.4 we have that the graph $\mathcal{G}(n/\mathbb{Z}_{\nu})$ is composed of the tree $T_0(n/\mathbb{Z}_{\nu})$ and a loop in 0. Therefore, it is sufficient to prove that $\mathcal{G}(g/V_a) \simeq \mathcal{G}(n/\mathbb{Z}_{\nu})$. To prove this last assertion suffices to prove that the function $\pi : V_a \to \mathbb{Z}_{\nu}$ is a bijection and $\pi \circ g = n \circ \pi$.

The equation $\pi \circ g = n \circ \pi$ can be directly checked. To prove that π is a bijection we observe that for each $\alpha \in \mathbb{Z}_{\nu}$, by the Chinese remainder theorem, there exists a unique $b \in \mathbb{Z}_{\nu\omega}$ such that $b \equiv \alpha \pmod{\nu}$ and $b \equiv w_0^{\eta(\alpha)} a \pmod{\omega}$. □

Corollary 5.1.8. *There exists a tree $T = T(n/\mathbb{Z}_{\nu\omega})$ such that*

$$\mathcal{G}(n/\mathbb{Z}_{\nu\omega}) \simeq \bigoplus_{d|\omega} \left\{ \frac{\varphi(d)}{o_d(n)} \times Cyc(o_d(n), T) \right\}.$$

Moreover, this tree T can be obtained from the graph $\mathcal{G}(n/\mathbb{Z}_{\nu})$ by deleting the loop in 0.

Corollary 5.1.9. *Let $T_0(n/\mathbb{Z}_\nu)$ be the tree attached to 0 in $\mathcal{G}(n/\mathbb{Z}_\nu)$. The isomorphism class of $T(n/\mathbb{Z}_{\nu\omega})$ does not depend on ω and $T_0(n/\mathbb{Z}_\nu)$ is a representative for this isomorphism class.*

The next objective is to prove that $T_0(n/\mathbb{Z}_\nu) = T_{\nu(n)}$. This requires a new operator on trees that we define next.

Definition 5.1.10. *Let d and m be positive integers such that $d \mid m$ and T a rooted tree with vertices $\mathbb{Z}_m$ and root 0. We denote by $\mathcal{H}_T$ the set of leaves (vertices of in-degree 0) except for the root in the case that the tree consists only of one vertex. We say that T is a (d,m)-tree if it verifies the following conditions:*

i) $indeg(0) \in \{0, d-1\}$,

ii) $indeg(x) = d$ *if* $x \notin \mathcal{H}_T, x \neq 0$,

iii) $\#\mathcal{H}_T = m - \frac{m}{d}$.

We denote by $Tree(d,m)$ the set of all (d,m)-trees.

Definition 5.1.11. *Let $d, m \in \mathbb{Z}^+$ with $d \mid m$ and $r = sd$ with $s \in \mathbb{Z}^+$. We define an operator*

$$c_r : Tree(d,m) \to Tree(sd, rm)$$

as follows. For $T \in Tree(d,m)$ we consider a pair $(\mathcal{P}, f)$ where $\mathcal{P}$ is a partition of $\mathbb{Z}_{rm}$ of the form $\mathcal{P} = \{D_x : x \in \mathbb{Z}_m\} \cup \{H_x : x \in \mathcal{H}_T\}$ where $\#D_x = s$ and $\#H_x = sd$; we observe that $s \cdot \#\mathbb{Z}_m + sd \cdot \#\mathcal{H}_T = sm + sd\left(m - \frac{m}{d}\right) = rm$. The set D_x is called the set of duplicates of x and the set H_x is the set of new predecessors of x. The function $f : \mathbb{Z}_m \to \mathbb{Z}_{rm}$ satisfies $f(0) = 0$ and $f(x) \in D_x$ for all $x \in \mathbb{Z}_m$.

If $\rho_T(x)$ denotes the set of predecessors of x in T, we define the rooted tree $c_r(T) = \widetilde{T}$ whose vertices are $\mathbb{Z}_{rm}$, the root is 0, the set of leaves is $\mathcal{H}_{\widetilde{T}} = \mathbb{Z}_{rm} \setminus Im(f)$ and for the other vertices we have:

$$\begin{array}{lll} \rho_{\widetilde{T}}(0) & = \biguplus_{y \in \rho_T(0)} D_y \uplus (D_0 \setminus \{0\}), & \\ \rho_{\widetilde{T}}(f(x)) & = \biguplus_{y \in \rho_T(x)} D_y & \text{if } x \notin \mathcal{H}_T, x \neq 0, \\ \rho_{\widetilde{T}}(f(x)) & = H_x & \text{if } x \in \mathcal{H}_T, x \neq 0. \end{array}$$

Remark 5.1.12. *Informally, if $T \in Tree(d,m)$ and $r = sd$ we obtain $c_r(T)$ attaching $d(s-1)$ new directed predecessors to each non-leaf vertex of T and attaching r new directed predecessors to each leaf of T.*

Proposition 5.1.13. *If $T \in Tree(d,m)$ with $d \mid m$ and $\widetilde{T} = c_r(T)$ where $r = sd$ with $s \in \mathbb{Z}^+$ (for some choice of pair $(\mathcal{P}, f)$ as in Definition 5.1.11), we have*

i) $\widetilde{T} \in Tree(sd, rm)$;

ii) the function $f : \mathbb{Z}_m \to \mathbb{Z}_{rm}$ induce an injective homomorphism between T and $\widetilde{T}$;

iii) the isomorphism class of $c_r(t) = \widetilde{T}$ does not depend on the choice of the pair $(\mathcal{P}, f)$.

Proof. i) If $m = 1$ then $d = 1$ and $r = s \in \mathbb{Z}^+$. In this case, by construction, we have $\mathcal{H}_{\widetilde{T}} = \mathbb{Z}_r \setminus \{0\}$, which implies $\text{indeg}(0) = r - 1$ and $\#\mathcal{H}_{\widetilde{T}} = r - 1 = r - \frac{r}{s}$, therefore $\widetilde{T} \in \text{Tree}(s, r)$.

For $m > 1$ we have

$$\text{indeg}(0) = \#\rho_{\widetilde{T}}(0) = s \cdot \#\rho_T(0) + s - 1 = s(d-1) + s - 1 = sd - 1.$$

For $x \notin \mathcal{H}_T, x \neq 0$ we have

$$\text{indeg}(f(x)) = \#\rho_{\widetilde{T}}(f(x)) = s \cdot \#\rho_T(x) = sd.$$

For $x \in \mathcal{H}_T, x \neq 0$ we have

$$\text{indeg}(f(x)) = \#H_x = sd.$$

With respect to the leaves, $\#\mathcal{H}_{\widetilde{T}} = rm - \#\text{Im}(f) = rm - m = rm - \frac{rm}{sd}$, and therefore $\widetilde{T} \in \text{Tree}(s, r)$.

ii) The fact that f is injective follows from the fact that $\mathcal{P}$ is a partition. On the other hand, by construction we have $D_y \subseteq \rho_{\widetilde{T}}(f(x))$ for all $y \in \rho_T(x)$. Hence, $y \in \rho_T(x)$ implies $f(y) \in D_y \subseteq \rho_{\widetilde{T}}(f(x))$ which proves that f is a homomorphism between T and $\widetilde{T}$.

iii) We consider $\widetilde{T}_1$ and $\widetilde{T}_2$ two constructions of $c_r(T)$, using the pairs $(\mathcal{P}_1, f_1)$ and $(\mathcal{P}_2, f_2)$, respectively. The partitions are of the form

$$\mathcal{P}_i = \{D_x^i : x \in \mathbb{Z}_m\} \cup \{H_x^i : x \in \mathcal{H}_T\} \quad \text{for } i = 1, 2.$$

Let $F : \mathbb{Z}_{rm} \to \mathbb{Z}_{rm}$ be a bijection that satisfies

1. $F(f_1(x)) = f_2(x)$ for all $x \in \mathbb{Z}_m$,
2. $F(D_x^1) = D_x^2$ for all $x \in \mathbb{Z}_m$,
3. $F(H_x^1) = H_x^2$ for all $x \in \mathcal{H}_T$.

We prove next that F is an isomorphism between $\widetilde{T}_1$ and $\widetilde{T}_2$.

First, we observe that $F(\mathcal{H}_{\widetilde{T}_1}) = \mathbb{Z}_{rm} \setminus F(\text{Im}(f_1)) = \mathbb{Z}_{rm} \setminus \text{Im}(f_2) = \mathcal{H}_{\widetilde{T}_2}$, that is, F maps leaves into leaves. Moreover, it follows from (1), (2) and (3) that $F(\rho_{\widetilde{T}_1}(f_1(x))) = \rho_{\widetilde{T}_2}(F(f_1(x)))$ for all $x \in \mathbb{Z}_m$ which prove that F is an isomorphism, and then $\widetilde{T}_1$ and $\widetilde{T}_2$ are isomorphic. □

Now, we can obtain a new characterization of the trees T_V where V is a ν-series.

Lemma 5.1.14. *If $V = (\nu_1, \nu_2, \ldots, \nu_D)$ is a ν-series then*

$$T_V = c_{\nu_1} \circ c_{\nu_2} \circ \cdots \circ c_{\nu_D}(\bullet),$$

where $\bullet$ denotes the tree with one vertex $0 \in \mathbb{Z}_1$.

