UNIVERZA NA PRIMORSKEM

FAKULTETA ZA MATEMATIKO, NARAVOSLOVJE IN
INFORMACIJSKE TEHNOLOGIJE

DOKTORSKA DISERTACIJA
(DOCTORAL THESIS)

SPLOŠNE KONSTRUCKICJE MINIMALMNIH KOD IZ POSEBNIH RAZREDOV FUNKCIJ NAD KONČNIMI POLJI

(GENERIC CONSTRUCTIONS OF MINIMAL CODES FROM SPECIAL CLASSES OF FUNCTIONS OVER FINITE FIELDS)

RENÉ RODRÍGUEZ ALDAMA

KOPER, 2022

UNIVERZA NA PRIMORSKEM

FAKULTETA ZA MATEMATIKO, NARAVOSLOVJE IN INFORMACIJSKE TEHNOLOGIJE

DOKTORSKA DISERTACIJA
(DOCTORAL THESIS)

SPLOŠNE KONSTRUCKICJE MINIMALMNIH KOD IZ POSEBNIH RAZREDOV FUNKCIJ NAD KONČNIMI POLJI

(GENERIC CONSTRUCTIONS OF MINIMAL CODES FROM SPECIAL CLASSES OF FUNCTIONS OVER FINITE FIELDS)

RENÉ RODRÍGUEZ ALDAMA

KOPER, 2022

MENTOR: PROF. DR. ENES PASALIC
SOMENTOR: DOC. DR. NASTJA CEPAK

Dedicado a
mi madre, mi luz; a mi hermana, mi inspiración; a la memoria de mi padre, y
a mi pequeño motor, Arlet.

Acknowledgements

There are (finitely) many people I wish to express my gratitude to. First off, I would like to thank my supervisor Dr. Enes Pasalic and my co-supervisor Dr. Nastja Cepak who have guided me and taught me so many things about cryptography and research through my doctoral studies. I got to learn a lot from my research projects.

Had lots of fun travelling and learning together with my friends within the crypto group: Amar, Nastja, Sadmir and Samir—thank you. I'm also grateful for having the opportunity to collaborate with Dr. Fengrong Zhang and Dr. Yongzhuang Wei in a number of occasions.

My sincere thanks to the doctoral committee members for their time taken to carefully read the thesis: Dr. Samir Hodžič, Dr. Sihem Mesnager and Dr. Fengrong Zhang. I'd also like to thank the doctoral disposition committee members Dr. Samir Hodžič, Dr. Sihem Mesnager and Dr. Marko Orel for their insightful comments/suggestions.

Starting a new life in a different place is never easy but people in Slovenia, in particular, the Famnit and UP staff, have made my settling in so easy since I've always felt like home in this beautiful country. My heartfelt thanks to all people working at these amazing institutions. Thanks to all professors at the Department of Mathematics at Famnit. Nastja and Nina, I appreciate your help with the Slovene translations.

We've all heard that teaching is a way of learning but you realize how important that is until you experience it—thanks to all of my students!

Sharing knowledge is one of the most fundamental parts of research, I believe there is always something to be learned from everyone. My Famnit colleagues and friends have been a valuable part of my PhD, I can't thank you enough. Special thanks go to Cuau, Jordan, Maheshya and Malvina.

There's no way I leave out any of my dearest friends: Abú, Adi, Ale, Andrés, Blas, Draži, José, Marija, Nataša, Patricio, Robert and Žiga. Thanks for always having my back. You're really special to me. I'm grateful for having met so many amazing people throughout my journey.

Gracias al universo, la naturaleza o a Dios por permitirme vivir tantos momentos tan inolvidables. Por poner en mi camino a gente tan maravillosa.

Nunca me olvidaré de agradecer a todos mis profesores y asesores de todos los niveles escolares en México. Los admiro infinitamente, ¡muchas gracias! Agradecimientos especiales a la Dra. María Luisa Pérez Seguí, al Dr. Elmar Wagner, Dr. Fernando Hernández Hernández y Dr. David Meza Alcántara quienes me enseñaron la belleza de las matemáticas.

A mis amigos incondicionales: Ari, Marco, Pedro y Luciano. A las personas que considero mi familia: Angie, Armando, la Sra. Margarita y el Sr. Armando. ¡Gracias por todo su apoyo, ánimo y enseñanzas! A mis ángeles que siempre me cuidan y protegen: Mi papá, mi abuelita y Don Fer.

Arlet, sobrina mía, tú no lo sabes pero tú fuiste mi (pequeño) motor en la parte final de mi doctorado; gracias a ti concluyo este proyecto con mucho agrado y emoción. Seguiré luchando por mis sueños para darte lo mejor de mí siempre.

Finalmente, con todo el amor, humildad y admiración que tengo en mi ser quiero expresar mis más sinceros agradecimientos a mi mamá y a mi hermana que sin ellas yo no estaría aquí y posiblemente no sería absolutamente nadie. Este sueño mío es para ellas. Ellas que siempre han estado ahí en las buenas y en las malas, luchando a mi lado; las únicas que creyeron en este proyecto desde el principio y que me apoyaron ciegamente en mis decisiones. Es por eso que este logro es de ustedes. Con todo mi corazón, las amo.

Abstract

In the last decades, minimal codes have received a lot of attention from the cryptographic community due to their important applications in security protocols such as secret sharing schemes [5, 50] and secure-two party computation [24], which are essential in today's digital world. This class of linear codes is characterized by a covering property, namely, a linear code is minimal provided that none of its non-zero codewords are covered by any other linearly independent codeword.

From a mathematical point of view, the properties and constructions of infinite families of minimal codes have become a fundamental topic in this area. Much work has been carried out towards a complete understanding of the combinatorial and geometrical properties of these codes [1, 3, 6, 11, 15, 20]. As for constructions, most of them had been based on Ashikhmin-Barg's sufficient condition relating the minimum weight and maximum weight of a code [2], more specifically, if the quotient of the minimum weight over the maximum weight of a q-ary code is strictly larger than $\frac{q-1}{q}$ then the code is minimal. In other words, this condition requires that the weights are close to each other. Linear codes satisfying Ashikhmin-Barg's condition are called narrow, whereas a code not satisfying it is termed wide.

It was a challenge to construct infinite families of wide minimal codes, even in the binary setting, since there were no known examples of such families until the pioneering work of Ding et. al. [20], where they provided three infinite families of wide minimal binary codes using certain constructions based on Boolean functions. Soon after, several methods were introduced to construct wide minimal codes using a vast number of techniques: simplicial complexes [13], characteristic functions [20, 29, 40], projective planes [3], cutting blocking sets [6, 55], maximal arcs [25], weakly regular bent functions [37, 60] and weakly regular plateaud functions [39, 40, 41, 42, 52], etc.

The purpose of this thesis is two-fold. First, elaborating on previous works

[6, 20, 38], we provide several constructions of wide minimal binary codes using the theory of Boolean functions, thus obtaining linear codes suitable for secret sharing or two-party computations protocols. These families have the feature of being flexible in terms of parameters so that they cover a wide range of possible minimum weights.

As a second outcome, some generic constructions of minimal codes will be provided, which are based on different well-known techniques from functions over finite fields together with some new concepts tailored to the construction of minimal codes (e.g. non-covering permutations). These constructions aim to provide a general framework to obtain minimal codes, that can or cannot be wide, in such a way that they have a larger dimension with respect to their length. This is in particular important when considering applications since a practical secure-two party computation protocol (based on linear codes) must be constituted by a minimal code with a high transmission rate. Together with the concept of non-covering permutations, the p-ary case is then treated under this general framework.

All in all, this thesis provides several constructions of (wide) minimal codes from generic constructions relying on the theory of Boolean and p-ary functions. These constructions are generic in the sense that one can, in principle, input any function satisfying certain weak assumptions and obtain different minimal codes which are not equivalent.

The rest of the document is organized as follows. In Chapter 1, the set up for our results together with some motivation are given. In particular, we introduce the concept of a minimal code and highlight its importance in the context of secret sharing schemes and multi-party computation protocols. The necessary definitions and preliminary results about functions, linear codes and minimal codes are presented in Chapter 2.

The main results lie in Chapter 3 and Chapter 4. In Chapter 3, we present four constructions of wide minimal binary linear codes from generic constructions using Boolean functions. For several instances of these constructions, we give a full specification of their weight distributions. These techniques are named with the word “method” and a distinctive mathematical object in question used as an adjective. Thus, we introduce the basis method (Subsection 3.2.2), the affine subspace method (Subsection 3.2.3), the hyperplane method (Section 3.3) and the general Maiorana-McFarland method (Section 3.4).

Finally, three methods to obtain wide minimal codes with a larger dimension are presented in Chapter 4. These approaches are based on standard operation of functions, such as the direct sum or derivatives. In Section 4.1, minimal codes are constructed out of the direct sum of two Boolean functions under some weak assumptions, namely, that one of the associated codes is minimal. For the same purpose of constructing (wide) minimal codes, a novel concept of “non-covering permutation” is introduced in Section 4.2. These permutations turn out to be useful when specifying linear codes associated to bent functions in the Maiorana-McFarland class. The last construction, referred as “the generic construction”, which is a combined version of the direct sum method and the derivative method is given in Section 4.3. Moreover, explicit examples of this approach are given in Section 4.3.1. The generalization of these results to the p-ary case is discussed in Section 4.4.

Four research papers are product of the investigation carried out in this thesis. Three out of four are already published in high impact journals and the fourth one is still in preparation. These articles are listed in the references as [44, 48, 64, 65].

Math. Subj. Class. (2020): 94C10 · 06E301

Keywords: Minimal linear codes · The Ashikhmin-Barg bound · Bent functions · Characteristic functions · Derivatives · Direct sum · Permutations

Povzetek

V zadnjih desetletjih so minimalne kode bile deležne veliko pozornosti kriptografske skupnosti zaradi svojih pomembnih aplikacij v varnostnih protokolih, kot so sheme deljenja skrivnosti [5, 50] in varno dvostransko računanje [24], ki so bistvenega pomena v današnjem digitalnem svetu. Za ta razred linearnih kod je značilna pokrivna lastnost, in sicer je linearna koda minimalna pod pogojem, da nobena od njenih neničelnih kodnih besed ni pokrita z nobeno drugo linearno neodvisno kodno besedo.

Z matematičnega vidika so lastnosti in konstrukcije neskončnih družin minimalnih kod postale temeljna tema na tem področju. Veliko dela je bilo opravljenega za popolno razumevanje kombinatoričnih in geometrijskih lastnosti teh kod [1, 3, 6, 11, 15, 20]. Kar zadeva konstrukcije, jih je večina temeljila na zadostnem Ashikhmin-Bargovem pogoju, ki povezuje najmanjšo in največjo težo kode [2], natančneje, če je količnik najmanjše teže q-arne kode nad njeno največjo težo strogo večji od $\frac{q-1}{q}$, potem je koda minimalna. Z drugimi besedami, ta pogoj zahteva, da so uteži blizu druga drugi. Linearne kode, ki izpolnjujejo pogoj Ashikhmin-Barg, imenujemo ozke, kode, ki tega ne izpolnjujejo, pa široke.

Konstruirati neskončne družine širokih minimalnih kod, tudi v binarni nastavitvi, je bil izziv, saj do pionirskega dela Dinga et. al. [20] nismo imeli nobenega primera. V omenjnem članku so nato predstavili tri neskončne družine širokih minimalnih binarnih kod z uporabo nekaterih konstrukcij, ki temeljijo na Boolovih funkcijah. Kmalu zatem je bilo uvedenih več metod za konstruiranje širokih minimalnih kod z uporabo velikega števila tehnik: simplicialni kompleksi [13], karakteristične funkcije [20, 29, 40], projektivne ravnine [3], rezane bločne množice [6, 55], maksimalni loki [25], šibko regularne ukrivljene funkcije [37, 60] in šibko regularne platojske funkcije [39, 40, 41, 42, 52], itd.

Namen disertacije je dvojen. Prvič, nadaljevanje raziskovalne smeri prejšnjih del [6, 20, 38] in iskanje več konstrukcij širokih minimalnih binarnih kod z uporabo

teorije Boolovih funkcij, s čimer pridobimo linearne kode, primerne za sheme deljenja skrivnosti ali protokole za dvostransko računanje. Te družine imajo značilnost, da imajo takšne prilagodljive parametre, da pokrivajo širok razpon možnih minimalnih uteži.

Kot drugi rezultat bodo predstavljene nekatere splošne konstrukcije minimalnih kod, ki temeljijo na različnih dobro znanih tehnikah funkcij nad končnimi polji, skupaj z nekaterimi novimi koncepti, prilagojenimi konstrukciji minimalnih kod (npr. nepokrivajoče permutacije). Cilj teh konstrukcij je zagotoviti splošen okvir za generacijo minimalnih kod, ki so široke, ali tudi ne, na tak način, da imajo večjo dimenzijo glede na svojo dolžino. To je še posebej pomembno pri obravnavi aplikacij, saj mora biti praktičen varen dvostranski računski protokol (ki temelji na linearnih kodah) sestavljen iz minimalne kode z visokim razmerjem. Skupaj s konceptom nepokrivajočih permutacij se p-arni primer nato obravnava v tem splošnem okviru.

Doktorska disertacija v splošnem ponuja več konstrukcij (širokih) minimalnih kod iz generičnih konstrukcij, ki se opirajo na teorijo Boolovih in p-arnih funkcij. Te konstrukcije so generične v smislu, da lahko kot vhodni podatek vnesemo poljubno funkcijo, ki izpolnjuje določene šibke predpostavke, in pridobimo različne minimalne kode, ki niso ekvivalentne.

Preostali del dokumenta je organiziran na sledeči način. V poglavju 1 so podane teoretične osnove naših rezultatov skupaj z nekaj motivacije. Predstavljen je koncept minimalne kode in poudarjen je njen pomen v kontekstu shem deljenja skrivnosti in večstranskih računskih protokolov. Potrebne definicije in preliminarni rezultati o funkcijah, linearnih kodah in minimalnih kodah so predstavljeni v poglavju 2.

Glavni rezultati so v poglavjih 3 in 4. V poglavju 3 predstavljamo štiri konstrukcije širokih minimalnih binarnih linearnih kod s splošnimi konstrukcijami z uporabo Boolovih funkcij. Za več primerov teh konstrukcij podajamo popolno specifikacijo njihove porazdelitve uteži. Te tehnike so poimenovane z besedo »metoda« in dodanim opisom najpomembnejšim predmeta. Tako uvajamo metodo baze (Poglavje 3.2.2), metodo afinega podprostora (Poglavje 3.2.3), metodo hiperravnine (Poglavje 3.3) in metodo splošne Maiorana-McFarland funkcije (Poglavje 3.4).

Nazadnje so v poglavju 4 predstavljene tri metode za pridobitev širokih minimalnih kod z večjo dimenzijo. Ti pristopi temeljijo na standardnem delovanju funkcij, kot so direktna vsota ali odvodi. V poglavju 4.1 so minimalne kode sestavljene iz direktne vsote dveh Boolovih funkcij pod določenimi šibkimi pred-

postavkami, in sicer, da je ena od povezanih kod minimalna. Za isti namen konstruiranja (širokih) minimalnih kod je v poglavju 4.2 predstavljen nov koncept »nepokrivajoče permutacije«. Te permutacije so uporabne pri določanju linearnih kod, povezanih z ukrivljenimi funkcijami v razredu Maiorana-McFarland. Zadnja konstrukcija, imenovana “splošna konstrukcija”, je kombinirana različica metode direktne vsote in metode odvodov. Podana je v poglavju 4.3 in njeni eksplicitni primeri so podani v poglavju 4.3.1. Posplošitev rezultatov na p-arni primer je obravnavana v poglavju 4.4.

Plod raziskave, opravljene v doktorskem delu, so štiri strokovni članki. Trije od štirih so že objavljeni v uglednih revijah, četrti pa je še v pripravi. Ti članki so v referencah navedeni kot [44, 48, 64, 65].

Math. Subj. Class. (2020): 94C10 · 06E301

Ključne besede: Minimalne linearne kode · Pogoj Ashikhmin-Barg · Ukrivljene funkcije · Karakteristične funkcije · Odvodi · Direktna vsota · Permutacije

Contents

List of Figures

List of Tables

Chapter 1

Introduction

A *code* is an algorithm that turns a source of information (*words*) into a different form (*codewords*). Typically, the source of information is given by means of a set of symbols, called an *alphabet*. An *error-correcting code* is a code for which any errors that are introduced can be detected and corrected. The ultimate purpose of encoding information is to recover the original source message when it is sent to a receiver over a noisy communication channel (see Figure 1.1 and Example 1.0.1).

The study of error-correcting codes belongs to the mathematical field of *Coding Theory*. Coding Theory dates back to 1948, when Claude E. Shannon published his fundamental work *A Mathematical Theory of Communication* [51], in which Shannon introduced the concept of information entropy as a measure of the information content in a message.

Formally, an $(n, M)_Q$-*code* is a proper subset C of Q^n with cardinality M, where Q is a finite non-empty set and n is a positive integer. A precise definition of a code in accordance with the above paragraphs should be given by an injection $\phi : Q^k \to Q^n$ with $M = |Q|^k$, thus, in our working definition, C is simply identified with the direct image of ϕ.

A measure of utmost importance when studying an error-correcting code C is the so-called *minimum distance* d, defined by

$$d := \min\{d_H(x, y) : x = (x_1, \ldots, x_n) \in C, y = (y_1, \ldots, y_n) \in C, x \neq y\}, \quad (1.1)$$

where the function d_H gives the number of coordinates where the input vectors differ. The *information rate* R of an $(n, M)_Q$ code is the proportion of the transmitted data that is not redundant, mathematically, $R := \log_{|Q|}(M)/n$.

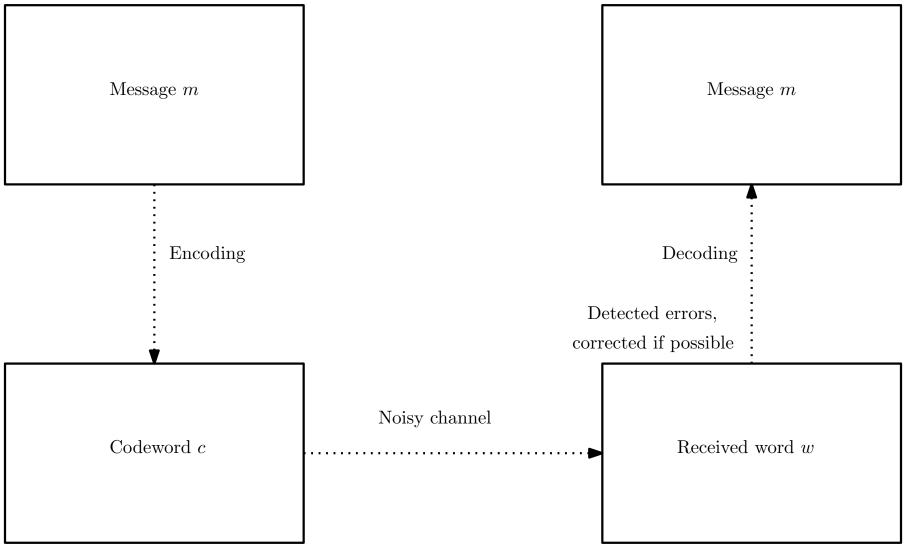


Figure 1.1: Schematic diagram of an error-correcting code.

