ROYAUME DU MAROC
Université Mohammed V - RABAT -
جامعة محمد الخامس – الرباط –
Faculté des sciences
كلية العلوم
CENTRE D'ETUDES DOCTORALES - SCIENCES ET TECHNOLOGIES

N° d'ordre 3691

THESE

En vue de l'obtention du : ***DOCTORAT***

Centre de recherche *: Centre de Recherches Mathématiques et Applications de Rabat*

Structure de Recherche *: Laboratoire Mathématiques, Informatique et Applications – Sécurité de l'Information*

Discipline *: Informatique*

Spécialité *: Théorie des Codes Correcteurs d'erreurs.*

Présentée et soutenue le : 14 /10/2022 par :

Soukaina BELABSSIR

New Families of Linear Error-Block Codes

Devant le Jury

Souad EL BERNOUSSI	PES, Université Mohamed V, Faculté des Sciences- Rabat	Présidente
Malika AIT BEN HADDOU	PES, Université Moulay Ismail, Faculté des Sciences-Meknès	Rapporteur/Examinateur
Mounia MIKRAM	PH, Université Mohamed V, Ecole des Sciences de l'Information-Rabat	Rapporteur/Examinateur
Ali OUADFEL	PES, Université Mohamed V, Faculté des Sciences-Rabat	Rapporteur/Examinateur
Fouad ZINOUN	PES, Université Mohamed V, Faculté des sciences-Rabat	Rapporteur/Examinateur
El Mamoun SOUIDI	PES, Université Mohamed V, Faculté des sciences-Rabat	Directeur de thèse

Année Universitaire : 2021-2022

This thesis is dedicated to my parents for their love, endless support and encouragement.

ACKNOWLEDGMENTS

This Ph.D. thesis was performed within the Laboratory of Mathematics, Computer Sciences and Application-Information Security (Lab MIA-SI), Center of Mathematical Research and Applications of Rabat (CeReMAR), Faculty of Sciences of Mohammed V University in Rabat. The realization of this thesis was only possible due to the several people's collaboration, to which I desire to express my gratefulness.

First of all, I would like to express my sincere gratitude to my supervisor M. **El Mamoun SOUIDI** (PES), Professor at Faculty of Sciences in Rabat, Mohammed V University, for having directed me in the realization of this work with as much rigor and vigilance and for his continuous support. His patience, his pedagogy, his availability, his encouragement and the confidence granted to me, have contributed to a very large extent, has the complete fulfillment of my work and the culmination of this memory thesis. It is for all these beautiful things I thank him very much.

Besides my supervisor, I would like to sincerely thank the rest of my thesis committee:

Mme. **Souad EL BERNOUSSI** (PES), Professor at Faculty of Sciences in Rabat, Mohammed V University. It is an honor for me that she chairs the examining board. I would like to thank her very much for his constant encouragement.

My thanks are also intended for the members of the jury in their capacity as examiner/ rapporteur:

I would like to express my deepest gratitude to Mme **Malika AIT BEN HADDOU**, Professor at Faculty of Sciences in Meknes, Moulay Ismail University in Meknes, for her expertise shared with me.

My sincere thanks also goes to Mme **Mounia MIKRAM**, Professor at the school of science of Information, Mohammed V University, for her encouragement, insightful comments, and hard questions.

I would like to express my deepest appreciation to M. **Ali OUADFEL**, Professor at Faculty of Sciences in Rabat, Mohammed V University, for his intangible support given to me.

I'm extremely grateful to M. **Fouad ZINOUN**, Professor at Faculty of Sciences in Rabat, Mohammed V University, for his inspiration advice and suggestions.

I take this opportunity to thank all the professors, doctorate students and staff of the Department of Mathematics and the Department of Computer Science. I also want to send a special thank to all my colleagues and researchers of Lab MIA-SI, not only for their encouragement and collaboration, but also for their advises and suggestions of the work.

And foremost, I would like to pay best regards and gratefulness to my all time support team, my parents , no words can be enough to thank them.

And praise to God in the beginning and in the end for guiding me in achieving this work.

Résumé

Les codes linéaires en blocs d'erreurs (codes LEB) sont une généralisation des codes correcteurs (aussi dit codes classiques). Ils ont été conçus pour la première fois en 2006 par l'équipe de Feng, pour généraliser les codes classiques puisqu'ils présentent plus d'avantages en matière d'applications en intégration numérique voir Feng *et al* [28]. Cette thèse est une étude de certaines familles de codes LEB. Notamment, les codes LEB parfaits, les codes LEB cycliques, les codes LEB simplexes et les codes LEB de Hamming, ainsi que le produit tensoriel de codes. Dans un premier temps nous vérifions l'existence des familles de codes LEB parfaits. Pour atteindre ce but, nous avons construit un algorithme qui génère des codes LEB vérifiant la borne de Hamming généralisée par l'équipe de Feng, et nous avons ensuite déterminé les paramètres qui assurent l'existence des codes LEB parfaits ayant une distance minimale 3 (au sens de la π-métrique). Dans un deuxième temps, nous avons étudié algébriquement les codes LEB constacycliques, puis nous avons déduit les structures des codes cycliques et négacycliques, et nous avons aussi décrit en détail un algorithme de décodage pour ces codes. En troisième lieu, nous avons généralisé quelques techniques de modification des codes LEB. En quatrième lieu, nous avons défini les codes LEB de Hamming utilisant leur matrice de contrôle et nous avons établi qu'ils sont parfaits. De plus nous avons construit les codes LEB simplexes, et nous avons montré qu'un code LEB est simplex si et seulement s'il est le dual d'un code de Hamming LEB. Nous avons fini par donner la formule des polynômes énnumérateurs de poids pour les codes LEB simplex et de Hamming, ainsi que le polynôme énumérateur de poids des codes LEB générés par la somme directe de deux codes LEB, et nous avons aussi déterminé les distributions de poids pour certains codes LEB. En dernier lieu, nous avons étudié le produit tensoriel de codes LEB dans le but de vérifier et/ou montrer que le produit tensoriel de deux codes classiques génère un code LEB ou génère une structure différente, ou si celui de deux LEB d'une famille donnée donne lieu à un code LEB appartenant à la même famille de codes LEB ou non.

Mots-clés : Codes Linéaires en Blocs d'Erreurs, Codes LEB parfaits, Codes LEB de Hamming, Codes LEB Simplex, Codes LEB Cycliques, Produit Tensoriel, Codes LEB Constacycliques, Codes LEB Négacycliques, Polynôme énumérateur de Poids, Puncturing, Shortening.

Abstract

Linear error-block codes (LEB codes) are a generalization of error correcting codes (also known as classical codes). They were first designed in 2006 by Feng's team, to generalize classical codes since they have more advantages in high-dimensional numerical integration compared to classical codes (see Feng *et al.* for more details). This thesis is a study of some families of LEB codes. In particular, the perfect LEB codes, cyclic LEB codes, simplex LEB codes and Hamming LEB codes, as well as the tensor product of some codes. First, we verify the existence of some families of perfect LEB codes. To achieve this end, we built an algorithm that generates LEB codes verifying the Hamming bound generalized by Feng's team. Then, we have determined the parameters that ensure the existence of perfect LEB codes having a minimum distance 3 (in the sense of π-metric). Secondly, we have studied constacyclic LEB codes algebraically; We have defined the constacyclicity for the LEB codes, then we gave a polynomial representation of a codeword of a constacyclic LEB code. Then, we have defined the product of a codeword with a polynomial of the quotient ring chosen and we have also described in details a decoding algorithm to these codes. Third, we have generalized some techniques of modifying LEB codes. Forth, we have defined the Hamming LEB codes using their control matrix and we have established that they are perfect. Moreover, we have constructed the simplex LEB codes, and we have shown that an LEB code is simplex if and only if it is the dual of a Hamming code LEB. Thereafter, we have given the formula of their weight enumerator polynomials, as well as the weight enumerator polynomial of the LEB codes generated by the direct sum of two LEB codes, and we have also determined the weight distributions for the cosets of an LEB code. Finally, we have studied the tensor product of LEB codes in order to verify and/or show that the tensor product of two classical codes generates an LEB code or generates a different structure, or if that of two LEB of a given family gives rise to an LEB code belonging to the same family of LEB codes or not.

Keywords : Linear Error-Block Codes, Perfect LEB codes, Hamming LEB Codes, Cyclic LEB Codes, Simplex codes, Tensor Product, Constacyclic LEB Codes, Negacyclic LEB Codes, Polynomial Enumerator Weight, Puncturing, Shortening.

Résumé Étendu

Cette thèse, intitulée "New Families of Linear error-block codes", a été préparée au sein du Laboratoire "Mathématiques, Informatique et Applications-Sécurité de l'Information" de la Faculté des Sciences de Rabat, Université Mohammed V - Agdal. Elle traite les codes en blocs d'erreurs qui sont une généralisation, apparue en 2006, des codes correcteurs classiques. Ce travail a fait l'objet de cinq publications (articles), et les résultats y inclus ont été présentés au cours de plusieurs conférences nationales et internationales.

Dans le premier chapitre de cette thèse, nous commençons par définir les notions de composition et de partition d'un nombre entier. Ces notions sont nécessaires pour introduire les codes linéaires en blocs d'erreurs. En effet, considérons une partition d'un nombre entier $n = \sum_{i=1}^{s} n_i$ notée $\pi = [n_1]\,[n_2]\ldots[n_s]$. Soit q une puissance d'un nombre premier et soit $\mathbb{F}_q$ le corps fini à q éléments. Notons $V_\pi = \mathbb{F}_q^{n_1} \oplus \mathbb{F}_q^{n_2} \ldots \oplus \mathbb{F}_q^{n_s}$. Les vecteurs de V_π sont aperçus comme une concaténation de vecteurs $v_i \in \mathbb{F}_q^{n_i}$ pour $i = 1, 2, \ldots, s$. La distance entre deux vecteurs $u = (u_1, u_2, \ldots, u_s)$ et $v = (v_1, v_2, \ldots, v_s)$ de V_π, appelée " π-distance", est donnée par le nombre de leurs sous-vecteurs (blocs) différents:

$$d_\pi(u, v) = \sharp\{i \mid 1 \leq i \leq s, u_i \neq v_i\}.$$

Un code en blocs d'erreurs ("linear error-block code" ou LEB code pour abréviation) est un sous espace vectoriel de V_π, que nous munissons de la π-distance définie ci-dessus. Le paramètre π est appelé "type du code". Les codes linéaires classiques sont la classe particulière des LEB codes de type $\pi = [1]^n$. Après les définitions, nous commençons par la généralisation des principales propriétés des codes linéaires classiques aux LEB codes. Nous passons en revue sur les bornes sur les LEB codes les plus utilisées. Nous commençons par étendre les définitions des rayons d'empilement et de recouvrement au

cas de blocs d'erreurs. Nous étudions leurs propriétés et donnons quelques bornes sur les paramètres des LEB codes. On introduit aussi un rappels sur les codes parfaits et les codes cycliques en bloc d'erreurs.

Le deuxième chapitre est consacré à l'étude des codes LEB parfait, nous avons construit des codes de blocs d'erreur linéaires binaires parfaits avec $d_\pi = 3$ et de types $\pi = [n_1] \dots [n_t][2]^s$ où $n_1 \geq \dots \geq n_t \geq 2$ et $t \geq 1$ et $s \geq 1$ et $\pi = [n_1] \dots [n_t][3]^s$ où $n_1 \geq \dots \geq n_t \geq 3$, $t = 1$ *ou* 2 et $s \geq 1$.

Dans un premier temps, nous avons montré les conditions pour un code binaire LEB de π-distance trois et de type $\pi = [n_1] \dots [n_t][2]^s$ where $n_1 \geq \dots \geq n_t \geq 2$ et $t \geq 1$ et $s \geq 1$ (et respectivement $\pi = [n_1][3]^s$ et $\pi = [n_1][n_2][3]^s$) pour atteindre cette limite. Et ensuite, nous donnons des conditions d'existence de codes LEB binaires parfaits. Par la suite, nous avons montré qu'il existe une famille infinie de codes de type $\pi = [n_1] \dots [n_t][2]s$ où $n_1 \geq \dots \geq n_t \geq 2$, $t \geq 1$ et $s \geq 1$.

Les LEB constacycliques sont minutieusement étudiés dans le troisième chapitre. nous avons défini les codes LEB constacycliques, et nous avons montré que tout code LEB constacyclique est un idéal de $R_{\lambda,\pi} = \frac{\mathbb{F}_q[X]}{X^n - \lambda}$. Ensuite, nous avons défini également le code LEB cyclique et négacyclique. Nous avons également donné une expression explicite des polynômes générateur et de contrôle de ces codes. De plus, nous avons donné une technique de codage aux codes LEB cycliques. Nous avons également généralisé l'algorithme de décodage Meggitt au cas LEB, et nous avons prouvé avec un exemple explicite que le décodeur de type Meggitt est efficace, et contrairement au décodage matriciel standard, même si deux erreurs se sont produites, nous pouvons toujours déterminer l'original vecteur avec certitude.

Dans le quatrième chapitre, nous avons introduit les notions de poinçonnage et de raccourcissement des codes LEB, et défini les propriétés des codes poinçonnés et raccourcis. Nous avons également trouvé une relation entre ces nouveaux codes LEB construits.

Dans le cinquième chapitre, nous avons construit de grandes familles de codes de Hamming de types $\pi = [m]^{\frac{q^r-1}{q^m-1}}$ et $\pi = [l][m]^{\frac{q^r-1}{q^m-1}}$ en utilisant leur matrice de contrôle de parité. Nous avons montré que les codes LEB de Hamming sont parfaits et avons donné des conditions aux codes parfaits construits pour être des codes de Hamming. Nous avons également donné des conditions d'existence des codes simplex. Puis nous avons montré que le dual d'un code LEB de Hamming de types $\pi = [m]^{\frac{q^r-1}{q^m-1}}$ est un code LEB Simplexe, cependant, le dual d'un code LEB de Hamming de type $\pi = [l][m]^{\frac{q^r-1}{q^m-1}}$ n'est pas un

code simplex, ce qui signifie que le dual d'un code Hamming LEB n'est pas un code LEB simplex en général.

Dans le sixième chapitre, nous avons cherché à étendre la notion d'énumérateur de π-poids au cas LEB, définir ses propriétés et déterminer la distribution de π-poids de certaines familles de codes LEB.

Tout d'abord, grâce à l'identité de MacWilliams, nous avons donné une formule simple au polynôme énumérateur π-poids des codes Hamming et LEB simplex.

Deuxièmement, nous avons étudié la notion d'énumérateur de π-poids pour les cosets d'un code LEB, et nous avons prouvé que certains cosets ont des distributions déterminées de manière unique. Nous avons également prouvé que lorsque la distribution des poids des cosets est connue, et que la dimension du code LEB est augmentée de un, le nouveau π-poids résultant est explicitement déterminé.

Troisièmement, nous avons montré que l'énumérateur de poids π du code obtenu à partir de la somme directe de deux codes LEB est la multiplication des énumérateurs de π-poids respectifs de ces deux codes.

Enfin, nous avons étudié la π-distribution des codes LEB poinçonnés et raccourcis.

Dans le septième chapitre, nous avons exploré les différentes possibilités en utilisant le produit tensoriel et les codes LEB, nous avons présenté deux constructions différentes de codes LEB utilisant le produit tensoriel. Nous avons montré que le produit tensoriel de deux codes LEB est un code LEB. Par ailleurs, nous avons montré que le produit tensoriel de deux codes LEB cycliques est un code LEB cyclique et que le produit tensoriel de deux codes LEB Simplex est également un code LEB simplex.

La recherche présentée dans cette thèse donne un aperçu algébrique de certaines familles particulières de codes LEB, et une construction intéressante de nouvelles familles de codes LEB. À cette fin, nous avons présenté une étude de certains résultats existants sur les codes linéaires à blocs d'erreurs, y compris de nouveaux résultats que nous avons introduits par nos publications.

Les travaux précédents dans la littérature évoquaient des résultats théoriques et quelques applications dans d'autres domaines comme la cryptographie et la sécurité de l'information. Le manque de résultats côté application est dû à l'insuffisance des résultats théoriques et surtout algébriques sur les codes LEB. D'où la motivation de cette étude.

LIST OF PUBLICATIONS

1. **S. Belabssir**, N. Sahllal, E. M. Souidi. Cyclic linear error-block codes, ***2nd international conference on applied mathematics, ICAM'2018***, AIP Conference Proceedings 2074, 020005 (2019); https://doi.org/10.1063/1.5090622.

2. **S. Belabssir**, E. B. Ayebie, E. M. Souidi. Perfect, Hamming and Simplex Linear Error-Block Codes with Minimum π-distance 3. Vol 11445 of **Lecture Notes in Computer Science**, Springer, 2019, pages 288–306; https://doi.org/10.1007/978-3-030-16458-4_17.

3. **S. Belabssir**, Nadir Sahlal. Tensor Product And Linear Error Block Codes, ***IAENG International Journal of Applied Mathematics***, pages 279-283, 51, 2021.

4. **S. Belabssir**, The Weight enumerator of Some Families of Linear Error-Block Codes. ***IAENG International Journal of Computer Science***, vol. 49, no. 3, pp728-735, 2022

5. **S. Belabssir**, E. M. Souidi. Constacyclic Linear Error-Block Codes, Submitted and accepted under conditions in ***IAENG Letters***.

CONTENTS

1

INTRODUCTION

Table Contents

1 Coding Theory

Coding theory is a fascinating field combining elegant mathematical theories with constructions of a major practical impact like error correcting codes, secrecy codes and codes used in data compression and other fields. It is most commonly used in communication systems, and it has been developed and engineered as one of inevitable release of communication, namely noise. Noise is always a major part of the communication that will keep on interfering and corrupting data. It can come from a lot of number of sources such as background sound of machine or people, radio disturbances, poor typing, lighting, poor hearing etc. Coding theory is divided into main branches named as source coding and channel coding. Source coding studies information measurement and its conversion into different forms, and Channel coding studies how much information a channel can transfer without error. Coding theory owes it origins to two roughly concurrent seminal works by Hamming [31] and Shannon [54] in the late of 1940s. It covers the study of two related,

but distinguishable, topics: The theory of "error correcting codes" and the mathematics behind "reliable communication in the presence of noise", and have a wide range of theoretical and practical applications from digital data transmission to modern medical research and code-based cryptography which is quantum-computer resistant. Coding theory aims to provide secure transmission of messages, in the sense that errors occurred during the transmission can be corrected. However, a redundancy of the transmitted data must be paid as a price to this capability.

In 1948, Shannon [54] wrote a detailed treatise on the mathematics behind communication, His paper "A Mathematical Theory of Communication" marks the beginning of the "Information Theory", part of which is coding theory. He installed the theoretical constructions of coding theory. He has demonstrated the existence of "good codes" without showing them. His proof was probabilistic and existential, not constructive. Constructing and implementing efficient codes stayed a big challenge for a long time. Hamming, motivated by the task of correcting small number of errors on magnetic storage media, wrote in 1950 the first paper entitled "Error detecting and correcting codes" inducing error-correcting codes [31]. He was studying devices to store information and wanted to design simple schemes to protect from the corruption of a small number of bits. Hamming realized the explicit need to consider sets of words or "codewords" where every pair differs in a large number of coordinates. He has also defined notion of the Hamming distance to be the distance between two elements over finite alphabets, and showed that this was a metric. Hamming also explicitly showed a family of codes that achieved nontrivial distance, and announcing by this work the birth of the theory of error-correcting codes. While Hamming's codes were a great advancement, they have some undesirable properties. First of all, they were not very efficient, requiring three check bits for every four data bits. Second, they only have the ability to correct a single error within a block. These problems were addressed by Marcel Golay [30], who generalized Hamming's construction. In the process, Golay discovered two very remarkable codes. The first one, is the binary Golay code, groups data into blocks of twelve bits and then calculates eleven check bits. The associated decoding algorithm is capable of correcting up

to three errors in the 23 bit code word. The second code is the ternary Golay code, which operates on ternary, rather than binary numbers. The ternary Golay code protects blocks of 6 ternary symbols with 5 ternary check symbols and has the capability to correct two errors in the resulting 11 symbol code word. Since error correcting block codes were first introduced, many new classes of block codes have been discovered and many applications have been found for these codes. As an example, the binary Golay code provided error control during the Jupiter fly-by of Voyager I [59]. However, Golay codes have been replaced in most current communication applications by more powerful codes. In 1954, Reed Muller (RM) [43] discovered and described the next main class of linear block codes, and then proposed the associated decoding algorithm[52]. RM codes sow extensive applications between 1969 and 1977 in the mariner missions to Mars, which used a ($field:\ q = 2,\ lenght\ n = 32,\ dimension\ k = 6,\ correction\ capacity\ t = 7$) RM code[59].

After the discovery of RM codes, came the discovery of cyclic codes, which were first discussed in 1957 by Prange of the Air Force Cambridge Research Center [51]. Cyclic codes are linear block codes that possess the additional property that any cyclic shift of a code word is also a codeword. The cyclic property adds a considerable amount of structure to the code, which can be exploited by reduced complexity encoders and reduced complexity decoders. Another benefit of cyclic codes is that they can be compactly specified by a polynomial of degree $n - k$, called the generator polynomial. Cyclic codes are also called cyclic redundancy check (CRC) codes, and can be decoded using different decoders like the Meggitt decoder [42]. Meggitt decoders have a complexity that increases exponentially with the number of correctable errors t, and are typically only used to correct single and double bit errors. For this reason, CRC codes are primarily used today for error detection applications rather than for error correction.

In 1959, an important subclass of the cyclic codes was discovered almost simultaneously by Hocquenghem [33] and by the team of Bose and Ray-Chaudhuri [15]. These codes are called BCH codes, and have length $n = q^{m-1}$, where m is an integer valued

design parameter. The number of errors that the binary ($q = 2$) BCH code can correct is at least $t = (n - k)/m$ but for some BCH codes it is more. And after this period a large number of papers defined both new families of codes and different applications of linear codes in other fields were appeared.

2 Linear Error-Block Codes

Linear error-block codes or LEB codes for abbreviation, were introduced by Feng, Xu and Hickernell in 2006 [28] to be a generalization of classical linear error correcting codes. Feng *et al.* [28] have claimed that LEB codes have application in experimental design since they yield mixed-level orthogonal arrays, and in high-dimensional numerical integration.

Let n be a positive integer, the space $\mathbb{F}_q^n$ can be viewed as a direct sum of spaces $\mathbb{F}_q^{n_i}$ where $i = 1, 2, \ldots, s$ are non null positive integers satisfying $n = \sum_{i=1}^{s} n_i$ and $n_1 \geq n_2 \geq \ldots \geq n_s \geq 1$. Each vector in $\mathbb{F}_q^n$ can be considred as a concatenation of s blocks $u = (u_1, u_2, \ldots, u_s)$ where $u_i \in \mathbb{F}_q^{n_i}$. Any change that happens inside a block causes a single error in the vector regardless to its magnitude. An LEB code is a linear subspace of $\mathbb{F}_q^n$ endowed with the metric that measures the number of distinct blocks. This metric, clearly related to the integers n_i (lengths of blocks), is called the π-metric where π is the partition of n noted $\pi = [n_1][n_2]\ldots[n_s]$ and called the type of the code. A classical linear error correcting code is a linear error-block code for which $n_i = 1$ for $i = 1, \ldots, s$.

The first publication talking about LEB codes [28] is aimed to determine optimal codes, where the authors have defined the Hamming and Singleton-like bounds for LEB codes, and have given specific constructions of some perfect and MDS codes. In its concluding section, a few open problems were stated. Starting from those problems, in [36], Ling and Özbudak obtained new bounds on the parameters of LEB codes and gave new constructions. Namely, they have presented a Gilbert-Varshamov type construction. Using their bounds and constructions they introduced some infinite families of optimal LEB codes over $\mathbb{F}_2$. They also studied the asymptotic behaviour of LEB codes. R. Dariti

et al. have also interested to resolve some of this problems. In [23], they have introduced cyclic and quasi cyclic LEB codes with fast decoding algorithms. The topic of perfect codes is an interesting topic in the theory of error-correcting codes. Perfect codes correct every word within the space. The Golay codes, the Hamming codes and the repetition codes of odd length are shown in [56, 62] to be the unique existing perfect code in the classical case. In [25], besides to the classical codes mentioned above, which are also perfect LEB codes, Dariti *et al.* introduced new families of perfect LEB codes. They have given a characterization of perfect LEB codes of minimum π-distance 3 and 4, and found parameters of perfect LEB codes of minimum π-distance 5 for which the existence is not yet discussed. They have realized that of the introduced codes are also MDS codes.

Determining optimal codes is so far a subject of research on LEB codes. In [57], optimal linear error-block codes were investigated in two directions: maximal dimension codes and maximal minimum π-distance codes. First perspective on optimizing a code is by studying lower bounds and upper bounds on the dimension of a code. Various bounds were developed providing tools used in obtaining more efficient codes which in some cases lead to optimal codes. The latter approach is by modifying suitable existing LEB codes. In [26], the authors have generalized some results on the packing and the covering radii to the error-block case. They have studied the properties of a LEB code when it undergoes some specific modifications and combinations with another code. They have given some bounds on the packing and the covering radii of these codes. They may also be used in cryptography as was done with the classical error correcting codes by McEliece (1978) and Niederreiter (1986). The McEliece cryptosystem is an asymmetric encryption algorithm developed in 1978 by Robert McEliece. It was the first such scheme to use randomization in the encryption process[39]. The algorithm is based on the hardness of decoding a general linear code [58]. For a description of the private key, an error-correcting code is selected for which an efficient decoding algorithm is known, and which is able to correct t errors. The original algorithm uses binary Goppa codes; these codes can be efficiently decoded, thanks to an algorithm due to Patterson [46]. The public key is derived from the private key by disguising the selected code as a general linear code. For this, the code's generator matrix

G is perturbated by two randomly selected invertible matrices S and P. McEliece with Goppa codes has resisted to cryptanalysis so far. The most effective attacks known use information-set decoding algorithms. A 2008 paper describes both an attack and a fix [21]. Another paper shows that for quantum computing, key sizes must be increased by a factor of four due to improvements in information set decoding [14]. The McEliece cryptosystem has some advantages over, for example, RSA. The encryption and decryption are faster. For a long time, it was thought that McEliece could not be used to produce signatures. However, a signature scheme can be constructed based on the Niederreiter scheme, the dual variant of the McEliece scheme. One of the main disadvantages of McEliece is that the private and public keys are large matrices. For a standard selection of parameters, the public key is 512 kilobits long [1]. In order to allow application in cryptography, especially in a McEliece-like cryptosystem, Dariti *et al.* [23] presented a method for decoding linear error-block codes inspired from the standard array classical method. The same authors presented in [22] some solutions on the use of LEB codes in codes-based cryptosystems, namely, the McEliece-like and Niederreiter cryptosystems, and realized that this solutions keep the size of the public key unchanged while it preserves, or even enhance, security parameters of the cryptosystem. They also used LEB codes in CFS signature scheme [22], and discovered that the use of LEB codes in CFS signature provide an improvement in the matter of density of decodable words with the π-metric, which will be grater. In the same work [22], a channel model which enables LEB codes to be used in correcting errors raised from transmission over a noisy channel was designed.

LEB codes have application in the field of steganography, where Dariti and Souidi [27] have introduced a protocol of steganography based on LEB codes. They have shown that employing convenient codes enhances the reliability of that protocol compared to other known steganography protocols. This steganographic protocol generalizes the idea of matrix encoding to be used with several bit planes. The scheme was ameliorated in [24].

3 Problematic and Contribution

Problematic

Since their appearance in 2006, many publications on the subject of LEB codes have appeared. The aim of this publications is to generalize existing families in the area of classical codes to the LEB case, this allows or improves their application in cryptography or information security. Perfect, MDS, Cyclic, quasi-cyclic, and algebraic-geometric LEB codes are the families which have been introduced until the beginning of our study. Furthermore, the characterization of perfect LEB codes was done, but either and the non-existence of some Perfect LEB codes were not formally studied. Also Cyclic and Quasi-Cyclic LEB codes have been introduced, however, an algebraic study of these codes have not been established. This thesis is a theoretical study of many families of codes. It first gives a study of the existence of some LEB perfect codes, then an algebraic representation of LEB constacyclic codes, and introduces further some families of LEB codes, namely Hamming and simplex LEB codes, punctured, shortned LEB codes and also tensor product of codes.

Our Contribution

This thesis has the following structure.

In chapter 1: We introduce the concept of linear error-block codes and give their essential properties.

In chapter 2 : We aimed to characterize perfect binary linear error-block codes with $d_\pi = 3$ and types $\pi = [n_1] \dots [n_t][2]^s$ where $n_1 \geq \dots \geq n_t \geq 2$ and $t \geq 1$ and $s \geq 1$ and $\pi = [n_1] \dots [n_t][3]^s$ where $n_1 \geq \dots \geq n_t \geq 3,\ t = 1$ or 2 and $s \geq 1$.