Proof. (Sketch of the proof) If T is a tree, the *defoliate* of T is another tree T' obtained from T by removing all its leaves. Since $T_1 \simeq T_2$ implies that $T_1' \simeq T_2'$, the defoliate is well defined on isomorphism classes of trees. Another important properties of the defoliate are $(T_1 \oplus T_2)' = T_1' \oplus T_2'$, $(n \times T)' = n \times T'$ and $\langle T_1, T_2, \ldots, T_k\rangle' = \langle T_1', T_2', \ldots, T_k'\rangle$ if at least one of the T_i is non-empty (by convention $\emptyset' = \emptyset$). Using the recursive definition of T_V we have that $T_V' \simeq T_{V'}$ where $V' = (\nu_2, \ldots, \nu_D)$ is a ν'-series, where $\nu' = \frac{\nu}{\nu_1}$.

As above, $\rho_T(x)$ denotes the set of predecessors of x in T, $\mathcal{H}_T$ denotes the set of leaves in T and we define $\rho_T^h(x) = \rho_T(x) \cap \mathcal{H}_T$ and $\operatorname{indeg}^h(x) = \#\rho_T^h(x)$.

We can choose T a representative of T_V and T_0 a representative of $T_{V'}$ with vertices $\mathbb{Z}_\nu$ and $\mathbb{Z}_{\nu'}$, respectively, and root $0 \in \mathbb{Z}_\nu$ and $0 \in \mathbb{Z}_{\nu'}$, respectively. Since $T_V' = T_{V'}$ we can define an injective homomorphism of trees $f : T_0 \to T$. Counting predecessors in T, we obtain $\operatorname{indeg}(0) = \frac{\nu_1}{\nu_2} \cdot \operatorname{indeg}^h(0) + \frac{\nu_1}{\nu_2} - 1$ and

- $\operatorname{indeg}(f(x)) = \frac{\nu_1}{\nu_2} \cdot \operatorname{indeg}^h(f(x))$ for $x \notin \mathcal{H}_{T_0}, x \neq 0$,
- $\operatorname{indeg}(f(x)) = \nu_1$ for $x \in \mathcal{H}_{T_0}, x \neq 0$.

This property allows us to define a partition $\mathcal{P}$ as in Definition 5.1.11 and we obtain that $T = c_{\nu_1}(T_0)$. Applying this several times we obtain the equivalence between both definitions of T_V. □

Lemma 5.1.15. *Let n and ν be integers such that $\operatorname{rad}(\nu) \mid \operatorname{rad}(n)$. We denote by $\nu_1 = \gcd(n, \nu)$ and by $\nu' = \frac{\nu}{\nu_1}$. We have that $T_0(n/\mathbb{Z}_\nu) \in \mathit{Tree}(\nu_1, \nu)$ and $T_0(n/\mathbb{Z}_\nu) = c_{\nu_1}(T_0(n/\mathbb{Z}_{\nu'}))$.*

Proof. For $\nu = 1$ we have $T_0(n/\mathbb{Z}_\nu) = \bullet$ the tree with only one vertex and it is clear that this tree belongs to $\operatorname{Tree}(1, 1)$. If $\nu > 1$ then $\nu' < \nu$ (because $\operatorname{rad}(\nu) \mid \operatorname{rad}(n)$) and by Proposition 5.1.13 it is sufficient to prove that $T_0(n/\mathbb{Z}_\nu) = c_{\nu_1}(T_0(n/\mathbb{Z}_{\nu'}))$ assuming $T_0(n/\mathbb{Z}_{\nu'}) \in \operatorname{Tree}(\nu_2, \nu')$ where $\nu_2 = \gcd(n, \nu')$.

Hence, we can assume $\nu > 1$ and if we denote by $T = T_0(n/\mathbb{Z}_\nu)$ and $T' = T_0(n/\mathbb{Z}_{\nu'})$ we prove that $T = C_{\nu_1}(T')$ from some adequate choice of $(\mathcal{P}, f)$.

We define the function $f : \mathbb{Z}_{\nu'} \to \mathbb{Z}_\nu$ as $f(x) = \nu_1 x \pmod{\nu}$. This function is well defined because $\nu/\nu_1 = \nu'$. We also define the partition $\mathcal{P} = \{D_t : t \in \mathbb{Z}_{\nu'}\} \cup \{H_t : t \in \mathcal{H}_{T'}\}$ where

$$D_t = \{\nu_1 t + k\nu' : 0 \leq k < \frac{\nu_1}{\nu_2}\} \qquad \text{for } t \in \mathbb{Z}_{\nu'},$$

$$H_t = \{\omega_0 t + k\nu' : 0 \leq k < \nu_1\} \qquad \text{for } t \in \mathcal{H}_{T'},$$

and where ω_0 is such that $\omega_0 \cdot \left(\frac{n}{\nu_1}\right) \equiv 1 \pmod{\nu'}$.

To prove that the sets D_t are disjoint and $\#D_t = \nu_1/\nu_2$ suffices to prove that for $t_1, t_2 \in \mathbb{Z}_{\nu'}$ and $0 \leq k_1, k_2 < \nu_1/\nu_2$, the congruence $\nu_1 t_1 + k_1\nu' \equiv \nu_1 t_2 + k_2\nu' \pmod{\nu}$ implies $k_1 = k_2$ and $t_1 = t_2$. We have that $\nu_1 t_1 + k_1\nu' \equiv \nu_1 t_2 + k_2\nu' \pmod{\nu}$ implies $k_1\nu' \equiv k_2\nu' \pmod{\nu_1}$, that is, $k_1 \equiv k_2 \pmod{\nu_1/\nu_2}$ (since $\gcd(\nu_1, \nu') = \nu_2$) and so $k_1 = k_2$. Now, $\nu_1 t_1 \equiv \nu_1 t_2 \pmod{\nu}$ implies $t_1 \equiv t_2 \pmod{\nu'}$, and so $t_1 = t_2$.

To prove that the sets H_t are disjoint and $\#H_t = \nu_1$ suffices to prove that for $t_1, t_2 \in \mathcal{H}_{T'}$ and $0 \leq k_1, k_2 < \nu_1$, the congruence $\omega_0 t_1 + k_1\nu' \equiv \omega_0 t_2 + k_2\nu' \pmod{\nu}$ implies $t_1 = t_2$ and $k_1 = k_2$. We have that $\omega_0 t_1 + k_1\nu' \equiv \omega_0 t_2 + k_2\nu' \pmod{\nu}$ implies $t_1 \equiv t_2 \pmod{\nu'}$ (because $\gcd(\omega_0, \nu') = 1$) and so $t_1 = t_2$. Now, $k_1\nu' \equiv k_2\nu' \pmod{\nu}$ implies $k_1 \equiv k_2 \pmod{\nu_1}$, and so $k_1 = k_2$.

As $D_t \subset \nu_2\mathbb{Z}_\nu$ for all $t \in \mathbb{Z}_{\nu'}$ and $H_t \cap \nu_2\mathbb{Z}_\nu = \emptyset$ for all $t \in \mathcal{H}_{T'}$ (because $t \in \mathcal{H}_{T'}$ implies $t \not\equiv 0 \pmod{\nu_2}$) we have that the sets in $\mathcal{P}$ are disjoint. Computing cardinalities we can conclude that $\mathcal{P}$ is a partition. It is immediate to check that $f(t) = \nu_1 t \in D_t$ for all $t \in \mathbb{Z}_{\nu'}$ and so we have $T = c_{\nu_1}(T')$. □

Theorem 5.1.16. *Let n and ν be integers such that $rad(\nu) \mid rad(n)$ then*

$$T(n/\mathbb{Z}_\nu) = T_{\nu(n)}.$$

Proof. If $\nu(n) = (\nu_1, \nu_2, \ldots, \nu_D)$, applying several times Lemma 5.1.15 we have

$$T(n/\mathbb{Z}_\nu) = c_{\nu_1}\left(T\left(n/\mathbb{Z}_{\frac{\nu}{\nu_1}}\right)\right) = c_{\nu_1} \circ c_{\nu_2}\left(T\left(n/\mathbb{Z}_{\frac{\nu}{\nu_1\nu_2}}\right)\right) = \cdots$$

$$= c_{\nu_1} \circ c_{\nu_2} \circ \cdots \circ c_{\nu_D}(T(n/\mathbb{Z}_1)) = T_{\nu(n)},$$

where in the last equation we use $T(n/\mathbb{Z}_1) = \bullet$ and Lemma 5.1.14. □

5.2 Application to Rédei functions

In this section we show how to translate dynamic properties of the n-map to the case of Rédei functions. Using results of the previous section we can obtain a complete description of the functional graph of Rédei function and a formula for the period and preperiod of points. We obtain a more explicit description for a special case and use it to obtain Rédei functions with prescribed cycles with length in a geometric progression that extends results obtained in [SSP].

We start this section by introducing some preliminaries about Rédei functions.

5.2.1 Background on Rédei functions

There are several equivalent definitions for Rédei function. The classical definition considers the binomial expansion $(x+\sqrt{y})^n = N(x,y) + D(x,y)\sqrt{y}$. Then, the *Rédei function* $R_n(x,a)$ defined over $\mathbb{P}^1(\mathbb{F}_q) := \mathbb{F}_q \cup \{\infty\}$ for $a \in \mathbb{F}_q$ is $R_n(x,a) = \frac{N(x,a)}{D(x,a)}$. Table 1 gives the first few Rédei functions for $a \in \mathbb{F}_q$.

$$
\begin{aligned}
R_1(x,a) &= x \\
R_2(x,a) &= (x^2+a)/2x \\
R_3(x,a) &= (x^3+3ax)/(3x^2+a) \\
R_4(x,a) &= (x^4+6ax^2+a^2)/(4x^3+4ax) \\
R_5(x,a) &= (x^5+10ax^3+5a^2x)/(5x^4+10ax^2+a^2) \\
R_6(x,a) &= (x^6+15ax^4+15a^2x^2+a^3)/(6x^5+20ax^3+6a^2x) \\
R_7(x,a) &= (x^7+21ax^5+35a^2x^3+7a^3x)/(7x^6+35ax^4+21a^2x^2+a^3)
\end{aligned}
$$

Table 5.1: First few Rédei functions $R_n(x,a)$ for $a \in \mathbb{F}_q$.