Example 1.0.1. *Suppose that the alphabet Q consists of the binary symbols (bits) 0 and 1. Let us say that words are all binary vectors of length 3, i.e., $k = 3$. Let C be the code consisting of the following binary vectors of length $n = 8$:*

$$
\begin{aligned}
&c_0 = (0,0,0,0,0,0,0,0);\\
&c_1 = (1,1,1,1,0,0,0,0);\\
&c_2 = (0,0,1,1,1,1,0,0);\\
&c_3 = (0,0,0,0,1,1,1,1);\\
&c_4 = c_1 + c_2 = (1,1,0,0,1,1,0,0);\\
&c_5 = c_1 + c_3 = (1,1,1,1,1,1,1,1);\\
&c_6 = c_2 + c_3 = (0,0,1,1,0,0,1,1);\\
&c_7 = c_1 + c_2 + c_3 = (1,1,0,0,0,0,1,1).
\end{aligned}
$$

The encoding ϕ will be given by

$$(x_1, x_2, x_3) \mapsto x_1c_1 + x_2c_2 + x_3c_3,$$

where $x_i \in \{0,1\}$. Note that the information rate of this code is then $\frac{3}{8}$. If a codeword $c \in C$ is sent over a noisy channel and either two or an odd number of errors are introduced, these can be detected as the received vector would not be a codeword. However, these cannot be corrected in general. For instance, if two errors occurred and the received vector is $(1,1,1,0,1,0,0,0)$, then errors *could have happened either to c_1 at the fourth and fifth coordinate or to c_4 at the third and sixth positions. On the other hand, if only one error occurred over the transmission, then this error can be corrected by computing the closest codeword to the received vector since this will be unique.*

The approach to decoding described in the last paragraph of the previous example is called the *minimum distance decoding*, or, the *nearest neighbor decoding*, and it is the prototypical decoding algorithm for a code.

Error-correcting codes have been widely investigated due to their important applications in consumer electronics, secure multi-party computation [15], secret sharing schemes [11, 22, 63], authentication, data storage systems, association schemes, and strongly regular graphs [9].

There are some assumptions that provide a more structured approach to studying codes such as *linearity*, which is undoubtedly one of the most important assumptions from a mathematical point of view. For a prime power q and a positive integer n, denote by $\mathbb{F}_q^n$ the n-dimensional vector space over the finite field $\mathbb{F}_q$ with q elements. A *linear* $[n, k, d]_q$*-code* is a k-dimensional linear subspace C of $\mathbb{F}_q^n$ whose minimum distance is d.

Since linear codes are subspaces of $\mathbb{F}_q^n$, it is natural to describe them by means of a basis. Given an $[n, k, d]_q$-code C, a $k \times n$ matrix G is called a *generator matrix* of C provided that its rows form a basis for C, i.e. $C = \{aG : a \in \mathbb{F}_q^k\}$. Similarly, an $(n-k) \times n$ matrix H is a *parity-check matrix* of C if its rows are a basis for $C^\perp$, where $C^\perp$ denotes the *dual code* of C, defined by

$$C^\perp = \{x \in \mathbb{F}_q^n : x \cdot y = 0 \text{ for every } y \in C\}, \tag{1.2}$$

where '$\cdot$' denotes the standard dot product in $\mathbb{F}_q^n$.

For linear codes, there exists a simple general decoding algorithm for detecting and correcting errors: let y be the received vector from a codeword x. Assume that at most $e = \lfloor \frac{d-1}{2} \rfloor$ errors of transmission have occurred (this number is called the *error correction capacity* of the code), where d denotes the minimum distance. Error detection works simply by checking if the so-called *syndrome* $s = Hy^T$ is the zero vector since this property characterizes codewords. Error correction works as follows: if the syndrome is not zero, then correcting errors of transmission is equivalent to determining the difference $\epsilon = y - x$, which is called the *error vector*. This can be achieved by visiting all vectors z of Hamming weight at most e in $\mathbb{F}_q^n$ and checking if $Hz^T = s$ since ϵ is the unique vector of Hamming weight at most e in $\mathbb{F}_q^n$ such that $H\epsilon^T = s$. This decoding method for linear codes is typically referred as *syndrome decoding*.

Example 1.0.2. *Continuing with Example 1.0.1, we see that C is a binary linear $[8,3,4]$-code. A parity-check matrix for this code is*

$$H = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Since we know the code C can correct a single error i.e. the error capacity e is equal to 1, we compute the syndromes of vectors of weight at most one[1] *as follows (we omit brackets and commas to simplify notation):*

Error vector ϵ	Syndrome $H\epsilon^T$
00000000	00000^T
10000000	00001^T
01000000	10000^T
00100000	00100^T
00010000	10101^T
00001000	01000^T
00000100	11001^T
00000010	00010^T
00000001	10011^T

For instance, assuming there has been at most one transmission error, the received vector $y = (0,0,1,1,0,1,0,0)$ whose syndrome is the column vector

$$Hy^T = (0,1,0,0,0)^T,$$

is corrected to the codeword

$$x = y - \epsilon = (0,0,1,1,0,1,0,0) - (0,0,0,0,1,0,0,0) = (0,0,1,1,1,1,0,0) = c_2.$$

Our aim in this thesis is to provide several constructions of a particular type of linear codes, called minimal codes, using the theory of Boolean/p-ary functions. The following subsections illustrate the importance of minimal linear codes in real-life applications and provide a sound motivation for their construction and study of their properties.

[1] In general, there is a one-to-one correspondence between syndromes and cosets of C. A vector of minimum weight in each coset is called a *coset leader*. Syndrome decoding then comes down to computing syndromes of coset leaders.

1.1 Secret sharing schemes

Suppose that a dealer knows a secret s which is meant to be distributed among a set of participants $\mathcal{U} = \{P_0, \ldots, P_{n-1}\}$, each of whom is allocated a corresponding share $u_0, \ldots, u_{n-1}$ of the secret. The dealer gives out the secret in such a way that only certain subsets of participants can access the secret when they pool their shares together.

An *access structure* Γ is the family of all the subsets of participants that are able to reconstruct the secret s from their partial information. The elements of Γ are called *authorized sets*, whereas the subsets that are not in Γ are called *unauthorized sets*. This setting is called a *secret sharing scheme* (Figure 1.2) and it was invented independently by George Blakley [5] and Adi Shamir [50] in 1979. Blakley described a type of secret sharing schemes using the fact that n nonparallel $(n-1)$-dimensional hyperplanes intersect at exactly one point [5]. In contrast, Shamir's secret sharing schemes are based on the Lagrange interpolation theorem [50].

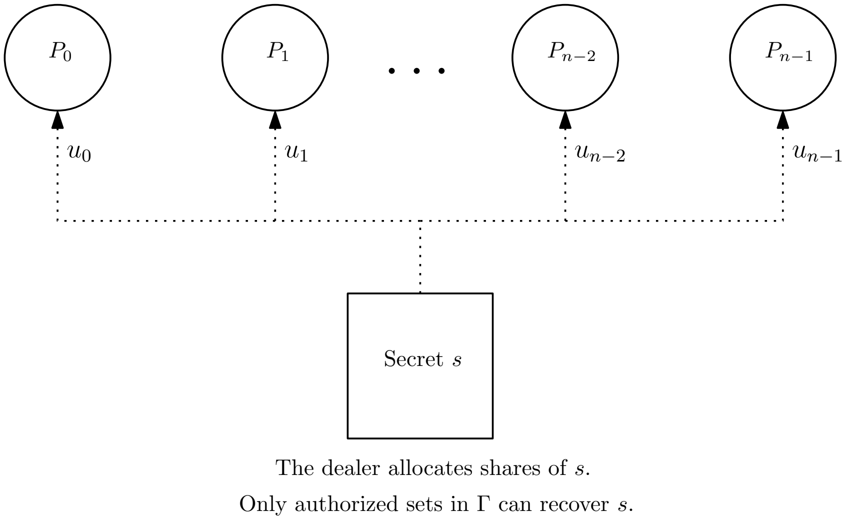

P_0
P_1
$\cdots$
P_{n-2}
P_{n-1}
u_0
u_1
u_{n-2}
u_{n-1}
Secret s
The dealer allocates shares of s.
Only authorized sets in Γ can recover s.

Figure 1.2: A secret sharing scheme.

A secret sharing scheme is called *perfect* when unauthorized sets of participants cannot determine the secret s. Any authorized set $A \in \Gamma$ is *minimal* if its a minimal element of the partially ordered set Γ under inclusion, i.e.

$$A' \subseteq A \text{ and } A' \in \Gamma \text{ implies that } A' = A.$$

A *monotone access structure* Γ is an access structure Γ which is upward closed with respect to inclusion, i.e. for every $A \in \Gamma$,

$$A \subseteq A' \text{ implies } A' \in \Gamma.$$

For monotone access structures, the collection of minimal authorized sets uniquely determines the access structure.

Any linear $[n,k,d]_q$-code C with generator matrix $G = [{g_0}^T \cdots {g_{n-1}}^T]$, where the superscript T means taking transpose, induces a perfect secret sharing scheme with $n-1$ participants $\mathcal{U} = \{P_1, \ldots, P_{n-1}\}$ for which the secret is an element of $\mathbb{F}_q$. The dealer randomly chooses a vector $x = (x_0, \ldots, x_{k-1}) \in \mathbb{F}_q^k$ such that $s = x \cdot g_0$ (out of the q^{k-1} possible choices). Then the dealer computes $u = (s, u_1, \ldots, u_{n-1}) := xG$ and gives the i-th co-ordinate u_i to the i-th participant. Since $s = x \cdot g_0$, the shares $u_{i_1}, \ldots, u_{i_l}$ determine the secret s if and only if g_0 is a linear combination of $g_{i_1}, \ldots, g_{i_l}$ for some l with $1 \leqslant l \leqslant n$. Moreover, if a set of participants can recover the secret, then so can any superset of it. Hence the access structure of such scheme is perfect and monotone. The access structure is then given by

$$\Gamma = \{A \subseteq \mathcal{U} : \exists A' = \{P_{i_1}, \ldots, P_{i_l}\} \subseteq A \text{ with } g_0 = \sum_{j=1}^{l} \lambda_j g_{i_j} \text{ for } \lambda_1, \ldots, \lambda_l \in \mathbb{F}_q\}.$$

This way of constructing secret sharing schemes from linear codes was first observed by James L. Massey [34].

Consider a codeword c in the dual code $C^\perp$ of the form

$$c = (1, 0, \ldots, 0, -c_{i_1}, 0, \ldots, 0, -c_{i_l}, 0, \ldots, 0) \tag{1.3}$$

where c_{i_j} is at coordinate i_j and $c_{i_j} \neq 0$ for at least one $j \in \{1, \ldots, l\}$. By definition, $Gc^T = 0$, which implies $g_0 = \sum_{j=1}^{l} c_{i_j} g_{i_j}$. Therefore, the existence of a codeword in $C^\perp$ of the form (1.3) is equivalent to the corresponding shares being able to recover the secret.

The access structure Γ of this type of secret sharing schemes based on a linear code can be completely determined by the family of minimal authorized sets since Γ is monotone. By the previous observation about dual codewords, it is enough to study *minimal codewords* of a linear code C.

The *support* of a vector $v = (v_1, \ldots, v_n) \in \mathbb{F}_q^n$ is the set of positions for which the corresponding coordinate is nonzero, i.e. $\operatorname{supp}(v) := \{i \in \{1, \ldots, n\} : v_i \neq 0\}$. The *weight* of the vector v, denoted $wt(v)$, equals $|\operatorname{supp}(v)|$. Given a linear code C, a codeword $c_1 \in C$ *covers* another codeword $c_2 \in C$ if the support of

c_1 contains that of c_2. The notation $c_2 \preceq c_1$ represents this relation, namely, that c_1 covers c_2. If a nonzero codeword covers only its scalar multiples, but no other nonzero codewords, then it is called a *minimal codeword*. If every non-zero codeword of a linear code C is minimal, then the code itself is called *minimal*.

At this point, it is clear that there is a one-to-one correspondence between the collection of minimal access sets and the collection of minimal codewords of the dual code $C^{\perp}$ whose first coordinate is one.

The secret sharing schemes based on a linear code are completely determined by its dual code, thus, exchanging the roles, one can study linear codes and consider the secret sharing schemes based on their duals.

In 2003, Jin Yuan and Cunsheng Ding [21] provided the following description of access structures related to minimal linear codes.

For a minimal $[n, k, d]_q$-code C with generator matrix $G = [{g_0}^T \cdots {g_{n-1}}^T]$ whose columns are non-zero, the secret sharing scheme based on $C^{\perp}$ satisfies the following:

- There are q^{k-1} minimal access sets;
- If, for some $1 \leqslant i \leqslant n-1$, g_i is a scalar multiple of g_0, then participant P_i must be in every minimal access set.
- If g_i is not a scalar multiple of g_0 for some $1 \leqslant i \leqslant n-1$, then participant P_i must be in $(q-1)q^{k-2}$ out of q^{k-1} minimal access sets.

1.2 Secure multi-party computation

The general idea behind *secure multi-party computation* is to correctly compute the output of a function, from a number of secret inputs, without leaking any information of the given inputs (see Figure 1.3). More formally, consider n parties or players $P_1, \ldots, P_n$. Suppose that each player P_i holds a secret input x_i and the players agree on some function f that takes n inputs. The final goal is to compute $y = f(x_1, \ldots, x_n)$ while making sure that the following two properties are satisfied:

- (Correctness) The correct value of y is computed;
- (Privacy) The output y is the only new information known to each player.

Unlike traditional cryptographic protocols, where the adversary is outside the set of participants, the cryptography in this model protects participants' privacy from each other, thus the adversaries can be thought as a subset of participants.

Secure multi-party computation was introduced in 1982 by Andrew Yao where he presented the so-called Millionaires' problem [61]. Later, the case $n = 2$ was refined by Yao using any computationally feasible function [62] whereas the multi-party case was studied by Oded Goldreich, Silvio Micali and Avi Wigderson [24].

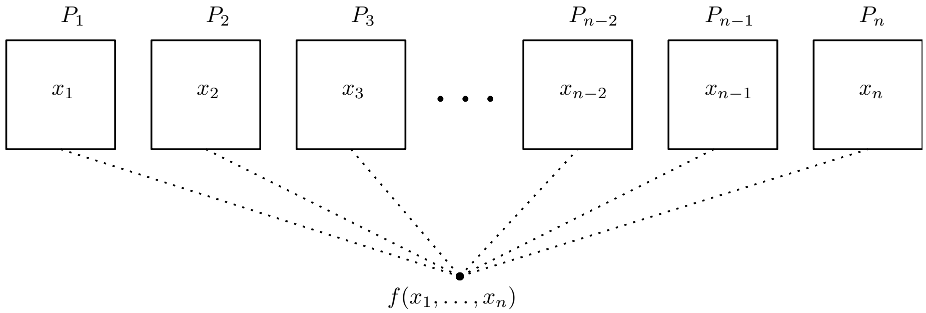


Figure 1.3: Secure multi-party computation protocol.

Let us focus on the particular case of *secure two-party computation* ($n = 2$). Yao's techniques to construct secure two-party computation protocols are based on *garbled circuits* and *oblivious transfer*. Oblivious transfer, introduced by Michael O. Rabin [47], enables a receiver R to obtain one out of N secrets $s_1, \ldots, s_N$ held by a sender S. The receiver chooses an index $i_R \in \{1, \ldots, N\}$, gets s_{i_R} and learns nothing about s_j for $j \neq i_R$. Symmetrically, the sender S learns nothing about i_R.

Linear codes can be used to construct secure two-party computation protocols using oblivious transfer as we describe in the following. For a broader discussion, we refer the reader to [12].

We will only consider the secure evaluation of functions f of the form $f : \mathbb{F}_q^r \times I \to \mathbb{F}_q$ given by $(X, Y) \mapsto \sum_{i=1}^{r} f_i(Y) \cdot x_i$, where I is any given set, and $f_i : I \to \mathbb{F}_q$ are arbitrary functions. The secure computation of these functions is important for several applications in cryptography and signal processing [12].

Let f be a function of the form described in the above paragraph. Suppose that the input of player P_1 is x and the input of player P_2 is y. Consider an $[n, k, d]$-linear code C with parity check matrix H. Denote by H_i the i-th row of H.

- P_1 randomly chooses an encoding $z = (z_1, \ldots, z_n) \in \mathbb{F}_q^n$ of x i.e. $x = Hz^t$ and inputs z.
- P_2 inputs y and computes the support of the vector $v = \sum_{i=1}^{n-k} f_i(y)H_i \in C^{\perp}$, say, $\operatorname{supp}(v) = \{i_1, \ldots, i_t\}$;
- P_1 and P_2 perform an oblivious transfer on $z_1, \ldots, z_n$ and $\{i_1, \ldots, i_t\}$;
- P_2 receives $z_{i_1}, \ldots, z_{i_t}$ not learning anything about the other coordinates and computes $f(X, Y) = \sum_{i=1}^{n-k} f_i(Y)x_i = \sum_{i=1}^{n-k}(f_i(Y)H_i) \cdot z^t$;
- P_2 sends the result to P_1.

The only computation that involves player P_1 uses a t-out-of-n oblivious transfer, thus P_1 does not learn anything about Y. However, the parameter t could leak some information about Y. This can be easily fixed either by using an oblivious transfer protocol that hides the number of items or letting P_2 make some dummy requests.

To ensure that x is not known to P_2 after knowing $f(x, y)$, the code $C^{\perp}$ is required to be a minimal code: For any $v \in C^{\perp}$, let $\Psi_v : C^{\perp} \to \mathbb{F}_q^{n-t}$ be the linear mapping given by $(c_1, \ldots, c_n) \mapsto (c_i)_{i \notin \operatorname{supp}(v)}$. If $C^{\perp}$ is minimal, then $\ker(\Psi_v) = \langle v \rangle$ and $\operatorname{rank}(\Psi_v) = \dim(C^{\perp}) - 1$. Therefore, the remaining coordinates of z that P_2 does not know about lie in an $(n - k - 1)$-dimensional subspace of $C^{\perp}$ so P_2 cannot learn more about x than the scalar $f(x, y)$.

Chapter 2

Definitions and preliminary results

2.1 Boolean functions

For a prime p, the vector space $\mathbb{F}_p^m$ can be identified with the finite field $\mathbb{F}_{p^m}$ by fixing a basis, thus these two objects share the same linear properties. A mapping f from $\mathbb{F}_p^m$ (or from $\mathbb{F}_{p^m}$) to $\mathbb{F}_p$ is called a *p-ary function*. A *vectorial p-ary function* is a mapping of the form $F : \mathbb{F}_p^m \to \mathbb{F}_p^l$ such that m and l are positive integers not necessarily equal. A (vectorial) 2-ary function is simply called a (vectorial) *Boolean function*. The set of m-variable Boolean functions will be denoted by $\mathcal{B}_m$.

Once an ordering of $\mathbb{F}_{p^m}$ is fixed, say, $\mathbb{F}_{p^m} = \{\alpha_0 = 0, \alpha_1, \ldots, \alpha_{p^m-1}\}$, any p-ary function $f : \mathbb{F}_{p^m} \to \mathbb{F}_p$ uniquely determines a sequence of output values, called the *truth table*, given as $[f(\alpha_0), f(\alpha_1), \ldots, f(\alpha_{p^m-1})]$, which in turn can be viewed as a vector of length p^m with entries in $\mathbb{F}_p$.

Throughout, the *lexicographic order* will be considered unless otherwise stated. A function $f : \mathbb{F}_{p^m} \to \mathbb{F}_p$ and its truth table are then treated as the same object whenever there is no ambiguity. The multivariate description of a vectorial function $F : \mathbb{F}_p^m \to \mathbb{F}_p^m$ is described using *coordinate functions* $f_1, \ldots, f_m : \mathbb{F}_p^m \to \mathbb{F}_p$ such that $F(x) = (f_1(x), \ldots, f_m(x))$.

Non-zero linear combinations of coordinate functions are called *component functions*. Then the component functions of F are mappings from $\mathbb{F}_p^m$ to $\mathbb{F}_p$ given by $x \mapsto \langle a, F(x)\rangle$, where $a \in (\mathbb{F}_p^m)^*$ and $\langle \cdot, \cdot \rangle$ is any nondegenerate bilinear form on $\mathbb{F}_p^m$. Equivalently, the component functions of $F : \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$ are the mappings $x \mapsto \mathrm{Tr}(aF(x))$ for $a \in \mathbb{F}_{p^m}^*$, where Tr denotes the *absolute trace* on $\mathbb{F}_{p^m}$, i.e. $\mathrm{Tr}(x) = x + x^p + x^{p^2} + \cdots + x^{p^{m-1}}$. For either $a \in (\mathbb{F}_p^m)^*$ or $a \in \mathbb{F}_{p^m}^*$, we will denote by $a \cdot F$ the corresponding component of F regardless of which algebraic structure is being considered.