Firstly, we have showed the conditions for a binary LEB code with π-distance three and type $\pi = [n_1] \dots [n_t][2]^s$ where $n_1 \geq \dots \geq n_t > 2$, $t \geq 1$ and $s \geq 1$ (and respectively

$\pi = [n_1][3]^s$ and $\pi = [n_1][n_2][3]^s$) to be perfect. In a second time we give the case where it is impossible to construct this type of perfect binary LEB codes. Then we have shown that there exists an infinite family of codes of type $\pi = [n_1] \dots [n_t][2]^s$ where $n_1 \geq \dots \geq n_t > 2,\ t \geq 1$ and $s \geq 1$.

In chapter 3: We have generalized the notion of constacyclic code to the linear error block (LEB) code case. Furthermore, we have described an algorithm to decode this new family of LEB code. We have generalized this notion to the LEB case, we have reviewed the family of π-cyclic codes, and we have given with details a decoding algorithm to this later. We have also introduced the notion of π-negacyclic codes.

In chapter 4: We have generalized the notion of puncturing an error correcting code, and then defined different characteristics of a puncturing LEB code. We have also defined shortened LEB codes and the give an interesting result which relay punctured LEB codes to shortened LEB code.

In chapter 5: We have defined Hamming and simplex codes. Large families of Hamming codes of types $\pi = [m]^{\frac{q^r-1}{q^m-1}}$ and $\pi = [l][m]^{\frac{q^r-q^l}{q^m-1}}$ where $l > m$ are constructed using their parity check matrix. Conditions of existence of simplex codes are given. We have showed that a Linear error-block code is simplex if and only if it is the dual of a Hamming code of type $\pi = [m]^{\frac{q^r-1}{q^m-1}}$.

In chapter 6: We have defined the notion of π-weight enumerator polynomial and we have given its properties, then we have given a simple formula for the π-weight enumerator polynomial of both Hamming and simplex codes. We have also studies the π-weight enumerator polynomial for the cosets of an LEB code, and also for the direct sum between two LEB codes.

In chapter 7: We have introduced the notion of tensor codes. We have explored the different possibilities using tensor product and LEB codes, we have presented two different constructions of LEB codes using tensor product. We have shown that the tensor product of two block codes is not an LEB code and that the tensor product of two Hamming codes

is in general not a perfect Hamming code. Besides, we have shown that the tensor product of two cyclic LEB codes is a cyclic LEB code and the tensor product of two Simplex LEB codes is also a simplex LEB code.

We conclude our thesis by a conclusion and some perspectives.

CHAPTER

1 LINEAR ERROR-BLOCK CODES

Table Contents

In this chapter we give an overview on linear error-block codes. We start by defining the LEB codes and give some of their properties. Next, we study several lower and upper bounds for the dimension and the $\pi-$distance, along with other bounds that are involved

by these parameters. Then, we revisit known and particular codes, namely perfect, cyclic and quasi-cyclic LEB codes.

1.1 Linear Error-block Codes

1.1.1 Partition and $\pi-$Metric

Definition 1.1.1. *A composition $\pi = [n_1]\dots[n_s]$ of a positive integer n is given by $n = n_1+\dots+n_s$ where $s, n_1, \dots, n_s$ are integers ≥ 1. A partition π of a positive integer n, is a sequence of nonnegative integers denoted by $\pi = [n_1][n_2]\dots[n_s]$, where s is an integer ≥ 1, and*

$$n = n_1 + n_2 + \dots + n_s \tag{1.1}$$

with $n_1 \geq n_2 \geq \dots \geq n_s \geq 1$.

If $n = \sum_{i=1}^{s} n_i = l_1m_1 + l_2m_2 + \dots + l_rm_r$ where $m_1 > m_2 > \dots > m_r \geq 1$, then π will be denoted by $\pi = [m_1]^{l_1}[m_2]^{l_2}\dots[m_r]^{l_r}$. The summands are called parts of the partition.

The set of all partitions of an integer n is denoted by $\prod_n$, and the number of partitions of n is a function denoted by $p(n)$. We take $p(n) = 0$ for all negative values of n and $p(0) = 1$ and we have

n	1	2	3	4	5	6	7	8	9	10
$p(n)$	1	2	3	5	7	11	15	22	30	42

Example 1.1.2. *The partitions of the integer 4 are*

$4 = 1+1+1+1;\ \pi_1 = [1][1][1][1]$, *then* $\pi_1 = [1]^4$

$4 = 2+1+1;\ \pi_2 = [2][1][1]$, *then* $\pi_2 = [2][1]^2$

$4 = 2+2;\ \pi_3 = [2][2]$, *then* $\pi_1 = [2]^2$

$4 = 3 + 1;\ \pi_4 = [3][1]$

$4 = 4;\ \pi_5 = [4]$ *Therefore,* $p(4) = 5$.

The problem of partitioning was first opened in 1674 when Leibniz asked Bernoulli in a letter about the number of "divulsion" of integers, which means the number of partitions of integers. Leibniz partitioned integers up till 6, and he suggested that the number $p(n)$ of partitions of any number would always be prime, which is wrong since 7 has 15 partitions.

In 1741, Euler produced the first publication [34] on partition integers where he gave a presentation on partitions. In [3], Euler discovered a number of theorems in the field of integers partitioning. E. Claude *et al.* showed in [17] that the number of partitions of a positive integer n into odd parts equals the number of partitions of n into distinct parts where odd parts mean partitions of n which comprises odd numbers only and distinct parts of n are partitions of n which contains no repeated numbers. In $1854 - 1929$, Percy Alexander MacMahon, a major in the British Royal Artillery and a master calculator, computed the values of $p(n)$ for all n up to 200. He found that $p(200) = 3972999029388$, and he did not count the partitions one-by-one: $200 = 199 + 1 = 198 + 2 = 198 + 1 + 1 = 197 + 3 = \ldots\ldots$

Srinivasa Ramanujan [1887−1920] found with Godfrey Harold Hardy a non-convergent asymptotic series that permit exact computation of the number of partitions of an integer [32]. After this dates, several papers on number partitioned were published. See [2, 5–9, 16, 19, 20, 29, 38, 45, 55, 60] for more details.

Definition 1.1.3. *Let* $\pi_1 = [n_1] \ldots [n_{s_1}]$ *and* $\pi_2 = [m_1] \ldots [m_{s_2}]$ *be partitions of two integers* n *and* m. *We note the concatenation of the partitions* π_1 *and* π_2 *by* $\pi = \pi_1\pi_2$. *It is the composition of* $n + m$ *given by*

$$\pi = \pi_1\pi_2 = [n_1] \ldots [n_{s_1}][m_1] \ldots [m_{s_2}]$$

Definition 1.1.4. *Let* n *be a positive integer, and* $\pi_1 = [n_1] \ldots [n_{s_1}]$ *and* $\pi_2 = [m_1] \ldots [m_{s_2}]$

be two elements of $\prod_n$ *the set of all partitions of the integer* n*. A partial order relation* " $\prec$ " *between* $\pi_1 = [n_1]\dots[n_{s_1}]$ *and* $\pi_2 = [m_1]\dots[m_{s_2}]$ *can be defined as follows* $\pi_1 \prec \pi_2$ *if and only if for all* $i = 1, 2, \dots, s_2$ *their exist* $(l_i)_{0\leq s_2}$ *such that* $m_i = \sum_{j=l_{i-1}+1}^{l_i} n_j$ *with* $l_0 = 0$ *and* $l_{s_2} = s$

i.e. each part of π_2 *is the concatenation of one or more parts of* π_1*.*

Proposition 1.1.5. *[22] Let* n *be a positive integer. We have*

- *For all* $\pi \in \prod_n$ *we have* $[1]^n \prec \pi \prec [n]$ *.*
- *If* $\pi_1 \prec \pi_2$ *then* $s_1 \prec s_2$*.*

1.1.2 Definition and Properties

Let $\pi = [n_1]\dots[n_s]$ $(s \geq 1)$ be a partition of the integer n, $\mathbb{F}_q$ the finite field of q (q is a prime power) elements,

$$V_i = \mathbb{F}_q^{n_i} (1 \leq i \leq s) \tag{1.2}$$

and the direct sum

$$V = V_1 \oplus V_2 \oplus \dots \oplus V_s \simeq \mathbb{F}_q^n. \tag{1.3}$$

Each vector in V can be written uniquely as $v = (v_1, v_2, \dots, v_s)$, where v_i is in V_i ($for\ 1 \leq i \leq s$). For $u = (u_1, u_2, \dots, u_s)$ and $v = (v_1, v_2, \dots, v_s)$ in V, the π-weight $w_\pi(u)$ and respectively the π-distance $d_\pi(u, v)$ are defined by:

$$w_\pi(u) = \#\{i/1 \leq i \leq s,\ 0 \neq u_i \in V_i\} \tag{1.4}$$

and

$$d_\pi(u, v) = w_\pi(u - v) = \#\{i/1 \leq i \leq s,\ u_i,\ v_i \in V_i \text{ and } u_i \neq v_i\}. \tag{1.5}$$

Remark 1.1.6. If $\pi_1 \prec \pi_2$, then $d_{\pi_1} \prec d_{\pi_2}$.

Definition 1.1.7. *Let* n *be a positive integer and let* π *be a partition of* n*. A linear error-block code (LEB code for short) over* $\mathbb{F}_q$ *of type* π *is an* $\mathbb{F}_q$*-linear subspace* C *of* V *defined*

by (1.3). The integer n is called the length of C, $k = dim_{\mathbb{F}_q} C$ is its dimension and

$$d_\pi = \min\{d_\pi(c, c')/c, c' \in C, c \neq c'\} = \min\{w_\pi(c)/0 \neq c \in C\}, \tag{1.6}$$

is its minimal π-distance. Such LEB code is denoted by $[n, k, d_\pi]_q$ code.

Remark 1.1.8. Linear error-block codes (LEB) are a generalization of classical codes. In fact, classical linear error-correcting code is a linear error-block code of type $\pi = [1]^n$.

Proposition 1.1.9. *Let C be an LEB code of type π with minimum $\pi-$distance d. Then there exists a codeword c for which $w_\pi(c) = d$.*

Proof. Let C be an LEB code of type π with minimum $\pi-$distance d, then their exist two codewords u and v such that $d_\pi(u, v) = d$. Take $c = u - v$, then c is a codeword in C and we have $w_\pi(c) = d_\pi(u - v) = d$. □

Example 1.1.10. *Let π be the partition $\pi = [3][2]^2[1]$. The code defined by*

$$C = \{000 \mid 00 \mid 00 \mid 0, 110 \mid 01 \mid 10 \mid 0, 100 \mid 10 \mid 00 \mid 1, 010 \mid 11 \mid 10 \mid 1\}$$

is an $[8, 2, 3]$ LEB code of type π. Consider C' as the same code but with type $\pi' = [2]^4$, then its minimum $\pi'-$distance is 2.

1.1.3 Matrix Representation

Definition 1.1.11. *A generator matrix of an $[n, k]$ LEB code, regardless of its type, is a $k \times n$ matrix whose rows form a basis of the code in $\mathbb{F}_q^n$.*

Before going further, note that there are two possible ways to define the orthogonality of two vectors in V, as shown in Definition 1.1.12.

Definition 1.1.12. *Let $\pi = [n_1] \dots [n_s]$ be a partition of a positive integer n and C an LEB code of type π and $u = (u_1, \dots, u_s)$ and $v = (v_1, \dots, v_s)$ in C. We say that u and v are*

strongly orthogonal if

$$u_i.v_i = 0 \ for \ all \ i = 1, \ldots, s \tag{1.7}$$

and we say that u and v are orthogonal if

$$\sum_{i=1}^{s} u_i.v_i = 0 \tag{1.8}$$

where $u_i.v_i$ denotes the classical scalar product in $V_i = \mathbb{F}_q^{n_i}$.

Equation (1.7) is a strong condition of orthogonality. Obviously, the strong orthogonality implies the orthogonality. We use (1.8) to specify the orthogonality in V as defined by (1.3) above.

Definition 1.1.13. *A parity-check matrix of an $[n, k]$ code, regardless of its type, is an $(n-k) \times n$ matrix whose rows are linearly independent and are orthogonal with the code.*

Proposition 1.1.14. *Let C be an $[n, k]$ LEB code where G and H are respectively its generator matrix and its parity check matrix, then C is completely defined by G or H respectively with the following equations:*

$$C = \{aG / a \in \mathbb{F}_q^n\} \tag{1.9}$$

$$c \in C \Leftrightarrow Hc^T = 0^T \tag{1.10}$$

where c^T denotes the transpose of c.

Remark 1.1.15. Let C be an $[n, k]$ LEB code of type $\pi = [n_1][n_2]\ldots[n_s]$, (with s is an integer ≥ 1, $n = n_1 + n_2 + \ldots + n_s$ and $n_1 \geq n_2 \geq \ldots \geq n_s \geq 1$) where G and H are respectively its generator and parity check matrix, then

- A generator matrix G can be viewed in a block form corresponding to the code type π as $G = [G_1 G_2 \ldots G_s]$, where G_i is the i^{th} block of G of size $k \times n_i$.

- A generator matrix is not unique.
- A parity-check matrix H can be defined in a block form corresponding to the code type π as $H = [H_1 H_2 \dots H_s]$, where H_i is the i^{th} block of G of size $(n-k) \times n_i$.
- We have $HG^T = 0$
- Unlike classical codes, generally, a generator matrix of an LEB code cannot always be written in the standard form $(I_k|A)$, but if it could, a parity-check matrix would be given by $H = (-A^T|I_{n-k})$, where I_k is the $k \times k$ identity matrix.

Definition 1.1.16. *Let C be an $[n,k]$ code of type $\pi = [n_1][n_2]\dots[n_s]$, whose generator matrix is G and whose parity-check matrix is H, the dual of C is an $[n, n-k]$ code of type $\pi = [n_1][n_2]\dots[n_s]$, whose generator matrix is H and whose parity-check matrix is G, and is denoted by $C^\perp = \{u.H/u \in \mathbb{F}_q^n\}$.*

As in the classical case, the minimum π-distance of a linear error-block code is straightforwardly determined using a parity-check matrix as follows:

Theorem 1.1.17 ([28])**.** *Let $H = [H_1, H_2, \dots, H_s]$ be a parity-check matrix of an $[n,k,d_\pi]$ code C over $\mathbb{F}_q$ of type $\pi = [n_1][n_2]\dots[n_s]$. Then the minimum π-distance is d_π if and only if the union of columns of any $d_\pi - 1$ blocks of H are $\mathbb{F}_q$-linearly independent and there exist d_π blocks columns of H which are linearly dependent.*

Example 1.1.18. *Let C be a $[7,2,2]$ binary code of type $\pi = [3][2][1]^2$ over $\mathbb{F}_2$ defined as follows:*

$$C = \{000|00|0|0, 101|10|1|0, 011|11|0|0, 110|01|1|0\}.$$

Then C is generated by the matrix

$$G = \left(\begin{array}{ccc|cc|c|c} 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 \end{array}\right).$$

1.2 Bounds on LEB Codes

1.2.1 Packing and Covering Radii of LEB Codes

When the parameters n and π are fixed, one would like to maximize both the dimension k which measures the size of the set of codewords and the minimum π-distance d which indicates its error-correction capacity. Unfortunately, it is impossible since they work in opposite direction. Therein, an optimal code means a code with maximum dimension or maximum π-distance.

The packing and covering radius are two characteristics of LEB codes of fundamental importance and that are directly relied to the minimum π-distance and the dimension. Consequently, another optimality criterion is to have a large packing radius and a small covering radius. The packing and covering of LEB codes are studied by Dariti *and al.* in [26],

Definition 1.2.1. *(The π-covering radius) Let C be a linear error-block code over V of type π where π is a partition of a positive integer n. The π-covering radius of C is the smallest integer ρ_π such that every element of V is contained in at least one ball of radius ρ_π centered at each codeword of C where*

$$\rho_\pi = max\{d_\pi(x, c),\ c \in C,\ x \in V\}$$

Definition 1.2.2. *(The π-Packing) Let C be a linear error-block code over V of type π, where π is a partition of a positive integer n. The π-packing radius of C is the largest integer t_π such that the set of balls of radius t_π centered at each codeword of C are pairwise disjoint. In other words, the π-packing radius of C is the biggest integer t_π such that any vector of the space is within π-distance up to t_π from at most one codeword.*

$$t_\pi = max\{r \geq 0 \text{ satisfying } \forall x \in V, \exists c \in C / d_\pi(c, x) \leq r\}$$

Proposition 1.2.3. *[26] Let C be an $[n, k, d_\pi]$ linear error-block code over V_π of type π and*

respectively π-packing and π-covering radius t_π and ρ_π. We have

(i) The code C corrects all errors of π-weight $\leq t_\pi$

(ii) The π-packing radius of C equals

$$t_\pi = [(d_\pi - 1)/2] \tag{1.11}$$

(iii) if $\pi \leq \pi'$ then $t_\pi \leq t_{\pi'}$ and $\rho_\pi \leq \rho_{\pi'}$.

(iv) $t_\pi \leq \rho_\pi$

Proof. [26]

1. If a received word x contains t_π errors or less, then there exists a unique codeword c such that the ball of radius t_π centered at c contains x, hence x is corrected to c.

2. In one hand, by definition of the packing radius, t_π is the biggest integer such that for all codewords c_1 and c_2 we have $d_\pi(c_1, c_2) > 2t_\pi$. In the other hand, we know that there exist two codewords $\hat{c}_1$ and $\hat{c}_2$ such that $d_\pi(\hat{c}_1, \hat{c}_2) = d_\pi$. Thus t_π satisfies $d_\pi > 2t_\pi$ and it is the biggest integer which satisfies it. Hence $t_\pi = [(d_\pi - 1)/2]$.

3. Suppose the balls of radius t_π centered at codewords, which are pairwise disjoint, do not cover the space V. There would exist a vector $v \in V$ which does not belong to none of these balls. But, as the balls of radius ρ_π cover V, it would belong to some ball of radius ρ_π. Hence balls of radius ρ_π larger than balls of radius t_π. We get the equality of radii in the case the balls at the same time are pairwise disjoint and cover the whole space V.

□

1.2.2 Hamming and Singleton Bounds

Hereafter we recall the Hamming and Singleton bounds for LEB codes which are introduced by Feng *et al.* [28].

Theorem 1.2.4. *Let C be an $[n, k, d_\pi]_q$ LEB code over $\mathbb{F}_q$ of type $\pi = [n_1][n_2]\dots[n_s]$. Then*

$$\begin{aligned} q^{n-k} &\geq b_\pi(l) \quad if \quad d_\pi = 2l+1, \\ q^{n-k} &\geq b'_\pi(l) \quad if \quad d_\pi = 2l \geq 2. \end{aligned} \tag{1.12}$$

where

$$b_\pi(l) = 1 + \sum_{\alpha=1}^{l} \sum_{1\leq i_1 \leq i_2 \leq \ldots \leq i_\alpha \leq s} (q^{n_{i_1}} - 1)(q^{n_{i_2}} - 1)\dots(q^{n_{i_\alpha}} - 1),$$

$$b'_\pi(l) = q^{n_1}\left(1 + \sum_{\alpha=1}^{l-1} \sum_{2\leq i_1 \leq i_2 \leq \ldots \leq i_\alpha \leq s} (q^{n_{i_1}} - 1)(q^{n_{i_2}} - 1)\dots(q^{n_{i_\alpha}}) - 1\right)$$

and

$$n - k \geq n_1 + n_2 + \ldots + n_{d_\pi - 1}. \tag{1.13}$$

The inequality (1.12) is called the Hamming bound and the inequality (1.13) is called the Singleton bound.

More bounds are defined in [26] and [57], hereafter we list some of them.

1.2.3 Redundancy Bound

Proposition 1.2.5. *The covering radius ρ_π of any $[n, k]$ LEB code satisfies $\rho_\pi \leq n - k$.*

1.2.4 Gilbert Bound

The Gilbert and Gilbert-Varshamov Bounds were generalized to the LEB case by Udomkavanich P. *et al.* in [57].

Theorem 1.2.6. *[57] Let $\pi = [n_1][n_2]\dots[n_s]$ be a partition of a given positive integer n and q be a prime power. Let $k, d \in \mathbb{N}$ such that $k \leq n$ and $d \leq s$. If $b_\pi(d-1) < q^{n-k+1}$, then there exists an $[n,k]$ code of type π over $\mathbb{F}_q$ with minimum π-distance at least d.*

1.2.5 Gilbert-Varshamov Bound

The concept of Gilbert-Varshamov bound is generalized to linear error-block codes by the following theorem.

Theorem 1.2.7. *[57] Let q be a prime power and let n, k, d and s be positive integers satisfying $2 \leq d \leq s$ and $k \leq n$. Let $\pi = [n_1][n_2]\dots[n_s]$ be a partition of n such that $n_i = 1$ for all $i \geq d-1$. If $b_{\pi'}(d-2) < q^{n-k}$ where $\pi' = [n_1][n_2]\dots[n_{s-1}]$, then there exists an $[n,k]$ code of type π over $\mathbb{F}_q$ with minimum π-distance at least d.*

1.2.6 Plotkin Bound

The generalization of the Plotkin upper bound for classical linear code, is presented in the following theorem.

Theorem 1.2.8. *[57] For each $[n,k,d]$ code C of type $\pi = [n_1][n_2]\dots[n_s]$ over $\mathbb{F}_q$, the following inequation holds:*

$$d \leq \frac{q^k(s - \sum_{i=1}^{s} \frac{1}{q^{n_i}})}{q^k - 1}.$$

1.3 Perfect and MDS LEB Codes

Definition 1.3.1. *An $[n,k,d_\pi]_q$ LEB code of type π is said to be perfect if it attains the Hamming bound (1.12) and is said to be MDS if it attains the Singleton bound (1.13).*

Perfect codes are an interesting class of codes and intensively studied by many researchers. LEB codes were defined in [28]. The authors defined an infinite family

of binary perfect codes. In [25], Dariti *et al.* constructed perfect LEB codes with minimum $\pi-$distance 3 and 4, some of these codes are both perfect and MDS. They also showed computationally that for the particular partition $\pi = [n_1][1]^{n-n_1}$, and for $q = 2, 3, \ldots, 10, n \leq 10000, 1 < n_1 < n$, there exists only one class of parameters for perfect linear error-block codes of minimum $\pi-$distance $d_\pi = 5$.

Feng *et al.* implemented a method that helps to construct perfect binary LEB codes of minimum $\pi-$distance $d_\pi = 30$ form binary LEB codes of minimum $\pi-$distance $d_\pi = 3$. In the following we summarize this method.

According to Equation (1.12), an $[n, k, d_\pi]_2$ binary LEB code of type $\pi = [n_1] \ldots [n_s]$ is said to be perfect if it satisfies the Hamming bound that is in this case :

$$2^{n-k} = b_\pi(1) = 1 + \sum_{i=1}^{s} (2^{n_i} - 1) \tag{1.14}$$

Proposition 1.3.2. *[28] Assume that there exists an $[n, k, 3]_2$ code C of type $\pi = [n_1][n_2] \ldots [n_s]$. Then there exists an $[n + N, k + N, 3]_2$ code C' of type $\pi = [n_1][n_2] \ldots [n_s][1]^N$, where $N = 2^{n-k} - 1 - \sum_{i=1}^{s} (2^{n_i} - 1)$ is positive. Moreover, C' is perfect.*

Example 1.3.3. *Let C be the $[5, 1, 3]_2$ code of type $\pi = [2][2][1]$ with parity-check matrix*

$$H = \left(\begin{array}{cc|cc|c} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{array}\right).$$

The code C is not perfect. In fact, using the inequality (1.14) we have

$$N = 2^{n-k} - \sum_{i=1}^{3} (2^{n_i} - 1) - 1 = 2 > 0$$

. So according to Proposition 1.3.2, the $[5+2, 1+2, 3]_2$ code of type $\tilde{\pi} = \pi[1]^2$ and parity-check matrix

$$H = \left(\begin{array}{cc|cc|cc|c|c|c} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \end{array}\right)$$

is perfect.

More constructions of perfect and MDS codes of type $\pi = [n_1][n_2]\dots[n_t][1]^N$ and π-distance 3 are given in [22], and generalized to a larger class of partitions.

1.4 Cyclic LEB Codes

The cyclic codes are an interesting class of error-correcting codes. In the literature they have been extensively studied and they have amazing algebraic properties. In [23] R. Dariti *et al.* introduced the notions of cyclic LEBC and quasi cyclic LEBC. They considered codes of type $\pi = [m]^s$ where π is only a composition where m and s are positive integers, and the coordinates are presented by blocks with different sizes, and as a consequence, the authors showed that the cyclicity of LEB codes is, first of all, predicted by the form of its type, and must allow that by some cyclic shift, the sizes of the coordinates remain unchanged. In order to allow application in cryptography, especially the McEliece-like cryptosystem, they presented a method of decoding this kind of codes. Furthermore they showed that there exist linear error-block codes with fast decoding algorithms. The algebraic study of cyclic codes gives the opportunity to a large number applications of this codes in cryptography and information security. The motivation of our work is to present an algebraic study of LEB cyclic codes. This may allows in the future to define strong cryptosystems using this family of codes.

Definition 1.4.1. *[23] Let q be a prime power, $\mathbb{F}_q$ be the finite field of q elements and π be a composition of an integer n of the form:*

$$\begin{aligned}\pi &= ([n_1][n_2]\dots[n_r])^l \\ &= \underbrace{\underbrace{[n_1][n_2]\dots[n_r]}\underbrace{[n_1][n_2]\dots[n_r]}\dots\underbrace{[n_1][n_2]\dots[n_r]}}_{l\ times}\end{aligned}$$

where r is the minimum integer satisfying this form.

Note $V_i = \mathbb{F}_q^{n_i}$ for $i = 1, 2, \dots, r, V_0 = \bigoplus_{i=1}^{r} V_i$ and $V_\pi = (V_0)^l$. Each vector $a \in V_\pi$ can be written uniquely as $a = (a_1, a_2, \dots, a_l)$, with $a_i \in V_0$ for $i = 1, \dots, l$.

An $[n, k]_q$ code C of type π is π-cyclic if for each $a \in C$ we have $\sigma_\pi(a) \in C$ where

$$\begin{aligned}\sigma_\pi : \underbrace{V_0 \oplus \dots \oplus V_0}_{l\ times} &\longrightarrow \underbrace{V_0 \oplus \dots \oplus V_0}_{l\ times} \\ (a_1, a_2, ..., a_l) &\longrightarrow (a_l, a_1, ..., a_{l-1})\end{aligned}$$

Example 1.4.2. *$\pi = ([3][1])^2, C = \{00000000, 10110110, 11001010, 01111100\}$. C is a $[8, 2, 2]$ π-cyclic code.*

Definition 1.4.3. *[23] An $[n, k, d]$ code C of type π is π-quasi-cyclic of order r if for each $a \in C$ we have $\sigma_\pi^r(a) \in C$.*

Remark 1.4.4. If $\pi = [1]^n$ then the classical definitions are found by setting $n_i = 1$ for all $i = 1, \dots, s$, $r = 1$ and $l = n$.

In [23] R. Dariti, *et al.* have generalized classical results on quasi-cyclic codes to π-cyclic LEB codes. [53] is an extention of the notion of π-cyclic codes to other partitions and gave an algebraic study to this class of codes. More construction and details are presented in Chapter 3.

CHAPTER

2 LEB PERFECT CODES

Table Contents

The topic of perfect codes is interesting in the theory of error-correcting codes. Perfect codes correct every word within the space. Golay, Hamming and repetition codes of odd length are shown in [56, 62] to be the unique existing perfect code in the classical case.

In this chapter, we construct infinite families of perfect binary linear error-block codes of minimum π-distance 3, of type $[n_1] \dots [n_t][2]^s$ $(t \geq 1)$, and of type $[n_1][n_t][3]^s$ $(t = 1 \text{ or } 2)$. We determine all possible parameters and sufficient conditions for these codes to

be perfect. The results of this chapter are published in [11].

Notation:

In this thesis, the expression " $a \equiv b[n]$" have the same meaning of that of :

"$a = b \mod n$".

2.1 Perfect LEB Codes of Type $\pi = [n_1] \dots [n_m][2]^s, m \geq 1$ with $d_\pi = 3$

2.1.1 Generation of Parity Check Matrix of an LEB Code of Type π

To provide new technical constructions of LEB codes, we are interested in the formal characterization of binary codes with π-distance 3. In [25], R. Dariti *et al.* have characterized perfect LEB codes, they have given parameters that define a perfect LEB code. However, the existence of these codes was not proven. By Algorithm 2.1, we try to verify the existence of perfect LEB codes.

Description of functions used in Algorithm 2.1

- getCanonicalBasis(r): returns the canonical basis of $\mathbb{F}_2^r$.
- NextComb($2^r, p$): returns the next set of P vectors in $\mathbb{F}_2^r$. This function does an exhaustive research of vectors in $\mathbb{F}_2^r$ to complete a basis to the used code. We begin by giving a vector v_1 which is linearly independent with the vectors of the canonical basis, and search an other v_2 vector linearly independent with the last vector and with the union of v_2 and the canonical basis of $\mathbb{F}_2^r$, and so forth.
- Rank(G): computes the Rank of G.
- Size(A): computes the number of blocks of A.