The most convenient way of writing Rédei functions for us is due to Carlitz [Car62]. For a fixed $a \in \mathbb{F}_q^*$ we define

$$R_n(x,a) = \sqrt{a}\,\frac{(x+\sqrt{a})^n + (x-\sqrt{a})^n}{(x+\sqrt{a})^n - (x-\sqrt{a})^n}, \quad \text{if } \mathrm{char}(\mathbb{F}_q) \neq 2.$$

In this section, we consider the Möbius function over finite fields defined as $\gamma(u) = \frac{u+\sqrt{a}}{u-\sqrt{a}}$ for $u \in \mathbb{P}^1(\mathbb{F}_q)$, with $\gamma(u) = \infty$ if $u = \sqrt{a}$. Then we can write

$$R_n(x,a) = \sqrt{a}\,\frac{\gamma(x)^n + 1}{\gamma(x)^n - 1}, \tag{5.2.1}$$

where we use the standard rules when $\gamma(x) = \infty$, that is $\infty^n = \infty$, $\frac{\infty}{\infty} = 1$ and $\infty \pm 1 = \infty$. If we define $R_n(x,a) = \infty$ when the denominator vanishes, we have a mapping $R_n : \mathbb{P}^1(\mathbb{F}_q) \to \mathbb{P}^1(\mathbb{F}_q)$. We are interested in understanding the functional graph of this mapping.

One important property of Rédei functions that we use in this section is that $R_n \circ R_m = R_{nm}$ for fixed $a \in \mathbb{F}_q^*$ and n, m positive integers; see [Réd46].

Another classical result that we use is that the Rédei function $R_n(x,a)$ induces a permutation function on $\mathbb{P}^1(\mathbb{F}_q)$ if and only if $\gcd(n, q-\chi(a)) = 1$ where χ is the quadratic character in $\mathbb{F}_q^*$ (that is, $\chi(a) = 1$ if a is a square in $\mathbb{F}_q^*$, and -1 otherwise). This is a well known fact about Rédei functions; see for example [Car62, Réd46]. Partial results giving the description in disjoint cycles of Rédei functions are presented in [SSP].

Rédei functions have been applied in many areas such as pseudorandom number generators [GW08a, GW08b, MW07], cryptography [Nöb85], to solve Pell equations [BCM10b], for interleavers in turbo codes [SSP], and to solve a conjecture about permutation trinomials [Zie13].

5.2.2 The functional graph of Rédei functions

Lemma 5.2.1. *Let $a \in \mathbb{F}_q^*$ be a non-square element in a non binary finite field, then we have $\gamma(\mathbb{P}^1(\mathbb{F}_q)) = U$, the multiplicative subgroup of order $q+1$ of $\mathbb{F}_{q^2}^*$.*

Proof. Since $\chi(a) = -1$ we have $\gamma(\mathbb{P}^1(\mathbb{F}_q)) \subseteq \mathbb{F}_{q^2}$. Let $x, y \in \mathbb{P}^1(\mathbb{F}_q)$. We need to prove that $\gamma(x)\gamma(y) \in \gamma(\mathbb{P}^1(\mathbb{F}_q))$. If $x = \infty$ or $y = \infty$ the assertion is clear. Otherwise we have

$$\begin{aligned}\gamma(x)\gamma(y) &= \frac{x+\sqrt{a}}{x-\sqrt{a}} \cdot \frac{y+\sqrt{a}}{y-\sqrt{a}} = \frac{xy+a+(x+y)\sqrt{a}}{xy+a-(x+y)\sqrt{a}} \\ &= \begin{cases} 1 = \gamma(\infty) & \text{if } x+y=0, \\ \gamma\left(\frac{xy+a}{x+y}\right) & \text{if } x+y \neq 0. \end{cases}\end{aligned}$$

In both cases we have $\gamma(x)\gamma(y) \in \gamma(\mathbb{P}^1(\mathbb{F}_q))$. □

When a is an square over $\mathbb{F}_q^*$ we restrict the domain of $R_n(x,a)$ to the set $\mathbb{D}_q = \mathbb{P}^1(\mathbb{F}_q) \setminus \{\pm\sqrt{a}\}$. Since in this case $\sqrt{a}$ and $-\sqrt{a}$ are isolated fixed point, the functional graph of the Rédei function over $\mathbb{P}^1(\mathbb{F}_q)$ and $\mathbb{D}_q$ are essentially the same. When $a \in \mathbb{F}_q^*$ is a non-square element we define $\mathbb{D}_q = \mathbb{P}^1(\mathbb{F}_q)$.

From here on we denote $\mathcal{G}(n,a,q)$ by $\mathcal{G}(R_n(x,a)/\mathbb{D}_q)$ and we let $\mathcal{G}^{\mathrm{per}}(n,a,q)$ be $\mathcal{G}^{\mathrm{per}}(R_n(x,a)/\mathbb{D}_q)$. The function γ is injective and $\gamma(\mathbb{D}_q) = U_{q+1}$ the multiplicative subgroup of order $q+1$ of $\mathbb{F}_{q^2}$ when $\chi(a) = -1$ (Lemma 5.2.1) or $\gamma(\mathbb{D}_q) = \mathbb{F}_q^*$ when $\chi(a) = 1$. If $R_n(x) = R_n(x,a)$ we have by direct calculation that in both cases $\gamma \circ R_n(x) = x^n \circ \gamma(x)$ for all $x \in \mathbb{D}_q$ and therefore the following diagram commutes:

$$\text{if } \chi(a) = -1: \quad \begin{array}{ccc} \mathbb{D}_q & \xrightarrow{R_n} & \mathbb{D}_q \\ {\scriptstyle\gamma}\downarrow & & \downarrow{\scriptstyle\gamma} \\ U_{q+1} & \xrightarrow{x^n} & U_{q+1} \end{array} \qquad \text{if } \chi(a) = 1: \quad \begin{array}{ccc} \mathbb{D}_q & \xrightarrow{R_n} & \mathbb{D}_q \\ {\scriptstyle\gamma}\downarrow & & \downarrow{\scriptstyle\gamma} \\ \mathbb{F}_q^* & \xrightarrow{x^n} & \mathbb{F}_q^* \end{array}$$

We observe that if G is a multiplicative cyclic group of order m then $x^n : G \to G$ is conjugate to $n : \mathbb{Z}_m \to \mathbb{Z}_m$ (multiplication by m) via any isomorphism $\varphi : G \to \mathbb{Z}_m$ and so $\mathcal{G}(x^n/G) \simeq \mathcal{G}(n/\mathbb{Z}_m)$. Since both U_{q+1} and $\mathbb{F}_q^*$ are multiplicative cyclic groups we have the following proposition.

Proposition 5.2.2. *Let $n \in \mathbb{Z}^+$ and $\mathbb{F}_q$ be a finite field and $a \in \mathbb{F}_q^*$. We have*

- $\mathcal{G}(n,a,q) \simeq \mathcal{G}(x^n/U_{q+1}) \simeq \mathcal{G}(n/\mathbb{Z}_{q+1})$ *if* $\chi(a) = -1$,
- $\mathcal{G}(n,a,q) \simeq \mathcal{G}(x^n/\mathbb{F}_q^*) \simeq \mathcal{G}(n/\mathbb{Z}_{q-1})$ *if* $\chi(a) = 1$.

If $q - \chi(a) = \nu\omega$ with $\mathrm{rad}(\nu)|\mathrm{rad}(n)$ and $\gcd(\omega, n) = 1$, we have in both cases $\mathcal{G}(n,a,q) \simeq \mathcal{G}(n/\mathbb{Z}_{\nu\omega}) \simeq \mathcal{G}(n/\mathbb{Z}_\nu \times \mathbb{Z}_\omega)$ where the last isomorphism is via the remainder Chinese theorem since $\gcd(\nu,\omega) = 1$.

We denote by $\{\bullet\}$ any graph consisting of a unique vertex v with a loop (v, v). If we apply the above observations together Definition 3.3.10, Corollary 5.1.8 and Theorem 5.1.16 we obtain the following proposition.