One of the most important tools to classify and analyze the behaviour of p-ary functions is the so-called *Walsh-Hadamard transform*. Given $f : \mathbb{F}_p^m \rightarrow \mathbb{F}_p$ and $\lambda \in \mathbb{F}_p^m$, the Walsh-Hadamard transform of f at the point λ is defined as

$$W_f(\lambda) = \sum_{x \in \mathbb{F}_p^m} \xi_p^{f(x) - \lambda \cdot x}, \tag{2.1}$$

where $\xi_p = e^{2\pi i/p}$ is the *complex primitive p-th root of unity*. The multi-set of values $\{\{W_f(\lambda) : \lambda \in \mathbb{F}_p^m\}\}$ is called the *Walsh spectrum* of f and it will be denoted by W_f. We use the superscript $*$ to indicate the subset of non-zero elements of a given set, e.g. $\mathbb{F}_{p^m}^* = \mathbb{F}_{p^m} \setminus \{0\}$ is the cyclic multiplicative group of $\mathbb{F}_{p^m}$.

A *cyclotomic field* $\mathbb{Q}(\xi_p)$ is a field obtained by adjoining ξ_p to the field of rational numbers $\mathbb{Q}$. The field extension $\mathbb{Q}(\xi_p)/\mathbb{Q}$ is a Galois extension[1] of degree $p-1$ whose Galois group $\mathrm{Gal}(\mathbb{Q}(\xi_p)/\mathbb{Q})$ is the set of canonical automorphisms $\{\phi_a : a \in \mathbb{F}_p^*\}$, where $\phi_a : \mathbb{Q}(\xi_p) \rightarrow \mathbb{Q}(\xi_p)$ is defined by $\phi_a(\xi_p) = \xi_p^a$ and $\phi(x) = x$ for every $x \in \mathbb{Q}$.

For several applications, it is important that a Boolean function is far from the set of affine functions. This measure is captured in the notion of *nonlinearity* of a function $f : \mathbb{F}_p^m \rightarrow \mathbb{F}_p$, which is the minimum distance between f and the set of all m-variable affine functions (denoted by $\mathcal{A}_m$), i.e.

$$\mathcal{N}_f = \min_{g \in \mathcal{A}_m} d_H(f, g). \tag{2.2}$$

A p-ary function f is said to be *p-ary bent* (or, simply, bent) if all its Walsh coefficients satisfy

$$|W_f(\lambda)|^2 = p^m. \tag{2.3}$$

In the binary case, a Boolean function $f : \mathbb{F}_2^m \rightarrow \mathbb{F}_2$ is bent if and only if $W_f(\lambda) = \pm 2^{\frac{m}{2}}$ for any $\lambda \in \mathbb{F}_2^m$ and the Walsh transform of a Boolean function f can be related to $\mathcal{N}_f$ using the equality

$$\mathcal{N}_f = 2^{m-1} - \frac{1}{2} \max_{\lambda \in \mathbb{F}_2^m} |W_f(\lambda)|. \tag{2.4}$$

Note that bent Boolean functions exist only for even m. Bent functions were named and introduced by Oscar Rothaus [49] in the 1960s although his research was not published until 1976.

[1] A Galois extension is an algebraic extension which is normal and separable, see [30].

A bent function $f : \mathbb{F}_p^m \to \mathbb{F}_p$ is said to be *regular bent* if for every $\lambda \in \mathbb{F}_p^m$,

$$p^{-m/2} W_f(\lambda) = \xi_p^{\tilde{f}(\lambda)} \tag{2.5}$$

for some mapping $\tilde{f} : \mathbb{F}_p^m \to \mathbb{F}_p$. Such a function $\tilde{f}$ is called the *dual function.* A bent function $f : \mathbb{F}_p^m \to \mathbb{F}_p$ is said to be a *weakly regular bent* function if there exists a complex number u with $|u| = 1$ such that

$$u p^{-m/2} W_f(\lambda) = \xi_p^{\tilde{f}(\lambda)} \tag{2.6}$$

for all $\lambda \in \mathbb{F}_p^m$. Regular bent functions can only be found for even m and for odd m with $p \equiv 1 \pmod 4$. Weakly regular bent functions always come in pairs, since their dual is bent as well. This, in general, does not hold for non-weakly regular bent functions.

Let m be a positive odd integer. A Boolean function $f : \mathbb{F}_2^m \to \mathbb{F}_2$ is called *semi-bent* if and only if its Walsh coefficients lie in $\{0, \pm 2^{\frac{m+1}{2}}\}$. A vectorial Boolean function $F : \mathbb{F}_2^m \to \mathbb{F}_2^m$ is called an *almost bent* or AB function if and only if the Walsh coefficients of its components belong to $\{0, \pm 2^{\frac{m+1}{2}}\}$, equivalently, if all of its components are semi-bent.

Another important parameter of a function $f : \mathbb{F}_p^m \to \mathbb{F}_p$ is its *algebraic degree*, which is the largest degree of all the monomials with a nonzero coefficient $a_i \in \mathbb{F}_p$ in the *algebraic normal form* (ANF) or *multivariate representation* of f, i.e.

$$f(x_1, \ldots, x_m) = \sum_{i=(i_1,\ldots,i_m) \in \mathbb{F}_2^m} a_i \prod_{j=1}^{m} x_j^{i_j} \tag{2.7}$$

For a vectorial function, if $f_1, \ldots, f_m$ are the coordinate functions of F, then the largest degree of the f_i is the algebraic degree of F.

The *derivative* of a function $F : \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$ at direction $\gamma \in \mathbb{F}_{p^m}^*$ is defined as

$$D_\gamma F(x) = F(x + \gamma) - F(x). \tag{2.8}$$

Although the symbol $D_\gamma F$ is not defined for $\gamma = 0$, it will be convenient to set $D_0 F$ to be the identically zero function. We make this convention whenever there is no room for ambiguity.

A mapping $F : \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$ is called *planar* provided that all of its derivatives are permutations. Planar functions can exist only when p is odd. A function $F : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ is called *almost perfect nonlinear* or APN if its derivatives are

2-to-1. For any $a \in \mathbb{F}_{2^m}^*$ and $b \in \mathbb{F}_{2^m}$, we define $\delta(a,b) = |\{x \in \mathbb{F}_{2^m} : D_aF(x) = b\}|$. The *differential uniformity* δ_F of $F : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ is defined as

$$\delta_F = \max_{a \in \mathbb{F}_{2^m}^*, b \in \mathbb{F}_{2^m}} \delta(a,b). \tag{2.9}$$

We also say that F is differentially δ_F-uniform, or simply, δ_F-uniform. The subindex F will be dropped whenever it is clear from the context which function we refer to. APN functions are exactly the 2-uniform functions. It is well-known that every AB function is APN [10]. Most known examples of APN functions and almost all known examples of planar functions are quadratic thus the construction of "new" non-quadratic planar or APN functions is a fundamental unsolved problem in this area.

Here "new functions" means that they are not equivalent under some of the following notions of equivalence. Two vectorial Boolean functions $F_1, F_2 : \mathbb{F}_2^m \to \mathbb{F}_2^l$ are called *affine equivalent* if there exist two affine automorphisms L, L' on $\mathbb{F}_2^m$ and $\mathbb{F}_2^l$, respectively, such that $F_2 = L' \circ F_1 \circ L$. If there also exists an affine vectorial Boolean function $L'' : \mathbb{F}_2^m \to \mathbb{F}_2^l$ such that $F_2 = L' \circ F_1 \circ L + L''$ then they are called *extended affine equivalent* (EA, for short). Moreover, if there exists an affine automorphism on $\mathbb{F}_2^m \times \mathbb{F}_2^l$ that maps the set $\{(x,y) \in \mathbb{F}_2^m \times \mathbb{F}_2^l : y = F_1(x)\}$ onto $\{(x,y) \in \mathbb{F}_2^m \times \mathbb{F}_2^l : y = F_2(x)\}$, then the functions are called *CCZ-equivalent* (Carlet-Charpin-Zinoviev).

Affine equivalence is strictly stronger than EA-equivalence, which in turn is strictly stronger than CCZ-equivalence [10]. The importance of these notions is that certain parameters are preserved, e.g. differential uniformity is preserved under CCZ-equivalence (hence under all of the mentioned equivalences).

The first known examples of AB functions have been *power functions* (or *monomials*) on the field $\mathbb{F}_{2^m}$ for odd m, namely, functions defined by $x \mapsto x^d$. The list of exponents d for which the power function $F(x) = x^d$ is AB are displayed in Table 2.1.

Table 2.1: Known exponents d corresponding to infinite classes of AB power functions up to CCZ-equivalence and inversion modulo $2^m - 1$.

Exponent	Conditions	Type
$2^i + 1$	$\gcd(i,m) = 1$	Gold
$2^{2i} - 2^i + 1$	$\gcd(i,m) = 1$	Kasami
$2^{(m-1)/2} + 3$		Welch
$2^{(m-1)/2} + 2^{(m-1)/4} - 1$	$m \equiv 1(\text{mod } 4)$	Niho
$2^{(m-1)/2} + 2^{(3m-1)/4} - 1$	$m \equiv 3(\text{mod } 4)$	Niho

It still is an open problem to show that the list of power AB functions in Table 2.1 is complete, as conjectured by Hans Dobbertin. There are examples of AB functions that are EA-inequivalent to power functions and EA-inequivalent to permutations. However, there are just some sporadic examples of AB functions that are CCZ-inequivalent to power functions. We refer the reader to [9] for more information related to this topic.

For $m = 4$, all APN functions are known and classified under EA-equivalence and CCZ-equivalence. So are they for $m = 5$. The case $m = 6$ is more complicated: the quadratic APN functions are fully classified; a complete classification of cubic APN functions in terms of CCZ equivalence was given [28]. For odd m, there are several infinite classes of APN permutations (e.g. power functions), whereas for even m, the only known APN permutation lies in $\mathbb{F}_{2^6}$ [8]. The existence of APN permutations for even m greater than or equal to eight is an open problem, usually referred as "the big APN problem."

2.2 Linear codes

As mentioned in the introduction, a linear $[n, k, d]_q$-code is a k-dimensional linear subspace C of $\mathbb{F}_q^n$ with minimum Hamming distance d. The code C is then referred as a *q-ary linear code*, or simply, a q-ary code. A 2-ary linear code is called a *binary linear code*. A generator matrix of C is a $k \times n$ matrix whose rows form a basis for C and a parity-check matrix of C is an $(n-k) \times n$ matrix H whose rows form a basis for $C^{\perp}$. Note the use of the variables n and q (a prime power) when discussing the length of a q-ary linear code. Typically, we will reserve m and p (a prime number) when discussing the dimension of the input space of a p-ary function.

Given a linear code C with parity check matrix H, we have that a vector x is in C if and only if Hx^T is the zero vector. Therefore, the minimum distance of a linear code equals the minimum number of $\mathbb{F}_q$-linearly dependent columns in any of its parity check matrix. Several well-known operations can be performed to obtain codes from existing ones [31], in particular, the *extended code* of C will be denoted by C^{ext} and the *punctured code* at the first coordinate will be represented by $C^{\times}$, which is the code obtained by deleting the first coordinate of each codeword in the original code.

For any integer k greater than two, the *Hamming code* $\mathcal{H}_k$ of length $n = \frac{q^k-1}{q-1}$ is defined as the linear code with a parity check matrix whose columns form a maximal pairwise linearly independent set (Figure 2.1). Its dual is called the *simplex code*, denoted by $\mathcal{S}_k$ (Figure 2.2). These codes have played important roles as many computers and protocols are based on them in one way or another [9, 31].

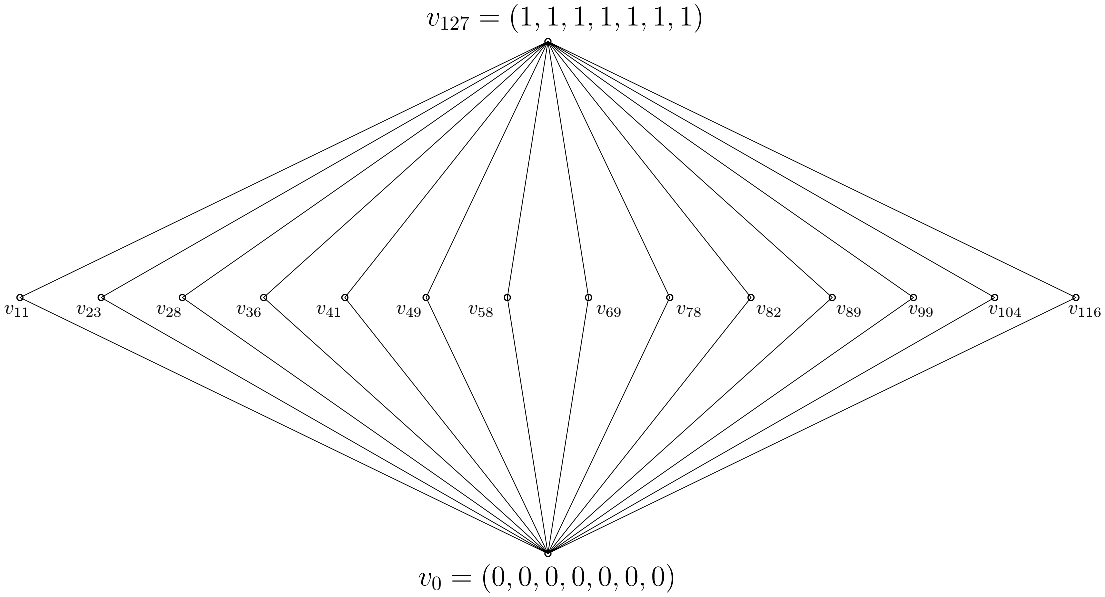


Figure 2.1: Hamming code $\mathcal{H}_3$.

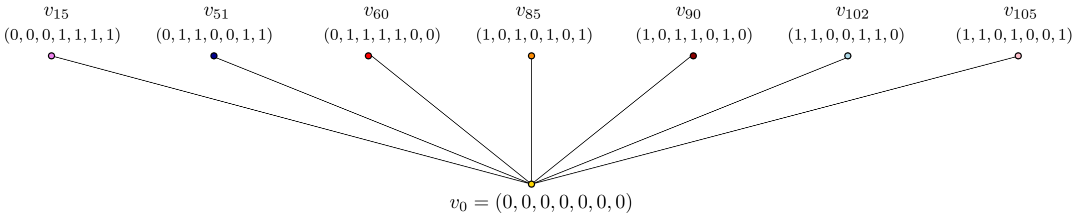


Figure 2.2: Simplex code $\mathcal{S}_3$.

Example 2.2.1. *A generator matrix of the Hamming code $\mathcal{H}_3$ with parameters $[7,4,3]_2$, equivalently, a parity check matrix for the simplex code $\mathcal{S}_3$ is*

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

Similarly, a generator matrix of the simplex code $\mathcal{S}_3$ with parameters $[7,3,4]_2$ (a parity check matrix for $\mathcal{H}_3$) is

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

For an $[n,k,d]_q$-code C, the number $\frac{k}{n}$ is called the *information rate* (sometimes called the *transmission rate*) of the code. We say that C is *distance-optimal*, or simply, optimal, provided that there does not exist an $[n,k,d']_q$-code with $d < d'$. The code C is called *almost optimal* if there is an optimal $[n,k,d+1]_q$-code, see [25, 27]. Two binary codes C and C' with the same parameters are called *equivalent*, if they coincide after some permutations of the positions of C'.

Let C be an arbitrary q-ary linear code of length n. The *weight enumerator polynomial* of C is the polynomial

$$A_C(z) = \sum_{i=0}^{n} A_i z^i, \tag{2.10}$$

where A_i is the number of codewords of weight i. The sequence $(A_i)_{0\leqslant i\leqslant n}$ is called the *weight distribution* of C. One of the most important results relating the weights of C and the weights of its dual $C^\perp$ is the so-called *MacWilliams' identity*:

$$(1+(q-1)z)^n A_C(\frac{1-z}{1+(q-1)z}) = q^k A_{C^\perp}(Z). \tag{2.11}$$

There are essentially two generic methods to define linear codes using p-ary functions [9, 19]. The first method specifies linear codes from a mapping $F : \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$ and linear functions on $\mathbb{F}_{p^m}$ [11], namely, the linear code $\mathcal{C}_F \subset \mathbb{F}_p^{p^m}$ is defined by

$$\mathcal{C}_F = \{c_{a,u} := (\mathrm{Tr}(aF(x)) + \mathrm{Tr}(ux))_{x\in\mathbb{F}_{p^m}} : a, u \in \mathbb{F}_{p^m}\}. \tag{2.12}$$

An equivalent definition of $\mathcal{C}_F$ can be obtained using the vector space representation of $\mathbb{F}_{p^m}$ and the standard dot product. The dimension of $\mathcal{C}_F$ is at most $2m$ and its length is p^m. If $F(0)$ is null, we may also consider the code obtained by puncturing the first coordinate at each vector in $\mathcal{C}_F$, i.e., $\mathcal{C}_F^{\times}$. In this case, the length is $p^m - 1$ while the dimension remains at most $2m$. For $p = 2$, the code $\mathcal{C}_F^{\times}$ can be used to characterize AB functions and APN functions [10].

When considering p-ary functions $f : \mathbb{F}_{p^m} \to \mathbb{F}_p$, the variable a in (2.12) will run over $\mathbb{F}_p$ only, thus the elements in $\mathcal{C}_f$ are of the form $c_{a,u} := (af(x) + \mathrm{Tr}(ux))_{x\in\mathbb{F}_{p^m}}$, and its dimension is at most $m+1$. If $F : \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$ has no linear components, then $\mathcal{C}_F$ has dimension $2m$. Similarly, if $f : \mathbb{F}_{p^m} \to \mathbb{F}_p$ is not linear, $\mathcal{C}_f$ has dimension $m+1$. Moreover, the weights of the linear codes derived from the generic construction in (2.12) can be determined through the Walsh transform of absolute trace functions [37] as

$$wt(c_{a,u}) = p^m - \frac{1}{p}\sum_{\omega\in\mathbb{F}_p} W_{\psi_{\omega a}}(\omega u), \tag{2.13}$$

where $\psi_\alpha : \mathbb{F}_{p^m} \to \mathbb{F}_p$ is defined by $x \mapsto \mathrm{Tr}(\alpha F(x))$ for $\alpha \in \mathbb{F}_{p^m}$. In particular, for $p = 2$, the non-zero weights of $\mathcal{C}_F$ are 2^{m-1} and $2^{m-1} - \frac{1}{2}W_{\alpha\cdot F}(\lambda)$ for $\alpha \in \mathbb{F}_{2^m}^*, \lambda \in \mathbb{F}_{2^m}$[19].

The second generic construction of linear codes from functions works as follows [16, 17, 56]. Fix a multi-set $D = \{\{d_1, d_2, \ldots, d_n\}\} \subset \mathbb{F}_{p^m}$, called the *defining (multi-)set*. Define

$$\mathcal{C}_D = \{c_x := (\mathrm{Tr}(d_1x), \mathrm{Tr}(d_2x), \ldots, \mathrm{Tr}(d_nx)) : x \in \mathbb{F}_{p^m}\}. \tag{2.14}$$

The length of $\mathcal{C}_D$ is n and its dimension is at most m. It can be noted that different orderings of D give equivalent linear codes $\mathcal{C}_D$. The weight $wt(c_x)$ of c_x is $n - Z_x$, where Z_x equals $|\{i \in \{1, \ldots, n\} : \mathrm{Tr}(xd_i) = 0\}|$. Moreover, since

$$pZ_x = n + \sum_{y\in\mathbb{F}_p^*}\sum_{i=1}^{n} \xi_p^{\mathrm{Tr}(yxd_i)}, \tag{2.15}$$

the weights of $\mathcal{C}_D$ are determined via the values $\sum_{y\in\mathbb{F}_p^*}\sum_{i=1}^{n} \xi_p^{\mathrm{Tr}(yxd_i)}$.

Not surprisingly, suitable choices for D lead to linear codes with interesting specific properties. The code $\mathcal{C}_f$ can be seen as an instance of the defining set method by selecting $D = \{(f(x), x) : x \in \mathbb{F}_p^m\} \subset \mathbb{F}_p^{m+1}$. The most natural choice for D is the support $\mathrm{supp}(f)$ of a p-ary function, which has been widely used. For instance, some codes with good parameters were derived [18, 19] using supports of classes of vectorial mappings from $\mathbb{F}_p^m$ to $\mathbb{F}_p^m$. In particular, when Boolean functions are considered, so that $f : \mathbb{F}_2^m \to \mathbb{F}_2$, this method gives optimal codes when bent and semi-bent functions are employed [16].