Algorithme 2.1 Generation of parity check matrix H of LEB code $\pi = [n_1] \cdots [n_m][2]^s$

Require: $A = \{n_1, \cdots, n_m\},\ r \geq n_1 + \cdots + n_m + 2,\ s > 0$
Ensure: H
$H \leftarrow \emptyset$ where $\emptyset$ denotes the empty set. Let B be an arbitrary set, $B[i]$ represent the i^{th} block of B and $B[i:k]$ represent a set composed of all the elements from position i to position k of B.
$Basis \leftarrow getCanonicalBasis(r)$
$j \leftarrow 0$
for all $i \in [0, m-1]$ **do**
  $H[i] \leftarrow basis[j : j + A[i]]$
  $j \leftarrow A[i]$
end for
while $Size(H) < s + m$ and $NextComb(2^r, 2) \neq Null$ **do**
  $x \leftarrow NextComb(2^r, 2)$
  for all $y \in H$ **do**
    if $Rank([y||x]) == Size([y||x])$ where $||$ denote the concatenation **then**
      $i \leftarrow i + 1$
      $H[i] \leftarrow x$
    end if
  end for
end while

Algorithm 2.1 takes as input an $[n, k, 3]_2$ LEB code of type $\pi = [n_1] \dots [n_m]^s$ where $n = n_1 + \ldots + n_m$ and outputs its corresponding parity check matrix. We start by generating the canonical basis of the vector subspace $\mathbb{F}_2^r$ that will form the first column vectors of our parity check matrix. We generate afterwards a linear combination of all the blocks of vectors of size $n_1, n_2, \ldots, n_m$ until obtaining exactly s blocks of size n_m and a block of size n_i $(1 \leq i \leq m)$ which are all pairwise linearly independent.

2.1.2 Construction of Perfect LEB Codes of Type $\pi = [n_1][2]^s (n_1 \geq 2)$ with $d_\pi = 3$

According to Definition 1.3.1, a code C of type π is said to be perfect if and only if it reaches the Hamming bound described in Theorem 1.2.4. Theorem 2.1.1 below, gives conditions of existence of perfect binary LEB codes of type $\pi = [n_1][2]^s$:

Theorem 2.1.1. *Let n be a positive integer and $\pi = [n_1][2]^s$ where $n_1 \geq 2$ a partition of n. An $[n, k, 3]_2$ LEB code of type π exists and is perfect if and only if n_1 and $r = n - k$*

are even and $s = \frac{2^r - 2^{n_1}}{3}$ *is an integer.*

Proof. 1. According to Definition 1.3.1, C is perfect if and only if

$$2^r = 1 + (2^{n_1} - 1) + s(2^2 - 1)$$

that is

$$s = \frac{2^r - 2^{n_1}}{3}$$

and since s is an integer, then $2^{n_1} \equiv 2^r[3]$. Hence $s = \frac{2^r - 2^{n_1}}{3}$ is an integer and r and n_1 have the same parity.

2. Existence of C : let C be an $[n, k, 3]_2$ LEB code of type $\pi_1 = [n_1]$ and let H_1 be a parity-check matrix of C. If $2^{n-k} - 1 > 2^{n_1} - 1$, then there exist $u_i, u_j \in \mathbb{F}_q^r$ $(1 \leq i \neq j \leq 2s,\ u_i \neq u_j)$ such that $\{u_i\} \cup H_1$ are linearly independent and $\{u_i\} \cup \{u_j\}$ are linearly independent. Then we obtain $H' = [H_1][H_2] \cdots [H_{s+1}]$ where $H_\lambda = [u_{i_\lambda}][u_{j_\lambda}]$ (concatenation of two vectors u_{i_λ} and u_{j_λ}) for all $1 \leq \lambda \leq s + 1$. The blocks H_λ are pairwise linearly independent.

Let C' be a linear error-block code with H' as a parity-check matrix. Then C' is an $[N, K, 3]_2$ code (where $N = n + 2s$ and $K = N - r = n + 2s - (n - k) = k + 2s$) of type $\pi = [n_1][2]^s$. Hence C' is perfect. □

Example 2.1.2. *The binary LEB code* C *of length* $n = 10$*, dimension* $k = 6$*, and type* $\pi = [2]^5$*; and whose parity-check matrix is:*

$$H = \left(\begin{array}{cc|cc|cc|cc|cc} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{array}\right)$$

is perfect and MDS. In fact, the columns of any two blocks are linearly independent and $2^{10-6} = 1 + 5(2^2 - 1)$ *and* $n - k = 10 - 6 = 2 + 2 = n_1 + n_2$.

Proposition 2.1.3. *There exists no perfect LEB code C of type $\pi = [n_1][2]^s$ with $d_\pi = 3$ and n_1 odd.*

Proof. Assume the existence of an $[n, k, 3]_2$ perfect binary LEB code C over $\mathbb{F}_2^n$ with type $\pi = [n_1][2]^s$ $(n_1 \geq 2)$ and $d_\pi = 3$ where n_1 is odd. The code C is of length $n = n_1 + 2s$ and dimension $k \leq n - n_1 = 2s$.
Let X be the set of $x \in \mathbb{F}_2^n$ which are of the form :

$$x = (\overbrace{0000000\ldots000010000000\ldots000000000000}^{one\ 1\ is\ randomly\ dispersed\ in\ the\ first\ block}, 01, 00, \ldots, 00)$$

Then $\omega_\pi(x) = 2$ and $\mid X \mid = n_1$ is the number of elements of X.

Since C is perfect, for all $x \in X$ there exists a unique $c \in C$ such that $d_\pi(c, x) = 1$. We have

$$1 = d_\pi(C) - \omega_\pi(x) \leq \omega_\pi(c) - \omega_\pi(x) \leq \omega_\pi(c - x) = 1 \tag{2.1}$$

i.e. $\omega_\pi(c) - \omega_\pi(x) = 1$. Then $\omega_\pi(c) = \omega_\pi(x) + 1 = 3$, this means that c must have the digit "1" in the block where x has.

Let $Y \subset C$ the set of y which are of the form:

$$y = (\overbrace{0000000\ldots000010000000\ldots0000100\ldots00000}^{two\ 1\ are\ randomly\ dispersed\ in\ the\ first\ block}, 01, 11, \ldots, 00, \ldots, 00)$$

We have $\omega_\pi(y) = 3$ and for all $x \in X$ there exists a unique y *in* Y such that the number of ones in $x - y$ equals to 2, then

$$\mid \{(x, y) \in X \times Y \setminus \text{ the number of one in } x - y \text{ equals to } 2 \} \mid = n_1.$$

However, for each $x \in X$ there exist exactly two vectors in X such that the number of one in $x - y$ equals to 2, indeed $2 \mid Y \mid = n_1$. Absurd since n_1 is odd. In conclusion, there exists no perfect LEB code C of type $\pi = [n_1][2]^s$ over $\mathbb{F}_2^n$ with $d_\pi = 3$ and n_1 odd. $\square$

2.1.3 Binary Perfect LEB Codes of Type $\pi = [n_1][n_2][2]^s$ with $d_\pi = 3$

Let C be an $[n, k, 3]_2$ code of type $\pi = [n_1][n_2][2]^s$ with $(n_1 \geq n_2 \geq 2)$. Set $r = n - k$. If C is perfect, then its parameters satisfy

$$2^r = 1 + (2^{n_1} - 1) + (2^{n_2} - 1) + s(2^2 - 1) \tag{2.2}$$

$$= 2^{n_1} + 2^{n_2} - 1 + 3s, \tag{2.3}$$

which means that $s = \frac{2^r - 2^{n_1} - 2^{n_2} + 1}{3}$. Since s must be an integer, then

$$2^r - 2^{n_1} - 2^{n_2} + 1 \equiv 0 \ [3].$$

Therefore, the existence of s and C is related to r, n_1 and n_2 by the following facts:

- If r is even:
  - If n_1 and n_2 are both even then $2^r - 2^{n_1} - 2^{n_2} + 1 \equiv 0$ [3] and s is an integer. Therefore, C is perfect.
  - If n_1 and n_2 are both odd then $2^r - 2^{n_1} - 2^{n_2} + 1 \equiv -2$ [3] and s is not an integer. Therefore, C is not perfect.
  - If n_1 or n_2 is odd then $2^r - 2^{n_1} - 2^{n_2} + 1 \equiv -1$ [3] and so s is not an integer. Therefore, C is not perfect.
- If r is odd:
  - If n_1 and n_2 are both odd then $2^r - 2^{n_1} - 2^{n_2} + 1 \equiv -1$ [3] and s is not an integer. Therefore, C is not perfect.
  - If n_1 and n_2 are both even then $2^r - 2^{n_1} - 2^{n_2} + 1 \equiv 1$ [3] and s is not an integer. Therefore, C is not perfect.
  - If n_1 is even or n_2 is odd then $2^r - 2^{n_1} - 2^{n_2} + 1 \equiv 0$ [3]. Therefore, C is perfect.

Thus we have proved the following result:

Theorem 2.1.4. *Let C be an $[n,k,3]_2$ code of type $\pi = [n_1][n_2][2]^s (n_1 \geq n_2 \geq 2)$. Set $r = n-k$, the code C is perfect if and only if $s = \frac{2^r - 2^{n_1} - 2^{n_2}}{3}$ and [(r, n_1 and n_2 are even) or (r is odd and n_1 or n_2 is even)].*

We use Algorithm 2.1 to generate codes of type $\pi = [n_1][n_2][2]^s (n_1 \geq n_2 \geq 2)$, with $d_\pi = 3$ and for which parameters verify the conditions of Theorem 2.1.4. We have the following result :

Theorem 2.1.5. *Let n be a positive integer and $\pi = [n_1][n_2][2]^s (n_1 \geq n_2 \geq 2)$ be a partition of n where s is a positive integer such that $s = \frac{2^r - 2^{n_1} - 2^{n_2}}{3}$. Set $r = n-k$. An $[n,k,3]_2$ binary code of type π exists only if r, n_1 and n_2 are all even.*

Proof. Assume r, n_1 are even, and n_2 is odd. We proceed as in Proposition 3.3.3 except that in this case, the first block of both $x \in X$ and $y \in Y$ are null and the remaining blocks are similar to those of $x \in X$ and $y \in Y$ respectively. □

Example 2.1.6. *The binary LEB code C of length $n = 36$, dimension $k = 30$, and type $\pi = [4][2][2]^{15}$ whose parity-check matrix is $H = \left(\begin{array}{c|c|c} H_1 & H_2 & H_3 \end{array} \right)$ is perfect and MDS where*

$$H_1 = \left(\begin{array}{cccc|cc|cc|cc|cc} 1&0&0&0&0&0&1&0&0&1&1&1 \\ 0&1&0&0&0&0&0&1&1&1&1&0 \\ 0&0&1&0&0&0&0&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0&0&0&0&0 \\ 0&0&0&0&1&0&1&0&1&0&1&0 \\ 0&0&0&0&0&1&0&1&0&1&0&1 \end{array} \right),$$

$$H_2 = \left(\begin{array}{cc|cc|cc|cc|cc|cc} 0&0&1&0&0&1&1&1&0&0&1&0 \\ 0&0&0&1&1&1&1&0&0&0&0&1 \\ 1&0&1&0&1&0&1&0&0&1&0&1 \\ 0&1&0&1&0&1&0&1&1&1&1&1 \\ 1&0&1&0&1&0&1&0&1&0&1&0 \\ 0&1&0&1&0&1&0&1&0&1&0&1 \end{array} \right),$$

and

$$H_3 = \left(\begin{array}{cc|cc|cc|cc|cc|cc} 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{array}\right).$$

2.1.4 Binary Perfect LEB Codes of type $\pi = [n_1] \dots [n_t][2]^s (t \geq 2)$ and $d_\pi = 3$

In this subsection we aim to generalize results about the existence of LEB codes of type $\pi = [n_1] \dots [n_t][2]^s$ where $n_1 \geq \dots \geq n_t \geq 2$. We have the following result:

Theorem 2.1.7. *Let C be an $[n, k, 3]_2$ LEB code of type $\pi = [n_1] \dots [n_t]$ where $n_1 \geq n_2 \geq \dots \geq n_t \geq 2$. Let $r = n - k$. If r and n_i are even for $i = 1, \dots, t$ then $s = \frac{2^r - \sum_{i=1}^{t} 2^{n_i} + t - 1}{3}$ is a positive integer and there exists an $[n + 2s, k + 2s, 3]_2$ LEB code C' of type $\pi = [n_1] \dots [n_t][2]^s$. Moreover, C' is perfect.*

Proof. 1. Since r and n_i are even for $i = 1, \dots, t$ so $2^r \equiv 1$ [3], we have $2^r - \sum_{i=1}^{t} 2^{n_i} + t - 1 \equiv 0$ [3]. Hence, s is an integer, and s is positive since $2^r - 1 \geq \sum_{i=1}^{t} (2^{n_i} - 1)$.

2. Existence of C' : Let $H = [H_1] \dots [H_t]$ be a parity-check matrix of C, where H_i is an $r \times n_i$ matrix, and represents the i^{th} block of the matrix H. If $2^r - 1 > \sum_{i=1}^{t} (2^{n_i} - 1)$ then there exist $u_i, u_j \in \mathbb{F}_q^r$ $(1 \leq i \neq j \leq 2s,\ u_i \neq u_j)$ such that $\{u_i\} \cup H_l$ where $(1 \leq l \leq t)$ are linearly independent and $\{u_i\} \cup \{u_j\}$ are linearly independent. Then we obtain $H' = [H_1] \dots [H_t][H_{t+1}] \dots [H_{t+s}]$ where $H_k = [u_i][u_j]$ (concatenation of two vectors u_i and u_j) for all $t + 1 \leq k \leq t + s$. The blocks H_k are pairwise linearly independent.

3. Let C' be the linear error-block code with H' as a parity-check matrix. Then C' is an $[N, K, 3]_2$ (where $N = n + 2s$ and $K = k + 2s$) code of type $\pi' = [n_1] \dots [n_t][2]^s$. Hence C' is perfect. □

Using Theorem 2.1.7 we can construct binary LEB codes of type $\pi = [n_1] \dots [n_t][2]^s$ where simply by taking an LEB code of type $\pi = [n_1] \dots [n_t]$ where $n_1 \geq \dots \geq n_t$ and then adding to $2s$ matrices H of length $(r \times 1)$ such that the union of the columns of each matrix and the columns of each block of H are linearly independent. Besides, this family of codes is infinite.

We now construct codes of type $\pi = [n_1][n_t][3]^s (n_1 \geq n_t \geq 3)$ and minimum π-distance 3.

2.2 Perfect LEB Codes of Type $\pi = [n_1][n_t][3]^s$, $t = 1$ or $t = 2$ with $d_\pi = 3$

2.2.1 Perfect LEB Codes of Type $\pi = [n_1][3]^s (n_1 \geq 3)$ and $d_\pi = 3$

The following lemma gives necessary conditions for an LEB code C of type $\pi = [n_1][3]^s$ to be perfect, in other words, conditions when parameters of C achieve the Hamming bound.

Lemma 2.2.1. *If C is an $[n, k, 3]_2$ perfect code of type $\pi = [n_1][3]^s$, and $r = n - k$ then $r \geq n_1 + 3$, $s = \frac{2^r - 2^{n_1}}{7}$ and $n_1 - r \equiv 0$ [3].*

Proof. Let C be an $[n, k, 3]_2$ perfect code of type $\pi = [n_1][3]^s$. Set $r = n - k$ then $r \geq n - 1 + 3$ and

$$2^r = 1 + (2^{n_1} - 1) + s(2^3 - 1) \tag{2.4}$$

$$= 2^{n_1} + 7s. \tag{2.5}$$

Then $s = \frac{2^r - 2^{n_1}}{7}$. Since s is an integer, then $2^r \equiv 2^{n_1}[7]$. Therefore, the existence of s and that of C is related to r and n_1 by the following relationship :

- Since, $2^3 \equiv 1[7]$. Therefore, if $n_1 - r \equiv 0$ [3], then $2^r \equiv 2^{n_1}$ [7] and so s is an integer. Then, C is perfect.

- If $n_1 - r \not\equiv 0[3]$, then $2^r \not\equiv 2^{n_1}[7]$, and so s is not an integer. Then, C is not perfect.

□

Using Lemma 2.2.1, we can define parameters of $[n, k, 3]_2$ perfect codes of type $\pi = [n_1][3]^s$. We list here some parameters of $[n, k, 3]_2$ perfect codes of type $\pi = [n_1][3]^s$ ($n_1 \geq 3$).

Example 2.2.2. *1.* $k = 21$, $n = 27$, $r = 6$, $\pi = [3]^9$.

2. $k = 45$, $n = 52$, $r = 7$, $\pi = [4][3]^{16}$.

Using Algorithm 2.1, we have been unable to generate the parity check matrices of the $[n, k, 3]_2$ codes of type $\pi = [n_1][3]^s$ where:

1. Length $n = 101$, dimension $k = 93$ and type $\pi = [5][3]^{32}$;
2. Length $n = 198$, dimension $k = 185$ and type $\pi = [6][3]^{64}$;
3. Length $n = 3463$, dimension $k = 3450$ and type $\pi = [7][3]^{1152}$.

Based on computation results, we conjecture the following:

Conjecture 2.2.3. *1. There exists no $[n, k, d_\pi]_2$ perfect code of type $\pi = [n_1][3]^s$ if $n_1 > 4$ (where $s = \frac{2^r - 2^{n_1}}{7}$, $r = n - k$ and $n_1 - r \equiv 0[3]$).*

2. There exists a $[27, 21, 3]_2$ perfect LEB code of type $\pi = [3]^9$ and parity-check matrix $H = (H_1|H_2)$ where

$$H_1 = \left(\begin{array}{ccc|ccc|ccc|ccc|ccc} 1&0&0&0&0&0&1&0&0&0&0&1&1&0&1 \\ 0&1&0&0&0&0&0&1&0&1&0&1&1&1&1 \\ 0&0&1&0&0&0&0&0&1&0&1&0&0&1&1 \\ 0&0&0&1&0&0&1&0&0&1&0&0&1&0&0 \\ 0&0&0&0&1&0&0&1&0&0&1&0&0&1&0 \\ 0&0&0&0&0&1&0&0&1&0&0&1&0&0&1 \end{array}\right),$$

$$H_2 = \left(\begin{array}{ccc|ccc|ccc|ccc} 0&1&0&1&1&0&0&1&1&1&1&1\\ 0&1&1&0&0&1&1&1&0&1&0&0\\ 1&0&1&1&0&0&1&1&1&1&1&0\\ 1&0&0&1&0&0&1&0&0&1&0&0\\ 0&1&0&0&1&0&0&1&0&0&1&0\\ 0&0&1&0&0&1&0&0&1&0&0&1 \end{array}\right).$$

3. *There exists a* $[52, 45, 3]_2$ *perfect LEB code of type* $\pi = [4][3]^{16}$ *and parity-check matrix* $(H_1|H_2|H_3|H_4)$ *where,*

$$H_1 = \left(\begin{array}{ccc|ccc|ccc|ccc} 1&0&0&0&0&0&0&1&0&0&0&1&0&1&1&0\\ 0&1&0&0&0&0&0&0&1&0&1&1&0&1&0&0\\ 0&0&1&0&0&0&0&0&0&1&0&0&0&0&0&1\\ 0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&1\\ 0&0&0&0&1&0&0&1&0&0&1&0&0&1&0&0\\ 0&0&0&0&0&1&0&0&1&0&0&1&0&0&1&0\\ 0&0&0&0&0&0&1&0&0&1&0&0&1&0&0&1 \end{array}\right),$$

$$H_2 = \left(\begin{array}{ccc|ccc|ccc|ccc} 0&0&0&1&0&0&0&1&0&1&1&0\\ 0&0&1&0&1&1&1&1&1&1&0&1\\ 1&0&1&1&0&0&1&0&1&1&0&0\\ 0&1&0&0&1&0&0&1&1&0&1&1\\ 1&0&0&1&0&0&1&0&0&1&0&0\\ 0&1&0&0&1&0&0&1&0&0&1&0\\ 0&0&1&0&0&1&0&0&1&0&0&1 \end{array}\right),$$

$$H_3 = \left(\begin{array}{ccc|ccc|ccc|ccc} 0&0&1&1&0&1&0&1&1&1&1&1\\ 0&0&1&0&1&1&1&1&1&1&0&1\\ 0&1&0&0&1&1&0&1&0&0&1&1\\ 1&1&1&1&1&1&1&1&0&1&1&0\\ 1&0&0&1&0&0&1&0&0&1&0&0\\ 0&1&0&0&1&0&0&1&0&0&1&0\\ 0&0&1&0&0&1&0&0&1&0&0&1 \end{array}\right),$$

$$H_4 = \left(\begin{array}{ccc|ccc|ccc|ccc} 0&0&1&1&0&1&0&1&1&1&1&1\\ 0&0&0&0&1&0&1&1&0&1&0&0\\ 1&1&1&1&1&0&1&1&1&1&1&0\\ 1&0&1&1&0&1&1&0&0&1&0&0\\ 1&0&0&1&0&0&1&0&0&1&0&0\\ 0&1&0&0&1&0&0&1&0&0&1&0\\ 0&0&1&0&0&1&0&0&1&0&0&1 \end{array}\right).$$

2.2.2 Perfect LEB Codes of Type $\pi = [n_1][n_2][3]^s$ with $d_\pi = 3$

The following lemma gives necessary conditions for an LEB code C of type $\pi = [n_1][n_2][3]^s$ to be perfect, in other words, conditions when the parameters of C achieve the Hamming bound.

Lemma 2.2.4. *If C is an $[n, k, 3]_2$ perfect code of type $\pi = [n_1][n_2][3]^s$, and $r = n - k$ then $r \geq n_1 + 3$, $s = \frac{2^r - 2^{n_1} - 2^{n_2} + 1}{7}$ and the parameters r and n_1 and n_2 verify one of the following conditions:*

- $r \equiv 1$ [3] *and* $[(n_1 \equiv 0$ [3] *and* $n_2 \equiv 1$ [3]) *or* $(n_1 \equiv 1$ [3] *and* $n_2 \equiv 0$ [3])]
- $r \equiv 0$ [3] *and* $n_1 \equiv 0$ [3] *and* $n_2 \equiv 0$ [3]
- $r \equiv 2$ [3] *and* $[(n_1 \equiv 0$ [3] *and* $n_2 \equiv 2$ [3]) *or* $(n_1 \equiv 2$ [3] *and* $n_2 \equiv 0$ [3])]

Proof. Let C be an $[n, k, 3]_2$ perfect code of type $\pi = [n_1][n_2][3]^s$. Set $r = n - k$ then $r \geq n - 1 + 3$ and

$$2^r = 1 + (2^{n_1} - 1) + (2^{n_2} - 1) + s(2^3 - 1) = 2^{n_1} + 2^{n_2} - 1 + 7s. \tag{2.6}$$

Hence $s = \frac{2^r - 2^{n_1} - 2^{n_2} + 1}{7}$. Since s is an integer, then $2^r + 1 \equiv 2^{n_1} + 2^{n_2}[7]$.

Therefore, the existence of s and C is related to r, n_1 and n_2 by the following:

- If $r \equiv 0$ [3] then $2^{n_1} + 2^{n_2} \equiv 2$ [3] which means that $n_1 \equiv 0$ [3] and $n_2 \equiv 0$ [3].
- If $r \equiv 1$ [3] then $2^{n_1} + 2^{n_2} \equiv 3[3]$ which means that $n_1 \equiv 0$ [3] and $n_2 \equiv 1$ [3] or $n_1 \equiv 1$ [3] and $n_2 \equiv 0$ [3].
- If $r \equiv 2$ [3] then $2^{n_1} + 2^{n_2} \equiv 5$ [3] which means that $n_1 \equiv 0$ [3] and $n_2 \equiv 2$ [3] or $n_1 \equiv 2$ [3] and $n_2 \equiv 0$ [3].

In the three cases cited above, s is an integer, with these parameters of C satisfying the Hamming bound. □

Example 2.2.5. *The $[n, k, 3]_2$ code where $k = 13797$, $n = 13812$ and $\pi = [9][6][3]^{4599}$ is perfect. In fact, $r \equiv 0$ [3] and $n_1 \equiv 0$ [3] and $n_2 \equiv 0$ [3].*

The question that arises now is the existence of code of type $\pi = [n_1][n_2][3]^s$ ($n_1 \geq n_2 \geq 3$) and with $d_\pi = 3$. Using Algorithm 1, and by computation we have been unable to generate the parity check matrices of some codes like:

- The $[n, k, 3]_2$ code where $k = 13797$, $n = 13812$ and $\pi = [9][6][3]^{4599}$.
- The $[1146, 1134, 3]_2$ code of type $\pi = [6][6][3]^{567}$.

Based on computation results we conjecture the following:

Conjecture 2.2.6. *There exist no $[n, k, d_\pi]_2$ perfect code of type $\pi = [n_1][n_2][3]^s$ (where s and r and n_1 verify the conditions of Lemma 2.2.4).*

2.3 Conclusion

In this chapter, we have constructed perfect binary linear error-block codes with $d_\pi = 3$ and types $\pi = [n_1] \dots [n_t][2]^s$ where $n_1 \geq \dots \geq n_t \geq 2$ and $t \geq 1$ and $s \geq 1$ and $\pi = [n_1] \dots [n_t][3]^s$ where $n_1 \geq \dots \geq n_t \geq 3$, $t = 1$ *or* 2 and $s \geq 1$.

Firstly, we have showed the conditions for a binary LEB code with π-distance three and type $\pi = [n_1] \dots [n_t][2]^s$ where $n_1 \geq \dots \geq n_t \geq 2$ and $t \geq 1$ and $s \geq 1$ (and respectively $\pi = [n_1][3]^s$ and $\pi = [n_1][n_2][3]^s$) to reache this bound. And then, we give conditions of existence of perfect binary LEB codes. Thereafter, we have shown that there exists an infinite family of codes of type $\pi = [n_1] \dots [n_t][2]s$ where $n_1 \geq \dots \geq n_t \geq 2$, $t \geq 1$ and $s \geq 1$.

CHAPTER

3 CONSTACYCLIC LINEAR ERROR-BLOCK CODES

Table Contents

The family of constacyclic codes has a significant role in the theory of error correcting codes. These codes can be efficiently encoded using shift registers, which justify their preferred role in engineering. The class of constacyclic codes has been known for a long time [13], and have been algebraically described in detail in [44]. Here, we generalize the notion of constacyclic codes to the LEB case. Constacyclic codes include in particular cyclic and negacyclic codes, which have been well studied since 1950's by Prange [47–50], while negacyclic codes over finite fields were initiated by Berlekamp in the late of 1960s [12, 13]. Cyclic codes are an important class of error-correcting codes. In the literature they have been extensively studied, since they have amazing algebraic properties. In fact, these codes are the most studied of all codes. Many well-known codes, such as BCH, Kerdock, Golay, Reed-Muller, Preparata, Justesen, and binary Hamming codes, are either

cyclic codes or are constructed from cyclic codes.

The motivation of this work is to extend the constacyclic codes notion to LEB codes.

In [23] R. Dariti *et al.* have considered a composition of an integer $n = l\sum_{i=1}^{s} n_i$ denoted by $\pi = ([n_1]\dots[n_s])^l$ where $n_1 > n_2 > \dots > n_s \geq 1$ and defined a cyclic LEB code C over $V_\pi = (V)^l$ where $V = \mathbb{F}_q^{n_1} \oplus \dots \oplus \mathbb{F}_q^{n_s}$ and q is a prime power to be a code stable by the cyclic shift σ_π defined as follows:

$$\begin{array}{rccc} \sigma_\pi : & \underbrace{V \oplus \dots \oplus V}_{l \text{ times}} & \longrightarrow & \underbrace{V \oplus \dots \oplus V}_{l \text{ times}} \\ & (a_1, a_2, \dots, a_l) & \longmapsto & (a_l, a_1, \dots, a_{l-1}) \end{array}$$

i. e. if c is a codeword of C, then

$$\sigma_\pi(c) \in C.$$

The notation $\pi = ([n_1]\dots[n_s])^l$ means that each block of a codeword c in C is partitioned into j sub-blocks of length n_i $(1 \leq i \leq s)$, and this block is of length $n = l\sum_{i=1}^{s} n_i$. Besides, the $\pi-$weight of each codeword remain unchanged even if we change the partition used into the sub-block. Therefore, the partition into sub-blocks plays no role in the definition of cyclicity of LEB codes. That is why, in this chapter we slightly modify this definition by talking about the constacyclic LEB codes only when the blocks of codewords among an LEB cyclic code have the same length m. i.e. the partition considered is $\pi = [m]^s$ $(m, s \in \mathbb{N}^\star)$ and $n = ms$ is the length of the code.