Theorem 5.2.3. *Let $n \in \mathbb{Z}^+$, $a \in \mathbb{F}_q^*$ and $\mathcal{G}(n, a, q)$ the functional graph of the Rédei function $R_n(x, a)$ as a map over $\mathbb{P}^1(\mathbb{F}_q)$. We express $q - \chi(a) = \nu\omega$ with $rad(\nu) \mid rad(n)$ and $\gcd(n, \omega) = 1$. If $\lambda \in \mathbb{R}$ is such that $n^\lambda = \nu$, then*

$$\mathcal{G}(n, a, q) \simeq \bigoplus_{d|\omega} \left\{ \frac{\varphi(d)}{o_d(n)} \times H_n(o_d(n), \lambda) \right\} \oplus (1 + \chi(a)) \times \{\bullet\}.$$

Example 5.2.4. *Let us describe the structure of the functional graph associated with $R_3(x, 1) = \frac{x^3+3x}{3x^2+1}$ over $P^1(\mathbb{F}_{37})$. First, we have $q - \chi(a) = 36 = 3^2 \cdot 2^2$, and so $n = 3$, $\lambda = 2$ and $\omega = 4$. Using Theorem 5.2.3 we get (see Fig. 5.1)*

$$\begin{aligned} \mathcal{G}(3, 1, 37) &\simeq \bigoplus_{d|4} \left\{ \frac{\varphi(d)}{o_d(3)} \times H_3(o_d(3), 2) \right\} \oplus \{\bullet, \bullet\} \\ &\simeq 2 \times H_3(1, 2) \oplus H_3(2, 2) \oplus \{\bullet, \bullet\} \end{aligned}$$

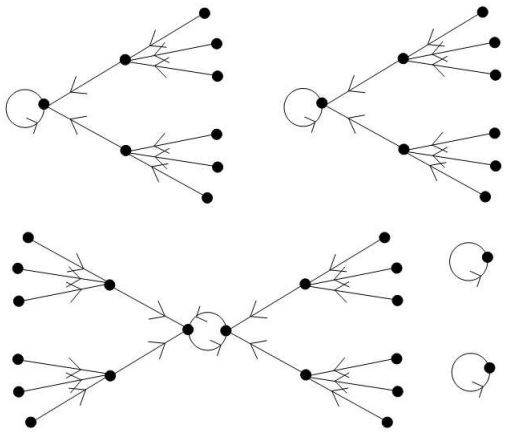


Figure 5.1: Structure of the functional graph associated with $R_3(x, 1) = \frac{x^3+3x}{3x^2+1}$ over $P^1(\mathbb{F}_{37})$.

An important consequence of Theorem 5.2.3 is that it allows us obtain a formula for the period and preperiod of Rédei functions.

Proposition 5.2.5. *Let $\mathcal{G}(n, a, q)$ be the functional graph of the Rédei function $R_n(x, a)$ as a map over $\mathbb{P}^1(\mathbb{F}_q)$ and $q - \chi(a) = \nu\omega$ with $rad(\nu) \mid rad(n)$ and $\gcd(n, \omega) = 1$. If $u \in \mathbb{P}^1(\mathbb{F}_q)$ and we express the multiplicative order over $\mathbb{F}_{q^2}$ as $\mathrm{ord}(\gamma(u)) = \nu_u d$ with $rad(\nu_u) \mid rad(n)$ and $\gcd(n, d) = 1$ (by convention $\mathrm{ord}(\infty) = \mathrm{ord}(0) = 1$) we have that $\nu_u \mid \nu$, $d \mid \omega$ and*

- $\mathrm{per}(u) = \mathrm{ord}_d(n)$,
- $\mathrm{pper}(u) = depth(\nu_u(n)) = \min\{t \in \mathbb{Z}^+ : \nu_u \mid n^t\}$.

There is a special case of interest when $\omega = p^\alpha$ or $\omega = 2p^\alpha$ where p is an odd prime and α is a positive integer. In this case it is possible to obtain a more explicit representation of the functional graph. We recall that ω is such that $q - \chi(a) = \nu\omega$ with $\mathrm{rad}(\nu) \mid \mathrm{rad}(n)$ and $\gcd(n, \omega) = 1$.

Theorem 5.2.6. *Let n, a, q, λ and ω be as in Theorem 5.2.3 with the additional condition $\omega = p^\alpha$ if n is even or $\omega = 2p^\alpha$ if n is odd, where p is an odd prime. Let $\eta = \frac{\varphi(\omega)}{o_\omega(n)} = p^h\kappa$ with $p \nmid \kappa$ and $f = \frac{p-1}{\kappa}$. We have the following isomorphism for the functional graph associated with the Rédei function $R_n(x, a)$ over $\mathbb{P}^1(\mathbb{F}_q)$.*

For n even:

$$\begin{aligned}\mathcal{G}(n, a, q) \;\simeq\; & H_n(1, \lambda) \oplus \frac{p^{h+1} - 1}{f} \times H_n(f, \lambda) \\ & \oplus \bigoplus_{i=h+2}^{\alpha} \{\kappa p^h \times H_n(f p^{i-h-1}, \lambda)\} \oplus (1 + \chi(a)) \times \{\bullet\},\end{aligned}$$

and for n odd:

$$\begin{aligned}\mathcal{G}(n, a, q) \;\simeq\; & 2 \times H_n(1, \lambda) \oplus \frac{2(p^{h+1} - 1)}{f} \times H_n(f, \lambda) \\ & \oplus \bigoplus_{i=h+2}^{\alpha} \{2\kappa p^h \times H_n(f p^{i-h-1}, \lambda)\} \oplus (1 + \chi(a)) \times \{\bullet\}.\end{aligned}$$

Proof. We observe first that

$$\eta = \frac{\varphi(\omega)}{o_\omega(n)} = \frac{p^{\alpha-1}(p-1)}{o_\omega(n)} = p^h\kappa \tag{5.2.2}$$

with $0 \le h \le \alpha - 1$ and $\kappa \mid p - 1$.

Let r be a primitive root modulo ω (and therefore a primitive root modulo d, for all $d \mid \omega$). As $\gcd(n, \omega) = 1$ then $n \equiv r^t \pmod{\omega}$ for some integer t, $1 \le t \le \varphi(\omega)$. Changing r for another primitive root if it is necessary, we can suppose that $t \mid \varphi(\omega)$ and in this case we have:

$$o_\omega(n) = o_\omega(r^t) = \frac{o_\omega(r)}{\gcd(t, \varphi(\omega))} = \frac{\varphi(\omega)}{t}.$$

Comparing with (5.2.2) we conclude that $t = \eta$ and $n \equiv r^\eta \pmod{\omega}$.

For $d \mid \omega$ of the form $d = p^i$ or $d = 2p^i$ with $1 \leq i \leq \alpha$ we have

$$\begin{aligned} o_d(n) &= o_d(r^\eta) = \frac{o_d(r)}{\gcd(o_d(r), \eta)} = \frac{\varphi(d)}{\gcd(\varphi(d), \eta)} = \frac{p^{i-1}(p-1)}{\gcd(p^{i-1}(p-1), p^h \kappa)} \\ &= \frac{p^{i-1}(p-1)}{p^{\min(i-1,h)}\kappa} = p^{\max(i-1-h,0)} f = \begin{cases} f & \text{if } i \leq h+1, \\ p^{i-h-1} f & \text{if } h+1 < i \leq \alpha. \end{cases} \end{aligned}$$

Then, we can rewrite Theorem 5.2.3 in the following way. For n even:

$$\begin{aligned} \mathcal{G}(n,a,q) &= \frac{\varphi(1)}{o_1(n)} \times H_n(1,\lambda) \oplus \left(\sum_{i=1}^{h+1} \frac{\varphi(p^i)}{o_{p^i}(n)} \right) \times H_n(f,\lambda) \\ &\quad \oplus \bigoplus_{i=h+2}^{\alpha} \left\{ \frac{\varphi(p^i)}{o_{p^i}(n)} \times H_n(f p^{i-h-1}, \lambda) \right\} \oplus (1+\chi(a)) \times \{\bullet\}. \end{aligned}$$

For n odd:

$$\begin{aligned} \mathcal{G}(n,a,q) = &\left(\frac{\varphi(1)}{o_1(n)} + \frac{\varphi(2)}{o_2(n)} \right) \times H_n(1,\lambda) \oplus \left(\sum_{i=1}^{h+1} \frac{\varphi(p^i)}{o_{p^i}(n)} + \frac{\varphi(2p^i)}{o_{2p^i}(n)} \right) \times H_n(f,\lambda) \\ &\oplus \bigoplus_{i=h+2}^{\alpha} \left\{ \left(\frac{\varphi(p^i)}{o_{p^i}(n)} + \frac{\varphi(2p^i)}{o_{2p^i}(n)} \right) \times H_n(f p^{i-h-1}, \lambda) \right\} \oplus (1+\chi(a)) \times \{\bullet\}. \end{aligned}$$

Note that for n odd and $i \geq 1$ we have $\varphi(p^i) = \varphi(2p^i)$ and $o_{p^i}(n) = o_{2p^i}(n)$, therefore $\frac{\varphi(p^i)}{o_{p^i}(n)} + \frac{\varphi(2p^i)}{o_{2p^i}(n)} = 2\frac{\varphi(p^i)}{o_{p^i}(n)}$.

We conclude the proof observing that in both cases we have

$$\sum_{i=1}^{h+1} \frac{\varphi(p^i)}{o_{p^i}(n)} = \sum_{i=1}^{h+1} \frac{p^{i-1}(p-1)}{f} = \kappa \sum_{i=1}^{h+1} p^{i-1} = \kappa \cdot \frac{p^{h+1}-1}{p-1} = \frac{p^{h+1}-1}{f},$$

and for $h+1 < i \leq \alpha$, we have

$$\frac{\varphi(p^i)}{o_{p^i}(n)} = \frac{p^{i-1}(p-1)}{p^{i-1-h} f} = \kappa p^h.$$

□

5.2.3 Rédei permutations and their cycle decomposition

Here we give other corollaries that can be obtained from Theorem 5.2.3 related to the cycle decomposition. In particular we give a way to construct Rédei functions whose length cycles are in arithmetic progression that extend results obtained in [SSP].