2.3 Minimal codes

Recall that a linear code C is minimal if every non-zero codeword of a linear code C is minimal, i.e. for every non-zero codewords $c, c' \in C$, if $\mathrm{supp}(c) \subseteq \mathrm{supp}(c')$, then there exists $\lambda \in \mathbb{F}_q$ such that $c = \lambda c'$.

A sufficient condition for a code to be minimal over $\mathbb{F}_q$ was given by Alexei E. Ashikhmin and Alexander Barg [2]. This condition states that if the minimum weight $w_{\min}$ and the maximum weight $w_{\max}$ of a linear code C are sufficiently close to each other, i.e.

$$\frac{w_{\min}}{w_{\max}} > \frac{q-1}{q}, \tag{2.16}$$

then the code C must be minimal. This sufficient condition will be referred as *Ashikhmin-Barg's condition*, or, the *Ashikhmin-Barg bound*.

A linear code is called *narrow* if it satisfies the Ashikhmin-Barg bound, namely, if $w_{\min}/w_{\max} > \frac{q-1}{q}$. Thus, the previous discussion can be summarized as "narrow linear codes are minimal." Conversely, linear codes satisfying $w_{\min}/w_{\max} \leqslant \frac{q-1}{q}$ are called *wide*.

Some sporadic examples of wide minimal codes were presented in [13, 15], however, there were no known examples of infinite families of wide minimal codes until the pioneering work of Cunsheng Ding, Ziling Heng and Zhengchun Zhou [20], where they provided three explicit classes of wide minimal linear codes over a binary alphabet.

Several methods have been devised to construct (wide) minimal codes, ranging from simplicial complexes [13], characteristic functions [20, 29, 40] and Kratchouk polynomials [20, 26, 40], to projective planes [3], maximal arcs [25], weakly regular bent functions [37, 60] and weakly regular plateaud functions [40, 42, 52]. The problem of designing minimal linear codes was also considered using the notion of cutting blocking sets and it was shown [6, 55] that cutting blocking sets and minimal codes are equivalent objects.

Since the property of minimality is related to the supports of codewords, it is natural to think of a characterization of minimality in terms of the weights of codewords within the given linear code. This is indeed the case, it can be proved

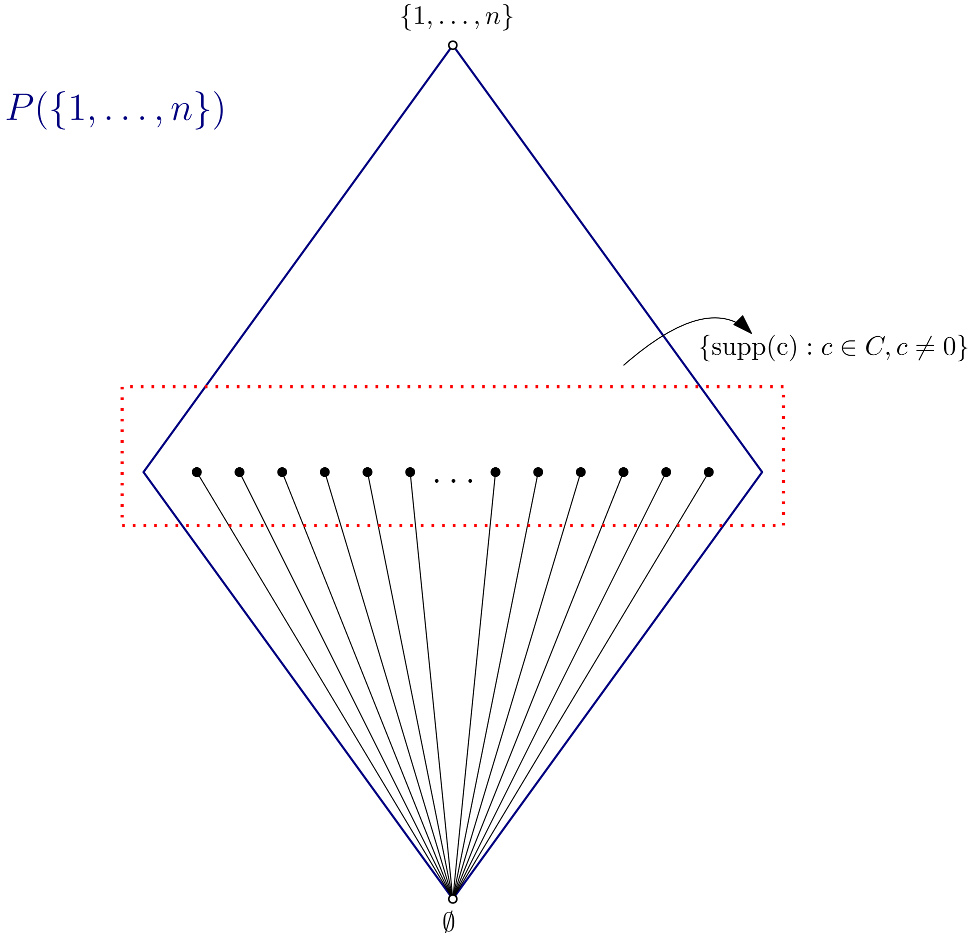


Figure 2.3: A prototypical example of a minimal code C of length n identified with an antichain in the lattice $P(\{1,\dots,n\})$ ordered by inclusion.

[26] that a code C is minimal if and only if for each pair of nonzero linearly independent codewords a and b in C,

$$\sum_{c\in\mathbb{F}_q^*} wt(a+cb) \neq (q-1)wt(a) - wt(b). \tag{2.17}$$

For a minimal code C with parameters $[n,k,d]_q$, it can be seen that the set of non-empty supports $\{\sup(c) : 0 \neq c \in C\}$ is a Sperner family[2] (see Figure 2.3), hence

$$|C| = q^k \leqslant 1 + (q-1)\binom{n}{\lfloor n/2 \rfloor} \tag{2.18}$$

due to Sperner's theorem.

Minimal codes are closely related to another particular class of linear codes. A code C is said to be *intersecting* provided that for every two non-zero codewords $c, c' \in C$, their supports overlap, i.e. $\sup(c)\cap\sup(c') \neq \emptyset$. More generally, a code C is *t-intersecting* if for every two non-zero codewords $c, c' \in C$, the cardinality of $\sup(c)\cap\sup(c')$ is at least t. In the binary case, the class of intersecting codes and the class of minimal codes coincide. In general, a minimal q-ary code is $(q-1)$-intersecting for $k \geqslant 2$.

Some bounds on the parameters of minimal codes are given as follows. The first one is called the *maximal bound* and it states that the ratio $R = k/n$ of a minimal code C asymptotically satisfies $R \leqslant \log_q(2)$ as n goes to infinity. An improvement of the maximal bound was proved in [1], where the authors showed that asymptotically $R \leqslant \frac{1}{q}$. For each minimal code C with parameters $[n,k,d]_q$, it holds that

$$n \geqslant (k-1)q + 1. \tag{2.19}$$

Moreover, the minimum distance d is constrained by $d \geqslant k + q - 2$ and the maximum distance $w_{\max}$ by $w_{\max} \leqslant n - k + 1$ [1, 15].

A class $\mathscr{C}$ of codes is called *asymptotically good* if there exists a positive ε such that for every positive integer n, there is a code $C \in \mathscr{C}$ with parameters $[n, k_n, d_n]_q$ such that $\frac{k_n}{n} \geqslant \varepsilon$ and $\frac{d_n}{n} \geqslant \varepsilon$. The class of minimal codes is asymptotically good as inferred from the *minimal bound* [12, 15]: For any rate $R = k/n$ such that

$$0 \leqslant R \leqslant \frac{1}{2}\log_q\left(\frac{q^2}{q^2-q+1}\right),$$

[2] A *Sperner family* (*clutter*, or, *independent system*), is a family $\mathcal{F}$ of subsets of a finite set F in which none of the sets contains another. Equivalently, a Sperner family is an antichain in the powerset $P(F)$ viewed as a lattice under inclusion.

there exists an infinite sequence of $[n,k]_q$ minimal codes.

Recall that the *direct product* (sometimes called the *Kronecker product*) $C_1 \otimes C_2$ of linear codes C and C' with parameters $[n,k,d]_q$ and $[n',k',d']_q$, respectively, is the linear code whose elements are $n \times n'$ matrices for which every column, respectively every row, is an element in C, respectively in C'. Thus $C_1 \otimes C_2$ is an $[nn', kk', dd']_q$-code. Moreover, if C and C' are minimal, then so is $C_1 \otimes C_2$.

Chapter 3

Infinite families of binary minimal codes

The aim of this chapter is to present several constructions of infinite families of wide minimal binary codes from Boolean functions using different combinatorial/algebraic techniques. The crux of most constructions is to build specific characteristic subsets of $\mathbb{F}_2^m$ to define Boolean functions, which will be used to generate wide minimal codes of length 2^m. Roughly speaking, the combinatorial properties of the characteristic sets will provide wideness of the resulting codes, whereas the algebraic properties will assure minimality. Throughout the chapter, we will set $p = 2$ and consider the linear code $\mathcal{C}_f$ described in (2.12) as defined using a Boolean function on the vector space $\mathbb{F}_2^m$ (not over the finite field $\mathbb{F}_{2^m}$). The results presented in this chapter are based on the results proved in [44] and in [64].

3.1 Wide minimal codes

Intrinsically, infinite families of wide minimal codes have been harder to specify since there were no know examples from the introduction of minimal codes in 1998 [2] until 2018 [20], when three infinite families of wide minimal binary linear codes were constructed. Additionally, some other efforts to exhibit such families have been made and examples of these families can be constructed using several approaches [20, 29, 40, 66].

The strategy used in [20] is quite simple but powerful: consider Boolean functions that resemble some classes of bent Boolean functions and plug them into the code $\mathcal{C}_f$ defined by means of (2.12). The bent-like shape of f provides a systematic way to compute the weights of $\mathcal{C}_f$ and conclude that the codes are minimal, whereas the fact that these functions are not bent gives enough room to "stretch out" the weights to get wide minimal codes. This strategy is very versatile and we will follow a similar approach on our constructions from the general $\mathcal{MM}$ class, see section 3.4.

The binary instance of equation (2.17) will be repeatedly used in the forthcoming results so that it is worth stating and proving it now.

Proposition 3.1.1. *[20] A binary linear code $C \subset \mathbb{F}_2^n$ is minimal if and only if for each pair of distinct nonzero codewords a and b in C,*

$$wt(a+b) \neq wt(a) - wt(b).$$

Proof. The support of the sum of two binary vectors equals the symmetric difference of their supports, hence $wt(a+b) = wt(a)+wt(b)-2|\text{supp}(a)\cap\text{supp}(b)|$ for every $a, b \in C$. Thus the equation $wt(a+b) = wt(a) - wt(b)$ is true if and only if $wt(b) = |\text{supp}(a) \cap \text{supp}(b)|$, which in turn holds if and only if $\text{supp}(b) \subseteq \text{supp}(a)$, i.e. $b \preceq a$. Therefore the existence of a pair of non-zero codewords $a, b \in C$ that cover each other is equivalent to $wt(a+b) = wt(a) - wt(b)$. □

Since the weights of the code $\mathcal{C}_f$ described in (2.12) are completely determined by the Walsh transform of f (Equation (2.13)), the minimality of the code $\mathcal{C}_f$ can be characterized via the Walsh values f.

Theorem 3.1.2. *[20] Let $f : \mathbb{F}_2^m \to \mathbb{F}_2$ be a non-affine Boolean function. The code $\mathcal{C}_f$ described in (2.12) is minimal if and only if for every pair of distinct $\beta_1, \beta_2 \in \mathbb{F}_2^m$ it holds that*

$$W_f(\beta_1) + W_f(\beta_2) \neq 2^m \text{ and } W_f(\beta_1) - W_f(\beta_2) \neq 2^m. \tag{3.1}$$

Equivalently, $\mathcal{C}_f$ is minimal if and only if for every Walsh coefficient $w = W_f(\beta)$, the integer $2^m \pm w$ is not a Walsh coefficient of f.

Proof. Since the extended simplex code $\mathcal{S}_m^{ext}$ is minimal, the only codewords to consider are those where f appears, so let $c_{a,u}, c_{a',u'}$ be arbitrary non-zero codewords in $\mathcal{C}_f$ such that $a \neq 0$ or $a' \neq 0$. By Proposition 3.1.1, $c_{a',u'} \npreceq c_{a,u}$ if and only if $wt(c_{a,u} + c_{a',u'}) \neq wt(c_{a,u}) - wt(c_{a',u'})$. When $a = 1$, it holds that $wt(c_{1,u}) = 2^{m-1} - \frac{1}{2}W_f(u)$, $wt(c_{a',u'})$ is equal to either 2^{m-1} (which forces $wt(c_{1,u}+c_{a',u'}) = 2^{m-1}-\frac{1}{2}W_f(u+u')$), or, $2^{m-1}-\frac{1}{2}W_f(u')$ (which forces $wt(c_{1,u}+c_{a',u'}) = 2^{m-1}$). Similarly, when $a = 0$, it holds that $wt(c_{1,u'}) = 2^{m-1} - \frac{1}{2}W_f(u')$, $wt(c_{0,u}) = 2^{m-1}$ and $wt(c_{0,u}+c_{1,u'}) = 2^{m-1}-\frac{1}{2}W_f(u+u')$. The result then follows by plugging these possible values into $wt(c_{a,u}+c_{a',u'}) \neq wt(c_{a,u})-wt(c_{a',u'})$. □

The characterization of minimality of the code $\mathcal{C}_f$ given in Theorem 3.1.2 enables us to state a sufficient condition for minimality using only the extremal spectral values of f. For this purpose, let the symbols $\mathcal{W}_{\max}$ (resp. $\mathcal{W}_{\min}$) denote the maximal (resp. minimal) Walsh value in the Walsh spectrum of a given Boolean function f.

Corollary 3.1.3. *Let f be a nonaffine Boolean function in $\mathcal{B}_m$. If the extremal Walsh values $\mathcal{W}_{\max}$ and $\mathcal{W}_{\min}$ satisfy*

$$\mathcal{W}_{\max} - \mathcal{W}_{\min} < 2^m \quad \text{and} \quad \mathcal{W}_{\max} < 2^{m-1}, \tag{3.2}$$

then $\mathcal{C}_f$ is minimal.

Proof. Let $\beta_1, \beta_2 \in \mathbb{F}_2^m$. Since $\mathcal{W}_{\max}$ is maximal, the sum $W_f(\beta_1) + W_f(\beta_2)$ is at most $2\mathcal{W}_{\max}$. By hypothesis, $\mathcal{W}_{\max} < 2^{m-1}$ so that $W_f(\beta_1) + W_f(\beta_2) < 2^m$. Since $W_f(\beta_2) \geqslant \mathcal{W}_{\min}$, the difference $W_f(\beta_1) - W_f(\beta_2)$ is at most $\mathcal{W}_{\max} - \mathcal{W}_{\min}$, hence $W_f(\beta_1) - W_f(\beta_2) < 2^m$ using the first condition in (3.2). The minimality of $\mathcal{C}_f$ then follows by Theorem 3.1.2. □

The following fact is a straightforward consequence of the proof of Theorem 3.1.2, which provides a simple characterization of the property of wideness of linear codes of the form $\mathcal{C}_f$.

Proposition 3.1.4. *Let f be a non-affine Boolean function in $\mathcal{B}_m$. The code $\mathcal{C}_f$ is wide if and only if $2\mathcal{W}_{\max} - \mathcal{W}_{\min} \geqslant 2^m$.*

Proof. Since f is non-affine, its Walsh spectrum contains at least one positive value and at least one negative value. This implies that $\mathcal{W}_{\max} > 0$ and $\mathcal{W}_{\min} < 0$. The existence of both positive and negative values in the Walsh spectrum can be easily confirmed using Titsworth theorem.[1] The minimum and maximum weights of the code correspond to these extremal Walsh coefficients so that $w_{\min} = 2^{m-1} - \frac{\mathcal{W}_{\max}}{2}$ and $w_{\max} = 2^{m-1} - \frac{\mathcal{W}_{\min}}{2}$. Replacing these values in the quotient $\frac{w_{\min}}{w_{\max}}$, we get that $\frac{w_{\min}}{w_{\max}}$ is at most $\frac{1}{2}$ if and only if $2^m \leqslant 2\mathcal{W}_{\max} - \mathcal{W}_{\min}$. □

It can be anticipated that the code $\mathcal{C}_f$ reveals information of the underlying Boolean function f. Moreover, properties of the code must impose some restrictions on f, too. For instance, the following result gives an upper bound on the nonlinearity of a Boolean function $f \in \mathcal{B}_m$ under the assumption that the linear code $\mathcal{C}_f$ is wide.

[1] *Titsworth theorem* states that the sum $\sum_{u \in \mathbb{F}_2^m} W_f(u)W_f(u+s) = 0$ is null for any $s \in \mathbb{F}_2^{m*}$.

Proposition 3.1.5. *Let $f \in \mathcal{B}_m$ be any non-affine Boolean function and $\mathcal{C}_f$ its associated code. The nonlinearity $\mathcal{N}_f$ of f equals $\min\{w_{\min}, 2^m - w_{\max}\}$, where $w_{\min}$ and $w_{\max}$ denote, respectively, the minimum and maximum weights in $\mathcal{C}_f$. Moreover, if $\mathcal{C}_f$ is wide, then $\mathcal{N}_f \leqslant \frac{2^m}{3}$.*

Proof. Note that either $\mathcal{W}_{\max}$ or $\mathcal{W}_{\min}$ attains the maximum absolute value in the Walsh spectrum of f. This yields that either

$$\mathcal{N}_f = 2^{m-1} + \frac{1}{2}\mathcal{W}_{\min}, \text{ or } \mathcal{N}_f = 2^{m-1} - \frac{1}{2}\mathcal{W}_{\max}$$

since $\mathcal{N}_f = 2^{m-1} - \frac{1}{2}\max_{u \in \mathbb{F}_2^m} |W_f(u)|$. Therefore, $\mathcal{N}_f = 2^m - w_{\max}$ or $\mathcal{N}_f = w_{\min}$. This gives $\mathcal{N}_f = \min\{w_{\min}, 2^m - w_{\max}\}$. From this, the value $2\mathcal{N}_f$ is at most $2w_{\min}$. If $\mathcal{C}_f$ is wide, then $2w_{\min} \leqslant w_{\max}$. Again, from the first part of the theorem, $w_{\max}$ is at most $2^m - \mathcal{N}_f$. Thus, $\mathcal{N}_f \leqslant \frac{2^m}{3}$. □

According to the above results, certain Boolean functions f cannot be used in the construction of wide minimal binary linear codes. For instance, assume that $\mathcal{W}_{\min} = -2^l$ and $\mathcal{W}_{\max} = 2^l$ for some $l \in \{\frac{m}{2}, \ldots, m-2, m-1\}$. If $l = m-1$, then $\mathcal{C}_f$ is clearly not minimal since $\mathcal{W}_{\max} - \mathcal{W}_{\min} = 2^m$. On the other hand, if $l \leqslant m-2$, then $2\mathcal{W}_{\max} - \mathcal{W}_{\min} = 3 \cdot 2^l \leqslant 3 \cdot 2^{m-2} < 2^m$. By Proposition 3.1.4, the code $\mathcal{C}_f$ is narrow (hence minimal). Note that some well-known classes of Boolean functions, such as bent and semi-bent functions, lie in this description so they cannot give rise to wide codes. Alternatively, this could be inferred from the bound on nonlinearity derived in Proposition 3.1.5.

3.2 The basis method and affine subspaces

The main idea of the constructions in this section will be to exploit the geometric and combinatorial structures of $\mathbb{F}_2^m$ to construct suitable “stretched” subsets $\Delta \subset \mathbb{F}_2^m$ which will define the support of a Boolean function $f : \mathbb{F}_2^m \to \mathbb{F}_2$, thus we will consider characteristic functions of subsets. The geometric properties will allow us to apply Theorem 3.2.2 below to obtain minimal codes, whereas the combinatorial properties should provide wideness.