In this chapter we define the notion of constacyclic LEB code, then, we generalize the polynomial representation of a codeword, and we next construct the binary operation of our ring $R_{\lambda,\pi}$ defined in Proposition 3.1.5, and we give its properties, then we elaborate the algebraic study of these codes. After that, we redefine the notion of cyclicity for the LEB case, we prove that LEB cyclic codes are ideals of $R_{\lambda,\pi}$. We next give formal representation of the generator polynomial (resp. generator matrix) and we also give some examples of cyclic codes, and we give the Meggit-like decoding algorithm for this family

of codes. In the end of this chapter, we generalize the negacyclic codes to the LEB case.

3.1 λ-Constacyclic Codes

Let π be a partition of an integer n of the form $\pi = [m]^s$. Let $V_\pi = \oplus_{i=1}^{s} \mathbb{F}_q^m$. Each vector $u \in V_\pi$ can be written uniquely as $u = (u_1, u_2, \ldots, u_s)$ with $u_i \in V_i = \mathbb{F}_q^m$ $(i = 1, \ldots, s)$.

Definition 3.1.1. *An $[n, k, d]$ code C of type $\pi = [m]^s$ is an LEB λ-constacyclic code if there is $\lambda \in \mathbb{F}_q - \{0\}$ such that for each $a \in C$ we have $\sigma_{\pi,\lambda}(a) \in C$ where*

$$\begin{array}{rccc} \sigma_{\pi,\lambda}: & \underbrace{\mathbb{F}_q^m \oplus \ldots \oplus \mathbb{F}_q^m}_{s \text{ times}} & \longrightarrow & \underbrace{\mathbb{F}_q^m \oplus \ldots \oplus \mathbb{F}_q^m}_{s \text{ times}} \\ & (u_1, u_2, \ldots, u_s) & \longmapsto & (\lambda u_s, u_1, \ldots, u_{s-1}) \end{array}$$

$\sigma_{\pi,\lambda}$ is a λ-constacyclic shift of one block to the right with multiplication of u_s by λ.

Remark 3.1.2. If $\pi = [1]^n$, the classical definition of a λ-constacyclic code is found by setting $m = 1$ and $s = n$.

Definition 3.1.3 (The internal low $\star$)**.** *Let $\mathbb{R} = (\mathbb{F}_q[X], +, .)$ be the ring of polynomials with coefficients in $\mathbb{F}_q$ and provided with the classical addition " + " and the classical multiplication "." of polynomials in $\mathbb{F}_q[X]$, $\lambda \in \mathbb{F}_q$ and $< X^n - \lambda >$ is the principal ideal generated by the polynomial $X^n - \lambda$ (i.e. $< X^n - \lambda >= \{f.(X^n - \lambda)/f \in \mathbb{R}\}$). We define " $\star$ " to be the application defined by:*

$$\begin{array}{rcl} \star : \dfrac{\mathbb{F}_q[X]}{< X^n - \lambda >} \times \dfrac{\mathbb{F}_q[X]}{< X^n - \lambda >} & \longrightarrow & \dfrac{\mathbb{F}_q[X]}{< X^n - \lambda >} \\ (P(X), Q(X)) & \longmapsto & P(X) \star Q(X) = X^{m-1}.P(X).Q(X). \end{array}$$

$\star$ is an internal low on $\frac{\mathbb{F}_q^n[X]}{<X^n-\lambda>}$ and verify the following properties:

Remark 3.1.4.

- for $i \in \mathbb{N}$; $X^i \star X^j = X^{i+m-1}.X^j = X^j \star X^i$ where "." is the classical multiplication.
- for $i, j, k \in \mathbb{N}$; $X^i \star (X^j \star X^k) = (X^i \star X^j) \star X^k$.

- $\overbrace{X \star \ldots \star X}^{\alpha \ time} = X^{\star\alpha} = X^{(\alpha-1)m+1}$ where α is an integer ≥ 1.
- $X^{\star 0} = \mathbf{1}^{\star}$ the unity element of the low $\star$.
- $1 \star X = X^m$ where 1 denotes here X^0.
- $X^{\star s} \star P(X) = \lambda.P(X)$. In fact,

$$X^{\star s} \star P(X) = X^{m-1}.X^{(s-1)m+1}.P(X) = X^{ms}.P(X) = \lambda.P(X)$$

.

- $1 \star X = X^m$ where 1 denotes here X^0

Proposition 3.1.5. *Let π be a partition of an integer n of the form $\pi = [m]^s$. Let $\mathbb{F}_q$ be the finite field of q elements and $R_{\pi,\lambda} = \frac{\mathbb{F}_q[X]}{<X^n-\lambda>}$ be the quotient, where $\lambda \in \mathbb{F}_q - \{0\}$. Then $(R_{\pi,\lambda}, +, \star)$ where " + " is the classical addition of polynomial and " $\star$ " is the polynomial multiplication defined by 3.1.3. Then $(R_{\pi,\lambda}, +, \star)$ is a commutative ring, with $\mathbf{1}^{\star} = \frac{1}{\lambda}X^{n-m+1}$ is the unity element of the law $\star$.*

Proof. Let $P(X) = \sum_{i=0}^{n-1} a_i X^i$, $Q(X) = \sum_{i=0}^{n-1} b_i X^i$ and $R(X) = \sum_{i=0}^{n-1} c_i X^i$ three polynomials in $R_{\lambda,\pi}$. Then

1. $(R_{\lambda,\pi}, +)$ is an abelian group (where + is the usual polynomial addition).
2. By construction, the low $\star$ is commutative and is distributive with respect to the low +.
3. The low $\star$ is associative. In fact

$$\begin{aligned}
(P(X) \star Q(X)) \star R(X) &= (\textstyle\sum_{i=0}^{n-1} a_i(X^i \star Q(X))) \star R(X) \\
&= (\textstyle\sum_{i=0}^{n-1} a_i X^{i+m-1}.Q(X)) \star R(X) \\
&= X^{m-1}.Q(X).(\textstyle\sum_{i=0}^{n-1} a_i.X^i \star R(X)) \\
&= X^{m-1}.Q(X).(\textstyle\sum_{i=0}^{n-1} a_i.X^{i+m-1}.R(X)) \\
&= X^{2m-2}.P(x).Q(X).R(X)
\end{aligned}$$

and

$$\begin{aligned} P(X) \star (Q(X) \star R(X)) &= P(X) \star (\textstyle\sum_{i=1}^{n-1} b_i (X^i \star R(X))) \\ &= P(X) \star (\textstyle\sum_{i=0}^{n-1} b_i X^{i+m-1}.R(X)) \\ &= (P(X) \star \textstyle\sum_{i=0}^{n-1} b_i.X^i).X^{m-1}.R(X) \\ &= (\textstyle\sum_{i=0}^{n-1} b_i.(P(X) \star X^i)).X^{m-1}.R(X) \\ &= (\textstyle\sum_{i=0}^{n-1} b_i.(P(X).X^{i+m-1})).X^{m-1}.R(X) \\ &= X^{2m-2}.P(x).Q(X).R(X). \end{aligned}$$

4. The low $\star$ admits a unity element $\mathbf{1}^\star = \frac{1}{\lambda} X^{n-m+1}$. In fact

$$\begin{aligned} \mathbf{1}^\star \star P(X) &= \tfrac{1}{\lambda}.X^{n-m+1} \star P(X) \\ &= \tfrac{1}{\lambda}.X^{n-m+1+(m-1)}.P(X) \\ &= \tfrac{1}{\lambda}.X^n.P(X) \\ &= P(X). \end{aligned}$$

Since $(R_{\lambda,\pi}, \star)$ is commutative, then $P(X) \star \mathbf{1}^\star = \mathbf{1}^\star \star P(X) = P(X)$.

□

Let C be an $[n,k]_q$ π-cyclic code of type $\pi = [m]^l$. Let $c = (c_1, c_2, \ldots, c_l)$ be a codeword of C. We associate with the vector c the polynomial

$$C(X) = c_1(X) + X \star c_2(X) + \ldots + X^{\star(l-1)} \star c_l(X)$$

where $c_i(X) = \sum_{j=0}^{m-1} \alpha_{ij}.X^j$ for $i = 1, \ldots, l$ and $\alpha_{i,j}$ is the j^{th} component of the vector c_i.

We have the following result:

Theorem 3.1.6. *An $[n,k,d_\pi]_q$ LEB code C is λ-constacyclic if and only if C is an ideal of $(R_{\lambda,\pi}, +, \star)$.*

Proof. Take $c = (c_1, c_2, \ldots, c_l)$ a codeword of C. Then $\hat{c} = \sigma_{\lambda,\pi}(c) = (\lambda.c_l, c_1, \ldots, c_{l-1})$

($\sigma_{\lambda,\pi}$ is the λ-constacyclic shift defined in Definition 3.1.1) is also a codeword of C and

$$\begin{aligned}
\hat{c}(X) &= \lambda.c_l(X) + X \star c_1(X) + \ldots + X^{\star(l-1)} \star c_{l-1}(X) \\
&= \lambda.c_l(X) + X \star c_1(X) + \ldots + X^{\star(l-1)} \star c_{l-1}(X) + X^{\star l} \star c_l(X) - X^{\star l} \star c_l(X) \\
&= X \star (c_1(X) + X \star c_2(X) + \ldots + X^{\star(l-1)} \star c_l(X)) + \lambda.c_l(X) - X^{\star l} \star c_l(X) \\
&= X \star c(X) + c_l(X).(\lambda - X^n) \\
&= X \star c(X) \in \ R_{\lambda,\pi}.
\end{aligned}$$

Since $\hat{c}(X) \in C$, then $X \star c(X) \in C$. By definition, $(C, +)$ is an abelian group, thus C is an ideal of $R_{\lambda,\pi}$. Reciprocally, if C is an ideal of $R_{\lambda,\pi}$, then for all $c(X)$ in C, $r(X) \star c(X)$ is in C where $r(X)$ is an arbitrary polynomial in $R_{\lambda,\pi}$. Let $c(X) = \sum_{i=0}^{ml-1} \alpha_i X^i$ in C where $\alpha_i \in \mathbb{F}_q$. Thus

$$\begin{aligned}
c(X) &= \textstyle\sum_{i=0}^{m-1} \alpha_i X^i + \sum_{i=m}^{2m-1} \alpha_i X^i + \ldots + \sum_{i=(l-1)m}^{n-1} \alpha_i X^i \\
&= \textstyle\sum_{i=0}^{m-1} \alpha_i X^i + X^m . \sum_{i=m}^{2m-1} \alpha_i X^{i-m} + \ldots + X^{m(l-1)} . \sum_{i=(l-1)m}^{n-1} \alpha_i X^{i-m(l-1)} \\
&= c_1(X) + X^m.c_2(X) + \ldots + X^{m(l-1)}.c_{l-1}(X) \text{ by definition of the low } \star \text{ we get} \\
&= c_1(X) + X \star c_2(X) + \ldots + X^{\star(l-1)} \star c_l(X).
\end{aligned}$$

where for all $i = 1, \ldots, l$ $c_i(X) = \sum_{j=(i-1)m}^{im-1} \alpha_{j-(i-1)m} X^{j-(i-1)m}$. The polynomial $c(X)$ is associated with vector $(c_1, c_2, \ldots, c_l)$. Now, if we multiply $c(X)$ by X we get

$$X \star c(X) = \lambda.c_l(X) + X \star c_1(X) + \ldots + X^{\star(l-1)} \star c_{l-1}(X)$$

which is a polynomial associated with the vector $(\lambda.c_l, c_1, \ldots, c_{l-1})$. Thus, multiplying $c(X)$ by X in $R_{\lambda,\pi}$ corresponds to a λ-constacyclic block shift. Finally, C is a λ-constacyclic code. □

In the following we study the special cases when $\lambda = 1$ and $\lambda = -1$.

3.2 π-Cyclic Codes

In this section, we introduce the notion of LEB cyclic codes. As for cyclic codes, we define and show that LEB cyclic codes are ideals, then we give the generator matrix (resp. the generator polynomial), and we define the duality and we give some examples of LEB cyclic codes, we also describe with details an algebraic decoding algorithm. It is the first existing algebraic decoder for LEB cyclic codes. In the literature, a cyclic code is a code that is invariant by a cyclic shift. This means that if the coordinates of a codeword are shifted to the next position, then the obtained word is a codeword.

Let π be a partition of an integer n of the form $\pi = [m]^s$. Let $V_\pi = \oplus_{i=1}^{s} \mathbb{F}_q^m$. Each vector $u \in V_\pi$ can be written uniquely as $u = (u_1, u_2, \ldots, u_s)$ with $a_i \in V_i = \mathbb{F}_q^m$ $(i = 1, \ldots, s)$.

Definition 3.2.1. *An $[n, k, d]$ code C of type $\pi = [m]^s$ is π-cyclic is an LEB 1-constacyclic code of type π. In other words, C is π-cyclic code if for each $a \in C$ we have $\sigma_\pi(a) \in C$ where*

$$\begin{array}{rccc} \sigma_\pi : & \underbrace{\mathbb{F}_q^m \oplus \ldots \oplus \mathbb{F}_q^m}_{s \text{ times}} & \longrightarrow & \underbrace{\mathbb{F}_q^m \oplus \ldots \oplus \mathbb{F}_q^m}_{s \text{ times}} \\ & (u_1, u_2, \ldots, u_s) & \longmapsto & (u_s, u_1, \ldots, u_{s-1}) \end{array}$$

Remark 3.2.2. If $\pi = [1]^n$, the classical definition of cyclic code is found by setting $m = 1$ and $s = n$.

Example 3.2.3. *Let $\pi = [3]^2$. The LEB code*

$$C = \{000|000; 010|110; 110|010; 100|100\}$$

of type π is a $[6, 2, 2]$ π-cyclic code.

Notation 3.2.4. *Let $v(X) \in \mathbb{F}_q[X]$ and $g(X)$ is the polynomial generator of a π-cyclic code, we denotes by $R_{g(X)}(v(X))$ the unique polynomial $r(X)$ verifying*

$$v(X) = g(X) \star f(X) + r(X). \tag{3.1}$$

with $r(X) = 0$ *or* $\star - deg(r(X)) \leq l - k$. *(The existence and the uniqueness of* $r(X)$ *verifying 3.1 are due two the existence and the uniqueness of* $r(X)$ *such that* $v(X) = g(X).X^{m-1}.f(X) + r(X)$, *and* $r(X) = 0$ *or* $deg(r(X)) \leq deg(g(X))$*).*

3.2.1 Algebraic Definition of a π-Cyclic Codes

Since the π-cyclic codes are special case of LEB constacyclic codes, then by setting $\lambda = 1$, we have $R_{1,\pi} = \frac{\mathbb{F}_q[X]}{<X^n-1>}$ is a commutative ring, with $\mathbf{1}^\star = X^{n-m+1}$ is the unity element of law $\star$. As for LEB constcyclic codes, a linear error-block code C is π-cyclic if and only if C is an ideal of $(R_{1,\pi}, +, \star)$.

Definition 3.2.5. *Let* $P(X) = \sum_{i=0}^{l-1} a_i(X)X^{\star i}$ *be a polynomial of* $R_{1,\pi}$ *with* $a_i(X) \in \mathbb{F}_q[X]$ *such that* $a_{l-1} \neq 0$. *The integer* $l - 1$ *is called the* $\star$*-degree and is denoted by* $\star - deg(P(X)) = l - 1$.

Definition 3.2.6. *Let* n *be a positive integer, and* l *and* l' *two integers* $\leq n$. *Let* $P(X) = \sum_{i=0}^{l-1} a_i(X)X^{\star i}$, *and* $Q(X) = \sum_{i=0}^{l'-1} b_i(X)X^{\star i}$ *be two polynomials of* $R_{1,\pi}$, *with* $a_i(X), b_i \in \mathbb{F}_q[X]$ *such that* $a_{l-1} \neq 0$ *and* $b_{l'-1} \neq 0$. *We say that* $\star - deg(P(X)) \leq \star - deg(Q(X))$ *if and only if* $(l < l'$ *or* $(l = l'$ *and* $deg(a_{l-1}) < deg(b_{l'-1}))$*).*

3.2.2 Polynomial Representation

Theorem 3.2.7. *Let* C *be an* $[n, k]_q$ π*-cyclic code of type* $\pi = [m]^l$.

1. *There exist a unique unitary polynomial* $g(X)$ *in* C, *of minimal degree.*
2. $g(X)$ $\star$*-divides every word* $c(X)$ *in* C.
3. $g(X)$ $\star$*-divides* $X^n - 1$ *in* $\mathbb{F}_q[X]$;

The polynomial g *thus defined is called the generator polynomial of the code* C.

Proof. 1. Suppose that there exist two such unit polynomials $g_1(X)$ and $g_2(X)$; then we can always construct a unitary polynomial of the form $a \star (g_1 - g_2)(X)$ (for a a constant polynomial of $R_{1,\pi}$) which belongs to the code and which is of degree strictly less than $deg(g_1)$. But since $deg(g_1) = deg(g_2)$ is the smallest possible degree, we get a contradiction and so $g(X)$ is unique.

2. Let $c(X)$ be a non-zero word of the code, then if we make the Euclidean division (respecting the law $\star$) of $c(X)$ by $g(X)$, we obtain $c(X) = g(X) \star q(X) + r(X)$ with $deg(r(X)) < deg(g(X))$. Then, $c(X) - g(X) \star q(X) = r(X)$. Since C is a π-cyclic and $g(X) \in C$, then $r(X) \in C$. But as $g(X)$ is of minimal degree, so $r(X) = 0$, which proves the result.

3. Write $X^n - 1 = g(X) \star q(X) + r(X)$ in $F[X]$, where $\deg r(X) < \deg g(X)$. In R_π this says $g(X) \star q(X) = -r(X) \in C$, a contradiction (since g is of minimal degree) unless $r(X) = 0$.

□

Theorem 3.2.8. *Let C be an $[n,k]_q$ π-cyclic code of type $\pi = [m]^l$ and with generator polynomial $g(X) = g_0(X) + X \star g_1(X) + \ldots + X^{\star r} \star g_r(X)$ where $g_0, g_1, \ldots, g_r$ are polynomials in $\frac{\mathbb{F}q[X]}{<X^m - 1>}$. Then*

1. $\dim C = k = l - r$.

2. *C is generated by the matrix*

$$G = \begin{pmatrix} g(X) \\ X \star g(X) \\ \ldots \\ X^{\star(l-1)} \star g(X) \end{pmatrix} =$$

$$\begin{pmatrix} g_0(X) & g_1(X) & \dots & g_r(X) & 0 & \dots & 0 & 0 \\ 0 & g_0(X) & g_1(X) & \dots & g_r(X) & 0 & \dots & 0 \\ \dots & & & & & & & \\ 0 & 0 & \dots & 0 & g_0(X) & g_1(X) & \dots & g_r(X) \end{pmatrix}$$

Proof. By Theorem 3.2.7, there exists $h(X)$ such that $g(X) \star h(X) = X^n - 1$. Hence $g_0 \neq 0$. The rows of G are linearly independent. By writing them as polynomials the lines of G are: $g(X), X \star g(X), \dots, X^{\star k-1} \star g(X)$. Let $c(X) \in C$, from Theorem 3.2.7 $c(X) = q(X) \star g(X)$ where $q(X)$ is a polynomial such that $deg(q(X)) < n - r$ since $deg(c(X)) < n$. Hence $q(X)$ is of the form

$$q(X) = q_0(X) + q_1(X) \star X + \dots + q_{l-r}(X) \star X^{\star(l-r-1)}$$

and

$$c(X) = g(X) \star q_0(X) + g(X) \star q_1(X) \star X + \dots + g(X) \star q_{l-r}(X) \star X^{\star(l-r-1)}$$

and $c(X)$ is a linear combination of the lines of G. So G is a generator matrix of C. □

Definition 3.2.9. *Let G and H respectively be the generator and the parity check matrix of a π-cyclic code of type $\pi = [m]^l$, we define $G \star H^t$ by $G \star H^t = G'.H^t$ where G' is the shifted matrix of G by m columns. We have $G \star H^t = 0$.*

We know that if G is a matrix generating a code C then a word $u \in C$ is coded as $uG \in C$. If C is an $[n, k]_q$ π-cyclic code of type $\pi = [m]^l$ and with generator polynomial $g(X)$ then $r = deg(g(X)) = l - k$ and the rows of G are $g(X), X \star g(X), \dots, X^{\star k-1} \star g(X)$.

Let $u = (u_1, u_2, \dots, u_k)$, then $u(X) = u_1 + u_2 \star X + \dots + u_k \star X^{\star k-1}$ and

$$u \star G = u(X) = u_1 + u_2 \star X + \dots + u_k \star X^{\star k-1} = u(X) \star g(X)$$

So, a polynomial message is encoded as $u(X) \star g(X)$.

Theorem 3.2.10. *If C is a cyclic code of length n over $\mathbb{F}_q$, then the Dual code $C^{\perp}$ of C is also a cyclic code.*

Proof. Saying that C is π-cyclique is is equivalent to saying that the automorphism group of C contains the circular permutation $(1, 2, 3, \ldots, s)$. Let H be a check matrix of C. Then for each $c \in C$ we have $H \star c^t = 0$. Since C is π-cyclic, then for every circular permutation P,

$$H \star (c \star P)^t = 0 = H \star P^t \star c^t = H \star P^{-1} \star c^t.$$

Therefore, each element of C is orthogonal to $H \star P^{-1}$. However, P^{-1} is also a circular permutation and the code generated by $H \star P^{-1}$ is $C^{\perp}$. Since the dual code $C^{\perp}$ is stable by the permutation P^{-1}, So it is cyclic. □

Example 3.2.11. *Let $C =< g(X) >$ be a π-cyclic code of type $\pi = [2]^7$ where $g(X) = 1 + X \star X + X^{\star 3} \star (1 + X)$. Then C is a $[14, 4]$ code generated by the matrix*

$$G = \left(\begin{array}{cc|cc|cc|cc|cc|cc|cc} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \end{array}\right).$$

3.2.3 Meggitt-Like Decoding of π-Cyclic Codes

Here we generalize a technique for decoding π-cyclic codes called Meggitt decoding, this technique was introduced by J. E. Meggitt in 1960 [40, 41]. Meggitt decoder is acceptable in practice in terms of substantially less complication and providing the best interference protection in comparison to a syndrome decoder.

Let C be an $[n, k, d]_q$ π-cyclic code of type $\pi = [m]^l$ with generator polynomial $g(X)$ of $\star$-degree $l - k$. So C will correct $t_\pi = [\frac{d_\pi - 1}{2}]$ errors (t_π is the error capacity). Suppose that $c(X) \in C$ is transmitted and $y(X) = c(X) + e(X)$ is received, where $e(X) = e_0 + e_1 \star X + \ldots + e_{l-1} \star X^{\star l-1} \in R_{1,\pi}$ and $e_i(X) = \sum_{j=0}^{m-1} e_{i,j}.X^j$ for $i = 1, \ldots, l$ and

$e_{i,j} \in \mathbb{F}_q$ is the error vector with $w_\pi(e(X)) \leq t_\pi$. The Meggit-like decoder store for each block syndroms of coordinate $m-1$ in error. In the literature, there are two versions of the Meggit Decoding, in this chapter, we generalize one of them to be the Meggitt-like decoding of π-cyclic codes. This version consists on shifting $y(X)$ at most l times, and then find the error vector $e(X)$ from the list of syndroms and then correct the errors. This decoding technique takes advantage from the cyclic nature of the code.

The function $R_{g(X)}$ (defined in 3.2.4) satisfies the following properties.

Theorem 3.2.12. *With the preceding notation the following hold:*

1. $R_{g(X)}(av(X)+bv'(X)) = aR_{g(X)}(v(X))+bR_{g(X)}(v'(X))$ *for all* $v(X), v'(X) \in \mathbb{F}_q[X]$ *and all* $a, b \in \mathbb{F}_q[X]$.

2. $R_{g(X)}(v(X) + a(X) \star (X^n - 1)) = R_{g(X)}(v(X))$.

3. $R_{g(X)}(v(X)) = 0$ *if and only if* $v(X) mod(X^n - 1) \in C$.

4. *If* $c(X) \in C$, *then* $R_{g(X)}(c(X) + e(X)) = R_{g(X)}(e(X))$.

5. $R_{g(X)}(v(X))) = v(X)$ *lf* $\star - deg(v(X)) < l - k$.

Proof. 1. Let $v(X), v'(X) \in R_\pi$ and $a, b \in \mathbb{F}_q[X]$, and set $r_1(X) = R_{g(X)}(av(X))$ and $r_2(X) = R_{g(X)}(bv'(X))$. Then there are two polynomials $f_1(X)$ and $f_2(X)$ in R_π such that $av(X) = f_1(X) \star g(X) + r_1(X)$ and $bv'(X) = f_2(X) \star g(X) + r_2(X)$ and $\star - deg(r_i(X)) < l - k$ or $r_i(X) = 0$ for $i = 1, 2$. Therefore, $av(X) + bv'(X) = (f_1(X) + f_2(X)) \star g(X) + (r_1 + r_2)(X)$. Since $\star - deg(r_1(X) + r_2(X)) \leq max(r_1(X), r_2(X)) \leq l - k$ then

$$R_{g(X)}(av(X) + bv'(X)) = (r_1 + r_2)(X) = aR_{g(X)}(v(X)) + bR_{g(X)}(v'(X)).$$

2. According the the result above, $R_{g(X)}(v(X) + a(X) \star (X^n - 1)) = R_{g(X)}(v(X)) + R_{g(X)}(a(X) \star (X^n - 1))$. Since $g(X)$ $\star$-divides $X^n - 1$, then $R_{g(X)}(a(X) \star (X^n - 1)) = 0$, and $R_{g(X)}(v(X) + a(X) \star (X^n - 1)) = R_{g(X)}(v(X))$

3.
$$\begin{aligned} v(X) mod(X^n - 1) \in C &\Leftrightarrow v(X) \star - divides\ g(X) \\ &\Leftrightarrow R_{g(X)}(v(X)) = 0 \end{aligned}$$

4. Let $c(X) \in C$, then $R_{g(X)}(c(X)) = 0$ and then

$$R_{g(X)}(c(X) + e(X)) = R_{g(X)}(c(X)) + R_{g(X)}(e(X)) = R_{g(X)}(e(X))$$

5. If $\star - deg(v(X)) < l - k$ then $v(X) = 0 \star g(X) + v(X)$, and $R_{g(X)}(v(X))) = v(X)$.

□

We now describe the Meggitt-like Decoding Algorithm and use an example to illustrate each step.

Definition 3.2.13. *Let C be an $[n, k, d]_q$ π-cyclic code of type $\pi = [m]^l$. We define the syndrome polynomial $S(v(X))$ of any polynomial $v(X) \in R_{1,\pi}$ to be $S(v(X)) = R_{g(X)}(X^{l-k} \star v(X))$.*

Step I Find all the syndrome polynomials $S(e(X))$ of error patterns $e(X) = e_0 + e_1 \star X + \ldots + e_{l-1} \star X^{\star l-1} \in R_{1,\pi}$ ($e_i(X) = \sum_{j=0}^{m-1} e_{i,j}.X^j$ for $i = 1, \ldots, l$, and $e_{i,j} \in \mathbb{F}_q$) such that $w_\pi(e(X)) \leq t_\pi$ and $e_{l-1} = 0$.