Corollary 5.2.7. *The Rédei function $R_n(x,a)$ induces a permutation of $\mathbb{P}^1(\mathbb{F}_q)$ if and only if $\gcd(n, q-\chi(a)) = 1$. In this case we have the following decomposition in disjoint*

cycles

$$\mathcal{G}(n,a,q) \simeq \bigoplus_{d|q-\chi(a)} \left\{ \frac{\varphi(d)}{o_d(n)} \times Cyc(o_d(n)) \right\} \oplus (1+\chi(a)) \times \{\bullet\},$$

where $Cyc(c)$ denotes a directed cycle of length c.

Proof. As a consequence of Theorem 5.2.3 it is easy to conclude that $R_n(x,a)$ induces a permutation if and only if $\lambda = 0$ (Remark 3.3.11). This is equivalent to $\gcd(n, q-\chi(a)) = 1$. In this case each $H_n\left(o_d(n), \lambda\right) = Cyc\left(o_d(n)\right)$, and so it is a directed cycle of length $o_d(n)$. □

Corollary 5.2.8. *The number of fixed points of $R_n(x,a)$ over $\mathbb{P}^1(\mathbb{F}_q)$ is given by the formula*

$$\gcd\left(n-1, q-\chi(a)\right) + \left(1+\chi(a)\right).$$

This corollary can be seen as a consequence of the following more general result (by taking $k=1$).

Corollary 5.2.9. *Let k be a positive integer. The number of points of $R_n(x,a)$ over $\mathbb{P}^1(\mathbb{F}_q)$ whose period divide k is given by the formula*

$$\gcd\left(n^k-1, q-\chi(a)\right) + \left(1+\chi(a)\right).$$

Proof. We consider the set $P_k = \{x \in \mathbb{P}^1(\mathbb{F}_q) : \mathrm{per}(x) \mid k\}$. If $x \in P_k$, x belongs to a connected component $H_n(o_d(n), \lambda)$ with $o_d(n) \mid k$. Now, $o_d(n) \mid k$ if and only if $n^k \equiv 1 \pmod{d}$ if and only if $d \mid n^k - 1$.

On the other hand, each component $H_n(o_d(n), \lambda)$ with $d \mid n^k - 1$ have exactly $o_d(n)$ points in P_k, so

$$\begin{aligned} \#P_k &= \sum_{d|\omega, d|n^k-1} \left\{ \frac{\varphi(d)}{o_d(n)} \cdot o_d(n) \right\} + (1+\chi(a)) \\ &= \sum_{d|\gcd(n^k-1,\omega)} \varphi(d) + (1+\chi(a)) = \gcd(n^k-1, \omega) + (1+\chi(a)) \\ &= \gcd(n^k-1, q-\chi(a)) + (1+\chi(a)). \end{aligned}$$

□

Remark 5.2.10. *Corollary 5.2.9 gives an alternative way to prove Theorem 3.14 of [SSP]. If we denote by N_j the number of cycles of length j, we obtain*

$$jN_j + \sum_{i|j, i<j} iN_i = \gcd(n^j-1, q-\chi(a)) + (1+\chi(a)).$$

In particular, when $\chi(a) = -1$ the point ∞ is an isolated fixed point and we can consider

$R_n(x,a) : \mathbb{F}_q \to \mathbb{F}_q$. *In this case we have*

$$jN_j + \sum_{i|j, i<j} iN_i = \gcd(n^j - 1, q - \chi(a)) - 1$$

as stated in Theorem 3.14 of [4].

The following corollary that characterize Rédei permutations with cycles of length 1 and j (where j is an integer greater than 1) appears in [SSP] and can be seen as a direct consequence of Theorem 5.2.3.

Corollary 5.2.11. *(Theorem 3.15 of [SSP]) If* $\gcd(n, q+1) = 1$ *and* $\chi(a) = -1$*, then the Rédei permutation* $R_n(x,a)$ *has all its cycles of length* 1 *or* j *if and only if for every divisor* d *of* $q+1$ *we have* $n \equiv 1 \pmod{d}$ *or* $j = \mathrm{ord}_d(n)$.

Proof. The length of the cycles are given by $o_d(n) = \mathrm{ord}_d(n)$ where d runs over the divisors of $q+1$ and $\mathrm{ord}_d(n) = 1$ if and only if $n \equiv 1 \pmod{d}$. □

A naive generalization of the above corollary is given next. It can be proved in the same way as above.

Corollary 5.2.12. *If* $\gcd(n, q+1) = 1$ *and* $\chi(a) = -1$*, then the Rédei permutation* $R_n(x,a)$ *has all its cycles of length belonging to a set* $S = \{1, j_1, \ldots, j_t\}$ *if and only if for every divisor* d *of* $q+1$ *we have* $\mathrm{ord}_d(n) \in S$.

Corollary 5.2.13. *The length of the largest cycle in* $\mathcal{G}(\ell, a, q)$ *is* $m = \mathrm{ord}_\omega(n)$*, where* $q - \chi(a) = n^\lambda \omega$ *and* $n \nmid \omega$ *as in Theorem 5.2.3.*

Proof. The lengths of the cycles are given by $o_d(n)$ where d runs over the divisors of ω. If d is a divisor of ω we have $n^m \equiv 1 \pmod{\omega}$ if and only if $n^m \equiv 1 \pmod{d}$ if and only if $o_d(n) \mid m$ and thus $m \geq o_d(n)$. □

Theorem 5.2.6 allows us to construct special types of Rédei functions.

Despite the fact that we have the above characterizations, it is not clear how to construct Rédei functions where all its non-trivial cycles (that is, cycles of length greater than one) have length j. We show next, a method to construct such Rédei functions. Moreover, given an integer $j \geq 2$ and an integer $t \geq 1$, the method allows us to construct Rédei functions whose non-trivial cycles have length $j, jp, jp^2, \ldots, jp^{t-1}$ for some prime number p (when $t = 1$ we obtain a Rédei function whose non-trivial cycles have length j).

Remark 5.2.14. *Let* j *and* t *be positive integers with* $j \geq 2$*, and* p *a prime number such that* $p \equiv 1 \pmod{j}$*. Let us suppose that we want to construct a Rédei function* $R_n(x,a)$ *defined over a finite field* $\mathbb{F}_q$ *with exactly* t *different lengths for the non-trivial cycles following the geometric progression* $j, jp, jp^2, \ldots, jp^{t-1}$*. We can apply the next steps:*

1. *Pick a number $\alpha \geq t$ such that $2p^\alpha - 1 = q$ is a power of prime.*

2. *Pick a non-square element in $\mathbb{Z}_{q+1}$.*

3. *Choose a primitive root r modulo $\mathbb{Z}_{q+1}$.*

4. *Compute $n \equiv r^{p^{\alpha-t}\left(\frac{p-1}{j}\right)} \pmod{q+1}$.*

Then, the Rédei function $R_n(x,a)$ defined over $\mathbb{F}_q$ has non-trivial cycles of length $j, jp, jp^2, \ldots, jp^{t-1}$ as required. Indeed, we have that $\chi(a) = -1$ and $\gcd(n, q+1) = 1$. With the notation used in Theorem 5.2.6, $\omega = q+1, \nu = 1, o_\omega(n) = j = f$ and n is odd (because $q+1$ is even). We obtain that $\nu = p^h\kappa$ where $h = \alpha - t$ and $\kappa = \frac{p-1}{j}$. By Theorem 5.2.6 we have the largest cycle in $\mathcal{G}(n,a,q)$ has length $fp^{\alpha-h-1} = jp^{t-1}$ which appear exactly $\kappa p^h = \frac{(p-1)p^h}{j}$ times. The other length cycles are $1, j, \ldots, jp^{t-2}$ and their multiplicities can be obtained from Theorem 5.2.6.

5.3 Estimates for the cycle structure of iterating Rédei functions

Shallit and Vasiga [VS04] obtain several results about tails and cycles in orbits of iterations of quadratic polynomials over prime fields. These results were extended to repeated exponentiation by Chou and Shparlinski [CS04]. In this section, using a different strategy based on isomophisms of Rédei iteration graphs, we show analogous results to Chou and Shparlinski but for Rédei functions and the n-map.

5.3.1 Some parameters related to the cycle structure

We consider a parametric family of rational functions with integer coefficients $\{f_u(x)\}_{u\in U}$ such that the denominator of such functions not vanish when they are considered modulo p for p large enough prime number. In this case, for $x \in \mathbb{P}^1(\mathbb{F}_p)$ we consider the least integers $s \geq 0$ and $r \geq 1$ such that $f_u^{(s+r)}(x) = f_u^{(s)}(x)$ (where $f^{(k)}$ is the k-th iterate of f) and we define:

- $c_{u,p}(x) = r$ (the cycle length or period of x),
- $t_{u,p}(x) = s$ (the tail length or pre-period of x).

We are interested in studying the following parameters:

- $C(u,p)$, the expected value of $c_{u,p}$.
- $T(u,p)$, the expected value of $t_{u,p}$.
- $T_0(u,p)$, the number elements for which $t_{u,p} = 0$.
- $N(u,p)$, the number of cycles in f_u as map in $\mathbb{P}^1(\mathbb{F}_q)$.

- $S(u, N)$, the expected value of $T(u, p)$ for p runs over all primes $p \leq N$.
- $S_0(u, N)$, the expected value of $T_0(u, p)$ for p runs over all primes $p \leq N$.

In [CS04], Chou and Shparlinski studied these parameters for the case $f_e(x) = x^e$. We are interested on the Rédei function case, that is when $f_{(n,a)}(x) = R_n(x, a)$. The dynamics of the Rédei function defined over $\mathbb{P}^1(\mathbb{F}_p)$, for the case when a is a square element in $\mathbb{F}_p$ is essentially the same that the dynamics of the map x^e over $\mathbb{F}_p^*$; in this sense our results on Rédei function can be seen as a generalization of [CS04].