3.2.1 Vectorial blocking sets

Very recently, a geometric approach for constructing minimal codes was introduced [6], where the authors showed a strong connection between cutting vectorial blocking sets and minimal codes. Surprisingly, it turns out that these two objects are the same [55].

For each non-zero vector u in $\mathbb{F}_2^m$, the symbol H_u will denote the complement of the hyperplane[2] determined by u, i.e.

$$H_u = \{x \in \mathbb{F}_2^m : u \cdot x = 1\}.$$

For any subset A of $\mathbb{F}_2^m$, the complement of A is denoted by $\overline{A}$. With this notation, $\overline{H}_u$ is the hyperplane determined by u.

A set $\mathcal{BS} \subseteq \mathbb{F}_2^m$ is a *vectorial blocking set* if it intersects non-trivially all hyperplanes of $\mathbb{F}_2^m$, i.e., $\mathcal{BS}^* \cap \overline{H}_u \neq \emptyset$ for each $u \in \mathbb{F}_2^m$ (Figure 3.1). A vectorial blocking set $\mathcal{BS}$ is said to be *d-dimensional* if its span is d-dimensional, that is, $\dim(\langle \mathcal{BS} \rangle) = d$. A vectorial blocking set $\mathcal{BS}$ is called a *vectorial* $(1, m-1)$-*blocking set* if $\mathcal{BS}$ does not include any hyperplane $\overline{H}_u$. A vectorial blocking set $\mathcal{BS}$ is *cutting* if the intersection between $\mathcal{BS}$ and every hyperplane is not included in any other hyperplane (Figure 3.2).

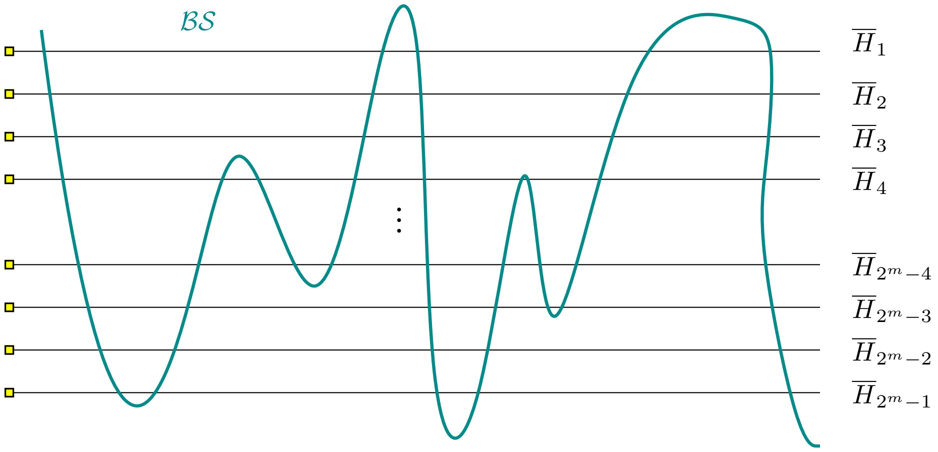


Figure 3.1: Graphical depiction of a vectorial blocking set $\mathcal{BS}$.

The following lemma is a trivial rephrasing of the introduced definitions on blocking sets, so that its proof is omitted. However, this simple result will be well-suited for the discussion in the sequel.

Lemma 3.2.1. *[6] A subset $\mathcal{BS}$ of $\mathbb{F}_2^m$ is an m-dimensional cutting vectorial $(1, m-1)$-blocking set if and only if the following two conditions hold.*

- *For every pair of distinct $u, u' \in (\mathbb{F}_2^m)^*$, it holds that $\mathcal{BS}^* \cap \overline{H}_u \not\subseteq \overline{H}_{u'}$;*
- *The set $\mathcal{BS}$ does not include any hyperplane.*

[2] A *hyperplane* in an m-dimensional vector space is an $(m-1)$-dimensional subspace.

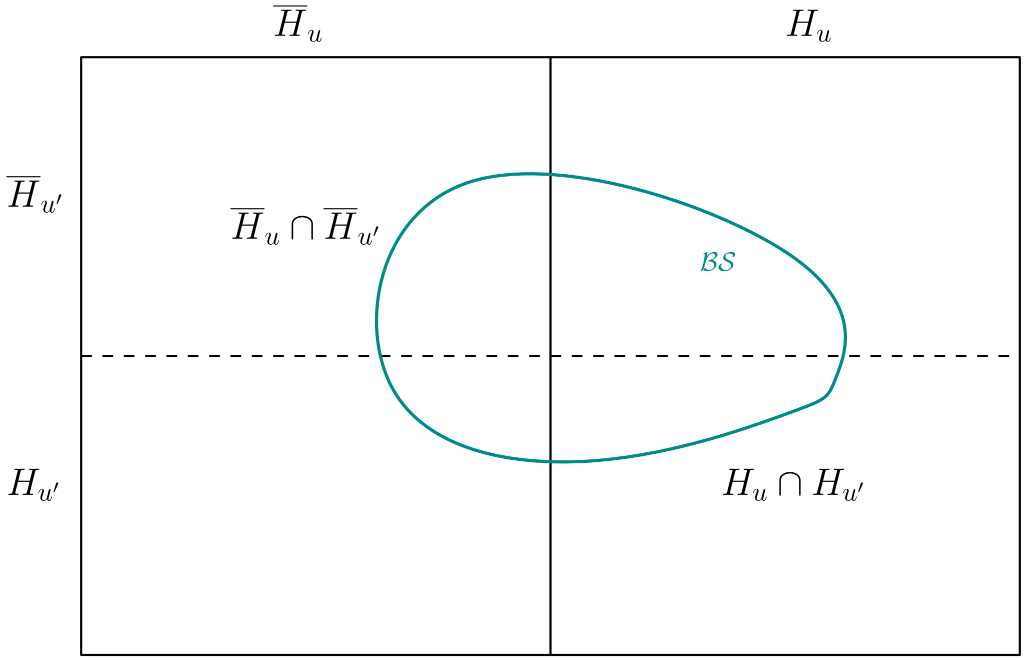


Figure 3.2: Representation of a cutting vectorial $(1, m-1)$-blocking set $\mathcal{BS}$.

Following [6], given a Boolean function $f : \mathbb{F}_2^m \to \mathbb{F}_2$, denote the *set of zeros* of f as $V(f)$, i.e.,

$$V(f) = \{x \in \mathbb{F}_2^m : f(x) = 0\}.$$

For every subset Δ of $\mathbb{F}_2^m$, the *characteristic function* (or *indicator function*) f of Δ is the Boolean function defined as

$$f(x) = \begin{cases} 1, & x \in \Delta, \\ 0, & x \in \mathbb{F}_2^m \setminus \Delta. \end{cases} \tag{3.3}$$

The following theorem provides the aforementioned connection between minimal codes and vectorial blocking sets. More precisely, it gives a sufficient condition for a linear code $\mathcal{C}_f$ to be minimal in terms of the geometry of $V(f)$. Vectorial cutting blocking sets in $\mathbb{F}_2^m$ can be described via hyperplanes as expressed by the following theorem.

Theorem 3.2.2. *[6] If $f : \mathbb{F}_2^m \to \mathbb{F}_2$ is a Boolean function such that:*

1) The set $V(f)$ is an m-dimensional cutting vectorial $(1, m-1)$-blocking set;

2) For every nonzero $u \in \mathbb{F}_2^m$, $\overline{H}_u \cup V(f) \neq \mathbb{F}_2^m$,

then the code $\mathcal{C}_f$ given by (2.12) is a minimal binary code.

Remark 3.2.3. *A full characterization of minimality using vectorial blocking sets has been given [55]. Every minimal code induces a vectorial cutting blocking set and vice versa, thus in principle one can track down a vectorial blocking set from any minimal code and one can create a minimal code from certain vectorial blocking sets.*

For the characteristic function f of a set Δ, the set of zeros $V(f)$ is equal to $\overline{\Delta}$, namely, $V(f) = \mathbb{F}_2^m \setminus \Delta$. This simple observation allows us to turn Theorem 3.2.2 into the following corollary, which will be more suitable for our purposes.

Corollary 3.2.4. *[6] Let Δ be a subset of $\mathbb{F}_2^m$ and f be its characteristic function. If the following properties hold:*

1) For each $u \in \mathbb{F}_2^{m*}$, $H_u \cap \Delta \neq \emptyset$ and $\overline{H}_u \cap \Delta \neq \emptyset$;

2) For every pair of distinct vectors u, u' in $(\mathbb{F}_2^m)^*$, $H_u \setminus H_{u'} \not\subseteq \Delta \setminus H_{u'}$,

then the code $\mathcal{C}_f$ is a minimal binary code.

Proof. These two conditions imply the hypotheses in Theorem 3.2.2 simply by considering the complementary statements. Note that the statement "for every nonzero $u \in \mathbb{F}_2^n$, $H_u \cap \Delta \neq \emptyset$" is equivalent to "for every nonzero $u \in \mathbb{F}_2^m$, $\overline{H}_u \cup V(f) \neq \mathbb{F}_2^m$", thus the first part in 1) is equivalent to the second condition in Theorem 3.2.2. Now we prove that $V(f)$ is an m-dimensional cutting vectorial $(1, m-1)$-blocking set. Indeed, suppose there is a hyperplane $\overline{H}_{u'}$ where $u' \neq 0$ such that the intersection $V(f)^* \cap \overline{H}_{u'}$ is contained in $\overline{H}_u$ for some $u \in (\mathbb{F}_2^m)^*$. Taking complements, $H_u \subseteq \Delta \cup \{0\} \cup H_{u'}$, which implies $H_u \setminus H_{u'} \subseteq \Delta \setminus H_{u'}$, thus contradicting 2). This shows that $V(f)$ is an m-dimensional cutting vectorial blocking set. Finally observe that $V(f)$ cannot contain any hyperplane $\overline{H}_v$ since this would yield $\Delta \subseteq H_u$, which is a contradiction to 1). We have proved that $V(f)$ is an m-dimensional cutting vectorial $(1, m-1)$-blocking set. □

3.2.2 Bases

In what follows, we provide an efficient method of selecting the support of f based on Corollary 3.2.2, which then ensures both minimality and wideness of the resulting codes. Most notably, the only requirement on the choice of a suitable support of $f \in \mathcal{B}_m$ is the inclusion of (any) basis for $\mathbb{F}_2^m$ and at least one particular element of its span.

Theorem 3.2.5 (The basis method)**.** *Let $m \geqslant 5$ be a positive integer. Let $\Delta \subset \mathbb{F}_2^m$ be an arbitrary subset and f be its characteristic function. If Δ satisfies the following conditions:*

a) $m+1 \leqslant |\Delta| \leqslant 2^{m-2}$;

b) The set Δ *includes a basis* $\mathscr{B} = \{a_1, \dots, a_m\}$ *for* $\mathbb{F}_2^m$ *and it contains a vector*

$$\tau_1 a_1 + \cdots + \tau_m a_m$$

with $(\tau_1, \dots, \tau_m) \in \mathbb{F}_2^m$ *such that* $wt(\tau_1, \dots, \tau_m)$ *is even.*

Then, the code $\mathcal{C}_f$ *given by (2.12) is a wide minimal binary linear code with parameters* $[2^m, m+1, |\Delta|]$.

Proof. We first claim that for every nonzero $u \in \mathbb{F}_2^m$ we have $H_u \cap \Delta \neq \emptyset$ and $\overline{H}_u \cap \Delta \neq \emptyset$, i.e., there exist $x_1, x_2 \in \Delta$ such that $u \cdot x_2 = 1$ and $u \cdot x_1 = 0$. For each $u \in (\mathbb{F}_2^m)^*$, there are two possibilities to consider.

i) If there exists an element $a_i \in \mathscr{B}$ such that $u \cdot a_i = 0$, then there must exist an $a_j \in \mathscr{B} \subset \Delta$ such that $u \cdot a_j = 1$ since the dimension of the orthogonal space of u equals $m-1$.

ii) If $u \cdot a_i = 1$ for all $i \in \{1, \dots, n\}$, then define $x_2 = \tau_1 a_1 + \cdots + \tau_m a_m \in \Delta$. Consequently, $u \cdot x_2 = 0$ since $wt(\tau_1, \dots, \tau_m)$ is even.

For every pair of non-zero vectors u, u', the set $H_u \setminus H_{u'}$ cannot be contained in $\Delta \setminus H_{u'}$ since $|H_u \setminus H_{u'}| = 2^{m-2}$ and $|\Delta \setminus H_{u'}| < 2^{m-2}$. Using Corollary 3.2.4, the code $\mathcal{C}_f$ is a minimal code. By assumption, $|\mathrm{supp}(f)| = |\Delta| \leqslant 2^{m-2}$, hence $w_{\min} \leqslant 2^{m-2}$. This yields $\frac{w_{\min}}{w_{\max}} \leqslant \frac{1}{2}$ since the weight of linear functions is 2^{m-1}. Finally, the weight of $c_{1,u} \in \mathcal{C}_f$, for $u \neq 0$, equals

$$|H_u| + |\Delta| - 2|H_u \cap \Delta|.$$

Since $|\Delta| \leqslant 2^{m-2}$, the number $|H_u| - 2|H_u \cap \Delta|$ is non-negative, thus $|\Delta|$ is the minimum weight in $\mathcal{C}_f$. □

Note that the weight distribution of the codes constructed using the previous theorem is very irregular. Nevertheless, their values completely rely on the cardinality of Δ and it can be shown that the maximum value in the Walsh spectrum of f is $2^m - 2|\Delta|$, whereas other Walsh values belong to the set

$$\{2|\Delta| - 4, 2|\Delta| - 8, \dots, 2|\Delta| - 4(|\Delta| - 1)\}.$$

Example 3.2.6. *Set* $m = 6$. *Consider the canonical basis* $\mathcal{E} = \{e_1, \dots, e_6\}$ *and* $\tau = (1,0,1,1,1,0)$. *Selecting* $\Delta = \mathcal{E} \cup \{\tau\}$ *we have* $|\Delta| = 7$. *The code* $\mathcal{C}_f$ *is wide and minimal with weight enumerator given by*

$$1 + z^7 + 5z^{27} + 10z^{29} + 15z^{31} + 63z^{32} + 20z^{33} + 11z^{35} + 2z^{37}.$$

Thus, its minimum and maximum distance are 7 *and* 37*, respectively. In other words,* $\mathcal{C}_f$ *is an* 8*-weight code with parameters* $[64, 7, 7]$.

If we additionally select 9 arbitrary vectors, say, $v_1, \ldots, v_9 \notin \Delta$ *so that* $\Delta' = \mathcal{E} \cup \{\tau, v_1, \ldots, v_9\}$*, then using* Δ' *we obtain a wide minimal code with parameters* $[64, 7, 16]$.

The following consequence of Theorem3.2.5 shows how to select a derivative of a function in such a way that its associated code is a wide minimal code. This will be important since derivatives of functions will play a crucial role in the upcoming chapters, see Section 4.2 and Section 4.3.

Theorem 3.2.7. *Let* $\mathscr{B} = \{a_1, \ldots, a_m\}$ *be a basis of* $\mathbb{F}_2^m$*. Define the set*

$$E = \{\tau_1 a_1 + \cdots + \tau_m a_m : \tau = (\tau_1, \ldots, \tau_m) \in \mathbb{F}_2^m, wt(\tau) \textit{ is even}\}.$$

Let S *be a non-empty subset of* E *such that* $|S| \leqslant 2^{m-3} - m$*. Consider* $\Delta = \mathscr{B} \cup S$ *and let* $f \in \mathcal{B}_m$ *be the characteristic function of* Δ*. Take any* $\tau' = (\tau'_1, \ldots, \tau'_m) \in (\mathbb{F}_2^m)^*$ *and define* $\gamma = \tau'_1 a_1 + \cdots + \tau'_m a_m$*. The following is true:*

(i) The code $\mathcal{C}_f$ *is a wide minimal binary* $[2^m, m+1, |\Delta|]$*-linear code.*

(ii) If $wt(\tau')$ *is an even integer strictly greater than two and* $S \ominus (\gamma + S) \neq \emptyset$*, where the symbol* $\ominus$ *denotes symmetric difference, then the code* $\mathcal{C}_{D_\gamma f}$ *is also a wide binary* $[2^m, m+1]$*-linear code.*

(iii) If $wt(\tau')$ *is an odd integer at least three and* $\mathscr{B} \cap (\gamma + S) = \emptyset$ *then the code* $\mathcal{C}_{D_\gamma f}$ *is a wide minimal binary* $[2^m, m+1]$*-linear code.*

Proof. (i) The statement follows directly from Theorem 3.2.5.
(ii) Suppose that $wt(\tau')$ is even and $wt(\tau') > 2$. It follows that $(\gamma + \mathscr{B}) \cap \mathscr{B} = \emptyset$ since $wt(\tau') > 2$. Observe that

$$\text{supp}(D_\gamma f) = (\gamma + \mathscr{B}) \cup \mathscr{B} \cup (S \ominus (\gamma + S)).$$

Since $|S| \leqslant 2^{m-3} - m$, the cardinality of $|\text{supp}(D_\gamma f)|$ is at most 2^{m-2}. The facts that $wt(\tau')$ is even and $S \ominus (\gamma + S)$ is non-empty imply that $\text{supp}(D_\gamma f)$ contains an element of the form $\tau_1 a_1 + \cdots + \tau_m a_m$ with $wt(\tau)$ even. By Theorem 3.2.5, the code $\mathcal{C}_{D_\gamma f}$ is wide and minimal.
(iii) Suppose that $wt(\tau')$ is odd, $wt(\tau') \geqslant 3$ and $\mathscr{B} \cap (\gamma + S) = \emptyset$. Again, $(\gamma + \mathscr{B}) \cap \mathscr{B}$ is empty since $wt(\tau') > 2$. So is $(\gamma + S) \cap S$ since $wt(\tau')$ is odd. Observe that

$$\text{supp}(D_\gamma f) = (\gamma + \mathscr{B}) \cup \mathscr{B} \cup (\gamma + S) \cup S.$$

As before, $|\mathrm{supp}(D_\gamma f)| \leqslant 2^{m-2}$ due to $|S| \leqslant 2^{m-3} - m$. Note that the set $(\gamma + \mathscr{B}) \cap E$ cannot be empty, thus $\mathrm{supp}(D_\gamma f)$ contains an element of the form $\tau_1 a_1 + \cdots + \tau_m a_m$ with $wt(\tau)$ even. An application of Lemma 3.2.5 gives the desired conclusion. □

From the proof of Theorem 3.2.7, the minimum distance of the code $\mathcal{C}_{D_\gamma f}$ is at most 2^{m-2} in both cases studied in Theorem 3.2.7.

Example 3.2.8. *Set $m = 7$. Consider the basis $\mathscr{B} \subset \mathbb{F}_2^7$ with elements*

$$\begin{array}{lll} a_1 = e_3 + e_5 + e_6; & a_2 = e_2 + e_5 + e_6; & a_3 = e_1 + e_2 + e_3 + e_4 + e_6; \\ a_4 = e_4 + e_6; & a_5 = e_1 + e_4 + e_6 + e_7; & a_6 = e_1 + e_6; \\ a_7 = e_1 + e_5 + e_6 + e_7, & & \end{array}$$

where e_i represents vectors in the canonical base. Define $S \subseteq E$ with elements

$$\begin{array}{lll} s_1 = a_1 + a_3 + a_4 + a_6; & s_2 = a_3 + a_4 + a_5 + a_7; & s_3 = a_1 + a_4; \\ s_4 = a_1 + a_2 + a_4 + a_5 + a_6 + a_7; & s_5 = a_2 + a_3 + a_5 + a_6; & \\ s_6 = a_1 + a_2 + a_3 + a_7; & s_7 = a_1 + a_2 + a_5 + a_6, & \end{array}$$

and take $\gamma = a_2 + a_4 + a_6 + a_7$. Note that $\tau' = (0, 1, 0, 1, 0, 1, 1)$, $wt(\tau') = 4$ and $|S| = 7 < 9 = 2^{7-3} - 7$. Computer-based simulations show that $|S \ominus (\gamma + S)| = 10$ and the code $\mathcal{C}_{D_\gamma f}$ is a wide minimal linear code, where f is the characteristic function of $\Delta = \mathscr{B} \cup S$. This is a $[128, 8, 24]$-code with $w_{\max} = 80$, so that $w_{\min}/w_{\max} = \frac{1}{3}$. This is in accordance with (ii) of Theorem 3.2.7.