Example 3.2.14. *For the code C defined in the example 3.2.11, we calculate the error patterns syndromes.*

$e_i(X)$	$S(e_i(X))$
$e_1(X) = 1 \star X^{\star 6}$	$1 \star X^{\star 2}$
$e_2(X) = X \star X^{\star 6}$	$X \star X^{\star 2}$
$e_3(X) = (1+X) \star X^{\star 6}$	$(1+X) \star X^{\star 2}$
$e_4(X) = 1 \star X^{\star 5}$	$1 \star X^{\star 1}$
$e_5(X) = 1 \star X^{\star 5}$	$X \star X^{\star 1}$
$e_6(X) = (1+X) \star X^{\star 5}$	$(1+X) \star X^{\star 1}$
$e_7(X) = 1 \star X^{\star 4}$	$1 \star \mathbf{1}^{\star}$
$e_8(X) = X \star X^{\star 4}$	$X \star \mathbf{1}^{\star}$
$e_9(X) = (1+X) \star X^{\star 4}$	$(1+X) \star \mathbf{1}^{\star}$
$e_{10}(X) = 1 \star X^{\star 3}$	$1 \star X^{\star 2} + 1 \star X^{\star 1} + 1 \star \mathbf{1}^{\star}$
$e_{11}(X) = X \star X^{\star 3}$	$X \star X^{\star 2} + 1 \star X^{\star 1} + \mathbf{1}^{\star} \star X$
$e_{12}(X) = (1+X) \star X^{\star 3}$	$(1+X) \star X^{\star 2} + (1+X) \star \mathbf{1}^{\star}$
$e_{13}(X) = 1 \star X^{\star 2}$	$(1+X) \star X^{\star 2} + 1 \star X^{\star 1} + (1+X) \star \mathbf{1}^{\star}$
$e_{14}(X) = X \star X^{\star 2}$	$1 \star X^{\star 3} + X \star X^{\star 2} + 1 \star X^{\star 1} + X \star \mathbf{1}^{\star}$
$e_{15}(X) = (1+X) \star X^{\star 2}$	$1 \star X^{\star 3} + 1 \star X^{\star 2} + 1 \star \mathbf{1}^{\star}$
$e_{16}(X) = 1 \star X^{\star 1}$	$1 \star (X^{\star 3} + X^{\star 2}) + X \star X^{\star 1} + (1+X) \star \mathbf{1}^{\star}$
$e_{17}(X) = X \star X^{\star 1}$	$1 \star X^{\star 3} + (1+X) \star (X^{\star 2} + X^{\star 1} + \mathbf{1}^{\star})$
$e_{18}(X) = (X+1) \star X^{\star 1}$	$X \star X^{\star 2} + 1 \star X^{\star 2}$
$e_{19}(X) = 1 \star \mathbf{1}^{\star}$	$1 \star X^{\star 3}$
$e_{20}(X) = X \star \mathbf{1}^{\star}$	$1 \star X^{\star 3} + X \star X^{\star 1} + 1 \star \mathbf{1}^{\star}$
$e_{21}(X) = (1+X) \star \mathbf{1}^{\star}$	$X \star X^{\star 1} + 1 \star \mathbf{1}^{\star}$

Table 3.1: Table of the Errors Patterns Syndroms of C

The computations of these syndrome polynomials were aided by Theorem 3.2.12. For example, in computing the syndrome polynomial of $e_1(X) = 1 \star X^{\star 6}$*, we have*

$$S(e_1(X)) = S(1 \star X^{\star 6}) = R_{g(X)}(X^{\star 3}(1 \star X^{\star 6})) = R_{g(X)}(1 \star X^{\star 9}) = R_{g(X)}(1 \star X^{\star 2}).$$

Since $\star - deg(1 \star X^{\star 2}) < \star - deg(g(X))$*, then* $S(1 \star X^{\star 6}) = 1 \star X^{\star 2}$*. In computing the syndrome polynomial for* $e_{11} = 1 \star X^{\star 3}$*, we have*

$$\begin{aligned} S(e_{11}(X)) &= S(1 \star X^{\star 3}) \\ &= R_{g(X)}(X^{\star 3} \star (1 \star X^{\star 3})) \\ &= R_{g(X)}(g(X) \star (X \star X^{\star 6} + (1+X) \star X^{\star 2} + 1 \star X^{\star 1} + X \star \boldsymbol{1}^{\star}) \\ &+ 1 \star X^{\star 2} + 1 \star X^{\star 1} + 1 \star \boldsymbol{1}^{\star}). \end{aligned}$$

Therefore in computing the syndrome polynomial for e_{11}, we have

$$S(e_{11}(X)) = 1 \star X^{\star 2} + 1 \star X^{\star 1} + 1 \star \mathbf{1}^{\star}.$$

The others follow similarly.

Step II Suppose that $y(X)$ is the received vector. Compute the syndrome polynomial $S(y(X)) = R_{g(X)}(X^{l-k} \star y(X))$. By Theorem 3.2.12, $S(y(X)) = S(e(X))$, where $y(X) = c(X) + e(X)$ with $c(X) \in C$. The vector $e(X)$ may be one of the $e_i(X)$ calculated in the list of syndromes, when one error which is accrued, or a sum of e_i when there is more then error.

Example 3.2.15. *Continuing with Example 3.2.11, suppose that*

$$y(X) = 1 \star X^{\star 1} + X \star X^{\star 2} + (1 + X) \star X^{\star 4} + 1 \star X^{\star 6}$$

is received. Then

$$\begin{aligned} S(y(X)) &= R_{g(X)}(X^{\star 3} \star (1 \star X^{\star 1} + X \star X^{\star 2} + (1 + X) \star X^{\star 4} + 1 \star X^{\star 6})) \\ &= R_{g(X)}(1 \star X^{\star 4} + X \star X^{\star 5} + (1 + X) \star X^{\star 7} + 1 \star X^{\star 9}) \\ &= R_{g(X)}(X^{\star} \star (1 \star \mathbf{1}^{\star} + X \star X^{\star 1} + (1 + X) \star X^{\star 3}) + 1 \star X^{\star 2}) \\ &= R_{g(X)}(X^{\star 4} \star (g(X)) + 1 \star X^{\star 2}) \\ &= 1 \star X^{\star 2} \end{aligned}$$

Step III If $S(y(X))$ is in the list computed in Step I, then we know the error polynomial $e(X)$ and this can be subtracted from $y(X)$ to obtain the codeword $c(X)$. If $S(y(X))$ is not in the list, go on to Step IV.

Example 3.2.16. *$S(y(X))$ from Example 3.2.15 is in the list of syndrome polynomials*

given in Example 3.2.14, with $S(y(X)) = S(e_1(X))$. *Thus the received word is* $c(X) = y(X) - e_1(X) = 1 \star X^{\star 1} + X \star X^{\star 2} + (1 + X) \star X^{\star 4}$.

Step IV Compute the syndrome polynomial of $X \star y(X), X^2 \star y(X), \ldots$ in succession until the syndrome polynomial is in the list from Step I. If $S(X^i \star y(X))$ is in this list and is associated with the error polynomial $e(X)$, then the received vector is decoded as $y(X) - X^{\star(l-i)} \star e(X)$.

Example 3.2.17. *Let us suppose that for a transmitted word is* $c'(X)$ *the received word is* $y(X) = X \star \mathbf{1}^{\star} + (1 + X) \star X^{\star 1} + X \star X^{\star 2} + (1 + X) \star X^{\star 3} + (1 + X) \star X^{\star 4}$. *We have*

$$\begin{aligned} S(y(X)) &= R_{g(X)}(X^{\star 3} \star (X \star \mathbf{1}^{\star} + (1 + X) \star X^{\star 1} + X \star X^{\star 2} + (1 + X) \star X^{\star 3} + (1 + X) \star X^{\star 4})) \\ &= X \star X^{\star 5} + X \star X^{\star 1} + X \star \mathbf{1}^{\star}. \end{aligned}$$

$S(y(X))$ *is not in the list of syndrome polynomials given in Example 3.2.14. Applying Step 3.2.3, we have*

$$\begin{aligned} S(X^{\star 1} \star y(X)) &= R_{g(X)}(X^{\star 3} \star X^{\star 1} \star (y(X))) \\ &= R_{g(X)}(g(X) \star (X^{\star 5} + X^{\star 4} + X^{\star 1}) + X^{\star 2} \star X + X^{\star 1} \star 1) \quad = X^{\star 2} \star X + X^{\star 1} \star 1. \end{aligned}$$

$X^{\star 1} \star S(y(X))$ *is in the list of syndrome polynomials given in Example 3.2.14, and correspond to the error* $e_{18} = (1 + X) \star X^{\star 1}$. *Hence, the transmitted word is*

$$\begin{aligned} c'(X) &= y(X) - X^{\star(7-1)} \star e_{18}(X) \\ &= 1 \star \mathbf{1}^{\star} + (1 + X) \star X^{\star 1} + X \star X^{\star 2} + (1 + X) \star X^{\star 3} + (1 + X) \star X^{\star 4} \\ &= g(X) \star (\mathbf{1}^{\star} + X^{\star 1}) \end{aligned}$$

3.3 π-Negacyclic codes

Let π be a partition of an integer n of the form $\pi = [m]^l$. Let $V_\pi = \oplus_{i=1}^{l} \mathbb{F}_q^m$. Each vector $u \in V_\pi$ can be written uniquely as $u = (u_1, u_2, \ldots, u_l)$ with $a_i \in V_i = \mathbb{F}_q^m$ $(i = 1, \ldots, l)$.

Definition 3.3.1. *An $[n, k, d]$ code C of type $\pi = [m]^s$ is π-negacyclic is an LEB -1-constacyclic code of type π. In other words, C is π-negacyclic code if for each $a \in C$ we have $\sigma_{-1,\pi}(a) \in C$ where*

$$\begin{array}{rccc} \sigma_{-1,\pi}: & \underbrace{\mathbb{F}_q^m \oplus \ldots \oplus \mathbb{F}_q^m}_{l \text{ times}} & \longrightarrow & \underbrace{\mathbb{F}_q^m \oplus \ldots \oplus \mathbb{F}_q^m}_{l \text{ times}} \\ & (u_1, u_2, \ldots, u_s) & \longmapsto & (-u_s, u_1, \ldots, u_{s-1}) \end{array}$$

Remark 3.3.2. By setting $m = 1$ and $l = n$, we obtain the classical definition of negacyclic code.

Using a quite similar polynomial representation to that of linear cyclic codes over a finite field $\mathbb{F}_q$, we obtain the following:

Proposition 3.3.3. *An $[n, k, d_\pi]_q$ LEB code C is a π-negacyclic code if and only if its polynomial representation is an ideal of $R_{-1,\pi} = \frac{\mathbb{F}_q[X]}{X^n+1}$.*

In fact every ideal in $R_{-1,\pi}$ is a principal ideal, so every π-negacyclic code C has generator polynomial $g(X)$. Let $C =< g(X) >$, where $g(X)$ is a unique monic and has minimal degree polynomial in C. Then the polynomial $h(X)$ defined to be the polynomial verifying $g(X) \star h(X) = X^n - 1$ is referred to as the check polynomial of C.

3.4 Conclusion

In this chapter, we have defined the constacyclic LEB codes, and we have showed that every constacyclic LEB code is an ideal of $R_{\lambda,\pi} = \frac{\mathbb{F}_q[X]}{X^n-\lambda}$. Then, We have defined also cyclic and negacyclic LEB code. We have also given an explicit expression of the generator and

check polynomials of these codes. Besides, we have given encoding technique to cyclic LEB codes. We have also generalized the Meggitt decoding algorithm to the LEB case, and we have proven with an explicit example that the Meggitt-like decoder is efficient, and unlike the standard array decoding, even if two errors have occurred, we still can determine the original vector with certainty.

CHAPTER

4 PUNCTURED AND SHORTENED LEB CODES

Table Contents

An $[n, k, d]$ code over $\mathbb{F}_q$ is called distance-optimal (respectively, dimension-optimal and length-optimal) if there is no $[n, k, d' \geq d + 1]$ (respectively, $[n, k' \geq k + 1, d]$ and $[n' \leq n - 1, k, d]$) linear code over $\mathbb{F}_q$. An optimal code is a code that is length-optimal, or dimension-optimal, or distance-optimal, or meets a bound for linear codes. An important problem in the theory and application of coding theory is the construction of optimal codes and codes with desirable parameters. To this end, one may construct a linear code with good or desirable parameters from a known linear code with optimal or good parameters. The puncturing and shortening technique are two important approaches to constructing new linear codes from old ones. In the past 70 years, a lot of progress on the puncturing technique has been made, and many works on punctured linear codes have been done. Many families of linear codes with interesting parameters have been obtained with the puncturing technique. In this chapter, we extend the notions of punctured and shortened codes to the LEB codes, and we give some properties of this code.

4.1 Puncturing LEB Codes

For the classical case, the puncturing technique consists on deleting coordinates from all its codewords. However, there exits two ways to puncture an LEB code. In this section, we define the puncturing technique for the LEB case, and we give the properties of a punctured code.

Definition 4.1.1. *Let C be an $[n,k]_q$ LEB code over $\mathbb{F}_q$ and of type $\pi = [n_1]\dots[n_s]$ (where s is an integer ≥ 1, $\sum_{i=1}^{s} n_i = n$, and $n_1 \geq \dots \geq n_s \geq 1$). For all $i = 1,\dots,s$, let consider $L_i = \{p_1,\dots,p_l\}$ be the set of any l coordinates locations in the i^{th} block of all codewords of C. Puncturing C on L_i consists on deleting entries of the i^{th} block of each codeword in C at locations in the set L_i.*

Definition 4.1.2. *Let C be an $[n,k]_q$ LEB code over $\mathbb{F}_q$ and of type $\pi = [n_1]\dots[n_s]$ (where s is an integer ≥ 1, $\sum_{i=1}^{s} n_i = n$, and $n_1 \geq \dots \geq n_s \geq 1$), and let consider $L = \{p_1,\dots,p_l\}$, the set of any l block locations. Puncturing C on L consists on deleting blocks from each codeword in C at locations in the set L.*

According to Definition 4.1.1, puncturing an LEB code C on a set L_i consists on puncturing the i^{th} block of each codeword of C. However in the Definition 4.1.2, we puncture C by removing l blocks from a generator matrix of C.

In this chapter, we are interested to the puncturing technique described in Definition 4.1.2. So, say that we have punctured a code C is say that we have removed some blocks in a generator matrix of C. In the following, we denote by C_p the resulting set after puncturing C.

Theorem 4.1.3. *Let C be an $[n,k,d]_q$ LEB code over $\mathbb{F}_q$ of type $\pi = [n_1]\dots[n_s]$ (where s is an integer ≥ 1, $\sum_{i=1}^{s} n_i = n$, and $n_1 \geq \dots \geq n_s \geq 1$.), and let consider $L = \{p_1,\dots,p_l\}$, the set of any l block locations. Then, the obtained set C_p after puncturing C on L, is an Linear error-block code of length $n_p = n - \sum_{i=1}^{l} n_{p_i}$ and of type $\pi_p = [n_1]\dots[n_{p_1-1}][n_{p_1+1}]\dots[n_{p_2-1}][n_{p_2+1}]\dots[n_{p_l-1}][n_{p_l+1}]\dots[n_s]$.*

To prove this theorem, we consider the case when the set L contains one component. The general case yields similarly.

Proof. Let C an LEB code satisfying conditions of Theorem 4.1.3, and i an integer such that $1 \leq i \leq s$. Let C_p be the set obtained by puncturing C on the i^{th} block. Clearly, $(C_p, +)$ is an abelian group. Let $x = (x_1, \ldots, x_s)$ and $y = (y_1, \ldots, y_s)$ two codewords in C, then for all $\lambda \in \mathbb{F}_q$, $x + \lambda y = (x_1 + \lambda y_1, \ldots, x_s \lambda y_s) \in C$. Besides, $\hat{x} = (x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_s)$ and $\hat{y} = (y_1, \ldots, y_{i-1}, y_{i+1}, \ldots, y_s)$ are in C_p, and we have also $\hat{x} + \lambda\hat{y} = (x_1 + \lambda y_1, \ldots, x_{i-1} + \lambda y_{i-1}, x_{i+1} + \lambda y_{i+1}, \ldots, x_s \lambda y_s) \in C_p$. By construction of C_p, C and C_p have the same neutral element for the usual multiplication low. Therefore, C_p is an $\mathbb{F}_q$-linear subspace of $V_p = \mathbb{F}_q^{n_1} \oplus \ldots \oplus \mathbb{F}_q^{n_{i-1}} \oplus \mathbb{F}_q^{n_{i+1}} \oplus \ldots \oplus \mathbb{F}_q^{n_s}$ of length $n_p = n - n_i$, and since we have deleted the i^{th} block from each codeword in C, then C_p is an LEB code of type $\pi_p = [n_1] \ldots [n_{i-1}][n_{i+1}] \ldots [n_s]$. □

Theorem 4.1.4. *Let C be an $[n, k, d]_q$ LEB code of type $\pi = [n_1] \ldots [n_s]$ where s is an integer ≥ 1, $\sum_{i=1}^{s} n_i = n$, and $n_1 \geq \ldots \geq n_s \geq 1$, and let C_p be the $[n_p, k_p, d_p]_q$ code obtained from puncturing C on the i^{th} block. Then, we have the following:*

1. *When $d = 1$, if there is no codeword in C of minimumn π-weight 1 whose i^{th} block is not nul, then $d_p = 1$ and $k_p = k$. Otherwise, if $k > 1$, then C_p is an $[n - n_i, k - 1, d_p \geq 1]_q$ LEB code of type $\pi_p = [n_1] \ldots [n_{i-1}][n_{i+1}] \ldots [n_s]$.*

2. *When $d > 1$, if there is a minimum π-weight whose i^{th} block is not null, then $d_p = d - 1$. Otherwise, $d_p = d$.*

This means that $d_p \geq d - 1$ and $k_p \geq k - 1$.

Proof. Let C and C_p two LEB codes satisfying conditions of Theorem 4.1.4. Therefore, when $d = 1$, suppose that there exists a codeword $c \in C$ of minimum π-distance 1 whose i^{th} block is not null. Then, by removing the i^{th} block of c we will get a codeword of C_p which is zero in all blocks and of length $n - n_i$. Thus, the minimum π-distance d_p of C_p

is at least d. Besides, $k_p = k - 1$. In fact, C contains q^k codewords and the only way that C_p could contain fewer codewords is if two codewords of C agree in all blocks but not in the i^{th} block. Now, if there is no codeword in C of minimumn π-weight 1 whose i^{th} block is not nul, then $d_p = 1$ and 1 is proven. Using the same idea of 1 we can prove the statement number 2. □

Remark 4.1.5. If G is a generator matrix for C, then a generator matrix for C_p is obtained from G by deleting block i (and omitting a zero or duplicate row that may occur).

Theorem 4.1.6. *Let C be an $[n, k, d]$ LEB code satisfying conditions of Theorem 4.1.3, $L = \{p_1, \ldots, p_l\}$ be the set of any l block locations, and let C_p be the $[n_p, k_p, d_p]_q$ code obtained from puncturing C on L. C_p is an $[n_p, k_p, d_p]$ LEB code with $k_p \geq k - l$ and $d_p \geq d - l$.*

We use induction reasoning (an induction on l) to prove this theorem as shown in the following.

Proof. Assuming conditions of Theorem 4.1.6. For $l = 1$, according to Theorem 4.1.4 $d_p \geq d - 1$ and $k_p \geq k - 1$. Let l be an integer ≥ 1, and assume that $k_p \geq k - l$ and $d_p \geq d - l$. Let $L' = L \cup \{p_{l+1}\}$ be a set of $l + 1$ block locations and C'_p be the $[n'_p, k'_p, d'_p]$ LEB code obtained from puncturing C on L'. Let us prove that $k'_p \geq k - l - 1$ and $d'_p \geq d - l - 1$. Since C_p is the code obtained after puncturing C on L, then by the recurrence hypothesis we have $k_p \geq k - l$ and $d_p \geq d - l$. Let us now puncture C_p on the $(p_{l+1})^{th}$ block. Then, the obtained LEB code is exactly C'_p and according to Theorem 4.1.4 we have $k'_p \geq k_p - l$ and $d'_p \geq d_p - l$. Therefore $k'_p \geq k - l - 1$ and $d'_p \geq d - l - 1$, and by induction we deduce that $k_p \geq k - l$ and $d_p \geq d - l$. □

Example 4.1.7. *Let C be the $[8, 2, 3]_2$ LEB code of type $\pi = [3][2][2][1]$ and defined by $C = \{000 \mid 00 \mid 00 \mid 0, 101 \mid 01 \mid 10 \mid 1, 100 \mid 00 \mid 01 \mid 1, 001 \mid 01 \mid 11 \mid 0\}$, and let $L = \{2, 4\}$. Then, the obtained code after puncturing C on L is an $[5, 2, 2]_2$ LEB code of type $\pi_p = [3][2]$ and defined by $C_p = \{000 \mid 00, 101 \mid 10, 100 \mid 01, 001 \mid 11\}$.*

Lemma 4.1.8. *Assuming conditions of Theorem 4.1.6 hold and that $d > 1$. When puncturing C on L, the deleted blocks of each codeword can be also viewed as vectors. So let S be the set of vectors deleted in the puncturing technique. Then, S is also an LEB and $d_p = d - d_{\pi'}(S)$ where $d_{\pi'}(S)$ is the minimum π-distance of S and $\pi' = [n_{p_1}] \dots [n_{p_l}]$.*

Proof. Easy to proof, just noticing that S is exactly the code obtained from the puncturing C on C_L^E the complement of L in C (where $E = \{1, \dots, s\}$), and then applying Theorems 4.1.4 and 4.1.6. □

Example 4.1.9. *Continuing with the Example 4.1.7, we have $S = \{00 \mid 0, 01 \mid 1, 00 \mid 1, 01 \mid 0\}$ and $d_{\pi'}(S) = 2$ where $\pi' = [2][1]$. Therefore, $d_p = d - d_{\pi'}(S) = 1$.*

4.2 Shortening LEB Codes

In this section, we define the shortening technique for the LEB case, and we give some properties of a shortened code.

Definition 4.2.1. *Let C and L be as defined in Definition 4.1.2. Then the shortening operation on C at block locations in the set L consists of two steps. In the first step, consider the set W of codewords in C that have zeros at the locations in the set L. In the second step, puncturing operation is performed on W at block locations in the set L.*

Remark 4.2.2. The code obtained after the above mentioned shortening operation is an LEB code of length $n - \sum_{i=1}^{l} n_{p_i}$, called the shortened code and denoted by C_s.

Example 4.2.3. *Let C be the $[9, 3, 1]$ binary LEB code with generator matrix*

$$G = \left(\begin{array}{cccc|ccc|cc} 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \end{array}\right).$$

Let $T = \{3\}$. A Generator matrix for the shortened code C_s is

$$G_s = \left(\begin{array}{cccc|ccc} 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{array}\right).$$

Theorem 4.2.4. *Let C and L be as defined in Definition 4.1.2. and Let C_p and C_s are respectively the resulting codes after puncturing and shortening C. Then*

$$(C^{\perp})_s = (C_p)^{\perp} \tag{4.1}$$

and

$$(C^{\perp})_p = (C_s)^{\perp} \tag{4.2}$$

Proof. Let c be a codeword of $C^{\perp}$ which is 0 on L and c^* the codeword with the block locations in L removed. So $c^* \in (C^{\perp})_s$. If $x \in C$, then $0 = x.c = x^*.c^*$, where x^* is the codeword x punctured on L. Thus $(C^{\perp})_s \subseteq (C_p)^{\perp}$. Any vector $c \in (C_p)^{\perp}$ can be extended to a vector c' by inserting $0s$ in the block positions of L. If $x \in C$, puncture x on L to obtain x^*. As $0 = x^*.c = x.c'$, $c \in (C_p)^{\perp}$. Thus $(C^{\perp})_s = (C_p)^{\perp}$. Replacing C by $C^{\perp}$ gives $(C^{\perp})_p = (C_s)^{\perp}$. □

4.3 Conclusion

In this chapter, we have introduced the notions of puncturing and shortening LEB codes, and defined the properties of punctured and shortened codes. We have also found a relationship between this new constructed LEB codes.

CHAPTER

5 HAMMING AND SIMPLEX LEB CODES

Table Contents

The Hamming single-error-correcting codes are an important family of codes which were invented by Richard Hamming in 1950 [31]. A Hamming code is an error-correcting code that can be used to detect and correct the errors that can occur when the data is transmitted from a sender to a receiver. Hamming codes are still widely used in computing, telecommunication, and other applications including data compression, popular puzzles. The dual code of a Hamming code is called a simplex code, and all its codewords have the same weight. In this chapter, we extended the definitions of Hamming and simplex codes to linear error-block codes. Large families of Hamming codes of types $\pi = [m]^{\frac{q^r-1}{q^m-1}}$ and $\pi = [l][m]^{\frac{q^r-q^l}{q^m-1}}$ where l and m are integers such that $l > m$ and q is a prime power are constructed using their parity check matrix. Furtheremore, conditions of existence of simplex codes are given. We showed that a linear error-block code is simplex if and only if it is the dual of a Hamming code of type $\pi = [m]^{\frac{q^r-1}{q^m-1}}$ [11]. Results about the π-weight enumerator polynomial are proven, we give simple formula for the π-weight enumerator polynomial of both Hamming and simplex codes [10].

5.1 Hamming LEB codes

In this section, we introduce Hamming codes for the error-block case, and we give some related results.

Lemma 5.1.1. *Let m and r be two integers where $m \geq 1$, and $r \geq 2m$. Set $s = \frac{q^r-1}{q^m-1}$. Then, s is an integer if and only if $r = \lambda m$ where $\lambda \geq 1$.*

Proof. If s is an integer, then $q^r - 1 \equiv 0\ [q^m - 1]$, write $r = \lambda m + \alpha$ where $0 \leq \alpha < m$. Since, $q^m \equiv 1\ [q^m - 1]$. Then, $(q^m)^\lambda \equiv 1\ [q^m - 1]$, and $q^{\lambda m+\alpha} \equiv q^\alpha\ [q^m - 1]$. Therefore $q^r - 1 \equiv q^\alpha - 1\ [q^m - 1]$. Thus $\alpha = 0$ which means $r = \lambda m$. Conversely, if $r = \lambda m$, then $q^r \equiv 1\ [q^m - 1]$. i. e. $q^r - 1 \equiv 0\ [q^m - 1]$. So s is an integer. □

Definition 5.1.2. *Let $\mathbb{F}_q$ be the finite field of q elements, and m and λ be integers where $m \geq 1$ and $\lambda \geq 1$. A Hamming LEB code denoted by π-Ham(r,q) over $\mathbb{F}_q$ of length $n = m\frac{q^r-1}{q^m-1}$ where $r = \lambda m \geq 2$ is the code whose parity check matrix H is an $r \times n$ matrix for which the union of columns of any two blocks is linearly independent.*

Remark 5.1.3. In a parity check-matrix of a $\pi - Ham(r, q)$ code there exists

- no null column.
- no column which is a multiple of an other one.

Theorem 5.1.4. *Let C be a $\pi - Ham(n - k, q)$ code satisfying conditions of Definition 5.1.2. If $m = 1$, then C is a Hamming code.*

Proof. Let C be a $\pi - Ham(n - k, q)$ code satisfying conditions of Definition 5.1.2. If $m = 1$, then by construction of C, $n = m.\frac{q^r-1}{q^m-1} = \frac{q^r-1}{q-1}$ is the length of C, and $k = n - r = \frac{q^r-1}{q^m-1} - r$ is the dimension of C. i. e. C is an $[\frac{q^r-1}{q-1}, \frac{q^r-1}{q-1} - 1]_q$ code. By definition 5.1.2, the columns of H are linearly independent. Thus, C is a Hamming code. □

Theorem 5.1.5. *Let m be an integer ≥ 1. The π-Ham(r,q) Hamming codes are perfect LEB codes over $\mathbb{F}_q$ with parameter $[n = m\frac{q^r-1}{q^m-1}, k = m\frac{q^r-1}{q^m-1} - r, d_\pi = 3]$.*

Proof. Let C be a $\pi - Hamm(r,q)$ code where $s = \frac{q^r-1}{q^m-1} \in \mathbb{N}$, and let H be a parity check matrix of C. Therefore $n = m\frac{q^r-1}{q^m-1}$ is the length of C.

Since r is the number of rows of H, then by Definition 5.1.2, $r = n - k = \lambda m$. Thus

$$dim_{\mathbb{F}_q}(C) \;=\; k \;=\; n - r \;=\; m\tfrac{q^r-1}{q^m-1} - r.$$

By Definition 5.1.2, the union of columns of any two blocks in H is linearly independent, then $d_\pi = 3$. Since $r = n - k = \lambda m$, and $n = sm$.

We have

$$\begin{aligned} 1 + \textstyle\sum_{i=1}^{s}(q^{n_i} - 1) &= 1 + \textstyle\sum_{i=1}^{s}(q^m - 1) \\ &= 1 + s(q^m - 1) \\ &= 1 + \tfrac{q^r-1}{q^m-1}(q^m - 1) \\ &= 1 + q^r - 1 \\ &= q^r. \end{aligned}$$

Therefore, the Hamming bound (1.12) is satisfied and then C is perfect.

□

Example 5.1.6. *The binary LEB code C of length $n = 10$, dimension $k = 6$, and type $\pi = [2]^5$ and whose parity check matrix is*

$$H = \left(\begin{array}{cc|cc|cc|cc|cc} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{array}\right)$$

is a $[2]^5 - Ham(4,2)$ code, and it is perfect because $2^4 = 1 + 5(2^2 - 1)$.

Definition 5.1.7. *Let $v = (v_1, \ldots, v_n)$ be a vector in $\mathbb{F}_q^n$. A block extension of v is an $n \times n$ matrix E defined as follows*

- *The columns of E are linearly independent.*

- *The sum of all columns of E is equal to v^T (transpose of v).*

Example 5.1.8. *A possible block extension of the vector $v = (0, 1, 1) \in \mathbb{F}_2^3$ is the matrix*

$$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

Remark 5.1.9. If E and E' are two blocks extensions of two different vectors v and v' in $\mathbb{F}_q^m$, then, the columns of the matrix

$$\left(\begin{array}{c|c} E & E' \\ I_m & I_m \end{array}\right)$$

are linearly independent where I_m is the matrix identity of size m.