Review of results on Rédei functions and the n-map

Here we review some results about isomorphism of Rédei function and the n-map to be used in the estimate of some parameters related to their cycle structure.

Let $\mathcal{G}(n, a, q)$ be the functional graph of the Rédei function $R_n(x, a)$ defined over $\mathbb{D}_a = \mathbb{P}^1(\mathbb{F}_q) \setminus \{\pm\sqrt{a}\}$ (where q is an odd prime power) and $\mathcal{G}(n/\mathbb{Z}_{\nu\omega})$ be the functional graph of the n-map defined over $\mathbb{Z}_{\nu\omega}$ where $\mathrm{rad}(\nu) \mid \mathrm{rad}(n)$ and $\gcd(n\omega) = 1$.

We are interested in the parametric family of Rédei functions, that is $\{f_u\}_{u\in U}$ where U consist of pairs $(n, a) \in \mathbb{Z}^+ \times \mathbb{F}_q^*$ and $f_{(n,a)}(x) = R_n(x, a)$ defined over $\mathbb{D}_a$.

In Proposition 5.2.2 we obtained the following isomorphism of graph

$$\mathcal{G}(n, a, q) \simeq \mathcal{G}(n/\mathbb{Z}_{q-\chi(a)})$$

where χ is the quadratic character in $\mathbb{F}_q^*$.

This proposition allows us to reduce our problem of obtain the parameters C, T, T_0, N, S and S_0 for the case of the n-mapping. The following results is a direct consequence of Corollary 5.1.8 and Theorem 5.1.16.

Proposition 5.3.1. *Let $q - \chi(a) = \nu\omega$ where $rad(\nu) \mid rad(n)$ and $\gcd(n, \omega) = 1$. Let $\nu(n) = (\nu_1, \nu_2, \ldots, \nu_D)$ the ν-serie generated by n. We have the following isomorphism formula*

$$\mathcal{G}(n/\mathbb{Z}_{q-\chi(a)}) = \bigoplus_{d|\omega} \left\{ \frac{\varphi(d)}{o_d(n)} \times Cyc(o_d(n), T_{\nu(n)}) \right\} \tag{5.3.1}$$

where the rooted tree $T_{\nu(n)}$ is defined by

$$\begin{cases} T^0 = \bullet \\ T^k = \langle \nu_k \times T^{k-1} \oplus \bigoplus_{i=1}^{k-1} (\nu_i - \nu_{i+1}) \times T^{i-1} \rangle, 1 \leq i < D \\ T_{\nu(n)} = \langle (\nu_D - 1) \times T^{D-1} \oplus \bigoplus_{i=1}^{D-1} (\nu_i - \nu_{i+1}) \times T^{i-1} \rangle \end{cases} \tag{5.3.2}$$

The following proposition is a direct consequence of Proposition 3.3.7 and Proposition 3.3.9.

Proposition 5.3.2. *If $rad(\nu) \mid rad(n)$ and $\nu(n) = (\nu_1, \nu_2, \ldots, \nu_D)$ the number of vertices of $T_{\nu(n)}$ is given by*

$$\#T_{\nu(n)} = \nu, \tag{5.3.3}$$

and its depth is satisfies

$$depth(T_{\nu(n)}) = depth(\nu(n)) = D. \tag{5.3.4}$$

5.3.2 Formulas for C, T, T_0, N

Let n and $m = \nu\omega$ be positive integers such that $\mathrm{rad}(\nu) \mid \mathrm{rad}(n)$ and $\gcd(n, \omega) = 1$. First, we deduce formulas for $N(n, m)$ the number of connected components of $\mathcal{G}(n/\mathbb{Z}_m)$, $T(n, m)$ the number of periodic points for the n-mapping over $\mathbb{Z}_m$ and for

$$C(n, m) = \frac{1}{m} \sum_{u \in \mathbb{Z}_m} per(u) \quad \text{and} \quad T(n, m) = \frac{1}{m} \sum_{u \in \mathbb{Z}_m} pper(u),$$

where $per(u)$ and $pper(u)$ denote the period (length cycle) and pre-period (length tail) of $u \in \mathbb{Z}_m$ with respect to the n-mapping, respectively.

Proposition 5.3.3. *Let n and $m = \nu\omega$ be positive integers with $rad(\nu) \mid rad(n)$ and $\gcd(n, \omega) = 1$, and let $\nu(n) = (\nu_1, \nu_2, \ldots, \nu_D)$ be the ν-serie associated to n. For the n-mapping over $\mathbb{Z}_m$ we have the following quantities:*

$$N(n, m) = \sum_{d \mid \omega} \frac{\varphi(d)}{o_d(n)}, \quad T_0(n, m) = \omega, \quad C(n, m) = \frac{1}{\omega} \sum_{d \mid \omega} \varphi(d) o_d(n)$$

$$\text{and} \quad T(n, m) = \frac{1}{\nu} \sum_{j=0}^{D-1} \nu_1 \ldots \nu_j.$$

Proof. The formula for $N(n, m)$ is straightforward from Equation (5.3.1) and also the formula for T_0 since $T_0(n, m) = \sum_{d \mid \omega} \frac{\varphi(d)}{o_d(n)} \cdot o_d(n) = \sum_{d \mid \omega} \varphi(d) = \omega$.
Using Equation (5.3.1) and Equation (5.3.3) we obtain:

$$\sum_{u \in \mathbb{Z}_m} per(u) = \sum_{d \mid \omega} \frac{\varphi(d)}{o_d(n)} \cdot o_d(n) \cdot \#T_{\nu(n)} \cdot o_d(n) = \sum_{d \mid \omega} \nu \varphi(d) o_d(n),$$

and dividing by $\nu\omega$ we obtain the formula for $C(n, m)$. If $h(j)$ denote the number of

vertices at depth j in $T_{\nu(n)}$, using Equation (5.3.1) we have

$$\sum_{u\in\mathbb{Z}_m} pper(u) = \sum_{d|\omega} \left\{ \frac{\varphi(d)}{o_d(n)} \cdot o_d(n) \cdot \sum_{j=1}^{D} jh(j) \right\} = \omega \sum_{j=1}^{D} jh(j). \tag{5.3.5}$$

Denoting $h_i(j)$ the number of vertices at depth j in T^i, using Equation (5.3.2) we have

$$\begin{cases} h_0(0) = 1 \text{ and } h_0(j) = 0 \text{ for } j > 0 \\ h_k(j) = \nu_k h_{k-1}(j-1) + \sum_{i=1}^{k-1} (\nu_i - \nu_{i+1}) h_{i-1}(j-1) \text{ for } 1 \leq k \leq D \end{cases}$$

from which we obtain $h_i(j) = \prod_{k=1}^{j} \nu_k$ for $0 \leq j \leq i$. Therefore $h(j) = h_D(j) - h_{D-1}(j-1) = p_j - p_{j-1}$ for $0 \leq j \leq D$, where $p_j = \nu_1\nu_2 \ldots \nu_j$. By partial summation we have $\sum_{j=1}^{D} jh(j) = \sum_{j=1}^{D} j(p_j - p_{j-1}) = D\nu - \sum_{j=0}^{D-1} p_j$ (since $p_D = \nu$). Substituting this in Equation (5.3.5) and dividing both sides by $\nu\omega$ we obtain the desired formula. □

Remark 5.3.4. *Since $\mathcal{G}(x^n/\mathbb{Z}_p^*) \simeq \mathcal{G}(n/\mathbb{Z}_{p-1})$, Theorem 1 of [CS04] is a particular case of Proposition 5.3.3 (taking $m = p-1$, p prime).*

Chapter 6
CONCLUSIONS AND PERSPECTIVES

In this thesis we derive several results on perfect codes in the Lee and Chebyshev metrics and on the cycle structure of Rédei functions. For the two dimensional case we characterize all perfect codes (linear and non-linear) in the p-Lee metric for $p = 1, \infty$. Regarding the Lee metric we prove that there is only one $(2, e, q)$-perfect code up to symmetry and for the Chebyshev metric we obtain a parametrization of the isometry classes and also of the isomorphism classes through certain generalized cosets of $\mathbb{Z}_d$. We approach the classification problem for Chebyshev perfect codes in arbitrary dimensions. Several construction of perfect codes in this metric from codes of smaller dimension and via sections are given. These constructions allow us to extend results obtained in dimension 2 to arbitrary dimensions as well as to derive interesting families of perfect codes (as those in Corollaries 4.3.8 and 4.3.9). We introduce a class of matrices (perfect matrices) which provides generator matrices with a special form for Chebyshev perfect codes. Characterizations of what group isomorphism classes can be represented by (n, e, q)-perfect codes in the two-dimensional case, the maximal case and in the cyclic case are provided. In all the above cases we prove that the set of admissible structures form an ideal in the set of isomorphism classes of abelian groups of order t^n. In the last chapter we characterize the functional graph of Rédei functions, using the dynamic of the n-map over cyclic groups. Results on the cycle decomposition of Rédei permutations and estimates for the period and preperiod of points are derived. A method for constructing Rédei functions with prescribed cycles is also presented. As an application of our structural theorem for Rédei function we obtain estimates for some parameters related to the cyclic structure of some maps.