Example 3.2.9. *Set $m = 7$. Consider the basis $\mathscr{B} \subset \mathbb{F}_2^7$ with elements*

$$\begin{array}{lll} a_1 = e_1 + e_2 + e_5 + e_6; & a_2 = e_1 + e_3 + e_6; & a_3 = e_4 + e_7; \\ a_4 = e_1 + e_4; & a_5 = e_4 + e_5; & a_6 = e_3 + e_5 + e_7; \\ a_7 = e_1 + e_2 + e_5. & & \end{array}$$

Define $S \subseteq E$ with elements

$$\begin{array}{lll} s_1 = a_1 + a_4 + a_5 + a_7; & s_2 = a_1 + a_2 + a_5 + a_6; & s_3 = a_1 + a_2 + a_4 + a_7; \\ s_4 = a_2 + a_3 + a_4 + a_5; & s_5 = a_1 + a_2 + a_5 + a_7; & s_6 = a_4 + a_7; \\ s_7 = a_1 + a_2 + a_3 + a_5 + a_6 + a_7; & s_8 = 0; & s_9 = a_4 + a_6, \end{array}$$

and take $\gamma = a_2 + a_5 + a_7$. Note that $\tau' = (0, 1, 0, 0, 1, 0, 1)$, $wt(\tau') = 3$, and $|S| = 9 = 2^{7-3} - 7$. Computer-based simulations show that $\mathcal{C}_{D_\gamma f}$ is a wide minimal $[128, 8, 28]$-linear code, where f is the indicator function of $\Delta = \mathscr{B} \cup S$. Furthermore, $w_{\max} = 74$, so that $w_{\min}/w_{\max} = \frac{8}{37}$. This is in accordance with (iii) of Theorem 3.2.7.

3.2.3 Affine subspaces

In this section, a slightly different approach for the purpose of constructing wide minimal codes which takes a Boolean function f whose support has cardinality greater than 2^{m-2}. Recall that a k-dimensional *affine subspace* or *coset* is a translation of a linear subspace of $\mathbb{F}_2^m$, i.e. a set of the form $a+V$, where $a \in \mathbb{F}_2^m$ and V is a k-dimensional subspace of $\mathbb{F}_2^m$.

Lemma 3.2.10. *Let $A = a+V$ and $B = b+W$ be two non-trivial affine subspaces of $\mathbb{F}_2^m$. Then either A and B are disjoint or $A \cap B$ is an affine subspace such that* $\dim(A \cap B) \geqslant \dim(A) + \dim(B) - m$.

Proof. Suppose that $A \cap B \neq \emptyset$. Take $x \in A \cap B$. By definition, $x = a+v$ and $x = b+w$ for some $v \in V$ and $w \in W$. We claim that $A \cap B = x + (V \cap W)$. Obviously, $x + (V \cap W) \subseteq A \cap B$. Let $y \in A \cap B$. By definition of A, $y = a+v'$ for some $v' \in V$. Likewise $y = b+w'$ for some $w' \in W$ as $y \in B$. Note that $y = x+v+v'$ and also $y = x+w+w'$. This readily implies that $v+v'$ belongs to $V \cap W$ so that y is in $x+(V \cap W)$. Thus $A \cap B$ is an affine space with underlying linear space equal to $V \cap W$. The second part of the lemma comes from the fact that for every two linear subspaces, it holds that $\dim(V+W) = \dim(V) + \dim(W) - \dim(V \cap W)$. □

Note that Lemma 3.2.10 is an easy consequence of the well-known similar result about the intersection of linear subspaces. When $\dim(A) + \dim(B) \leqslant m$, the bound obtained thereby is quite loose and no additional information about the intersection is provided. On the contrary, when $\dim(A) + \dim(B) > m$ (which will be considered in the main theorems below), the intersection bound becomes non-trivial.

The following lemma is useful for specifying wide minimal linear codes from characteristic functions that include an $(m-2)$-dimensional affine subspace in their support.

Lemma 3.2.11. *Let V be an $(m-2)$-dimensional linear subspace of $\mathbb{F}_2^m$. Let $a \notin V$ and $A = a+V$ be an $(m-2)$-dimensional affine space. There exists a unique $u_A \in (\mathbb{F}_2^m)^*$ such that $A \cap H_{u_A}$ is empty.*

Proof. Let $\mathcal{V} = \{v_1, \ldots, v_{m-2}\}$ be a basis of V. Since $a \notin V$, the set $\mathcal{V} \cup \{a\}$ is linearly independent, therefore $U := \langle \mathcal{V} \cup \{a\} \rangle$ is an $(m-1)$-dimensional subspace. This implies that $U = \overline{H}_{u_A}$, for some $u_A \in \mathbb{F}_2^m$. Any $a+v \in A$ satisfies $u_A \cdot (a+v) = 0$, thus $A \subseteq \overline{H}_{u_A}$. In other words, $A \cap H_{u_A} = \emptyset$ since $H_{u_A} \cup \overline{H}_{u_A} = \mathbb{F}_2^m$. Note that u_A is unique because if there were another $u' \in \mathbb{F}_2^m$

such that $H_{u'} \cap A = \emptyset$ then $A \subseteq (\overline{H}_{u_A} \cap \overline{H}_{u'}) \setminus \{0\}$ which is impossible as $|(\overline{H}_{u_A} \cap \overline{H}_{u'}) \setminus \{0\}| = 2^{m-2} - 1$. □

To get minimal codes, the characteristic sets must intersect all hyperplanes and their complements. The strategy will be to puncture an affine subspace A and adjoint a suitable disjoint set Γ, which will take care of the affine hyperplane H_{u_A} grosso modo.

Theorem 3.2.12 (The affine subspace method)**.** *Let $m \geqslant 4$ be a positive integer and $A = a + V$ be an $(m-2)$-dimensional affine subspace of $\mathbb{F}_2^m$. Fix an element $p_0 \in A$ and consider $S = A \setminus \{p_0\}$. Suppose that there is a non-empty set $\Gamma \subset \mathbb{F}_2^m \setminus (A \cup \{0\})$ of cardinality strictly smaller than 2^{m-3} such that $\Gamma \cap H_{u_A}$ is non-empty. Let $\Delta = S \cup \Gamma \cup \{0\}$ and let $f \in \mathcal{B}_m$ be its characteristic function. The code $\mathcal{C}_f$ is then a minimal binary linear code with minimum distance $d \in \{2^{m-2} - |\Gamma| + 2, \ldots, 2^{m-2} + |\Gamma|\}$. Moreover, if $|\Gamma \cap H_{u_A}| \leqslant 2^{m-3} - \frac{|\Gamma|}{2}$ then $\mathcal{C}_f$ is wide.*

Proof. According to Lemma 3.2.10, for every $u \in (\mathbb{F}_2^m)^*$ such that $u \neq u_A$, it must be that either $A \subset H_u$ or $|A \cap H_u| = 2^{m-3}$. To prove minimality of the code, we will verify the conditions in Corollary 3.2.4 taking into account these possibilities. The hypothesis on Γ guarantees that $\Delta \cap H_{u_A} \neq \emptyset$. Note that the difference $A \setminus \Delta$ equals $\{p_0\}$, hence $H_u \cap \Delta$ contains at least $2^{m-3} - 1$ elements. Given that $m \geqslant 4$, it holds $H_u \cap \Delta$ is non-empty for every $u \in \mathbb{F}_2^m$. Additionally, $0 \in \overline{H}_u \cap \Delta$ for each $u \in \mathbb{F}_2^m$ so that $\overline{H}_u \cap \Delta \neq \emptyset$.
Now let us check that $H_u \setminus H_{u'} \nsubseteq \Delta \setminus H_{u'}$ for every pair of distinct $u, u' \in (\mathbb{F}_2^m)^*$. Suppose, for the sake of contradiction, that $H_u \setminus H_{u'}$ is included in $\Delta \setminus H_{u'}$ for some different non-zero u, u'. Note that $|H_u \setminus H_{u'}| = 2^{m-2}$ and consider the following three cases:

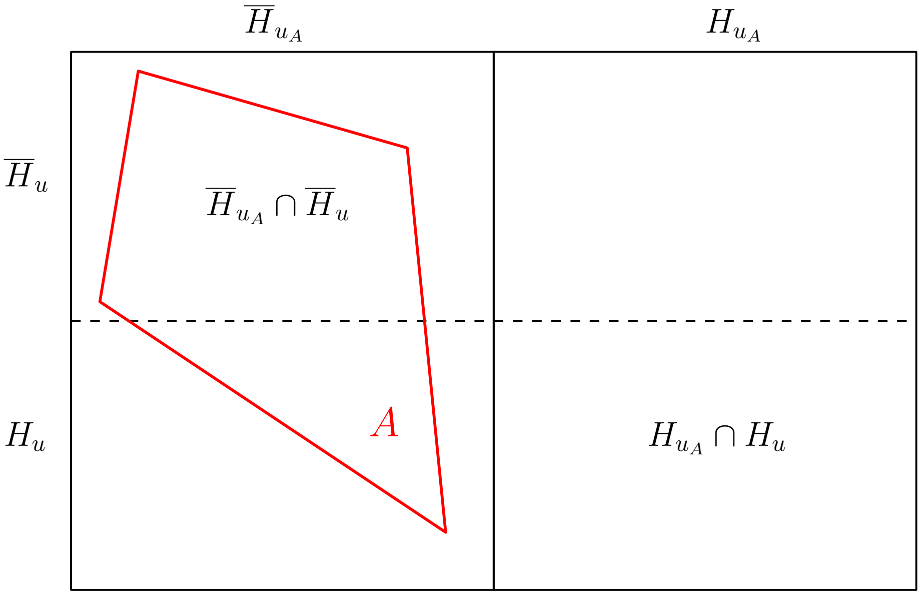
Case 1: The set $H_{u'} \cap A$ is empty, that is, $u' = u_A$. Then, either

$$|A \cap (H_u \setminus H_{u_A})| = 2^{m-3} \text{ or } |A \cap (H_u \setminus H_{u_A})| = 2^{m-2}.$$

In the latter case, $p_0 \in H_u \setminus H_{u_A}$ while at the same time $p_0 \notin \Delta$, a contradiction. The former case implies

$$H_u \setminus H_{u_A} \subseteq (\Delta \cap H_u) \setminus H_{u_A}.$$

However, $|(\Delta \cap H_u) \setminus H_{u_A}| < 2^{m-2}$ and $|H_u \setminus H_{u_A}| = 2^{m-2}$, a contradiction. Therefore, $H_u \setminus H_{u_A} \nsubseteq \Delta \setminus H_{u_A}$ (see Figure 3.3).



$$\begin{array}{l} |A| = 2^{m-2} \\ |H_u \setminus H_{u_A}| = 2^{m-2} \end{array} \quad \to \quad |A \cap (H_u \setminus H_{u_A})| = 2^{m-2} \text{ or } 2^{m-3}$$

Figure 3.3: Case $u' = u_A$ in the proof of Theorem 3.2.12.

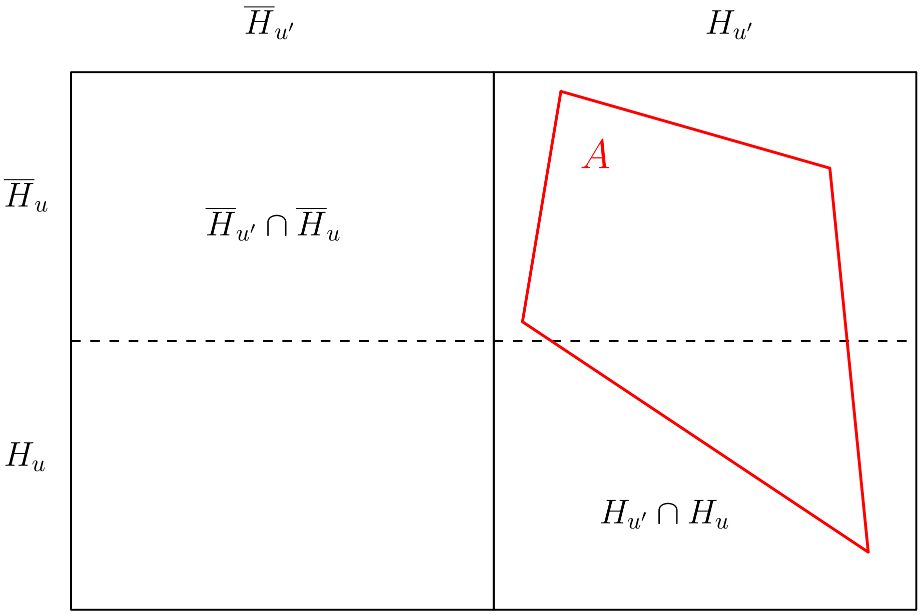


Figure 3.4: Case $A \subset H_{u'}$ in the proof of Theorem 3.2.12.

Case 2: The affine subspace A is a subset of $H_{u'}$. In this case, the cardinality of $\Delta \setminus H_{u'}$ is at most 2^{m-3} since $S \subset H_{u'}$. This implies that $H_u \setminus H_{u'}$ cannot be contained in $\Delta \setminus H_{u'}$ (see Figure 3.4).

Case 3: The affine subspace $A \cap H_{u'}$ has cardinality 2^{m-3}. Observe that

$$|\Delta \setminus H_{u'}| < 2^{m-3} + 2^{m-3} = 2^{m-2}$$

since S can only contribute with at most 2^{m-3} elements to this difference. Therefore, $H_u \setminus H_{u'}$ cannot be contained in $\Delta \setminus H_{u'}$ (see Figure 3.5).

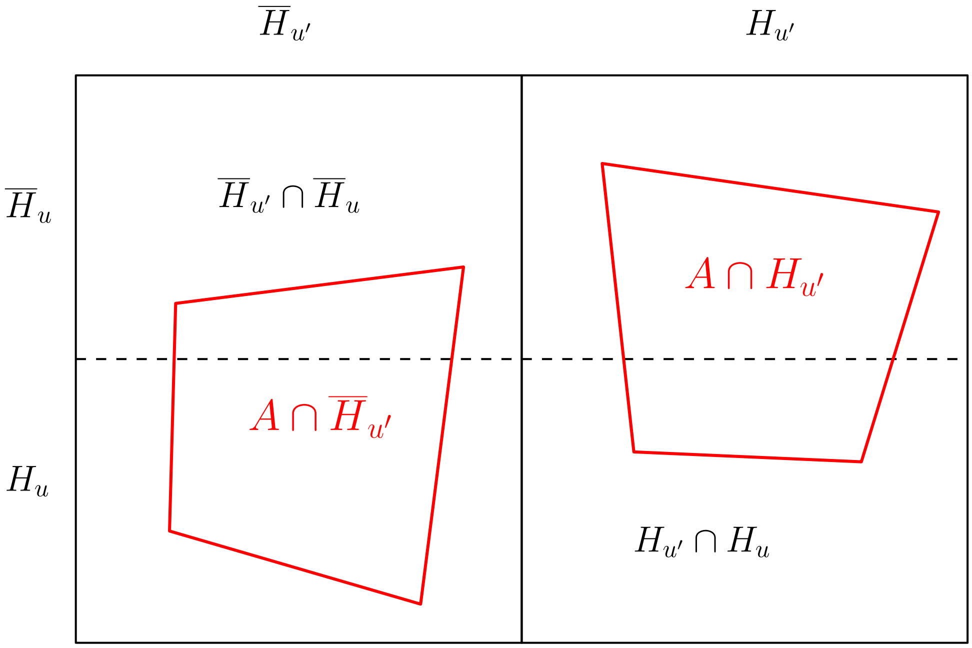


Figure 3.5: Case $|A \cap H_{u'}| = 2^{m-3}$ in the proof of Theorem 3.2.12.

These three cases show that $H_u \setminus H_{u'} \not\subseteq \Delta \setminus H_{u'}$ for every pair of distinct $u, u' \in (\mathbb{F}_2^m)^*$. The conditions of Corollary 3.2.4 are thus satisfied, hence $\mathcal{C}_f$ is minimal. Assume that $|\Gamma \cap H_{u_A}| \leqslant 2^{m-3} - \frac{|\Gamma|}{2}$. Set $\kappa = |\Gamma \cap H_{u_A}|$. Notice that $|\Gamma| \leqslant 2^{m-2} - 2\kappa$ and

$$|\Delta \setminus H_{u_A}| = 2^{m-2} + |\Gamma| - \kappa \text{ and } |H_{u_A} \setminus \Delta| = 2^{m-1} - \kappa.$$

This gives that the codeword c_{1,u_A} has weight $2^{m-1} + 2^{m-2} + |\Gamma| - 2\kappa$, hence

$$w_{\max} \geqslant 2^{m-1} + 2^{m-2} + |\Gamma| - 2\kappa.$$

Since $|\Delta| = 2^{m-2}+|\Gamma|$, the minimum weight $w_{\min}$ is at most $2^{m-2}+|\Gamma|$. Putting everything together,

$$2w_{\min} \leqslant 2^{m-1} + 2|\Gamma| \leqslant 2^{m-1} + |\Gamma| + 2^{m-2} - 2\kappa \leqslant w_{\max},$$

which implies that $\frac{w_{\min}}{w_{\max}} \leqslant \frac{1}{2}$. □

The first question that should come to the thorough reader's mind is about the existence of suitable sets Γ that satisfy the conditions in Theorem 3.2.12. A special case given below is when $|\Gamma| \in \{1, 2\}$.

Corollary 3.2.13. *Let $m \geqslant 4$ and $\mathscr{B} = \{a_1, \dots, a_m\}$ be a basis of $\mathbb{F}_2^m$ such that a_m has odd weight and it is orthogonal to all the other a_i's, i.e., $a_m \cdot a_i = 0$ for $1 \leqslant i \leqslant m-1$. Define $V = \langle a_1, \dots, a_{m-2}\rangle$ and assign $A = a_{m-1} + V$. Let $S = A \setminus \{p_0\}$ for some $p_0 \in A$. Fix $(\tau_1, \dots, \tau_{m-1}) \in \mathbb{F}_2^{m-1} \setminus \{0\}$ and define Γ as follows:*

$$\Gamma = \begin{cases} \{a_m\} & \text{if } m = 4, \\ \{a_m, a_m + \tau_{m-1}a_{m-1} + \dots + \tau_1 a_1\} & \text{if } m > 4. \end{cases}$$

Suppose Δ and f are defined as in Theorem 3.2.12. Then, $\mathcal{C}_f$ is a wide minimal code.

Proof. The only non-trivial condition in 3.2.12 to prove is that the unique hyperplane disjoint to A is H_{a_m}, thus $u_A = a_m$. Indeed, since a_m is orthogonal to each a_i, it holds that

$$\langle a_1, \dots, a_{m-1}\rangle \cap H_{a_m} = \emptyset,$$

which yields $A \cap H_{a_m} = \emptyset$. Since the weight of a_m is odd, the element a_m lies in H_{a_m}, hence $\Gamma \cap H_{a_m} \neq \emptyset$. The code $\mathcal{C}_f$ is then minimal.

To show that $\mathcal{C}_f$ is wide, note that, for $m = 4$, $|\Gamma \cap H_{a_m}| = 1 < \frac{3}{2} = 2 - \frac{1}{2}$. For $m \geqslant 5$, the vector

$$a_m + \tau_{m-1}a_{(m-1)} + \dots + \tau_1 a_1$$

lies in H_{a_m} since $a_m \cdot a_i = 0$ for every i smaller than m and also $a_m \in H_{a_m}$ as a_m has odd weight. Hence, $|\Gamma \cap H_{a_m}| = 2 < 2^{m-3} - 1$ and the code $\mathcal{C}_f$ is therefore wide by Theorem 3.2.12. □

The minimum distance d depends on the intersection of the $(m-2)$-dimensional affine subspace A with the affine hyperplanes H_u. The following examples illustrate this dependence concretely.