Theorem 5.1.10. *Let m be an integer ≥ 1 and $\pi = [m]^s$ where $s = \frac{q^r-1}{q^m-1} \geq 2$.*

Consider a $\pi - Ham(r, q)$ code C over the field $\mathbb{F}_q$ of type π, $r = \lambda m$ and $\lambda \geq 2$. The matrix H_λ defined recursively as follows :

$$H_2 = \left(\begin{array}{c|c|c|c|c} I_m & E_1 & \ldots\ldots & E_{q^m-1} & 0_m \\ 0_{m-1} & I_m & \ldots\ldots & I_m & I_m \end{array}\right) \tag{5.1}$$

and for $\lambda \geq 3$

$$H_\lambda = \left(\begin{array}{c|c|c|c|c} I_m & A_1 & \ldots\ldots & A_{q^m-1} & A_0 \\ 0_{m(\lambda-1)} & H_{\lambda-1} & \ldots\ldots & H_{\lambda-1} & H_{\lambda-1} \end{array}\right) \tag{5.2}$$

where

- *$E_1, \ldots, E_{q^m-1}$ are the extensions of non-zero vectors in $\mathbb{F}_q^m$.*
- *For all $1 \leq i \leq q^m - 1$, $A_i = (\underbrace{E_i, \ldots, E_i}_{s_{\lambda-1} \ time})$ where $s_{\lambda-1} = \frac{q^{(\lambda-1)m}-1}{q^m-1}$.*

- $A_0 = (\underbrace{0_m, \ldots, 0_m}_{s_{\lambda-1}\ time})$ *where* 0_m *is the* $m \times m$ *null matrix.*

is a parity check matrix of C*.*

Proof. Considering

$$H_2 = \left(\begin{array}{c|c|c|c|c} I_m & E_1 & \ldots\ldots & E_{q^m-1} & 0_m \\ 0_m & I_m & \ldots\ldots & I_m & I_m \end{array} \right)$$

and for $\lambda \geq 3$, define inductively H_λ by:

$$H_\lambda = \left(\begin{array}{c|c|c|c|c} I_m & A_1 & \ldots\ldots & A_{q^m-1} & A_0 \\ 0_{m(\lambda-1)} & H_{\lambda-1} & \ldots\ldots & H_{\lambda-1} & H_{\lambda-1} \end{array} \right)$$

As a matrix generating an LEB code S_λ.

We state that S_λ is the dual code of a $\pi - Ham(r,q)$ code of type $\pi = [m]^{s_\lambda}$ where $s_\lambda = \frac{q^{m\lambda}-1}{q^m-1}$ and $\lambda \geq 2$.

To prove that H_λ generates the $(\pi - Ham(r,q))^\perp$, we will prove that H_λ has r rows, $s_\lambda = \frac{q^{\lambda m}-1}{q^m-1}$ blocks, and the union of columns of any two blocks are linearly independent.

- Clearly, H_λ has m more rows than $H_{\lambda-1}$, and H_2 has $2m$ rows, then H_λ has $r = m\lambda$ rows.

- It is clear that

$$s_2 = 1 + q^m = \frac{q^{2m}-1}{q^m-1}.$$

We assume that $s_{\lambda-1} = \frac{q^{(\lambda-1)m}-1}{q^m-1}$. By definition of H_λ we deduce

$$\begin{aligned} s_\lambda &= q^m.s_{\lambda-1} + 1 \\ &= q^m.\tfrac{q^{(\lambda-1)m}-1}{q^m-1} + 1 \\ &= \tfrac{q^{\lambda m}-q^m+q^m-1}{q^m-1} \\ &= \tfrac{q^{\lambda m}-1}{q^m-1} \end{aligned}$$

- The columns of any block of H_2 are pairwise distinct, and the columns of any two blocks of H_2 are linearly independent. Clearly by construction, the columns of any block of H_λ are pairwise distinct, and the columns of any two blocks of H_λ are linearly independent if the columns of any block of $H_{\lambda-1}$ are pairwise distinct, and the columns of any two blocks of $H_{\lambda-1}$ are linearly independent. Then by induction, H_λ generates the dual S_λ of a $\pi - Ham(r,q)$ code of type $\pi = [m]^{s_\lambda}$ where $s_\lambda = \frac{q^{\lambda m}-1}{q^m-1}$ and $\lambda \geq 2$. Thus, H_λ is a parity check matrix of a $\pi - Ham(r,q)$ code of type $\pi = [m]^{s_\lambda}$ where $s_\lambda = \frac{q^{\lambda m}-1}{q^m-1}$.

□

Example 5.1.11. *The dual of the $\pi - Ham(6,2)$ code of type $\pi = [3]^9$ is generated by the matrix G defined by*

$$G = \left(\begin{array}{c|c} G_1 & G_2 \end{array} \right)$$

where,

$$G_1 = \left(\begin{array}{ccc|ccc|ccc|ccc} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{array} \right),$$

$$G_2 = \left(\begin{array}{ccc|ccc|ccc|ccc|ccc} 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{array} \right)$$

Theorem 5.1.12. *LEB perfect codes of type $\pi = [m]^s (m \geq 1,\ s \geq 2)$ and with minimum*

π-distance $d_\pi = 3$ over $\mathbb{F}_q$ are π-Hamming codes.

Proof. Let m be an integer ≥ 1. Let C be an $[n, k, 3]_q$ perfect code of type $\pi = [m]^s$ where $s \geq 1$ over $\mathbb{F}_q$. Set $r = n - k$. Then by Definition 1.3.1, C satisfies the equation

$$q^r = 1 + s(q^m - 1). \tag{5.3}$$

Hence,

$$s = \frac{q^r - 1}{q^m - 1}.$$

Since s is an integer, then by Lemme 5.1.1, $r = m\lambda$ where λ is an integer ≥ 1. Thus

$$n = ms = m\frac{q^r - 1}{q^m - 1},$$

and

$$k = n - r = m\frac{q^r - 1}{q^m - 1} - r.$$

Since $d_\pi = 3$ then the union of columns of any two blocks of H the parity check matrix of C is linearly independent.

Finally, C is a $\pi - Ham(r, q)$ code of type $\pi = [m]^s$ where $s = \frac{q^r-1}{q^m-1}$ and $r = n - k$.

□

Corollary 5.1.13. *Perfect codes of types $[n_1] \dots [n_t][2]^s$ (where $t \geq 1$), and $[n_1] \dots [n_t][3]^s$ (where $t = 1$ or $t = 2$) and with minimum π-distance $d_\pi = 3$ over $\mathbb{F}_q$ are π-Hamming codes if is all blocks have the same length.*

Proof. This is yielded by direct analogy to the proof of Theorem 5.1.12. □

Theorem 5.1.14. *Let $\pi = [l][m]^s$ where $l > m$ and s is an integer≥ 1 a partition of a positive integer n (i.e., $n = l + sm$). Take C a π-Ham($n - k$,q) code of type π, and set $r = n - k$. If C is perfect, then l and r have the same remainder of division by m, and $s = \frac{q^r-q^l}{q^m-1}$.*

Proof. Let C be a π-Ham($n-k$,q) code of type $\pi = [l][m]^s$ where $l > m$ and $s \geq 1$ and $n = l + ms$. Set $r = n - k$, then

$$\begin{array}{lll}
\text{C is perfect} & \Leftrightarrow & q^r = 1 + \sum_{i=1}^{s}(q^{n_i} - 1) \\
& \Leftrightarrow & q^r = 1 + (q^l - 1) + s(q^m - 1) \\
& \Rightarrow & s = \frac{q^r - q^l}{q^m - 1} \text{ and } s \in \mathbb{N} \\
& \Rightarrow & s = \frac{q^r - q^l}{q^m - 1} \text{ and } q^r - q^l \equiv 0[q^m - 1] \\
& \Rightarrow & s = \frac{q^r - q^l}{q^m - 1} \text{ and } q^r \equiv q^l[q^m - 1] \\
& \Rightarrow & s = \frac{q^r - q^l}{q^m - 1} \text{ and } r \equiv l[m] \\
\text{Thus, C is perfect} & \Rightarrow & s = \frac{q^r - q^l}{q^m - 1} \text{ and } r \text{ and } l \text{ have the same of remainder of division by} m.
\end{array}$$

□

Example 5.1.15. *The π-Ham(6,2) of type $\pi = [4][2]^{16}$ and whose parity-check matrix :* $H' = \left(\begin{array}{c|c|c} H_1 & H_2 & H_3 \end{array} \right)$
where:

$$H_1 = \left(\begin{array}{cccc|cc|cc|cc|cc} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{array} \right),$$

$$H_2 = \left(\begin{array}{cc|cc|cc|cc|cc|cc} 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{array} \right),$$

$$H_3 = \left(\begin{array}{cc|cc|cc|cc|cc|cc} 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{array}\right).$$

is perfect.

Remark 5.1.16. Let C be a perfect π-Ham($n-k$,q) code of type $\pi = [l][m]^s$ where $l > m$ and $s = \frac{q^{n-k}-q^l}{q^m-1} \geq 1$ and $n = l + sm$. Set $r = n - k$, then by Theorem 5.1.14, we have $r = mt + \alpha$ and $l = t'm + \alpha$ where $0 \leq \alpha < m$.

By the Singleton bound $r \geq l + m \Leftrightarrow l \leq r - m \Leftrightarrow t' \leq t + 1$.

If C is an MDS code and $t = 3$, then $t' = t - 1 = 2$.

If C is not an MDS code, then $t' < t - 1$.

Theorem 5.1.17. *Let C be a perfect π-Ham($n-k$,q) code of type $\pi = [l][m]^s$ where $l > m$ and $s = \frac{q^{n-k}-q^l}{q^m-1} \geq 1$ and $n = l + sm$. Set $r = n - k = mt + \alpha$ where $0 < \alpha < m$ and $l = t_1 m + \alpha$ where $0 < \alpha < m$, then $S_{r,t}$ the dual of C is generated by the matrix $G_{r,t}$ where:*

$G_{r,2} =$

$$\left(\begin{array}{c|ccccccccccccccc} I_l & 0_m & \dots & E_{q^m-1} & 0_m & \dots & \dots & E_{q^m-1} & \dots & \dots & \dots & \dots & \dots & \dots & 0_m & \dots & E_{q^m-1} \\ & 0_m & \dots & 0_m & e_1 & \dots & e_1 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & e_{q^m-1} & \dots & e_{q^m-1} \\ 0_{(r-l)\times l} & 0_m & \dots & 0_m & 0_m & \dots & 0_m & e_1 & \dots & e_1 & \dots & \dots & \dots & \dots & e_{q^m-2} & \dots & e_{q^m-2} \\ & \dots\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ & 0_m & \dots & 0_m & 0_m & \dots & 0_m & 0_m & \dots & 0_m & e_1 & \dots & e_1 & \dots & e_{q^m-\alpha} & \dots & e_{q^m-\alpha} \\ \hline & I_m & I_m & \dots & I_m & I_m & I_m & \dots & I_m & \dots & I_m & I_m & \dots & I_m & I_m & \dots & I_m \end{array}\right)$$

for $t \geq 3$

$$G_{r,t} = (M_1|M_2)$$

where

$$M_1 = \left(\begin{array}{c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c} I_l & 0_m & \dots & E_{q^m-1} & 0_m & \dots & \dots & E_{q^m-1} & \dots & \dots & \dots & \dots & \dots & \dots & 0_m & \dots & E_{q^m-1} \\ & 0_m & \dots & 0_m & e_1 & \dots & e_1 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & e_{q^m-1} & \dots & e_{q^m-1} \\ 0_{(r-l)\times l} & 0_m & \dots & 0_m & 0_m & \dots & 0_m & e_1 & \dots & e_1 & \dots & \dots & \dots & \dots & e_{q^m-2} & \dots & e_{q^m-2} \\ & \dots\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ & 0_m & \dots & 0_m & 0_m & \dots & 0_m & 0_m & \dots & 0_m & e_1 & \dots & e_1 & \dots & e_{q^m-\alpha} & \dots & e_{q^m-\alpha} \\ \hline & \multicolumn{15}{c}{0_{(m(t-2))\times q^l}} \\ \hline & I_m & I_m & \dots & I_m & I_m & I_m & \dots & I_m & \dots & I_m & I_m & \dots & I_m & I_m & \dots & I_m \end{array}\right)$$

$$M_2 = \left(\begin{array}{c|c|c|c} E_1 \dots E_1 & \dots & E_{q^m-1} \dots E_{q^m-1} & 0_m \dots 0_m \\ \hline G_{r,t-1} & \dots & G_{r,t-1} & G_{r,t-1} \end{array}\right)$$

Where $E_0, E_1, \dots, E_{q^m-1}$ are the extensions of non-zero vectors in $\mathbb{F}_q^m$, and e_i are the non-zero elements of $\mathbb{F}_q^m$.

Proof. Let $S_{r,t}$ a $[n, r]$ code of type $\pi = [l][m]^{\frac{q^r-q^l}{q^m-1}}$ where $r = tm + \alpha$ and $l = t_1 m + \alpha$ and $0 < \alpha < m$ generated with matrix defined in Theorem 5.1.17. We claim the code $S_{r,t}$ is the dual of a $\pi - Ham(r, q)$ code of type π.

Set $s_{r,t}$ the number of blocks in G_r^t of length m, and $\lambda = q^{l-m}$.

Obviously, $G_{r,t}$ has m more rows then G_r^{t-1}, and $G_{r,2}$ has $2m + \alpha$ rows, then $G_{r,t}$ has $r = (t-1)m + \alpha + m = tm + \alpha$ rows.

clearly, $S_{r,2} = \lambda \times q^m = q^{l-m+m} = q^l = q^{m+\alpha} = \frac{q^{2m+\alpha}-q^{m+\alpha}}{q^m-1}$. Assume that

$$s_{r,t-1} = \frac{q^{(t-1)m+\alpha} - q^{(t_1)m+\alpha}}{q^m - 1}.$$

Then, by construction of $G_{r,t}$, we have

$$\begin{aligned} s_{r,t} &= 2^l + 2^m.s_{r,t-1} \\ &= q^l + q^m.\frac{q^{(t-1)m+\alpha}-q^{t_1 m+\alpha}}{q^m-1} \\ &= \frac{q^{l+m}-q^l+q^{tm+\alpha}-q^{l+m}}{q^m-1} \\ &= \frac{q^r-q^l}{q^m-1}. \end{aligned}$$

Then by induction

$$s_{r,t} = \frac{q^r - q^l}{q^m - 1}.$$

The columns of any block of $G_{r,2}$ are pairwise distinct, and the columns of any two blocks of $G_{r,2}$ are linearly independents. Clearly by construction, the columns of any block of $G_{r,t}$ are pairwise distinct, and the columns of any two blocks of $G_{r,t}$ are linearly independent if the columns of any block of $G_{r,t-1}$ are pairwise distinct, and the columns of any two blocks of $G_{r,t-1}$ are linearly independent. Then by induction, $G_{r,t}$ is a parity check matrix of a $\pi - Ham(n-k,q)$ code of type $\pi = [l][m]^{\frac{q^r-1}{q^m-1}}$. Thus $S_{r,t}$ is the dual of a $\pi - Ham(n-k,q)$ code of type $\pi = [l][m]^{\frac{q^r-1}{q^m-1}}$.

□

Theorem 5.1.18. *Let C be a perfect $\pi - Ham(n-k,q)$ code of type $\pi = [l][m]^s$ where $l > m$ and $s = \frac{q^{n-k}-q^l}{q^m-1} \geq 1$ and $n = l + sm$. Set $r = n - k = mt$ and $l = t_1 m$, then $C^\perp$ the dual of C is generated by the matrix $G_{r,t}$ where:*

$G_{r,2} \mid_{t_1=1}=$

$$\left(\begin{array}{c|c|c|c|c|c|c|c|c|c|c|c|c} I_l & 0_m & E_1 & \dots & E_{q^m-1} & 0_m & E_1 & \dots & E_{q^m-1} & \dots & 0_m & E_1 & \dots & E_{q^m-1} \\ 0_{(r-m)\times l} & 0_m & 0_m & \dots & 0_m & E_1 & E_1 & \dots & E_1 & \dots & E_{q^m-1} & E_{q^m-1} & \dots & E_{q^m-1} \\ \hline & I_m & I_m & \dots & I_m & I_m & I_m & \dots & I_m & \dots & I_m & I_m & \dots & I_m \end{array}\right)$$

for $t \geq 3$

$$G_{r,t} = (M_1|M_2)$$

where

$$M_1 = \left(\begin{array}{c|c|c|c|c} I_l & M & M & & \\ ldots & M & & & \\ \hline & 0_m \dots 0m & E_1 \dots E_1 & \dots & E_{q^m-1} \dots E_{q^m-1} \\ \cline{2-5} 0_{(r-m)\times l} & 0_{(t_1-3)m\times q^l} & & & \\ & & & & \\ \cline{2-5} & I_m \dots I_m & I_m \dots I_m & \dots & I_m \dots I_m \end{array}\right)$$

with

$$M = \left(\begin{array}{c|c|c|c|c|c|c|c|c|c|c|c} 0_m & E_1 & \dots & E_{q^m-1} & 0_m & E_1 & \dots & E_{q^m-1} & \dots & 0_m & E_1 & \dots & E_{q^m-1} \\ 0_m & 0_m & \dots & 0_m & E_1 & E_1 & \dots & E_1 & \dots & E_{q^m-1} & E_{q^m-1} & \dots & E_{q^m-1} \end{array}\right)$$

$$M_2 = \left(\begin{array}{c|c|c|c} E_1 \dots E_1 & \dots & E_{q^m-1} \dots E_{q^m-1} & 0_m \dots 0_m \\ \hline & & & \\ G_{r,t-1} & \dots & G_{r,t-1} & G_{r,t-1} \\ & & & \\ & & & \end{array}\right)$$

Where E_i *is the matrix representing the* i^{th} *element of* $\mathbb{F}_q^m$ *in its canonic basis, and for all* $i = 1, \dots, q^m - 1$, e_i *are the non-zero elements of* $\mathbb{F}_q^m$.

Proof. Easy to prove by analogy to the proof of Th 5.1.17. □

Example 5.1.19. *The dual code of the perfect π-Ham$(17, 2)$ code C of type $\pi = [4][3]^{16}$ is generated by the matrix*

$$G = \left(\begin{array}{c|c|c|c} G_1 & G_2 & G_3 & G_4 \end{array} \right)$$

where

$$G_1 = \left(\begin{array}{ccc|ccc|ccc|ccc|ccc} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{array} \right)$$

$$G_2 = \left(\begin{array}{ccc|ccc|ccc|ccc} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{array} \right)$$

$$G_3 = \left(\begin{array}{ccc|ccc|ccc|ccc} 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{array} \right)$$

$$G_4 = \left(\begin{array}{ccc|ccc|ccc|ccc} 0&0&1&1&0&1&0&1&1&1&1&1\\ 0&0&0&0&1&0&1&1&0&1&0&0\\ 1&1&1&1&1&0&1&1&1&1&1&0\\ 1&0&1&1&0&1&1&0&0&1&0&0\\ 1&0&0&1&0&0&1&0&0&1&0&0\\ 0&1&0&0&1&0&0&1&0&0&1&0\\ 0&0&1&0&0&1&0&0&1&0&0&1 \end{array}\right)$$

The dual code of the perfect $\pi - Ham(17,2)$ *code* C' *of type* $\pi = \pi = [4][2]^{16}$ *is generated by the matrix*

$$G' = \left(\begin{array}{c|c|c} G'_1 & G'_2 & G'_3 \end{array}\right)$$

where

$$G'_1 = \left(\begin{array}{cccc|cc|cc|cc} 1&0&0&0&0&0&1&0&0&1&1&1\\ 0&1&0&0&0&0&0&1&1&1&1&0\\ 0&0&1&0&0&0&0&0&0&0&0&0\\ 0&0&0&1&0&0&0&0&0&0&0&0\\ 0&0&0&0&1&0&1&0&1&0&1&0\\ 0&0&0&0&0&1&0&1&0&1&0&1 \end{array}\right),$$

$$G'_2 = \left(\begin{array}{cc|cc|cc|cc|cc|cc} 0&0&1&0&0&1&1&1&0&0&1&0\\ 0&0&0&1&1&1&1&0&0&0&0&1\\ 1&0&1&0&1&0&1&0&0&1&0&1\\ 0&1&0&1&0&1&0&1&1&1&1&1\\ 1&0&1&0&1&0&1&0&1&0&1&0\\ 0&1&0&1&0&1&0&1&0&1&0&1 \end{array}\right),$$

$$G_3' = \left(\begin{array}{cc|cc|cc|cc|cc|cc} 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{array}\right).$$

5.2 Simplex LEB codes

Definition 5.2.1. *A code is said to be simplex if all its non-zero codewords have the same weight.*

Example 5.2.2. *The binary LEB code C of length $n = 10$, dimension $k = 6$, and type $\pi = [2]^5$; and whose generator matrix:*

$$G = \left(\begin{array}{cc|cc|cc|cc|cc} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{array}\right)$$

is simplex. In fact, all non-zero codewords of C have only one nul block. Then, the π-weight of any codeword of C is 4.

Theorem 5.2.3. *Let π-Ham(r,q) be a Hamming code of type $\pi = [m]^s$. The dual code $(\pi\text{-}Ham(r,q))^\perp$ is a Simplex code and the common π-weight of its non-zero codewords is $w_\lambda = q^{r-m} = q^{(\lambda-1)m}$ where $\lambda = \frac{r}{m}$ is an integer ≥ 1.*

Proof. Let C' be a dual code of a $\pi - Ham(r,q)$ code C of type $\pi = [m]^s$. Then by Theorem 6.2.4, C' is generated by H_λ, where

$$H_2 = \left(\begin{array}{c|c|c|c|c} I_m & E_1 & \dots & E_{q^m-1} & 0_m \\ 0_m & I_m & \dots & I_m & I_m \end{array}\right)$$

For $\lambda \geq 3$

$$H_\lambda = \left(\begin{array}{c|c|c|c|c} I_m & A_1 & ..... & A_{q^m-1} & A_0 \\ 0_{m(\lambda-1)} & H_{\lambda-1} & ..... & H_{\lambda-1} & H_{\lambda-1} \end{array} \right)$$

- Set s_λ and w_λ where $r = n - k = m\lambda$ and $t \geq 2$ respectively the number of blocks of H_λ and the weight of a codeword c in S_λ.

- The non-zero codewords generated by H_2, have the weight

$$w_2 = s_2 - 1 = \frac{q^{2m} - 1}{q^m - 1} - 1 = q^m - 1 + 1 = q^{(2-1)m}.$$

  In fact, they have one of the following forms : $c = (e \mid a_1 \mid a_2 \mid \ldots \mid a_{q^m} \mid 0)$ or $c = (0 \mid e_1 \mid e_2 \mid \ldots \mid e_{q^m})$ where for all $i = 1, \ldots, q^m,\ a_i$ is a codeword generated by $H_{\lambda-1}$, e_i is in $\mathbb{F}_q^m$ and e is an element of the canonic basis of $\mathbb{F}_q^m$.

- We assume that the non-zero codewords generated by $H_{\lambda-1}$ have the weight $w_{\lambda-1} = q^{r-2m} = q^{r(\lambda-2)}$.

- Then, the non-zero codewords of the sub-code generated by the last $(r - m)$ rows of H_λ have the form $c = (0 \mid a_1 \mid a_2 \mid \ldots \mid a_{q^m})$ where for all $i = 1, \ldots, q^m,\ a_i$ is a codeword generated by $H_{\lambda-1}$. Therefore,

$$w_\lambda = q^m.w_{\lambda-1} = q^m(q^{r-2m}) = q^{r-m}.$$

- The remaining non-zero codewords generated by $H_{\lambda-1}$ have the form $c = (e \mid a_1 \mid a_2 \mid \ldots \mid a_{q^m-1}, \underbrace{0 \ldots 0}_{s_{\lambda-1} time})$ where for all $i = 1, \ldots, q^m,\ a_i \neq 0$ and e is an element of the canonical basis of $\mathbb{F}_q^m$. These codewords have the weight

$$\begin{aligned} w_\lambda &= s_\lambda - s_{\lambda-1} \\ &= \frac{q^{m\lambda}-1}{q^m-1} - \frac{q^{m(\lambda-1)}-1}{q^m-1} \\ &= \frac{q^{m\lambda}-q^{m(\lambda-1)}}{q^m-1} \\ &= q^{m(\lambda-1)}\left(\frac{q^m-1}{q^m-1}\right) \\ &= q^{m(\lambda-1)} = q^{r-m} \end{aligned}$$

- Thus by induction, all the non-zero codewords of C' have the weight

$$w_\lambda = q^{r-m} = q^{(\lambda-1)m}.$$

□

Example 5.2.4. *The non-zero codewords of the simplex code C' of type $\pi = [4]^{17}$ generated by the matrix*

$$G = (G_1 \mid G_2 \mid G_3)$$

where

$$G_1 = \left(\begin{array}{cccc|cccc|cccc|cccc|cccc|cccc} 1&0&0&0&0&0&0&0&1&0&0&0&0&1&0&0&1&1&0&0&0&0&0&1 \\ 0&1&0&0&0&0&0&0&0&1&0&0&1&1&0&0&1&0&0&0&0&0&1&1 \\ 0&0&1&0&0&0&0&0&0&0&1&0&0&0&0&1&0&0&1&1&1&0&1&0 \\ 0&0&0&1&0&0&0&0&0&0&0&1&0&0&1&1&0&0&1&0&0&1&0&1 \\ 0&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0 \\ 0&0&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0 \\ 0&0&0&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0 \\ 0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1 \end{array}\right),$$

$$G_2 = \left(\begin{array}{cccc|cccc|cccc|cccc|cccc} 1&0&0&1&0&1&0&1&1&1&0&1&0&0&1&1&1&0&1&1 \\ 0&1&1&1&1&1&1&1&1&0&1&1&0&0&1&0&0&1&1&0 \\ 1&0&0&0&1&0&1&1&1&0&0&1&0&1&0&1&0&1&1&1 \\ 0&1&0&0&0&1&1&0&0&1&1&1&1&1&1&1&1&1&1&0 \\ 1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0 \\ 0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0 \\ 0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0 \\ 0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1 \end{array}\right)$$

and

$$G_3 = \left(\begin{array}{cccc|cccc|cccc|cccc|cccc} 0&1&1&1&1&1&1&1&0&0&1&0&1&0&1&0&0&1&1&0&1&1&1&0 \\ 1&1&1&0&1&0&1&0&0&0&0&1&0&1&0&1&1&1&0&1&1&0&0&1 \\ 0&1&0&0&0&1&1&0&1&1&1&1&1&1&0&1&1&1&1&0&1&1&0&0 \\ 1&1&0&0&1&1&0&1&1&0&1&0&1&0&1&1&1&0&0&1&1&0&0&0 \\ 1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0 \\ 0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0 \\ 0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0 \\ 0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1 \end{array}\right)$$

all codewords of $C_{2,8}$ *have the weight* $2^{8-4} = 16$

have all the weight $2^{8-4} = 16$

Remark 5.2.5. The dual of an LEB perfect π-Hamming code is not a simplex LEB codes in general.

In fact, for the dual code of the perfect $\pi - Ham(17, 2)$ code C' of type $\pi = [4][2]^{16}$

defined in the Example 5.1.19,

$$c_1 = (0010 \mid 00 \mid 00 \mid 00 \mid 00 \mid 10 \mid 10 \mid 10 \mid 10 \mid 01 \mid 01 \mid 01 \mid 01 \mid 11 \mid 11 \mid 11 \mid 11)$$

and

$$c_2 = (0000 \mid 01 \mid 01 \mid 01 \mid 01 \mid 01 \mid 01 \mid 01 \mid 01 \mid 01 \mid 01 \mid 01 \mid 01 \mid 01 \mid 01 \mid 01)$$

are codewords of C' of respective π-weight $w_\pi(c_1) = 13$ and $w_\pi(c_2) = 16$. Then, C' is not a simplex code.

5.3 Conclusion

In this chapter, we have constructed large families of Hamming codes of types $\pi = [m]^{\frac{q^r-1}{q^m-1}}$ and $\pi = [l][m]^{\frac{q^r-1}{q^m-1}}$ using their parity check matrix. We have showed that LEB Hamming codes are perfect and have given conditions to the constructed perfect codes to be Hamming codes. We have also given conditions of existence of simplex codes. Then we have showed that the dual of a Hamming LEB code of types $\pi = [m]^{\frac{q^r-1}{q^m-1}}$ is a Simplex LEB codee, however, the dual of a hamming LEB code of type and $\pi = [l][m]^{\frac{q^r-1}{q^m-1}}$ is not a simplex code, which means that the dual of a Hamming LEB code is not a simplex LEB code in general.

Chapter 6 π-Weight enumerator of Particular Families of Linear Error-Block Codes

Table Contents

The weight enumerator of a linear code is a classifying polynomial associated with the code. Besides its intrinsic importance as a mathematical object, it is used in the probability theory around codes. For example, the weight enumerator of a binary code is very useful if we want to study the probability that a received message is closer to a different codeword than to the codeword sent (Or, rephrased: the probability that a maximum likelihood decoder makes a decoding error.). The weight distribution of a linear code is probably one of the most important characteristics of a code. Sometimes the weight distribution can uniquely identify a linear code. One key important fact about weight distributions is how they are linked to the dual. In fact, MacWilliams [37] showed that the Hamming weight enumerator of the dual code is uniquely determined by the Hamming weight enumerator of a code over a finite field. In [28], Feng *et al.* generalized the definition of the homogeneous π-weight enumerator and the MacWilliams Identity to

the LEB case.