Potential further problems related to this work are described next. It may be possible, in dimension 2, to extend our results on Lee perfect codes and Chebyshev perfect codes to p-Lee perfect codes for other values of $p \neq 1, \infty$. Another problem closely related to this is to find a p-Lee perfect code which is neither a Lee perfect code nor a Chebyshev perfect code, or prove that such code does not exist (see Conjecture 4.2.50). Regarding Chebyshev perfect codes in arbitrary dimensions, the fact that every linear perfect code is standard (which is consequence of Minkoski-Hajós theorem) guarantee that the permutation associated to a code (Definition 4.4.2) is well defined. It is likely to

be possible to extend some of our results from the linear case to non-linear codes for which the permutation associated to the code is well defined. We can also consider isometries acting on perfect non-linear codes aiming to classify isometry classes and [KP12c, MC03] could be helpful in this sense. In Section 4.4 we obtain a parametrization for linear perfect codes in such a way that isometry classes and isomorphism classes correspond to certain generalized cosets (Theorem 4.2.46), so it would be interesting to obtain an analogous result for higher dimensions (Theorems 4.4.27 and 4.4.29 provide a partial answer for the maximal case). One of the obstacles when we try to generalize this theorem is obtaining a generator matrix for $t^{-1}C$ (see Notation 4.3.5) from a generator matrix for C, where $C \in LPL^{\infty}(n, e, q)$. Other open question is regarding to the description of the (n, e, q)-admissible structures (isomorphism classes that can be represented by a (n, e, q)-perfect code), we prove that this set form an ideal in the graph $\mathcal{G}_n(t)$ of isomorphism classes of abelian groups of order t^n in several cases (in dimension 2, in the maximal case and in the cyclic case) and we wonder if this is always true. In [Kol98], tilings by the notched cube and by the extended cube were considered, it may be possible to extended some of results obtained here for these more general shapes. Regarding iterating Rédei functions, in [BCM10a] a generalization of Rédei function is given. It may be possible to explain the dynamics of such generalization. In particular one could characterize when they give a permutation and in this case, describe their decomposition into disjoint cycles. One could also attempt to extend the characterization of the functional graph associated with the n-map in cyclic groups to more general endomorphism over finite abelian groups. Another natural question is to understand when two functional graphs associated with Rédei functions are isomorphic. A partial answer can be obtained using the results of [Den13] and our remarks in Section 5.2.2 for the case when the second parameters of the Rédei functions are congruent modulo a square. It could be interesting to obtain conditions when the functional graphs associated with $R_n(x, a)$ and $R_m(x, b)$ are isomorphic for the case $\chi(a) \neq \chi(b)$ (over the domain $\mathbb{P}^1(\mathbb{F}_q)$). Finally, as in [Gas14], we could define a tower of field extensions related to Rédei functions and then study how rational primes decompose in such tower of field extensions.

BIBLIOGRAPHY

[AC13] Carina Alves, Sueli Costa. Commutative group codes in $\mathbb{R}^4, \mathbb{R}^6, \mathbb{R}^8$ and $\mathbb{R}^{16}$ - Approaching the bound. *Discrete Mathematics*, 313:1677–1687, 2013.

[AHM09] Bader AlBdaiwi, Peter Horak, and Lorenzo Milazzo. Enumerating and decoding perfect linear Lee codes. *Designs, Codes and Cryptography*, 52(2):155–162, 2009.

[And04] Moreno Andreatta. On group-theoretical methods applied to music: some compositional and implementational aspects. *Perspectives in Mathematical Music Theory*, 2004.

[Ast82] Jaakko Astola. A note on perfect Lee codes over small alphabets. *Discrete Applied Mathematics*, 4(3):227–228, 1982.

[BBV98] Mario Blaum, Jehoshua Bruck, and Alexander Vardy. Interleaving schemes for multidimensional cluster errors. *IEEE Transactions on Information Theory*, 44(2):730–743, 1998.

[BCM10a] Stefano Barbero, Umberto Cerruti, and Nadir Murru. Generalized Rédei rational functions and rational approximations over conics. *Int. J. Pure Appl. Math*, 64(2):305–317, 2010.

[BCM10b] Stefano Barbero, Umberto Cerruti, and Nadir Murru. Solving the Pell equation via Rédei rational functions. *Fibonacci Quarterly*, 48:348–357, 2010.

[BM10] Alexander Barg and Arya Mazumdar. Codes in permutations and error correction for rank modulation. *IEEE Transactions on Information Theory*, 56(7):3158–3165, 2010.

[Car62] L Carlitz. A note on permutation functions over a finite field. *Duke Mathematical Journal*, 29(2):325–332, 1962.

[CCJ+14] Sueli IR Costa, Antonio Campello, Grasiele C Jorge, João Strapasson, and Claudio Qureshi. Codes and lattices in the ℓ_p metric. In *Information Theory and Applications (ITA)*, pages 1–4, 2014.

[CJC+15] Antonio Campello, Grasiele C Jorge, Sueli IR Costa and João Strapasson. Perfect codes in the ℓ_p metric. Preprint arXiv:1506.02517, 2015.

[CMA+04] Sueli IR Costa, Marcelo Muniz, Edson Agustini and Reginaldo Palazzo. Graphs tessellations, and perfect codes on flat tori. *IEEE Transactions on Information Theory*, 50(10):2363–2377, 2004.

[CS90] K Corrádi and S Szabó. A combinatorial approach for Keller's conjecture. *Periodica Mathematica Hungarica*, 21(2):95–100, 1990.

[CS04] Wun-Seng Chou and Igor E Shparlinski. On the cycle structure of repeated exponentiation modulo a prime. *Journal of Number Theory*, 107(2):345–356, 2004.

[CS13] John Horton Conway and Neil James Alexander Sloane. *Sphere packings, lattices and groups*, volume 290. Springer Science & Business Media, 2013.

[Den13] Guixin Deng. Isomorphic digraphs from affine maps of finite cyclic groups. *ISRN Combinatorics*, 2013, 2013.

[SIP07] Mathieu Dutour Sikirić, Yoshiaki Itoh, and Alexei Poyarkov. Cube packings, second moment and holes. *European Journal of Combinatorics*, 28(2007):715–725.

[EVY10] Tuvi Etzion, Alexander Vardy and Eitan Yaakobi. Dense error-correcting codes in the Lee metric. *IEEE Information Theory Workshop*, 2010.

[EVY13] Tuvi Etzion, Alexander Vardy, and Eitan Yaakobi. Coding for the Lee and Manhattan metrics with weighing matrices. *IEEE Transactions on Information Theory*, 59(10):6712–6723, 2013.

[EY09] Tuvi Etzion and Eitan Yaakobi. Error-correction of multidimensional bursts. *IEEE Transactions on Information Theory*, 55(3):961–976, 2009.

[Fra13] John B Fraleigh. *First Course in Abstract Algebra, A: Pearson New International Edition*. Pearson Higher Ed, 2013.

[Gas14] T Alden Gassert. Chebyshev action on finite fields. *Discrete Mathematics*, 315:83–94, 2014.

[GLV00] Robert Gallant, Robert Lambert, and Scott Vanstone. Improving the parallelized Pollard lambda search on anomalous binary curves. *Mathematics of Computation of the American Mathematical Society*, 69(232):1699–1705, 2000.

[GMP98] Sylvain Gravier, Michel Mollard, Charles Payan. On the existence of three-dimensional tiling in the Lee metric. *European Journal of Combinatorics*, 19(1998):567–572.

[Gol69] Solomon Golomb. A general formulation of error matrices (corresp.). *IEEE Transactions on Information Theory*, 15(3):425–426, 1969.

[GW70] Solomon W. Golomb and Lloyd R. Welch. Perfect Codes in the Lee Metric and the Packing of Polyominoes. *SIAM Journal on Applied Mathematics*, 18(2):302–317, 1970.

[GW08a] Domingo Gomez and Arne Winterhof. Multiplicative character sums of recurring sequences with Rédei functions. In *Sequences and Their Applications-SETA 2008*, pages 175–181. Springer, 2008.

[GW08b] Jaime Gutierrez and Arne Winterhof. Exponential sums of nonlinear congruential pseudorandom number generators with Rédei functions. *Finite Fields and Their Applications*, 14(2):410–416, 2008.

[KP08] Peter Horak and Bader AlBdaiwi. Non-periodic Tilings of $\mathbb{R}^n$ by Crosses. *Discrete & Computational Geometry*, 47(1):1–16, 2012.

[Haj42] Georg Hajós. Über einfache und mehrfache Bedeckung des n-dimensionalen Raumes mit einem Würfelgitter. *Mathematische Zeitschrift*, 47(1):427–467, 1942.

[Har20] Godfrey Harold Hardy. *Some famous problems of the theory of numbers and in particular Waring's problem.* Oxford, UK, 1920.

[HG14] Peter Horak and Otokar Grošek. A new approach towards the Golomb–Welch conjecture. *European Journal of Combinatorics*, 38(2014):12–22.

[HH14] Peter Horak and Viliam Hromada. Tiling $\mathbb{R}^5$ by Crosses. *Discrete & Computational Geometry*, 51(2):269–284, 2014.

[Hor09] Peter Horak. On perfect Lee codes. *Discrete Mathematics*, 309(18):5551–5561, 2009.

[Hun03] Thomas W Hungerford. *Algebra.* Springer-Verlag, New York, 2003.

[JCC13] Grasiele C Jorge, Antonio Campello, and Sueli IR Costa. q-ary lattices in the ℓ_p norm and a generalization of the Lee metric. In *International Workshop on Coding and Cryptography*, 2013.

[JMV01] Don Johnson, Alfred Menezes, and Scott Vanstone. The elliptic curve digital signature algorithm (ECDSA). *International Journal of Information Security*, 1(1):36–63, 2001.