Example 3.2.14. *Let $m = 5$. Consider the 3-dimensional linear subspace*

$$V = \langle (1,1,0,0,0),(1,0,1,0,1),(0,0,1,0,1)\rangle$$

and define $A = (1,1,1,1,1) + V$. Let $p_0 = (1,1,1,1,1) + (1,1,0,0,0) = (0,0,1,1,1)$ and define $S = A \setminus \{p_0\}$. Let

$$\Gamma = \{(0,0,1,1,0),(1,1,0,1,1)\}.$$

Suppose that Δ and f are defined as in Theorem 3.2.12. Using computer-based simulations, one can confirm that $\mathcal{C}_f$ is a wide minimal code with parameters $[32,6,8]$. Furthermore, $w_{\min} = 8$ and $w_{\max} = 22$. Moreover, the set $H_{(0,0,1,0,1)}$ is the affine hyperplane disjoint to A and Γ is included in it.

Example 3.2.15. *Again, let $m = 5$. Consider the linear subspace*

$$V = \langle (1,1,1,1,1),(1,1,0,1,0),(1,1,0,1,1)\rangle$$

and define $A = (1,0,1,1,0) + V$. Let $p_0 = (1,0,1,1,0) + (1,1,1,1,1) = (0,1,0,0,1)$ and define $S = A \setminus \{p_0\}$. Let

$$\Gamma = \{(0,0,1,0,1),(0,0,1,1,0)\}.$$

Again, specifying Δ and f as in Theorem 3.2.12, one can verify that $\mathcal{C}_f$ is a wide minimal code with parameters $[32,6,10]$. Furthermore, $w_{\min} = 10$ (which is different from Example 3.2.14) and $w_{\max} = 24$. In this case, the set $H_{(1,0,0,1,0)}$ is the affine hyperplane disjoint to A and $|\Gamma \cap H_{(1,0,0,1,0)}| = |\{(0,0,1,1,0)\}| = 1$.

When the set Γ contains only two elements, there are just a few possibilities for the cardinality of the intersection of Γ with the affine hyperplanes H_u. Consequently, the weight distribution of the codes described in Corollary 3.2.13 can be found since these cardinalities depend uniquely on the choice of the vector $(\tau_1,\ldots,\tau_{m-1})$. The weight distributions are listed in descending order in Tables 3.1, 3.2 and 3.3.

Weight w	Number of codewords A_w
$2^{m-1}+2^{m-2}-2$	1
$2^{m-1}+2$	$2^m-2^{m-2}-3$
2^{m-1}	2^m-1
$2^{m-1}-2$	$2^{m-2}-1$
$2^{m-2}+2$	3

Table 3.1: Weight distribution of 5-weight wide minimal codes $\mathcal{C}_f$, $(\tau_1,\ldots,\tau_{m-1}) = (0,0,\ldots,0,1)$.

Weight w	Number of codewords A_w
$2^{m-1}+2^{m-2}-2$	1
$2^{m-1}+4$	2^{m-3}
$2^{m-1}+2$	$2^m-5\cdot 2^{m-3}-3$
2^{m-1}	$2^m-1+3\cdot 2^{m-3}$
$2^{m-1}-2$	$2^{m-3}-1$
$2^{m-2}+2$	3

Table 3.2: Weight distribution of 6-weight wide minimal codes $\mathcal{C}_f$, when $(\tau_1,\dots,\tau_{m-1})$ is such that $\tau_{m-1}=1$ and $(\tau_1,\dots,\tau_{m-2})$ is nonzero.

Weight w	Number of codewords A_w
$2^{m-1}+2^{m-2}-2$	1
$2^{m-1}+4$	$2^{m-3}-1$
$2^{m-1}+2$	$2^m-2^{m-3}-3$
2^{m-1}	$2^m+2^m-2^{m-3}-4$
$2^{m-1}-2$	$2^{m-3}-1$
$2^{m-2}+4$	1
$2^{m-2}+2$	1
2^{m-2}	1

Table 3.3: Weight distribution of 8-weight wide minimal codes $\mathcal{C}_f$, when $(\tau_1,\dots,\tau_{m-1})$ is such that $\tau_{m-1}=0$ and $(\tau_1,\dots,\tau_{m-2})$ is nonzero.

3.3 The hyperplane method

In this section, another way to derive wide minimal codes is given. We will introduce two general results similar to Theorem 3.2.12. The main modification is the use of hyperplanes instead of $(m-2)$-dimensional affine subspaces, thus giving the cardinality of the support Δ of f will be $|\Delta|=2^{m-1}-|\Gamma|+1$ for a suitably chosen Γ with $3\leqslant|\Gamma|\leqslant 2^{m-2}$. It is worth mentioning that the minimality of the codes constructed in this section is not a consequence of Corollary 3.2.4.

Theorem 3.3.1 (The hyperplane method)**.** *Let $m\geqslant 4$ be a positive integer. Fix $u_0\in(\mathbb{F}_2^m)^*$ and select a point $p_0\in H_{u_0}$. Suppose that there is a non-empty subset Γ of $\overline{H}_{u_0}$ which contains at least three elements but no more than 2^{m-2} and with the property that for each $u\in(\mathbb{F}_2^m)^*$ different from u_0 such that $p_0\in H_u$, the intersection $\Gamma\cap H_u$ is non-empty. Let $\Delta=(\overline{H}_{u_0}\setminus\Gamma)\cup\{p_0\}$ and f*

be its characteristic function. The code $\mathcal{C}_f$ given by (2.12) is wide and minimal with parameters $[2^m, m+1, 2^{m-1} - |\Gamma| + 1]$. Moreover, $w_{\max} = 2^m - |\Gamma| - 1$.

Proof. Recall that the weight of a codeword $c_{a,u} = af(x) + u \cdot x$ in $\mathcal{C}_f$ is given by $|\text{supp}(c_{a,u})|$, where

$$\text{supp}(c_{a,u}) = \begin{cases} \Delta \ominus H_u & \text{if } a \neq 0; u \neq 0 \\ \Delta & \text{if } a \neq 0, u = 0; \\ H_u & \text{if } a = 0, u \neq 0; \\ \emptyset & \text{if } a = 0, u = 0. \end{cases}$$

Let us estimate the possible non-zero values for $|\text{supp}(c_{a,u})|$. The only unknown values are for $a \neq 0$ and $u \neq 0$ since $|H_u| = 2^{m-1}$ for $u \neq 0$ and $|\Delta| = 2^{m-1} - |\Gamma| + 1$. Let $a \neq 0$ and u be a non-zero element in $\mathbb{F}_2^m$. There are two possibilities to consider.

(i) If $u = u_0$, then $H_{u_0} \cap \Delta = \{p_0\}$ so that

$$wt(c_{1,u_0}) = |\Delta \ominus H_{u_0}| = |\Delta| + |H_{u_0}| - 2 = 2^m - |\Gamma| - 1.$$

(ii) Suppose that $u \neq u_0$. The intersection $\overline{H}_{u_0} \cap H_u$ has cardinality 2^{n-2}. The cardinality of $\Delta \cap H_u$ relies on the way $\Gamma \cup \{p_0\}$ intersects H_u. It attains the smallest value when Γ is a subset of H_u and $p_0 \notin H_u$, hence

$$|\Delta \cap H_u| \geqslant 2^{m-2} - |\Gamma|.$$

On the other hand, by the definition of Γ, it cannot hold simultaneously that Γ is disjoint to H_u and $p_0 \in H_u$, henceforth $|\Delta \cap H_u| \leqslant 2^{m-2}$. Putting these two bounds together gives

$$2^{m-2} - |\Gamma| \leqslant |\Delta \cap H_u| \leqslant 2^{m-2}.$$

The weight $wt(c_{1,u})$ is then bounded by

$$2^{m-1} - |\Gamma| + 1 \leqslant wt(c_{1,u}) \leqslant 2^{m-1} + |\Gamma| + 1.$$

Note that the value $2^{m-1} + |\Gamma| + 1$ is bounded above by $2^m - |\Gamma| - 1$ since $|\Gamma| \leqslant 2^{m-2}$. From this, for each $u \in \mathbb{F}_2^m$ and $a \in \{0, 1\}$, the value $wt(c_{a,u})$ is at most $2^m - |\Gamma| - 1$, which is attained by c_{1,u_0}, hence $w_{\max} = 2^m - |\Gamma| - 1$. Now, for each $u \in \mathbb{F}_2^m$ and $a \in \{0, 1\}$, the value $wt(c_{a,u})$ is at least $|\Delta| = 2^{m-1} - |\Gamma| + 1$, which is attained by $c_{1,0}$ so $w_{\min} = |\Delta| = 2^{m-1} - |\Gamma| + 1$.

To show the minimality and wideness of $\mathcal{C}_f$, we use the derived expressions for $w_{\min}$ and $w_{\max}$. A simple computation on the minimum and maximum weights shows that the code is wide, namely,

$$2w_{\min} = 2^m - 2|\Gamma| + 2 \leqslant 2^m - |\Gamma| - 1 = w_{\max}$$

since $|\Gamma| \geqslant 3$. Thus $\frac{w_{\min}}{w_{\max}} \leqslant \frac{1}{2}$. To prove the minimality of $\mathcal{C}_f$, compute the maximum and minimum Walsh values of f as

$$\mathcal{W}_{\min} = 2^m - 2w_{\max} = -2^m + 2|\Gamma| + 2$$

and

$$\mathcal{W}_{\max} = 2^m - 2w_{\min} = 2|\Gamma| - 2.$$

Since $|\Gamma| \leqslant 2^{m-2}$, the maximal Walsh value $2|\Gamma| - 2$ is strictly smaller than 2^{m-1}. Similarly,

$$\mathcal{W}_{\max} - \mathcal{W}_{\min} = (2|\Gamma| - 2) - (-2^m + 2|\Gamma| + 2) = 2^m - 4 < 2^m.$$

By Corollary 3.1.3, we get that $\mathcal{C}_f$ is minimal. □

The following result, similar to Theorem 3.3.1, can be proved using the same lines of reasoning in a *complementary* setting. This particularly means that the selection of p_0 and Γ are performed using the complements of the relevant hyperplanes. Observe that the method described below is indeed almost verbatim compared to Theorem 3.3.1.

Theorem 3.3.2 (The hyperplane method, complementary setting)**.** *Let $m \geqslant 4$ be a positive integer. Fix $u_0 \in (\mathbb{F}_2^m)^*$ and select a point $p_0 \in \overline{H}_{u_0}$. Suppose that there is a non-empty set $\Gamma \subset H_{u_0}$ with at least m elements but $|\Gamma| < 2^{m-2}$, such that the following two conditions hold:*

- *for every $u \in (\mathbb{F}_2^m)^*$, $u \neq u_0$, if $p_0 \in H_u$, then Γ intersects H_u; and*
- *for every $u \in (\mathbb{F}_2^m)^*$, $u \neq u_0$, if $p_0 \in \overline{H}_u$, then Γ intersects $\overline{H}_u$.*

Let $\Delta = (H_{u_0} \setminus \Gamma) \cup \{p_0\}$ and f be its characteristic function. The code $\mathcal{C}_f$ is wide and minimal with parameters $[2^m, m+1, |\Gamma|+1]$. Moreover, the maximum weight satisfies $w_{\max} \leqslant 2^{m-1} + |\Gamma| - 1$.

Proof. Similarly to the proof of Theorem 3.3.1, estimate the value $|\mathrm{supp}(c_{a,u})|$ for different $u \in \mathbb{F}_2^m$. Assume that $a = 1$. Note that $\mathrm{supp}(c_{1,0}) = \Delta$ and $|\Delta| = 2^{m-1} - |\Gamma| + 1$.

(i) Suppose that $u = u_0$. In this case, the fact that Γ is a subset of the affine hyperplane H_{u_0} and the definition of Δ imply that the intersection $H_{u_0} \cap \Delta$ has $2^{m-1} - |\Gamma|$ many elements, thus

$$wt(c_{1,u_0}) = |\Delta \ominus H_{u_0}| = |\Gamma| + 1.$$

(ii) Suppose that $u \neq 0$ and $u \neq u_0$. The cardinality of $\Delta \cap H_v$ depends on the way $\Gamma \cup \{p_0\}$ intersects H_u. By the definition of Γ, it is impossible that Γ is a subset of H_u and $p_0 \notin H_u$ at the same time therefore

$$|\Delta \cap H_u| \geqslant 2^{m-2} - |\Gamma| + 1,$$

where we tacitly use $|H_{u_0} \cap H_u| = 2^{m-2}$. On the other hand, it cannot happen simultaneously that Γ is disjoint to H_u and $p_0 \in H_u$ therefore

$$|\Delta \cap H_u| \leqslant 2^{m-2}.$$

Putting these bounds together, we get

$$2^{m-2} - |\Gamma| + 1 \leqslant |\Delta \cap H_u| \leqslant 2^{m-2}.$$

As before, the weight $wt(c_{1,u})$ can be then bounded as follows

$$2^{m-1} - |\Gamma| + 1 \leqslant wt(c_{1,u}) \leqslant 2^{m-1} + |\Gamma| - 1.$$

Now it is evident that the maximum weight in the code satisfies $w_{\max} \leqslant 2^{m-1} + |\Gamma| - 1$ and that $|\Gamma|+1$ is the minimum weight (due to the restriction $|\Gamma| < 2^{m-2}$).

The wideness of $\mathcal{C}_f$ is hence easy to show, the ratio $\frac{w_{\min}}{w_{\max}} \leqslant \frac{|\Gamma|+1}{2^{m-1}}$ is less than $\frac{1}{2}$, therefore $\mathcal{C}_f$ is wide. We turn to prove the minimality of the code $\mathcal{C}_f$. Note that

$$\mathcal{W}_{\min} = 2^m - 2w_{\max} \geqslant -2|\Gamma| + 2$$

and

$$\mathcal{W}_{\max} = 2^m - 2w_{\min} = 2^m - 2|\Gamma| - 2.$$

In this case, Corollary 3.1.3 cannot be applied directly since $\mathcal{W}_{\max} = 2^m - 2|\Gamma| - 2 \geqslant 2^{m-1}$. Instead, we will use a different approach that uses the second largest Walsh coefficient as well.

From the paragraphs above, observe that the minimum weight is attained by a single codeword and the second smallest weight is $2^{m-1} - |\Gamma| + 1$. This yields that the largest Walsh value of f is attained once and the second largest, say, w, is equal to $2|\Gamma| - 2$. Compute the sum of these two values to get

$$\mathcal{W}_{\max} + w = 2^m - 2|\Gamma| - 2 + 2|\Gamma| - 2 = 2^m - 4$$

which is strictly smaller than 2^m. Since the largest Walsh coefficient is attained exactly once, for every distinct $u, v \in \mathbb{F}_2^m$, it holds that

$$W_f(u) + W_f(v) \leqslant \mathcal{W}_{\max} + w < 2^m,$$

and

$$W_f(u) - W_f(v) \leqslant \mathcal{W}_{\max} - \mathcal{W}_{\min} \leqslant (2^m - 2|\Gamma| - 2) - (-2|\Gamma| + 2) = 2^m - 4 < 2^m.$$

According to Theorem 3.1.2, $\mathcal{C}_f$ is minimal. □

3.3.1 Root functions

For the purpose of constructing explicit classes of wide minimal codes, we now employ the so-called root functions analyzed in [43], which proved to be useful for hardware circuits testing. A Boolean function $f : \mathbb{F}_2^m \to \mathbb{F}_2$ is called a *root function* if for every $x \in \mathbb{F}_2^m$, the output $f(x)$ is null if and only if there is a $y \in \mathbb{F}_2^m$ at distance one from x such that $f(y) = 1$. A family of non-affine root functions of maximal weight was constructed in [43] using the following procedure.

- Consider the affine function $l_m(x) = x_m + \cdots + x_1 + \epsilon$, where $\epsilon \in \mathbb{F}_2$. It is readily seen that l_m is a root function of weight 2^{m-1};
- Select $p_0 \notin \mathrm{supp}(l_m)$ and switch up the value of l_m at p_0, i.e., define $l_m^{(1)}$ such that $l_m^{(1)}(p_0) = 1$ and $l_m^{(1)}(x) = l_m(x)$ for every $x \neq p_0$;
- Define r_m^ϵ by the property that $r_m^\epsilon(x) = 0$ for every $x \in \mathbb{F}_2^m$ such that $d(x, p_0) = 1$ and $r_m^\epsilon(x) = l_m^{(1)}(x)$ otherwise.

In a more compact way, for the affine function $l_m(x) = x_m + \cdots + x_1 + \epsilon$ and a fixed $p_0 \notin \mathrm{supp}(l_m)$, define

$$r_m^\epsilon(x) = \begin{cases} 1 & \text{if} \quad x = p_0; \\ 0 & \text{if} \quad d(x, p_0) = 1; \\ l_m(x) & \text{otherwise.} \end{cases} \tag{3.4}$$

Theorem 3.3.3. *[43] The functions $r_m^\epsilon : \mathbb{F}_2^m \to \mathbb{F}_2$ described in (3.4) are root functions of weight $2^{m-1} - m + 1$. For $m > 3$, there are exactly 2^m root functions having this weight, and when $m = 3$ there are 2^{m-1} such functions.*

Theorem 3.3.4. *Let $m \geqslant 4$ and consider a root function r_m^ϵ with weight $2^{m-1} - m + 1$ described in (3.4). The code $\mathcal{C}_{r_m^\epsilon}$ is a wide minimal code with parameters $[2^m, m+1, d]$, where $d = 2^{m-1} - m + 1$ when $\epsilon = 1$ and $d = m+1$ when $\epsilon = 0$.*

Proof. Let Δ denote the support of r_m^ϵ. The construction of r_m^ϵ gives that

$$\Delta = (\sup(l_m) \setminus \{x \in \mathbb{F}_2 m : d(x, p_0) = 1\}) \cup \{p_0\}.$$

Consider two cases according to the values of ϵ.

(i) Suppose that $\epsilon = 1$. In this case, set u_0 to be the all-one vector in $\mathbb{F}_2^m$, hence $\mathrm{supp}(l_m) = \overline{H}_{u_0}$ and $p_0 \in H_{u_0}$. Define

$$\Gamma := \{x \in \mathbb{F}_2^m : d(x, p_0) = 1\}$$

and observe that Γ is a subset of the hyperplane $\overline{H}_{u_0}$ with m elements. With this notation, write $\Delta = (\overline{H}_{u_0} \setminus \Gamma) \cup \{p_0\}$. In order to apply Theorem 3.3.1, it is enough to show that for every $u \in (\mathbb{F}_2^m)^*$ with $u \neq u_0$ such that $p_0 \in H_u$, the intersection $\Gamma \cap H_u$ is non-empty. In fact, we will prove the stronger statement that $\Gamma \cap H_u \neq \emptyset$ for every non-zero u in $\mathbb{F}_2^m$ different from u_0.
Choose an ordering of the elements in Γ, say, $\Gamma = \{x_1, \ldots, x_m\}$, in such a way that $x_1, \ldots, x_{wt(p_0)}$ have weight equal to $wt(p_0) - 1$ and $x_{wt(p_0)+1}, \ldots, x_m$ have weight $wt(p_0) + 1$. Moreover, if $0 \in \Gamma$, then $x_1 = 0$. Since $wt(p_0)$ is odd (recall that $p_0 \notin \sup(l_m)$), the set $\{x_2, \ldots, x_m\}$ is linearly independent over $\mathbb{F}_2$. Thus, there are $m-1$ linearly independent vectors in $\overline{H}_{u_0}$, thus this is also a spanning set, i.e. $\langle x_2, \ldots, x_m \rangle = \overline{H}_{u_0}$. Let $u \in (\mathbb{F}_2^m)^*$ with $u \neq u_0$. If $\Gamma \cap H_u = \emptyset$, then $\langle x_2, \ldots, x_m \rangle \cap H_u = \emptyset$ which contradicts the fact that $|\overline{H}_{u_0} \cap H_u| = 2^{m-2}$. By Theorem 3.3.1, the code $\mathcal{C}_{r_m^1}$ is then a wide minimal code.