In this chapter, we extend the definition of the weight enumerator to linear error-block codes case, and give a simple formula for the π-weight for some families of LEB codes, namely the Hamming and the Simplex codes, cosets leaders of LEB codes, and the direct sum of two LEB codes as well as the puncturing and the Shortening techniques. This paper is organized as follows. In Section 1, a definition of the π-weight enumerator and some related results are reached. In Section 2, we give the π-weight enumerator of simplex codes. In Section 3, the study is focused on the π-weight enumerator for cosets of an LEB codes. In Section 4, we determine the π-weight distribution of LEB codes generated from the direct sum of two LEB codes. The π-weight distribution of LEB codes generated from the puncturing and shortening techniques is determined in Section 5. Finally, the conclusion and the perspective of this chapter are given in Section 6. The results of this chapter are published in [10].

6.1 π-Weight Enumerator of an LEB Code

In this section, we introduce the notion of π-weight distribution for an LEB code, and we give some relevant results.

Definition 6.1.1. *Let C be an $[n, k, d]_q$ code of type $\pi = [n_1][n_2]\dots[n_s]$ where $n_1 \geq n_2 \geq \dots \geq n_s \geq 1$ with $s \geq 1$ and $\sum_{i=1}^{s} n_i = n$. Let*

$$A_i(C) =\mid \{c \in C / w_\pi(c) = i\} \mid$$

be the number of codewords in C of π-weight i for $i = 0, 1, \dots, s$.

The π-weight spectrum of C is defined as the following

$$S_\pi(C) = \{(i, A_i(C)) / i = 1, \dots, s\}.$$

And the weight distribution of a linear code C is the vector

$$A(C) = (A_0(C), \ldots, A_s(C)),$$

it simply shows the number of codewords of a particular π-weight in the code.

The so called π-weight enumerator is a convenient representation of the weight spectrum.

Definition 6.1.2. *Let C be an $[n, k, d]_q$ code of type $\pi = [n_1][n_2]\ldots[n_s]$ where $n_1 \geq n_2 \geq \ldots \geq n_s \geq 1$ and $s \geq 1$ with $\sum_{i=1}^{s} n_i = n$.*

- *The π-weight enumerator of C is defined as the following polynomial*

$$w_{\pi,C}(Z) = \sum_{i=0}^{s} A_i(C) Z^i.$$

  where $A_i(C)$ is the number of codewords in C of π-weight i.

- *The homogeneous π-weight enumerator of C is defined as*

$$\begin{aligned} W_{\pi,C}(X, Y) &= \sum_{c \in C} X^{s - w_\pi(c)} Y^{w_\pi(c)} \\ &= \sum_{i=0}^{s} A_i(C) X^{s-i} Y^i. \end{aligned}$$

  where $A_i(C)$ is the number of codewords in C of π-weight i.

Remark 6.1.3. Note that $w_{\pi,C}(Z)$ and $W_{\pi,C}(X, Y)$ are equivalent in representing the weight spectrum. They determine each other uniquely by the following equations:

$$w_{\pi,C}(Z) = W_{\pi,C}(1, Z)$$

and

$$W_{\pi,C}(X, Y) = X^s w_{\pi,C}(Y.X^{-1})$$

Proposition 6.1.4. *Let C be an $[n, k, d]$ LEB code over $\mathbb{F}_q$. Then*

1. *$A_0 = 1$ and $A_j = 0$ for $0 < j < d$.*
2. *$\sum_j A_j = q^k$*

Proof. easy to prove by analogy to the classical case. □

Example 6.1.5.

- *The zero code has one codeword of π-weight is zero. Then*

$$W_{\pi,C}(X, Y) = A_0(C)X^{s-0}Y^0 = X^s.$$

- *For an $[n, k, d]_q$ MDS code C of type $\pi = [m]^s$, the π-weight distribution of C is:*

$$A_i(C) = \tbinom{s}{i}(q^m - 1)\sum_{j=0}^{i-d}\tbinom{i-1}{j}q^{m(i-d-j)}(-1)^j$$

for $d \leq i \leq s$.

$A_i = 0$ for $1 \leq i < d$, and $A_0 = 1$.

Thus, the π-weight distribution of C is

$$W_{\pi,C}(X, Y) = \sum_{i=0}^{s} A_i(C)X^{s-i}Y^i$$

The weight enumerator satisfies the MacWilliams Identity, which was showed for codes of type $\pi = [m]^s$ in [28] as follows:

Theorem 6.1.6. *[28] Let C be a linear code over $\mathbb{F}_q$ of type $\pi = [m]^s$. Then*

$$W_{\pi,C^\perp}(X, Y) = \frac{1}{\mid C \mid}W_{\pi,C}(X + (q^m - 1)Y, X - Y).$$

6.2 π-Weight Enumerator of Hamming And Simplex Codes of Type $\pi = [m]^s$ Where $s = \frac{q^r-1}{q^m-1}$

In this section, we consider simplex codes of type $\pi = [m]^s$ with $s = \frac{q^r-1}{q^m-1}$ where $r = \lambda m$, $\lambda \geq 2$ and $dim_{\mathbb{F}_q}(C) = n - r$. These codes give interesting results about the π-weight enumerator described in Theorem 6.2.1 and Theorem 6.2.2.

Theorem 6.2.1. *Let C be an $[n, r, d = 3]_q$ simplex LEB code over $\mathbb{F}_q$ of type $\pi = [m]^s$ where $s = \frac{q^r-1}{q^m-1}$, $r = \lambda m$, $\lambda \geq 2$ and $r \geq 1$. Then, the homogeneous π-weight of C equals :*

$$W_{\pi,C}(X, Y) = X^s + (q^r - 1)X^{s-r+m}Y^{r-m}$$

Proof. Let C be an $[n, r, 3]_q$ simplex code over $\mathbb{F}_q$ of type $\pi = [m]^s$ where $s = \frac{q^r-1}{q^m-1}$ and $r = n - dim_{\mathbb{F}_q}(C)$, then by Theorem 5.2.3 of Chapter 5 all non-zero codewords of C have the π-weight q^{r-m}. Therefore,

$$\begin{aligned} W_{\pi,C}(X, Y) &= \sum_{w_\pi=0}^{s} A_{w_\pi}(C)X^{s-w_\pi(c)}Y^{w_\pi(c)} \\ &= A_0(C)X^{s-0}Y^0 + A_{q^{r-m}}(C)X^{s-r+m}Y^{r-m} \\ &= X^s + (\mid C \mid -1)X^{s-r+m}Y^{r-m} \\ &= X^s + (q^r - 1)X^{s-r+m}Y^{r-m} \end{aligned}$$

□

Theorem 6.2.2. *Let H_π be an $[n, k, d = 3]_q$ perfect $\pi - ham(n - k, q)$ code of type $\pi = [m]^s$ where $s = \frac{q^r-1}{q^m-1}$, $r = \lambda m$, $\lambda \geq 2$ and $k = n - r \geq 1$. Then the homogeneous π-weight of H_π equals :*

$$\begin{aligned} W_{\pi,H_\pi}(X, Y) = \frac{1}{q^k}[&(X + (q^m - 1)Y)^s + (q^r - 1) \\ &(X + (q^m - 1)Y)^{s-r+m}(X - Y)^{r-m}] \end{aligned}$$

Proof. Let H_π be an $[n,k,3]_q$ perfect $\pi - ham(n-k,q)$ code of type $\pi = [m]^s$ where $s = \frac{q^r-1}{q^m-1}$, r is a multiple of m and $r = n-k \geq 1$.

Then H_π is the dual code of an $[n,k,3]_q$ simplex code C of type $\pi = [m]^s$ where $s = \frac{q^r-1}{q^m-1}$. Hence, the MacWilliams Identity states that

$$W_{\pi,H_\pi}(X,Y) = \frac{1}{\mid C \mid} W_{\pi,C}(X + (q^m-1)Y, X - Y)$$

Thanks to Theorem 6.2.1,

$$W_{\pi,C}(X,Y) = X^s + (q^r-1)X^{s-r+m}Y^{r-m}$$

. Then,

$$\begin{aligned} W_{\pi,H_\pi}(X,Y) = \frac{1}{q^k}[&(X + (q^m-1)Y)^s + (q^r-1) \\ &(X + (q^m-1)Y)^{s-r+m}(X-Y)^{r-m}] \end{aligned}$$

□

Example 6.2.3. *Let S be the simplex $[10,4,3]_2$ code of type $\pi = [2]^5$ generated by the matrix*

$$G = \left(\begin{array}{cc|cc|c|c|c} 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{array}\right)$$

Therefore,

$$W_{\pi,S}(X,Y) = X^5 + 15X^3Y^2$$

is the homogeneous π-weight of S, and

$$W_{\pi,H_\pi}(X,Y) = \frac{1}{16}[(X+15Y)^5 + 15(X+15Y)^3(X-Y)^2]$$

is the homogeneous π-weight of H_π, where H_π is the $\pi - Ham(6,2)$ LEB code of type $\pi = [2]^5$.

Let C be an LEB code over $\mathbb{F}_q^n$ and v be any vector in $\mathbb{F}_q^n$. A coset of C is a set $v+C$ defined by

$$v + C = \{v + c, c \in C\}.$$

Just like codes, the cosets have a π-weight distribution and a minimum π-weight. A vector in a coset with minimum π-weight is called a coset leader. In this section, the π-weight distribution of cosets of an LEB codes are studied. We will show that some cosets have uniquely determined distributions. We will also prove that when the weight distribution of the cosets is known, and that the dimension of the LEB code is increased by one, the new resulting π-weight is explicitly determined.

Theorem 6.2.4. *Let C be an $[n,k,d]$ LEB code over $\mathbb{F}_q^n$, of type $\pi = [n_1]\dots[n_s]$ ($n_1 \geq \dots \geq n_s \geq 1$, $s \geq 1$ and $n_1 = \sum_{i=0}^{s} n_i$) and with π-weight enumerator $W_{\pi,C}(X)$. Let u be a vector in $\mathbb{F}_q^n$ which is not in C (i.e. $u \in \mathbb{F}_q^n \setminus C$). Let C' be the $[n,k+1]$ LEB code generated by C and u, and $\alpha \in \mathbb{F}_q$. Then,*

i) The weight distributions of $u+C$ and $\alpha u + C$ are identical, when $\alpha \neq 0$.

ii) $W_{\pi,C'} = (q-1)W_{\pi,u+C} + W_{\pi,C}$.

Proof. Since $\alpha u + C = \alpha(u+C)$, the weight distributions of $\alpha u + C$ and $\alpha(u+C)$ are identical. Moreover, the π-weight $w_\pi(\alpha(u+c)) = w_\pi(u+c)$ for all $c \in C$. Thus, (i) is proven. Let $u \in \mathbb{F}_q^n \setminus C$, and C' be the $[n,k+1]$ LEB code generated by C and u. Then, the generator matrix of C' is the generator matrix G of C with the vector u appended as a new row, and so, C' is the same code as $C \cup (u+C)$. From Theorem 1.1. in [22], we

state that $\mathbb{F}_q^n$ is just the union of q^{n-k} distinct cosets of C, and since C is the coset $0+C$, then, $C \cap \alpha u + C$ is empty for all $\alpha \in \mathbb{F}_q^n \setminus \{0\}$. Thus, $A_i(C') = (q-1)A_i(\alpha u + C) + A_i(C)$. Since $A_i(\alpha u + C) = A_i(u + C)$ by (i) then, $A_i(C') = (q-1)A_i(u+C) + A_i(C)$ for all $i \in \{0, \ldots, s\}$ and

$$\begin{aligned} W_{\pi,C'}(X) &= \sum_{i=0}^{s} A_i(C')X^i \\ &= \sum_{i=0}^{s} (A_i(C) + (q-1)A_i(u+C))X^i \\ &= \sum_{i=0}^{s} A_i(C)X^i + (q-1)\sum_{i=0}^{s} A_i(u+C)X^i \\ &= (q-1)W_{\pi,u+C} + W_{\pi,C} \end{aligned}$$

□

6.3 π-Weight Enumerators and Direct Sum

Let C_1 and C_2 be $[n_1, k_1, d_1]_q$ and $[n_2, k_2, d_2]_q$ LEB codes types $\pi_1 = [n_1] \ldots [n_{s_1}]$ ($n_1 \geq \ldots \geq n_{s_1} \geq 1$ and $n_1 = \sum_{i=0}^{s_1} n_i$) and $\pi_2 = [m_1] \ldots [m_{s_2}]$ ($m_1 \geq \ldots \geq m_{s_2} \geq 1$ and $m_2 = \sum_{i=0}^{s_2} m_i$), and with generator matrices G_1 and G_2 respectively. We denote by $\pi_1\pi_2$ the partition defined by

$$\pi = \pi_1\pi_2 = [n_1] \ldots [n_{s_1}] [m_1] \ldots [m_{s_2}]$$

The direct sum of C_1 and C_2 is the

$$[n_1 + n_2, k_1 + k_2, min(d_1, d_2)]$$

LEB code C of type $\pi = [\pi_1][\pi_2]$ where

$$C = C_1 \oplus C_2 = \{(c_1, c_2)/c_1 \in C_1, c_2 \in C_2\}.$$

In the following theorem, we give the π-weight Enumerator of C:

Theorem 6.3.1. *Let C_1 and C_2 be $[n_1, k_1]_q$ and $[n_2, k_2]_q$ LEB codes types of π_1 and π_2, and with π-weights enumerators $W_{\pi_1,C_1}(X)$ and $W_{\pi_2,C_2}(X)$ respectively. The π-weight enumerator of the code $C = C_1 \oplus C_2$ is*

$$W_{\pi,C_1\oplus C_2}(X) = W_{\pi_1,C_1}(X).W_{\pi_2,C_2}(X),$$

where $\pi = [\pi_1][\pi_2]$.

Proof. Let C_1 and C_2 be two LEB codes as defined above, with generator matrices G_1 and G_2 respectively. Then, the generator matrix of $C = C_1 \oplus C_2$ is

$$G = \begin{pmatrix} G_1 & 0 \\ 0 & G_2 \end{pmatrix}$$

Let $A(C_1)$, $A(C_2)$ and $A(C)$ be the weight distributions for C_1, C_2 and C respectively. Furthermore, let $A_i(C_1)$, $A_i(C_2)$ and $A_i(C)$ be the number of codewords of C_1, C_2 and C of π-weight i respectively. Let c_1 and c_2 two codewords of C_1 and C_2 respectively and such that $w_\pi(c_1) = i$ and $w_\pi(c_2) = j$. The vectors $(c_1, 0)$, $(0, c_2)$ and (c_1, c_2) are codewords of C, with π-weights i, j and $i + j$ respectively. Thus, $A_k = A_i(C_1) \times A_j(C_2)$ for all i, j such that $k = i + j$.

$A(C)$ being the result of a convolution of π-weights distribution vectors $A(C_1)$ and $A(C_2)$, we get

$$\begin{aligned} W_{\pi,C}(X) &= \sum_{k=0}^{s_1+s_2} A_k(C)X^k \\ &= \sum_{j+i=k} A_i(C_1)X^i A_j(C_2)X^j \\ &= \sum_{j+i=k} A_i(C_1)A_j(C_2)X^{i+j} \\ &= W_{\pi_1,C_1}(X).W_{\pi_2,C_2}(X) \end{aligned}$$

□

Example 6.3.2. *Let C_1 and C_2 be $[4,3,1]_2$ and $[3,1,1]$ LEB code of types $\pi_1 = [2][1]^2$ and $\pi_2 = [3]^1$, and defined using their generator matrices*

$$G_1 = \left(\begin{array}{cc|c|c} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{array}\right)$$

and

$$G_1 = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$$

respectively. Then, C_1 have the weight distribution $A_0(C_1) = 1$, $A_1(C_1) = 1$, $A_2(C_1) = 5$ and $A_3(C_1) = 1$, and C_2 have the weight distribution $A_0(C_2) = 1$ and $A_1(C_2) = 1$. Thus,

$$W_{\pi,C_1}(X) = 1 + X + 5X^2 + X^3$$

and

$$W_{\pi,C_2}(X) = 1 + X$$

. Hence, $C = C_1 \oplus C_2$ is a $[7,4,1]$ code with generator matrix

$$G = \begin{pmatrix} G_1 & 0 \\ 0 & G_2 \end{pmatrix}.$$

Moreover, the π-weights enumerator of C is

$$\begin{aligned} W_{\pi,C}(X) &= W_{\pi_1,C_1}(X).W_{\pi_2,C_2}(X) \\ &= 1 + 2X + 6X^2 + 6X^3 + X^4. \end{aligned}$$

6.4 π-Weight Enumerators of Punctured and Shortened LEB Codes

In this section, we aim to determine the π-weight enumerator of punctured and shortened LEB codes.

The π-weight distribution of an LEB code obtained from a known LEB code by either puncturing or shortening techniques is in general not determined by the π-weight distribution of the original code. But, after adding some conformity conditions, thus, our original LEB code can determine the π-weight distribution of the punctured and shortened LEB codes. One of these conditions, is the homogeneity of an LEB code that we define bellow.

Definition 6.4.1 (Homogenous LEB Code)**.** *Let C be an $[n,k]_q$ LEB code over $\mathbb{F}_q$ and of type $\pi = [n_1]\dots[n_s]$ (where s is an integer ≥ 1, $\sum_{i=1}^{s} n_i = n$, and $n_1 \geq \dots \geq n_s \geq 1$). Let M be a $q^k \times n$ matrix whose rows consisting on all codewords of C, and for $i = 1, \dots, s$ such that $A_i(C) \neq 0$, let consider M_i, the sub-matrix of M, consisting of all codewords with π-weight i.*

C is said to be homogeneous if and only if all blocks of M_i have the same π-weight. (Note that to have the π-weight of a block we should take this block as a vector in blocks.)

Example 6.4.2. *Let C be an $[8,2,2]_2$ LEB codes of type $\pi = [3][2]^2[1]$ defined as follows:*

$$C = \{000 \mid 00 \mid 00 \mid 0; 101 \mid 11 \mid 00 \mid 0; 000 \mid 00 \mid 01 \mid 1; 101 \mid 11 \mid 01 \mid 1\}.$$

Let $i = 3$, the punctured and the shortened codes in the i^{th} block location are respectively the codes

$$C_p = \{000 \mid 00 \mid 0; 101 \mid 11 \mid 0; 000 \mid 00 \mid 1; 101 \mid 11 \mid 1\},$$

and

$$C_s = \{000 \mid 00 \mid 0; 101 \mid 11 \mid 0\}.$$

Moreover, C is a homogeneous LEB code. In fact, For

$$M_0 = (000 \mid 00 \mid 00 \mid 0)$$

each block of M_0 is of π-weight 0. *For*

$$M_2 = \left(\begin{array}{c|c|c|c} 101 & 11 & 00 & 0 \\ 000 & 00 & 01 & 1 \end{array}\right),$$

each block of M_1 is of π-weight 1.

For

$$M_4 = (101 \mid 11 \mid 01 \mid 1),$$

each block of M_1 is of π-weight 1.

We have the following results:

Theorem 6.4.3. *Let C be a homogeneous $[n, k, d > 1]_q$ LEB code over $\mathbb{F}_q$ and of type $\pi = [n_1] \dots [n_s]$ (where s is an integer ≥ 1, $\sum_{i=1}^{s} n_i = n$, and $n_1 \geq \dots \geq n_s \geq 1$). Let C_p and C_s respectively, the obtained LEB codes after puncturing C in the i^{th} block location. Then, for $i = 1, \dots, s-1$ we have:*

1. $A_i(C_p) = \frac{s-i}{s} A_i(C) + \frac{i+1}{s} A_{i+1}(C)$
2. $A_i(C_s) = \frac{s-i}{s} A_i(C)$

Proof. Let C be a homogeneous $[n, k]_q$ LEB code over $\mathbb{F}_q$ and of type $\pi = [n_1] \dots [n_s]$ (where s is an integer ≥ 1, $\sum_{i=1}^{s} n_i = n$, and $n_1 \geq \dots \geq n_s \geq 1$). Let C_p and C_s respectively, the obtained LEB codes after puncturing C in the i^{th} block location. Let $1 \leq i \leq s-1$, then a vector of π-weight i in C_p comes either from a vector of π-weight i in C with a zero in the punctured block, or a vector of π-weight $i+1$ in C with a nonzero block in the punctured block; as $d > 1$, then no vector in C_p could be found in both ways.

On the other hand, the number of nonzero blocks in all rows of M_i is $sw_{\pi,i} = iA_i(C)$ where $w_{\pi,i}$ is the π-weight of a block of M_i. Since C is homogeneous, then the π-weight is independent of the block, and thus $w_{\pi,i} = \frac{i}{s}A_i$. Therefore, M_i has $\frac{s-i}{s}A_i(C)$ null block. Hence, 1) holds. Since, a vector of π-weight i in C_s comes from a vector of π-weight i in C with a zero on the shortened block, then 2) is yield. □

Example 6.4.4. *Continuing with the Example 6.4.2, we have* $s = 4$, $A_0(C) = 1$, $A_1(C) = 0$, $A_2(C) = 2$ *and* $A_4(C) = 1$, *and*

$$\begin{aligned} A_0(C_p) &= \frac{s-0}{s}A_0(C) + \frac{0+1}{s}A_{0+1}(C) \\ &= 1, \end{aligned}$$

$$\begin{aligned} A_1(C_p) &= \frac{s-1}{s}A_1(C) + \frac{1+1}{s}A_{1+1}(C) \\ &= 1, \end{aligned}$$

$$\begin{aligned} A_2(C_p) &= \frac{s-2}{s}A_2(C) + \frac{2+1}{s}A_{2+1}(C) \\ &= 1, \end{aligned}$$

and

$$\begin{aligned} A_3(C_p) &= \frac{s-3}{s}A_3(C) + \frac{3+1}{s}A_{3+1}(C) \\ &= 1. \end{aligned}$$

we have also

$$\begin{aligned} A_0(C_s) &= \frac{s-0}{s}A_0(C) \\ &= 1, \end{aligned}$$

$$A_1(C_s) = \frac{s-1}{s} A_1(C)$$
$$= 0,$$

$$A_2(C_s) = \frac{s-2}{s} A_2(C)$$
$$= 1$$

and

$$A_3(C_s) = \frac{s-3}{s} A_3(C)$$
$$= 0.$$

6.5 Conclusion

In this chapter, we aimed to extend the notion of π-weight enumerator to the LEB case, define its properties and determine the π-weight distribution of some families of LEB codes.

Firstly, thanks to the MacWilliams Identity, we have given a simple formula to the π-weight enumerator polynomial of both Hamming and simplex LEB codes.

Secondly, we have studied the notion of π-weight enumerator for the cosets of an LEB code, and we have proven that some cosets have uniquely determined distributions. We have also proven that when the weight distribution of the cosets is known, and that the dimension of the LEB code is increased by one, the new resulting π-weight is explicitly determined.

Thirdly, we have shown that the π-weight enumerator of the code obtained from the direct sum of two LEB codes, is the multiplication of the respective π-weight enumerators of these two codes.

Finally, we have studied the π-distribution of punctured and shortened LEB codes.

Forthcoming work involves determining the π-weight enumerator polynomial of some other families of LEB codes such as the family of LEB π-constacyclic codes.

CHAPTER

7 LEB CODES AND TENSOR PRODUCT

Table Contents

Tensor codes (TP codes for abbreviation) were introduced by J.K Wolf in [61] and were generalized in [35]. They are the result of the tensor product of the parity check of two constituent codes. These particular codes have found applications in digital storage systems and digital recording systems [4, 18].

The codes generated using tensor product and called tensor codes have properties and composition similar to Linear Error Block codes. In this chapter we study in depth the construction of new LEB codes using tensor product (TP). We also show that the TP code

formed by two LEB codes is also an LEB code. We prove that the TP of two Hamming codes is not a Hamming code with minimum distance 3, besides, it is not a perfect LEB code. We show that the TP code formed by two π-cyclic codes (resp. simplex LEB codes) is a π-cyclic code (resp. simplex LEB code).

7.1 Tensor Product Codes

Definition 7.1.1. *Let $A = (a_{ij})$ be an m-by-n matrix and let $B = (b_{ij})$ be a p-by-q matrix. The tensor product of A and B is an mp-by-nq matrix defined as*

$$A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B & \dots & a_{1n}B \\ a_{21}B & a_{22}B & \dots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \dots & a_{mn}B \end{bmatrix} \tag{7.1}$$

Definition 7.1.2. *The Tensor Product (TP) of two codes is formed by taking the tensor product of the parity-check matrices or generator matrices of the two codes [61].*

7.2 Tensor Product of Two Linear Block Codes

Remark 7.2.1. The tensor product code of two Hamming codes is not a Hamming code. In fact, let C_1 and C_2 be respectively an $[n_1 = 2^m - 1, 2^m - 1 - m, 3]$ and an $[n_2 = 2^l - 1, 2^l - 1 - l, 3]$ (m and l are integers bigger than 2) Hamming codes and C the TP code resulting from the tensor product of C_1 and C_2.

To be also a Hamming code, C needs to be written as $[N = 2^M - 1, 2^M - 1 - M, 3]$ with M a positive integer bigger than 2.

The code C is the TP code generated using C_1 and C_2. Then by definition

$$\begin{aligned} N &= n_1 \times n_2 \\ 2^M - 1 &= (2^m - 1) \times (2^l - 1) \\ 2^M - 1 &= 2^{m+l} - 2^m - 2^l + 1 \\ 2^M &= 2^{m+l} - 2^m - 2^l + 2 \\ 2^{M-1} &= 2^{m+l-1} - 2^{m-1} - 2^{l-1} + 1 \end{aligned}$$

the last equality is only possible if the integers m, l and M are equal to 1 which is absurd since we supposed that these integers are bigger or equal to 2.

There is an interesting property that is transmitted to the TP code formed by two Hamming codes, which is the blocks of the check matrix of the generated codes are pairewaise linearly independent. However, there exist three blocks such that, the union of columns of those blocks are linearly dependent. Therefore:

Remark 7.2.2. The minimal distance of the TP code formed by two Hamming codes is equal to 3.

Remark 7.2.3. In general the TP code of two classical codes is not an LEB code.

Theorem 7.2.4. *The resulting code of the TP code of two classical codes, is not a linear error-block code.*

Proof. We give the proof for the case $d = 3$ and the case $d = 4$ is done in the same way with some minor modifications. Let C_1 be an $[n_1, k_1, 3]$ code of parity-check matrix H_1 and C_2 be an $[n_2, k_2, 3]$ code of parity check matrix H_2. The parity-check matrix of the TP code C formed from these two codes is of size $r \times n$ where $r = (n_1 - k_1) \times (n_2 - k_2)$ and $n = n_1 \times n_2$. Set $r_1 = n_1 - k_1$ and $r_2 = n_2 - k_2$. If C is an LEB code with minimum $\pi-$distance $d = 3 = 2 \times 1 + 1$ then $\pi = [n_1]^{n_2}$ and it satisfies the Hamming bounds defined as follows:

$$q^r \geq 1 + \sum_{i=1}^{s} (q^{n_i} - 1). \tag{7.2}$$

We have $q^r = q^{r_1 r_2}$ and $1 + \sum_{i=1}^{s}(q^{n_i} - 1) = 1 + n_2(q^{n_1} - 1)$. Since $n = n_1 n_2$, then $1 + n_2(q^{n_1} - 1) >> q^{r_1 r_2}$. Therefore $1 + \sum_{i=1}^{s}(q^{n_i} - 1) > q^r$ and this is a contradiction with

(7.2). Thus C is not an LEB code. □

Example 7.2.5. *The TP code C formed from two binary Hamming codes C_1 and C_2 with the same parameters $[7, 4, 3]$ is not a linear error-block code. In fact, set $r_1 = r_2 = 7 - 4 = 3$. If C is an LEB code of type π then $\pi = [7]^7$ and according to the Hamming bounds we will have the following:*

$$2^r \geq 1 + \sum_{i=1}^{s} (2^{n_i} - 1). \tag{7.3}$$

Where $r = r_1.r_2 = 3.3 = 9$, $s = 7$ and for all $i = 1, \ldots, s$, $n_i = 7$.

We have

$$\begin{aligned} 2^r - (1 + \sum_{i=1}^{s} (2^{n_i} - 1)) &= 2^9 - (1 + \sum_{i=1}^{7} (2^7 - 1) \\ &= 512 - (1 + 7.127) \\ &= 512 - 890 < 0 \end{aligned}$$

Thus $2^r < (1 + \sum_{i=1}^{s} (2^{n_i} - 1))$ which makes a contradiction with 7.3. Finally, C is not an LEB code.

7.3 Construction of LEB Codes Using Tensor Product by Parity Check-Matrices

In this section, we are motivated to explore the other ways we can use the tensor product to produce LEB. To do, we explore two constructions which we will explain in more details.

7.3.1 The Tensor Product of Two LEB Codes

Our first construction is inspired from the construction of tensor codes in the classical case. It is the tensor product of two LEB codes. From different examples and some

theoretical proof, we gathered that this product can produce another LEB code.