[Kel30] O. H. Keller. Über die lückenlose Einfüllung des Raumes mit Würfeln. *J. Reine Angew. Math.*, 163:231–248, 1930.

[Kis13] Andrzej P Kisielewicz. On the structure of cube tilings of $\mathbb{R}^3$ and $\mathbb{R}^4$. *Journal of Combinatorial Theory, Series A*, 120(1):1–10, 2013.

[KLM+13] Sergei V Konyagin, Florian Luca, Bernard Mans, Luke Mathieson, Igor E Shparlinski, and Min Sha. Functional graphs of polynomials over finite fields. *Journal of Combinatorial Theory, Series B* (to appear), preprint arXiv:1307.2718v3, 2013.

[Kol98] Mihail Kolountzakis. Lattice tilings by cubes: whole, notched and extended. *The Electronic Journal of Combinatorics*, 5(1):#14, 1998.

[KP08] Andrzej P Kisielewicz and Krzysztof Przesławski. Polyboxes, cube tilings and rigidity. *Discrete & Computational Geometry*, 40(1):1–30, 2008.

[KP12a] Andrzej P Kisielewicz and Krzysztof Przesławski. The coin exchange problem and the structure of cube tilings. *The Electronic Journal of Combinatorics*, 19(2):#P26, 2012.

[KP12b] Andrzej P Kisielewicz and Krzysztof Przesławski. Rigidity and the chessboard theorem for cube packings. *European Journal of Combinatorics*, 33(6):1113–1119, 2012.

[KP12c] Andrzej P Kisielewicz and Krzysztof Przesławski. The structure of cube tilings under symmetry conditions. *Discrete & Computational Geometry*, 48(3):777–782, 2012.

[Lee58] C. Y. Lee. Some properties of nonbinary error-correcting codes. *IRE Transactions on Information Theory*, 4(2):77–82, 1958.

[Lin82] Jacobus HV Van Lint. *Introduction to Coding Theory (Graduate Texts in Mathematics)*. Springer, 1998.

[LP11] Magdalena ŁYsakowska and Krzysztof PrzesłAwski. On the structure of cube tilings and unextendible systems of cubes in low dimensions. *European Journal of Combinatorics*, 32(2011):1417–1427.

[LS92] Jeffrey C Lagarias and Peter W Shor. Keller's cube-tiling conjecture is false in high dimensions. *Bulletin of the American Mathematical Society*, 27(2):279–283, 1992.

[LS94] Jeffrey C Lagarias and Peter W Shor. Cube-tilings of $\mathbb{R}^n$ and nonlinear codes. *Discrete & computational geometry*, 11:359–391, 1994.

[Mac02] John Mackey. A cube tiling of dimension eight with no facesharing. *Discrete and Computational Geometry*, 28(2):275–279, 2002.

[Mar03] Jacques Martinet. Perfect lattices in Euclidean spaces, volume 327 of Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], 2003.

[MC03] Marcelo Muniz and Sueli IR Costa. Labelings of Lee and Hamming spaces. *Discrete mathematics*, 260(1):119–136, 2003.

[Min07] Hermann Minkowski. *Diophantische approximationen: eine einfü hrung in die zahlentheorie*. Teubner, Leipzig, 1907. Reprint: Physica-Verlag, Würzberg, 1961.

[Moo05] Todd K Moon. *Error correction coding: Mathematical Methods and Algorithms*. Wiley-Interscience, 2005.

[MP12] Andrew MacFie and Daniel Panario. Random mappings with restricted preimages. In *Progress in Cryptology–LATINCRYPT 2012*, pages 254–270. Springer, 2012.

[MP13] Gary L Mullen and Daniel Panario. *Handbook of finite fields*. CRC Press, 2013.

[MR91] John G Michaels and Kenneth H Rosen. *Applications of discrete mathematics*. McGraw-Hill Higher Education, 1991.

[MS78] Florence Jessie MacWilliams and Neil James Alexander Sloane. *The theory of error-correcting codes*. North-Holland, Amsterdam, 1978.

[MW02] Horst Martini and Walter Wenzel. Covering and Packing Problems in Lattices Associated with the n-cube. *European Journal of Combinatorics*, 23(2002):63–75.

[MW07] Wilfried Meidl and Arne Winterhof. On the linear complexity profile of nonlinear congruential pseudorandom number generators with Rédei functions. *Finite Fields and Their Applications*, 13(3):628–634, 2007.

[Nöb85] R Nöbauer. Cryptanalysis of the Rédei scheme. In *Contributions to General Algebra 3: Proceedings of the Vienna Conference*, pages 255–264, 1985.

[Pei08] Chris Peikert. Limits on the Hardness of Lattice Problems in ℓ_p Norms. *computational complexity*, 17(2):300–351, 2008.

[Per40] Oskar Perron. Über lückenlose Ausfüllung des n-dimensionalen Raumes durch kongruente Würfel. *Mathematische Zeitschrift*, 46(1):1–26, 1940.

[PMMnY01] A Peinado, F Montoya, J Muñoz, and AJ Yuste. Maximal periods of $x^2 + c$ in $\mathbb{F}_q$. In *Applied algebra, algebraic algorithms and error-correcting codes*, pages 219–228. Springer, 2001.

[Pos75] Karel A Post. Nonexistence theorems on perfect Lee codes over large alphabets. *Information and Control*, 29(4):369–380, 1975.

[QC13] Claudio Qureshi and Sueli IR Costa. Classificação dos códigos bidimensionais na métrica de Lee (in portuguese). *XXXI Simpósio brasileiro de telecomunicações*, pages 1–5, 2013.

[QC15a] Claudio Qureshi and Sueli IR Costa. Classification of the perfect codes in the infinity-Lee metric. *XXXIII Simpósio brasileiro de telecomunicações*, pages 1–4, 2015.

[QC15b] Claudio Qureshi and Sueli IR Costa. On cube tilings of tori and classification of perfect codes in the maximum metric. Preprint, 2015.

[QP15] Claudio Qureshi and Daniel Panario. Rédei actions on finite fields and multiplication map in cyclic group. *SIAM Journal on Discrete Mathematics*, 29(3):1486–1503, 2015.

[Réd46] Ladislaus Rédei. Über eindeutig umkehrbare polynome in endlichen körpern. *Acta Sci. Math.(Szeged)*, 11:85–92, 1946.

[Rog96] Thomas D Rogers. The graph of the square mapping on the prime fields. *Discrete Mathematics*, 148(1):317–324, 1996.

[RS87] Jason A Rush and NJA Sloane. An improvement to the Minkowski-Hlawka bound for packing superballs. *Mathematika*, 34(1):8–18, 1987.

[RS94] Ron M Roth and Paul H Siegel. Lee-metric BCH codes and their application to constrained and partial-response channels. *IEEE Transactions on Information Theory*, 40(4):1083–1096, 1994.

[Sch94] James H Schmerl. Tiling space with notched cubes. *Discrete Mathematics*, 133(1):225–235, 1994.

[Sch07] Kai-Uwe Schmidt. Complementary sets, generalized Reed–Muller codes, and power control for OFDM. *IEEE Transactions on Information Theory*, 53(2):808–814, 2007.

[Sha48] C. E. Shannon. A Mathematical Theory of Communication. *The Bell system technical journal*, 27:379–423, 1948.

[Sha12] Min Sha. Digraphs from endomorphisms of finite cyclic groups. *Journal of Combinatorial Mathematics and Combinatorial Computing*, 83:105–120, 2012.

[SI10] Mathieu Dutour Sikirić and Yoshiaki Itoh. Combinatorial cube packings in the cube and the torus. *European journal of combinatorics*, 31(2):517–534, 2010.

[SIP07] Mathieu Dutour Sikirić, Yoshiaki Itoh and Alexei Poyarkov. Cube packings, second moment and holes. *European Journal of Combinatorics*, 28(2007):715–725.

[SSP] Amin Sakzad, Mohammad-Reza Sadeghi, and Daniel Panario. Cycle structure of permutation functions over finite fields and their applications. *Advances in Mathematics of Communications*, 6:347-361, 2012.

[Ste90] Sherman Stein. The notched cube tiles $\mathbb{R}^n$. *Discrete Mathematics*, 80(3):335–337, 1990.

[Sza04] Sandor Szabó. *Topics in factorization of abelian groups*. Springer Science & Business Media, 2004.

[Ugo14] S Ugolini. On the iterations of certain maps $x \mapsto k \cdot (x + x^{-1})$ over finite fields of odd characteristic. *Journal of Number Theory*, 142:274–297, 2014.

[Ulr57] Werner Ulrich. Non-binary error correction codes. *Bell System Technical Journal*, 36(6):1341–1387, 1957.

[VS04] Troy Vasiga and Jeffrey Shallit. On the iteration of certain quadratic maps over $GF(p)$. *Discrete Mathematics*, 277(1):219–240, 2004.

[WZ99] Michael J Wiener and Robert J Zuccherato. Faster attacks on elliptic curve cryptosystems. In *Selected Areas in Cryptography*, pages 190–200. Springer, 1999.

[Zam09] Ram Zamir. Lattices are everywhere. In *Information Theory and Applications Workshop, 2009*, pages 392–421. IEEE, 2009.

[Zie13] Michael E Zieve. Permutation polynomials on $\mathbb{F}_q$ induced from Rédei function bijections on subgroups of $\mathbb{F}_q^*$. *Monatshefte fúr Mathematik* (to appear), arXiv preprint arXiv:1310.0776, 2013.

[Zong] C. Zong. What is known about unit cubes. *Bulletin of the American Mathematical Society*, 42(2):181–211, 2005.