In general, we denote two LEB codes C_1 defined as $[n_1, k_1, d_1]$ and C_2 defined by $[n_2, k_2, d_2]$ with partitions $\pi_1 = [m_1]^{s_1}$ and $\pi_2 = [m_2]^{s_2}$ respectively.

We use the Hamming LEB code to illustrate the different cases, but we will always give the corresponding analogy to the general case.

As a reminder, here is the Hamming LEB code (binary of length $n_1 = 10$, dimension $k = 6$ and type $\pi = [2]^5$) control matrix:

$$H = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} \tag{7.4}$$

When we do the tensor product of $H \otimes H$ the resulting matrix is a 16 by 100 matrix.

$$H \otimes H = \begin{bmatrix} H & 0 & 0 & 0 & 0 & H & H & 0 & H & H \\ 0 & H & 0 & 0 & H & 0 & H & H & 0 & H \\ 0 & 0 & 0 & H & 0 & H & 0 & H & 0 & H \\ 0 & 0 & H & 0 & H & 0 & H & 0 & H & 0 \end{bmatrix} \tag{7.5}$$

After doing the tensor product comes the choice of the partition which is one of the most important factors in a LEB code. There are two natural choices that seem worthy of trial, that are:

we have $n_1 = n_2 = 10,\ k_1 = k_2 = 6, s_1 = s_2 = 5$

$\pi = [2]^{50}$ $([m_1]^{s_1.m_2.s_2} = [m_1]^{s_1.n_2})$ This choice does actually generate an LEB code, but it defies the purpose of the tensor construction. Also, we do not make use of the structure

of the constituent codes.

$\pi = [10]^{10}$ $([m_1.s_1]^{m_2.s_2} = [n_1]^{n_2})$ This choice is in our opinion the most suitable. We get 10 blocks of length 10 each, but also every underlying block keeps the structure of one of the constructing codes (that we hope to use to simplify the decoding procedure of the lengthy code). By definition it is still an LEB code.

In the following corollary, we prove the LEB structure of this tensor product.

Corollary 7.3.1. *Let C_1 and C_2 be two LEB codes with parameters $[n_1, k_1, d_1]$ and $[n_2, k_2, d_2]$, of types $\pi_1 = [n_1] \dots [n_{s_1}]$ and $\pi_2 = [m_1] \dots [m_{s_2}]$ (where $n_1 = \sum_{i=1}^{s_1} n_i$, and $n_2 = \sum_{i=1}^{s_2} m_i$ such that, $n_1 \geq \dots \geq n_{s_1} > 1$ and $m_1 \geq \dots \geq m_{s_2} > 1$). Then, the TP code of C_1 and C_2 is also an LEB code.*

Proof. To prove that the TP code C of two LEB codes C_1 and C_2 with parameters $[n_1, k_1, d_1]$ and $[n_2, k_2, d_2]$ is an LEB code, we prove that C is a sub-space of $\mathbb{F}_2^n$. Take c_1 and c_2 two codewords of C and α and λ two elements of $\mathbb{F}_2$. Since $c_i^t.H = 0$ for $i = 1, 2$, then $(\alpha c_1 + \beta c_2)^t.H = 0$ and $\alpha c_1 + \beta c_2$ is a codeword of C. Since $(C, +)$ is an abelian group then C is a subspace of $\mathbb{F}_2^n$. □

Example 7.3.2. *Let C_1 be an $[n_1, k_1, 3]$ $\pi - Ham(r_1, q)$ code of type $\pi = [m_1]^{s_1}$ and C_2 be an $[n_2, k_2, 3]$ $\pi - Ham(r_2, q)$ code of type $\pi = [m_2]^{s_2}$. The TP code C of C_1 and C_2 is an LEB code of type $\pi = [n_1]^{n_2}$.*

7.3.2 Classical Code Tensor LEB

Unlike the previous constructions, the construction presented in this section is more of an hybrid construction between LEB codes and classical codes. We will try both sides to see the resulting code if it is in fact an LEB code and what properties they hold.

To illustrate this construction, we use the $[7, 4, 3]$ Hamming code and the $[10, 6]$ LEB Hamming code (a code of H parity check matrix shown in (7.4)).

The parity check matrix of the Hamming code $[7, 4, 3]$ is

$$A = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \tag{7.6}$$

The tensor product of H and A, will also give a 12 by 70 check matrix of an LEB code

$$H \otimes A = \begin{bmatrix} A & 0 & 0 & 0 & 0 & A & A & 0 & A & A \\ 0 & A & 0 & 0 & A & 0 & A & A & 0 & A \\ 0 & 0 & 0 & A & 0 & A & 0 & A & 0 & A \\ 0 & 0 & A & 0 & A & 0 & A & 0 & A & 0 \end{bmatrix} \tag{7.7}$$

We come back again to the choice of the partition π and the most suitable choice is $\pi = [7]^{10}$.

7.4 Construction of TP Codes of LEB Codes Using Generators Matrices

7.4.1 Tensor Product of Two Cyclic Linear Error-Block Codes

Theorem 7.4.1. *Let C_1 and C_2 be respectively $[n_1, k_1, d_1]$ and $[n_2, k_2, d_2]$ cyclic LEB codes of types $\pi_1 = [m_1]^{s_1}$ and $\pi_2 = [m_2]^{s_2}$ where $s_1 \wedge s_2 = 1$, then the code $C = C_1 \otimes C_2$ of type $\pi = [n_1 m_2]^{s_2}$ is an $[n_1 n_2, k_1 k_2, d_1]$ cyclic LEB code.*

Proof. Assume C_1 and C_2 are two $[n_1, k_1, d_1]$ and $[n_2, k_2, d_2]$ π-cyclic codes of types $\pi_1 = [m_1]^{s_1}$ and $\pi_2 = [m_2]^{s_2}$, and of generator polynomials $g(X) = \sum_{i=0}^{s_1-k_1} g_i(X) \star X^i$ and $g'(X) = \sum_{j=0}^{s_2-k_2} g'_j(X) \star X^j$ respectively, where $g_i(X), g_j(X) \in R_{1,\pi}$ ($R_{1,\pi}$ is defined in Proposition 3.1.5). The code $C = C_1 \otimes C_2$ of type $\pi = [n_1 m_2]^{s_2}$ is defined by its generator matrix

$$G = G_1 \otimes G_2 = \left(\begin{array}{c|c|c|c|c|c} \gamma_0 & \dots & \gamma_r & 0 & \dots\dots & 0 \\ 0 & \gamma_0 & \dots & \gamma_r & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \gamma_0 & \dots & \gamma_r \end{array}\right).$$

where $\gamma_i = g_i(x) \star G_2$, G_1 and G_2 are generator matrices of C_1 and C_2 respectively and $\star$ is the multiplication low defined in Definition 3.1.3 Chapter 3.

A codeword $c(X,Y)$ of $C = C_1 \otimes C_2$ can be obtained from the matrix representation $(\alpha_{ij})_{0 \leq i < s_1 - 10 \leq j < s_2 - 1}$ as follows

$$c(X,Y) = \sum_{i=0}^{s_1-1} \sum_{i=0}^{s_2-1} \alpha_{ij} \star X^{\star i} \star Y^{\star j} mod(X^{m_1 m_2} - 1).$$

Where $\alpha_{i,j} \in R_{1,\pi}$ Since $X^{n_1} = 1$ and $Y^{n_2} = 1$, then $X \star c(X,Y)$ and $Y \star c(X,Y)$ represent cyclic shifts of the rows and the columns, and also belong to $C = C_1 \otimes C_2$. Therefore C is an ideal of $(\frac{\mathbb{F}q[X]}{<X^{m_1 m_2 - 1>}}, \star)$. To represent $C(X,Y)$ as a polynomial $\tilde{C}(Z)$ with unique variable Z, we suppose s_1 and s_2 are relatively prime. Then by the Chineese remainder for each pair i, j where $0 \leq i < s_1 - 1$ and $0 \leq j < s_2 - 1$, there is a unique integer $0 \leq I(i_1, i_2) < s_1 s_2$ such that $I(i,j) \equiv i \ mod[s_1]$ and $I(i,j) \equiv j \ mod[s_2]$ and

$$\tilde{C}(Z) = \sum_{i=0}^{s_1-1} \sum_{i=0}^{s_2-1} \alpha_{ij} \star Z^{\star I(i,j)} mod(Z^{m_1 m_2 - 1}).$$

where $Z = X \star Y$.

Since $C(X,Y) \in C$, $Y \star C(X,Y) \in C$, then $Z \star \tilde{C}(Z) = X \star Y \star C(X,Y) \in C$. Therefore C is an LEB π-cyclic code. □

7.4.2 Tensor Product of Two Simplex Linear Error-Block Codes

Theorem 7.4.2. *Let C_1 and C_2 two simplex codes with parameters $[n_1, k_1]$ and $[n_2, k_2]$, and of types $\pi_1 = [m_1]^{s_1}$ and $\pi = [m_2]^{s_2}$ respectively. The TP code C of C_1 and C_2 is a*

simplex code of type $\pi = [n_1 m_2]^{s_2}$ *and the common* π*-weight of the non zero codewords of* C *is*

$$w_{\lambda_2} = 2^{r_2 - m_2} = 2^{(\lambda_2 - 1)m_2}$$

where $\lambda_2 = \frac{r_2}{m_2}$ *is an integer and for* $i = 1, 2$ $s_i = \frac{q^{r_i}-1}{q^{m_i-1}-1}$ *and* $r_i = n_i - k_i$.

Proof. Suppose C_1 and C_2 are simplex, then the LEB code of type $\pi = [n_1 m_2]^{s_2}$ is an $[n_1 n_2, k_1 k_2, d_1]$ defined by its generator matrix $G_2 = G_{1,\lambda=2} \otimes G_{2,\lambda=2} =$

$$\left(\begin{array}{c|c|c|c|c} I_{m_2} \otimes G_{1,\lambda=2} & E_1 \otimes G_{1,\lambda=2} & \ldots\ldots & E_{q^{m_2}-1} \otimes G_{1,\lambda=2} & 0_{m_2} \otimes G_{1,\lambda=2} \\ 0_{m_2} \otimes G_{1,\lambda=2} & I_{m_2} \otimes G_{1,\lambda=2} & \ldots\ldots & I_{m_2} \otimes G_{1,\lambda=2} & I_{m_2} \otimes G_{1,\lambda=2} \end{array}\right)$$

and for $\lambda_2 \geq 3$, define inductively G_{λ_2} by: $G_{\lambda_2} = G_{1,\lambda} \otimes G_{2,\lambda} =$

$$\left(\begin{array}{c|c|c|c|c} I_{m_2} \otimes G_{1,\lambda} & A_1 \otimes G_{1,\lambda} & \ldots & A_{q^{m_2}-1} \otimes G_{1,\lambda} & A_0 \otimes G_{1,\lambda} \\ 0_{m_2(\lambda_2-1)} \otimes G_{1,\lambda} & H_{\lambda_2-1} \otimes G_{1,\lambda} & \ldots & H_{\lambda_2-1} \otimes G_{1,\lambda} & H_{\lambda_2-1} \otimes G_{1,\lambda} \end{array}\right)$$

where $E_1, \ldots, E_{q^m-1}$ are the extensions of non-zero vectors in $\mathbb{F}_q^m$ (see Definition 5.1.7 for more details), and $G_{1,\lambda}$ with $(\lambda \geq 3)$ and $G_{2,\lambda}$ are respectively generator matrices of C_1 and C_2 with the form defined in Equations (5.1) and (5.2).

- Set s_{λ_2} and w_{λ_2} where $r_2 = n_2 - k_2 = m_2\lambda$ respectively the number of blocks of G_{λ_2} and the weight of a codeword c in S_{λ_2}.
- The non-zero codewords generated by G_2, have the weight

$$w_2 = s_{2,\lambda_2=2} - 1 = \frac{q^{2m_2}-1}{q^{m_2}-1} - 1 = q^{m_2} - 1 + 1 = q^{(2-1)m_2}.$$

In fact, each non-zero codeword generated by G_2 is defined by one of the following

forms of matrices :

$$c = (e \otimes G_{1,\lambda} \mid a_1 \otimes G_{1,\lambda} \mid a_2 \otimes G_{1,\lambda} \mid \ldots \mid a_{q^{m_2}} \otimes G_{1,\lambda} \mid 0 \otimes G_{1,\lambda})$$

or

$$c = (0 \otimes G_{1,\lambda} \mid e_1 \otimes G_{1,\lambda} \mid e_2 \otimes G_{1,\lambda} \mid \ldots \mid e_{q^{m_2}} \otimes G_{1,\lambda})$$

where for all $i = 1, \ldots, q^{m_2},\ a_i$ is a codeword generated by $H_{\lambda_2 - 1}$, e_i is in $\mathbb{F}_q^{m_2}$ and e is an element of the canonic basis of $\mathbb{F}_q^{m_2}$.

- We suppose the non-zero codewords generated by $H_{\lambda_2 - 1}$ have the weight

$$w_{\lambda_2 - 1} = q^{r_2 - 2m_2} = q^{r_2(\lambda_2 - 2)}.$$

- Then, the non-zero codewords of the sub-code generated by the last $(r_2 - m_2)$ rows of G_{λ_2} are defined by the matrix $c = (0 \otimes G_{1,\lambda} \mid a_1 \otimes G_{1,\lambda} \mid a_2 \otimes G_{1,\lambda} \mid \ldots \mid a_{q^m} \otimes G_{1,\lambda})$ where for all $i = 1, \ldots, q^m,\ a_i$ is a codeword generated by $H_{\lambda_2 - 1}$. Therefore,

$$w_{\lambda_2} = q^{m_2}.w_{\lambda_2 - 1} = q^{m_2}(q^{r_2 - 2m_2}) = q^{r_2 - m_2}.$$

- The remaining non-zero codewords generated by $H_{\lambda_2 - 1}$ is defined by the matrix $(e \otimes G_{1,\lambda} \mid a_1 \otimes G_{1,\lambda} \mid a_2 \otimes G_{1,\lambda} \mid \ldots \mid a_{q^m - 1} \otimes G_{1,\lambda}, \underbrace{0 \otimes G_{1,\lambda} \ldots 0 \otimes G_{1,\lambda}}_{s_{\lambda_2 - 1} time})$ where for all $i = 1, \ldots, q^{m_2},\ a_i \neq 0$ and e is an element of the canonic basis of $\mathbb{F}_q^{m_2}$. These codewords have the weight

$$\begin{aligned} w_{\lambda_2} &= s_{2,\lambda_2} - s_{2,\lambda_2 - 1} \\ &= \frac{q^{m_2 \lambda_2} - 1}{q^{m_2} - 1} - \frac{q^{m_2(\lambda_2 - 1)} - 1}{q^{m_2} - 1} \\ &= \frac{q^{m_2 \lambda_2} - q^{m_2(\lambda_2 - 1)}}{q^{m_2} - 1} \\ &= q^{m_2(\lambda_2 - 1)}\left(\frac{q^{m_2} - 1}{q^{m_2} - 1}\right) \\ &= q^{m_2(\lambda_2 - 1)} = q^{r_2 - m_2} \end{aligned}$$

- Thus by induction on λ_2, all the non-zero codewords of C' have the weight

$$w_{\lambda_2} = q^{r_2 - m_2} = q^{(\lambda_2 - 1)m_2}.$$

□

7.5 Conclusion

In this chapter we have explored the different possibilities using tensor product and LEB codes, we have presented two different constructions of LEB codes using tensor product. We have shown that the tensor product of two LEB codes is an LEB code. Besides, we have shown that the tensor product of two cyclic LEB codes is a cyclic LEB code and the tensor product of two Simplex LEB codes is also a simplex LEB code.

Conclusion and Perspectives

The research presented in this thesis gives an algebraic survey of some particular families of LEB codes, and an interesting construction of new families of LEB codes. To this end, we have presented a study of some existing results on linear error-block codes, including new results that we have introduced by our publications.

For perfect LEB codes. We first have given conditions of existence of perfect LEB codes with minimum π-distance 3 and type $\pi = [n_1] \dots [n_t][2]^s$ where $n_1 \geq \dots \geq n_t \geq 2$ and $t \geq 1$ and $s \geq 1$ (and respectively $\pi = [n_1][3]^s$ and $\pi = [n_1][n_2][3]^s$) and we have giving an algorithm to generate these codes. Then, we have shown that there exists an infinite family of codes of type $\pi = [n_1] \dots [n_t][2]^s$ where $n_1 \geq \dots \geq n_t \geq 2$, $t \geq 1$ and $s \geq 1$.

For Hamming and Simplex LEB codes. We have given a construction of large families of Hamming codes of types $\pi = [m]^{\frac{q^r-1}{q^m-1}}$ using their parity check matrix. We have shown that LEB Hamming codes are perfect and give conditions to the constructed perfect codes to be Hamming codes. Finally, We have given conditions of existence of Simplex LEB codes. We show that the dual of a Hamming LEB code of type $\pi = [m]^{\frac{q^r-1}{q^m-1}}$ is a Simplex LEB code.

For constacyclic LEB codes. We have started by giving an algebraic study of LEB constacyclic codes. Then we have interested to two speacial subfamilies of constacyclic LEB codes. The first one is the family of cyclic LEB code, after the definition we have

shown that LEB cyclic codes are ideals, we have given a matrix representation of this family of codes, then, we have described an efficient decoding algorithm to these codes, which is actually the first algebraic decoding algorithm defined for the cyclic LEB codes. The second one, is the family of negacyclic LEB codes.

For Shortened and punctured LEB codes. We have extended the definitions of puncturing and shortening a code to the LEB case, and we have defined some properties of the resulting codes after the puncturing and the shortening operations. We have also studied the relation between punctured and shortened LEB codes, which may help to construct new families of optimal LEB codes.

Finally, for tensor product and LEB codes. We have verified if tensor product codes are themselves LEB. We have constructed new LEB codes based on the tensor product of two particular LEB codes.

In this thesis we have defined the π-weight enumerator of an LEB code and given its properties, we have also given simple formulas for the π-weight enumerator polynomial of both Hamming and Simplex codes. We have also shown that some cosets will have uniquely determined distributions, and finally, we have given the related π-weight enumerator of the direct sum of two LEB codes.

Further to the contributions presented in this thesis, hereafter we state some perspectives we expect to address in forthcoming works.

Firstly, we will continue our research about optimal LEB codes by modifying the LEB codes constructed during this study, using the puncturing and shortening techniques.

Secondly, we will try to give the algebraic construction of LEB BCH codes. To this end, we will give algorithm to factorize $x^n - 1$ on $R_{1,\pi}$ in the sense of the $\star$ multiplication.

Thirdly, we will show that we can construct an infinite perfect binary $[n + 2p.s, k + 2p.s, 3]$ (with p a non zero positive integer) codes of type $\pi = [n_1] \dots [n_t][2p]^s$ where $n_1 \geq \dots \geq n_t \geq 2p$ and $t \geq 1$ and $s \geq 1$, with specification of necessary conditions to

these codes.

Fourthly, we will try to construct binary perfect LEB codes with π-distance 4 and 5, and determine some particular bounds for LEB codes like the Griesmer bound.

Fifthly, we will give the algebraic structure for Goppa and Golay LEB codes.

Finally, we will try to use different subfamilies of LEB cyclic codes in cryptography.

Bibliography

[1] ebats: Ecrypt benchmarking of asymmetric systems. *http://bench.cr.yp.to*, 25 August 2018.

[2] Scott Ahlgren and Ken Ono. Congruence properties for the partition function. *National Academy of Sciences*, 98(23):12882–12884, 2000.

[3] H. L. Alder. Partition identities-from euler to the present. 1707, 1969. Leonhard Euler Tercentenary.

[4] H. Alhussien and J. Moon. An iteratively decodable tensor product code with application to data storage. *IEEE J. Sel. Areas Commun*, 2(28):228–240, 2010.

[5] Zachary A Kent Amanda Folsom and Kent Ono. l-adic properties of the partition function. 3(229):1586–1609, 2012. Advances in Mathematics.

[6] George E. Andrews. The theory of partitions. *Pennsylvania, USA: Addison-Wesley*, 1976. https://doi.org/10.1017/CBO9780511608650.

[7] George E. Andrews. The theory of partitions. *Cambridge University Press*, 1984.

[8] George E. Andrews and F. G. Garvan. Dyson's crank of a partition. 1988. American Mathematical Socitey, vol. 18, no. 2, pp. 167-171.

[9] Richard Askey. The work of george andrews: A madison perspective. 42:24, 1999.

[10] S. Belabssir. π-weight enumerator of particular families of linear error-block codes. *IAENG- International Journal of Computer Sciences*, 49(3):728–735, 2022.

[11] S. Belabssir, E. B. Ayebie, and E. M. Souidi. Perfect, hamming and simplex linear error-block codes with minimum π -distance 3. In *Codes, Cryptology and Information Security - Third International Conference, C2SI 2019, Rabat, Morocco, April 22-24, 2019, Proceedings*, volume 11445 of *Lecture Notes in Computer Science*, pages 288–306. Springer, 2019.

[12] E. R. Berlekamp. Negacyclic codes for the lee metric. *in Proceedings of the Conference on Combinatorial Mathematics and Its Applications*, page 298–316, 1968.

[13] E.R. Berlekamp. Algebraic coding theory. 1984. Aegean Park Press, Walnut Creek.

[14] Daniel J. Bernstein. Grover vs. mceliece. *International Workshop on Post-Quantum Cryptography 2010. Lecture Notes in Computer Science*, 6061:73–80, 2010.

[15] R. C. Bose and D. K. Ray-Chaudhuri. On a class of error correcting binary group codes. *Information and Control*, 3:68–79, Mars 1960.

[16] Henry Bottomley. Partition and composition calculator. http://btinternet.com/ sel16/js/partitions.htm.

[17] E. Calude C. S. Calude and M. S. Queen. The complexity of euler's integer partition theorem. *University of Auckland, NZ, Massey University at Auckland, NZ, Dartmouth College, USA, Centre for Discrete Mathematics and Theoretical Computer Science*, Research Report Series 2011.

[18] P. Chaichanavong and P. H. Siegel. Tensor-product parity code for magnetic recording. *IEEE Trans. Magn.*, 42(2):350–352, 2006.

[19] chilton computing. http://www.chilton-computing.org.uk/acl/associates/permanent/atkin.htm. [Online].

[20] Willard G. Connor. Partition theorems related to some identities of rogers and watson. 214, 1975. Transactions of the American Mathematical Society.

[21] Tanja Lange Daniel J. Bernstein and Christiane Peters. Attacking and defending the mceliece cryptosystem. *Proc. 2nd International Workshop on Post-Quantum Cryptography. Lecture Notes in Computer Science.*, 5299:31–46, 8 August 2008.

[22] R. Dariti. Linear error-block codes and applications. *Thèse de Doctorat, Université Mohammed V-Agdal, Faculté des Sciences*, 2012.

[23] R. Dariti and E. M. Souidi. Cyclicity and decoding of linear error-block codes. *Journal of Theorecal and Applied Information Technology*, 25:39–42, 2011.

[24] R. Dariti and E. M. Souidi. An application of linear error-block codes in steganography. *International Journal of Digital Information and Wireless Communications*, 1:426–433, 2012.

[25] R. Dariti and E. M. Souidi. New families of perfect linear error-block codes. *International Journal of Information and Coding Theory*, 2(2/3):84–95, 2013.

[26] R. Dariti and E. M. Souidi. Packing and covering radii of linear error-block codes. *International Journal of Mathematical and Computational Sciences*, 7(4):13–17, 2013.

[27] Rabiî Dariti and El Mamoun Souidi. Improving code-based steganography with linear error-block codes. *Communications in Computer and Information Science, Springer Berlin Heidelberg*, 189:310–321, 2011. https://doi.org/10.1109/TIT.1978.1055873.

[28] Xu L. Hickernell F.J. Feng, K. Linear error-block codes. 2006. Finite Fields and Their Applications, 12, pp 638–652.

[29] F. G. Garvan. A simple proof of watson's partition congruences for powers of 7. *Australian Mathematical Society*, 36(3):316–334, 1984. https://doi.org/10.1017/S1446788700025386.

[30] M. J. E. Golay. Notes on digital coding. *Proc. IEEE*, 37:657, 1949.

[31] R. W. Hamming. Error detecting and error correcting codes. *The Bell System Technical Journal*, 29(2):147–160, April 1950.

[32] G. H. Hardy. Ramanujan: Twelve lectures on subjects suggested by his life and works. Ams Chelsea Pub.

[33] A. Hocquenghem. Codes correcteurs d'erreurs. *Chiffres*, 2:147–156, 1959.

[34] Brian Hopkins and Robin Wilson. Euler's science of combinations. 2007. Leonhard Euler Tercentenary, no. 1707.

[35] H. Imai and H. Fujiya. Generalized tensor product codes,. *Transactions on Information Theory*, 27(2):181–187, 1981. IEEE.

[36] San Ling and Ferruh Özbudak. Constructions and bounds on linear error-block codes. 45(3):297–316, 2007.

[37] F. J. MacWilliams. A theorem on the distribution of weight in a systematic code. 42(1).

[38] Karl Mahlburg. Partition congruences and the andrews–garvan–dyson crank. *National Academy of Sciences*, 102(43):15373–15376, 2005.

[39] Robert J. McEliece. A public-key cryptosystem based on algebraic coding theory. *DSN Progress Report*, 44:114–116, 1978.

[40] J. E. Meggitt. Error-correcting codes and their implementation. *IRE Trans. Inform. Theory IT*–6, page 459–470, 1960.

[41] J. E. Meggitt. Error-correcting codes for correcting bursts of errors. *IBM J. Res. Develop.*, 4:329–334, 1960.

[42] J. E. Meggitt. Error correcting codes and their implementation. *IRE Trans. Inform. Theory*, 7:232–244, Oct 1961.

[43] D. E. Muller. Application of boolean algebra to switching circuit design. *IEEE Trans. on Computers*, 3:6–12, Sept 1954.

[44] D. K. Ray-Chaudhuri N. Aydin, I. Siap. The structure of 1-generator quasi-twisted codes and new linear codes. *Des. Codes Cryptogr.*, 24:313–326, 2001.

[45] Ken Ono and Jan Hendrik Bruinier. Algebraic formulas for the coeffiecients of half-integral weight harmonic weak mass forms. *Advances in Mathematics*, 46:198–219, 20 October 2013.

[46] N. J. Patterson. The algebraic decoding of goppa codes. *IEEE Transactions on Information Theory*, 21(2):203–207, 1975.

[47] E. Prange. Cyclic error-correcting codes in two symbols. *Tech. Rep. TN*-57 − 103*, Air Force Cambridge Research Labs*, 1957.

[48] E. Prange. Some cyclic error-correcting codes with simple decoding algorithms. *Tech. Rep. TN*-58 − 156*, Air Force Cambridge Research Center*, 1958.

[49] E. Prange. An algorithm for factoring $xn1$ over a finite field. *Tech. Rep. TN*-59 − 175, 1959.

[50] E. Prange. The use of coset equivalence in the analysis and decoding of group codes. *Tech. Rep. TN*-59 − 164, 1959.

[51] E. Prange. Cyclic error-correcting codes in two symbols. *Tech. Rep.TN-57-103, Air Force Cambridge Research Center, Cambridge, MA*, 1957 Sept.

[52] I. S. Reed. A class of multiple-error-correcting codes and a decoding structure. *IEEE Trans. Inform. Theory*, 4:38–49, Sept 1954.

[53] E. M. Souidi S. Belabssir, N. Sahllal. Cyclic linear error-block codes. *AIP Conference Proceedings*, 2074:020005, 02 2019.

[54] C. E. Shannon. A mathematical theory of communication. *The Bell System Technical Journal*, 27:379–423 and 623–656, 1948.

[55] M. V. Subbarao and M. Vidyasagar. On watson's quintuple product identity. *Proceeding of the Americain Mathematical Society*, 26(2):23–27, Sep 1970. https://doi.org/10.23072036795.

[56] A. Tietäväinen. On the nonexistence of perfect codes over finite fields. *SIAM Journal on Applied Mathematics*, 24(1):88–96, 1973.

[57] P. Udomkavanich and S. Jitman. Bounds and modifications on linear error-block codes. 5:35–50, 2010. International Mathematical Forum.

[58] E. Berlekamp; R. McEliece; H. van Tilborg. On the inherent intractability of certain coding problems. *IEEE Transactions on Information Theory*, 24(3):384—-386, 1978. https://doi.org/10.1109/TIT.1978.1055873.

[59] S. Wicker. Error control systems for digital communicationsand storage. *Englewood Cliffs, NJ: Prentice Hall, Inc.*, July 1994.

[60] Herbert S. Wilf. Lectures on partitions. 2000. From PIMS lectures given in summer 2000 at U. of Victoria.

[61] J. K. Wolf. An introduction to tensor product codes and applications to digital storage systems. *Information Theory Workshop*, pages 6–10, 2006.

[62] V. A. Zinovev and V. K. Leontev. Nonexistence of perfect codes over galois fields. *Probl Control Inf Theory*, 2(2):123–132, 1973.