(ii) Suppose that $\epsilon = 0$. This case is similar to (i) with the only difference that we apply Theorem 3.3.2 instead. Set u_0 to be the all-one vector, whence $\mathrm{supp}(l_m) = H_{u_0}$ and $p_0 \in \overline{H}_{u_0}$. Define

$$\Gamma = \{x \in \mathbb{F}_2^m : d(x, p_0) = 1\}.$$

Observe that Γ is indeed a subset of H_{u_0} and has m elements. Write $\Delta = (H_{u_0} \setminus \Gamma) \cup \{p_0\}$. To apply Theorem 3.3.2, we must show two conditions, namely,

- for every $u \in (\mathbb{F}_2^n)^*$ with $u \neq u_0$, if $p_0 \in H_u$, then $\Gamma \cap H_u \neq \emptyset$;
- for every $u \in (\mathbb{F}_2^n)^*$ with $u \neq u_0$, if $p_0 \in \overline{H}_u$, then $\Gamma \cap \overline{H}_u \neq \emptyset$.

In fact, we will prove the stronger statement that Γ intersects every affine hyperplane H_u and every hyperplane $\overline{H}_u$ for $u \in (\mathbb{F}_2^m)^*$ different from u_0. To show this, note that the elements of Γ are linearly independent since $wt(p_0)$ is even, hence, Γ is a basis for $\mathbb{F}_2^m$ consisting of elements of H_{u_0}.

For each non-zero vector u in $\mathbb{F}_2^m$, the intersection $\Gamma \cap H_u$ is non-empty, otherwise Γ would be a linearly independent subset within the $(m-1)$-dimensional subspace $\overline{H}_u$. Let us now turn to prove the second condition, i.e. for every non-zero $u \in \mathbb{F}_2^m$ with $u \neq u_0$, $\Gamma \cap \overline{H}_u \neq \emptyset$. Suppose this is not true, that is, assume there is a $u \in (\mathbb{F}_2^m)^*$ such that $\Gamma \subseteq H_u$. Let $\Gamma = \{\gamma_1, \ldots, \gamma_m\}$ and select an arbitrary point $x_0 \in H_{u_0} \setminus H_u$. Since Γ is a basis for $\mathbb{F}_2^m$, there exist a positive integer k and $\gamma_{i_1}, \ldots, \gamma_{i_k} \in \Gamma$ such that $x_0 = \gamma_{i_1} + \cdots + \gamma_{i_k}$. By the choice of x_0, $u_0 \cdot x_0 = 1$ and $u \cdot x_0 = 0$. On the one hand, replacing the expression of x in terms of Γ

$$1 = u_0 \cdot x_0 = u_0 \cdot (\gamma_{i_1} + \cdots + \gamma_{i_k}) = (u_0 \cdot \gamma_{i_1}) + \cdots + (u_0 \cdot \gamma_{i_k}).$$

Since $\Gamma \subseteq H_{u_0}$, the integer k must be odd. On the other hand,

$$0 = u \cdot x_0 = u \cdot (\gamma_{i_1} + \cdots + \gamma_{i_k}) = (u \cdot \gamma_{i_1}) + \cdots + (u \cdot \gamma_{i_k}). \tag{3.5}$$

Since $\Gamma \subseteq H_u$, k must be even, too. This is a contradiction that establishes the result.

□

Example 3.3.5. *Let $m = 6$ and consider a root function r_6^1 with weight 27. The code $\mathcal{C}_{r_6^1}$ is a wide minimal $[64, 7, 27]$-code with weight enumerator given by*

$$1 + 6z^{27} + 15z^{29} + 20z^{31} + 63z^{32} + 15z^{33} + 6z^{35} + z^{37} + z^{57}.$$

Similarly, consider a root function r_6^0 with weight 27. The code $\mathcal{C}_{r_6^1}$ is a wide minimal $[64, 7, 7]$-code with weight enumerator given by

$$1 + z^7 + z^{27} + 6z^{29} + 15z^{31} + 63z^{32} + 20z^{33} + 15z^{35} + 6z^{37}.$$

3.3.2 Weight distributions and asymptotic behaviour

For every $m \geqslant 4$, we have seen that the code $\mathcal{C}_{r_m^\epsilon}$ is wide and minimal. The asymptotic behaviour of the ratio $\frac{w_{\min}}{w_{\max}}$ can be easily established.

Corollary 3.3.6. *Let $\mathcal{C}_{r_m^\epsilon}$ be the linear code described in Theorem 3.3.4. Denote by a_m^ϵ the quotient $\frac{w_{\min}}{w_{\max}}$, where $\epsilon \in \{0, 1\}$. The numbers a_m^ϵ satisfy*

$$\lim_{m\to\infty} a_m^1 = \frac{1}{2} \qquad \text{and} \qquad \lim_{m\to\infty} a_m^0 = 0.$$

Proof. For each positive integer m at least four, the minimum weight $w_{\min}$ of the code $\mathcal{C}_{r_m^1}$ is $= 2^{m-1} - m + 1$ and the maximum weight $w_{\max}$ is $2^m - m - 1$. Hence

$$\lim_{m\to\infty} a_m^1 = \frac{2^{m-1} - m + 1}{2^m - m - 1}$$

is clearly equal to $\frac{1}{2}$. For $\epsilon = 0$, $w_{\min} = m+1$ and $w_{\max} = 2^{m-1}+m-1$, therefore

$$a_m^0 = \frac{m+1}{2^{m-1} + m - 1},$$

which is zero as m goes to infinity. □

The weight distribution of the provided codes is directly related to the Walsh spectra of root functions of maximal weight. These values are given in the Tables 3.4–3.7 below.

Case	Walsh spectra
m even	$\pm 2, \pm 6, \pm 10, \dots, \pm 2m-2,\ -2^m + 2m + 2$
m odd	$0, \pm 4, \pm 8, \dots, \pm 2m-2,\ -2^m + 2m + 2$

Table 3.4: Walsh spectral values of r_m^1 w.r.t. the parity of m.

Case	Weights
m even	$2^{m-1} \pm (m-1), 2^{m-1} \pm (m-3), \dots, 2^{m-1} \pm 1, 2^{m-1}, 2^m - (m+1)$
m odd	$2^{m-1} \pm (m-1), 2^{m-1} \pm (m-3), \dots, 2^{m-1} \pm 2, 2^{m-1}, 2^m - (m+1)$

Table 3.5: Nonzero weights of codewords of $\mathcal{C}_{r_m^1}$.

Case	Walsh spectra
m even	$\pm 2, \pm 6, \pm 10, \dots, \pm(2m-2),\ 2^m - 2m - 2$
m odd	$0, \pm 4, \pm 8, \dots, \pm(2m-2),\ 2^m - 2m - 2$

Table 3.6: Walsh spectral values of r_m^0 w.r.t. the parity of m.

Case	Weights
m even	$2^{m-1} \pm (m-1), 2^{m-1} \pm (m-3), \dots, 2^{m-1} \pm 1, 2^{m-1}, m+1$
m odd	$2^{m-1} \pm (m-1), 2^{m-1} \pm (m-3), \dots, 2^{m-1} \pm 2, 2^{m-1}, m+1$

Table 3.7: Nonzero weights of codewords of $\mathcal{C}_{r_m^0}$.

3.4 The general Maiorana-McFarland class

In what follows, we explore two slight modifications of some existing design methods to construct wide binary linear codes given in [20], and, recently, in [40]. These constructions make use of the general Maiorana-McFarland class of Boolean functions. The codes presented in this section achieve a larger minimum distance compared to the codes introduced in [20] and [40].

The *general Maiorana-McFarland class* of Boolean functions, denoted by $\mathcal{GMM}$, contains all the Boolean functions of the form:

$$f(x,y) = y \cdot \phi(x) + \mu(x), \tag{3.6}$$

where $x \in \mathbb{F}_2^\kappa, y \in \mathbb{F}_2^\lambda$, ϕ is an arbitrary mapping from $\mathbb{F}_2^\kappa$ to $\mathbb{F}_2^\lambda$ and $\mu : \mathbb{F}_2^\kappa \to \mathbb{F}_2$. If $\kappa = \lambda$ and ϕ is a permutation on $\mathbb{F}_2^\kappa$, then f is said to belong to the *Maiorana-McFarland class*, denoted by $\mathcal{MM}$. It can be proved that every function in $\mathcal{MM}$ is bent [35].

We will exclusively consider simple functions for μ, such as the constant one function over $\mathbb{F}_2^\kappa$, the identically one function over $(\mathbb{F}_2^\kappa)^*$, abbreviated by $\mu \equiv 1$ and defined by $\mu(x) = 1$ for all $x \in (\mathbb{F}_2^\kappa)^*$ and $\mu(0) = 0$, or the identically zero function over $\mathbb{F}_2^\kappa$.

First let us recall some useful properties of Krawtchouk polynomials, which will be used in the proofs of the main results. Let m be a positive integer, and let x be a variable taking non-negative integer values. The k-th Krawtchouk polynomial is defined by

$$P_k(x,m) = \sum_{j=0}^{k} (-1)^j \binom{x}{j} \binom{m-x}{k-j} \tag{3.7}$$

where $0 \leqslant k \leqslant m$. For simplicity, we will simply write $P_k(x)$ instead of $P_k(x,m)$ whenever there is no ambiguity. Using well-known properties of Krawtchouk polynomials [20],

$$P_k(i) = (-1)^i P_{m-k}(i),\ 0 \leqslant i \leqslant m. \tag{3.8}$$

Moreover, for each $u \in \mathbb{F}_2^m$ with Hamming weight $wt(u) = i$, the k-th Krawtchouk polynomial evaluated at i, $P_k(i)$, satisfies

$$\sum_{wt(v)=k} (-1)^{u \cdot v} = P_k(i). \tag{3.9}$$

3.4.1 The first family of wide minimal codes from $\mathcal{GMM}$

As we have done so far, we will consider a suitable Boolean function to plug it into the code $\mathcal{C}_f$. The particular properties of f should provide the desired minimality and wideness conditions. The authors' idea in [20] is very simple—define $f \in \mathcal{GMM}$ via an injection ϕ of the complement of the set U of elements with weight at least two. In this case, the weight distribution of the resulting codes will be easy to derive by the form of the function f.

Theorem 3.4.1. *[20] Let $r \geqslant 7$ be an odd integer. Set $\kappa = (r+1)/2$ and $\lambda = (r-1)/2$. Let $U = \{x \in \mathbb{F}_2^\kappa : wt(x) \geqslant 2\}$ and f be the Boolean function defined in (3.6), where $\mu \equiv 1$ and ϕ is an injection from $\mathbb{F}_2^\kappa \setminus U$ to $(\mathbb{F}_2^\lambda)^*$ such that $\phi(x) = 0$ for any $x \in U$. The punctured code $\mathcal{C}_f^\times$ is a wide minimal $[2^r - 1, r+1, 2^{r-1} - 2^{\lambda-1}(\kappa - 1)]$-code.*

Note that the code in Theorem 3.4.1 is defined over $(\mathbb{F}_2^r)^*$ hence its length is $2^r - 1$.

We now present the following modification of 3.4.1. The proof of this result uses a similar reasoning to that in [20, Theorem 5.5]. However, the presented theorem gives codes with a better minimum distance in certain cases.

Theorem 3.4.2 (The $\mathcal{GMM}$ method I)**.** *Let $r \geqslant 7$ be an odd integer, $\kappa = (r+1)/2$ and $\lambda = (r-1)/2$. Let $U = \{x \in \mathbb{F}_2^\kappa : wt(x) \leqslant \kappa - 2\}$ and $f \in \mathcal{B}_r$ be the Boolean function defined in (3.6), where μ is the identically one function, ϕ is an injection from $\mathbb{F}_2^\kappa \setminus U$ to ${\mathbb{F}_2^\lambda}^*$ such that $\phi(x) = 0$ for any $x \in U$. The code $\mathcal{C}_f$ is a minimal binary code with length 2^r, dimension $r+1$ and the following hold:*

(i) For odd κ, the code $\mathcal{C}_f$ has minimum distance $2^{r-1} - 2^{\lambda-1}(\kappa - 1)$.

(ii) For even κ, the code $\mathcal{C}_f$ has minimum distance $2^{r-1} - 2^{\lambda-1}(\kappa - 3)$.

Moreover, if $r \geqslant 9$ and $r \neq 11$, then $\mathcal{C}_f$ is wide.

Proof. According to Equation 3.9, we have

$$\sum_{x \in U} (-1)^{\nu_1 \cdot x} = \begin{cases} |U|, & if\ \nu_1 = 0, \\ -(P_{\kappa-1}(i) + (-1)^{wt(\nu_1)}), & if\ wt(\nu_1) = i, \end{cases} \tag{3.10}$$

where $P_{\kappa-1}(i) = (-1)^i P_{\kappa-(\kappa-1)}(i) = (-1)^i P_1(i,\kappa) = (-1)^i(\kappa - 2i)$ due to (3.7) and (3.8). Working out the sums involved in $W_f(\nu_1, \nu_2)$,

$$\begin{aligned} W_f(\nu_1, \nu_2) &= \sum_{x \in \mathbb{F}_2^\kappa} \sum_{y \in \mathbb{F}_2^\lambda} (-1)^{\phi(x)\cdot y + 1 + \nu_1 \cdot x + \nu_2 \cdot y} \\ &= \sum_{x \in (\mathbb{F}_2^\kappa \setminus U)} \sum_{y \in \mathbb{F}_2^\lambda} (-1)^{\phi(x)\cdot y + 1 + \nu_1 \cdot x + \nu_2 \cdot y} + \sum_{x \in U} \sum_{y \in \mathbb{F}_2^\lambda} (-1)^{1 + \nu_1 \cdot x + \nu_2 \cdot y}. \end{aligned}$$

Using (3.10), this implies that the possible values of the Walsh coefficients are given by

$$W_f(\nu_1, \nu_2) = \begin{cases} -(2^\kappa - \kappa - 1)2^\lambda & if\ \nu_1 = 0, \nu_2 = 0; \\ (-1)^i(\kappa - 2i + 1)2^\lambda & if\ \nu_1 \neq 0, wt(\nu_1) = i, \nu_2 = 0; \\ -(-1)^{\nu_1 \cdot \phi^{-1}(\nu_2)} 2^\lambda & if\ \nu_2 \in Im(\phi) \setminus \{0\}; \\ 0 & if\ \nu_2 \notin Im(\phi), \end{cases} \tag{3.11}$$

where $i = 1, 2, \ldots, \kappa$. From (3.11), we get that

$$W_f(\nu_1, \nu_2) \pm W_f(\omega_1, \omega_2) \neq 2^r$$

for any pair of distinct $(\nu_1, \nu_2), (\omega_1, \omega_2) \in \mathbb{F}_2^\kappa \times \mathbb{F}_2^\lambda$. By Theorem 3.1.2, it follows that $\mathcal{C}_f$ is minimal. The weight distribution of $\mathcal{C}_f$ is fully specified by Tables 3.8-3.11.

For κ odd, set $wt(\nu_1) = \kappa, wt(\nu_2) = 0$. This yields

$$wt(\phi(x)\cdot y + 1 + \nu_1 \cdot x + \nu_2 \cdot y) = 2^{r-1} - \frac{1}{2} W_f(\nu_1, \nu_2) = 2^{r-1} - 2^{\lambda-1}(\kappa - 1), \tag{3.12}$$

which can be used together with Tables 3.8 and 3.9 to prove (i). The minimum distance $2^{r-1} - 2^{\lambda-1}(\kappa - 1)$ corresponds to the second row in Tables 3.8 and 3.9, namely, when the weight $2^{r-1} - 2^{\lambda-1}(\kappa + 1 - 2i)$ for $i = \kappa$.

For κ even, from Table 3.10 and Table 3.11, we know that if $wt(\nu_1) = 2, wt(\nu_2) = 0$, then

$$wt(\phi(x)\cdot y + 1 + \nu_1 \cdot x + \nu_2 \cdot y) = 2^{r-1} - \frac{1}{2} W_f(\nu_1, \nu_2) = 2^{r-1} - 2^{\lambda-1}(\kappa - 3), \tag{3.13}$$

so this weight is attained and it can be seen to be equal to $w_{\min}$, hence (ii) holds. Additionally, it can be easily verified (from Tables 3.8- 3.11) that

$$w_{\max} = wt(\phi(x) \cdot y + 1) = 2^{r-1} + 2^{\lambda-1}(2^\kappa - \kappa - 1). \tag{3.14}$$

Combining (3.12), (3.13) and (3.14), for $\kappa \geqslant 5$ and $\kappa \neq 6$, the ratio $\frac{w_{\min}}{w_{\max}}$ is at most $\frac{1}{2}$, in other words $\mathcal{C}_f$ is wide when $r \geqslant 9$ and $r \neq 11$. □

The weight distributions of the codes specified in Theorem 3.4.2 are given below for different values of κ modulo four.

Table 3.8: Weight distribution of $\mathcal{C}_f$ in Theorem 3.4.2 for $\kappa \equiv 1 \mod 4$.

Weight w	Number of codewords A_w
$2^{r-1} + 2^{\lambda-1}(2^{\kappa} - \kappa - 1)$	1
$2^{r-1} + 2^{\lambda-1}(\kappa + 1 - 2i)$ $for\ 1 \leqslant i \leqslant \kappa, i \neq (\kappa+1)/2\ and\ i\ odd$	$\binom{\kappa}{i}$
$2^{r-1} - 2^{\lambda-1}(\kappa + 1 - 2i)$ $for\ 1 \leqslant i \leqslant \kappa\ and\ i\ even$	$\binom{\kappa}{i}$
$2^{r-1} + 2^{\lambda-1}$	$(\kappa+1)2^{\kappa-1}$
$2^{r-1} - 2^{\lambda-1}$	$(\kappa+1)2^{\kappa-1}$
2^{r-1}	$2^r - 1 + 2^{\kappa}(2^{\lambda} - \kappa - 2) + \binom{\kappa}{(\kappa+1)/2}$
0	1

Table 3.9: Weight distribution of $\mathcal{C}_f$ in Theorem 3.4.2 for $\kappa \equiv 3 \mod 4$.

Weight w	Number of codewords A_w
$2^{r-1} + 2^{\lambda-1}(2^{\kappa} - \kappa - 1)$	1
$2^{r-1} + 2^{\lambda-1}(\kappa + 1 - 2i)$ $for\ 1 \leqslant i \leqslant \kappa\ and\ i\ odd$	$\binom{\kappa}{i}$
$2^{r-1} - 2^{\lambda-1}(\kappa + 1 - 2i)$ $for\ 1 \leqslant i \leqslant \kappa, i \neq (\kappa+1)/2\ and\ i\ even$	$\binom{\kappa}{i}$
$2^{r-1} + 2^{\lambda-1}$	$(\kappa+1)2^{\kappa-1}$
$2^{r-1} - 2^{\lambda-1}$	$(\kappa+1)2^{\kappa-1}$
2^{r-1}	$2^r - 1 + 2^{\kappa}(2^{\lambda} - \kappa - 2) + \binom{\kappa}{(\kappa+1)/2}$
0	1

Table 3.10: Weight distribution of $\mathcal{C}_f$ in Theorem 3.4.2 for $\kappa \equiv 0 \mod 4$.

Weight w	Number of codewords A_w
$2^{r-1}+2^{\lambda-1}(2^{\kappa}-\kappa-1)$	1
$2^{r-1}+2^{\lambda-1}(\kappa+1-2i)$ $for\ 1 \leqslant i \leqslant (\kappa-2)/2\ and\ i\ odd$	$\binom{\kappa}{i}+\binom{\kappa}{\kappa+1-i}$
$2^{r-1}-2^{\lambda-1}(\kappa+1-2i)$ $for\ 1 \leqslant i \leqslant (\kappa-2)/2\ and\ i\ even$	$\binom{\kappa}{i}+\binom{\kappa}{\kappa+1-i}$
$2^{r-1}+2^{\lambda-1}$	$(\kappa+1)2^{\kappa-1}$
$2^{r-1}-2^{\lambda-1}$	$(\kappa+1)2^{\kappa-1}+\binom{\kappa}{\kappa/2}+\binom{\kappa}{(\kappa+2)/2}$
2^{r-1}	$2^r-1+2^{\kappa}(2^{\lambda}-\kappa-2)$
0	1

Table 3.11: Weight distribution of $\mathcal{C}_f$ in Theorem 3.4.2 for $\kappa \equiv 2 \mod 4$.

Weight w	Number of codewords A_w
$2^{r-1}+2^{\lambda-1}(2^{\kappa}-\kappa-1)$	1
$2^{r-1}+2^{\lambda-1}(\kappa+1-2i)$ $for\ 1 \leqslant i \leqslant (\kappa-2)/2\ and\ i\ odd$	$\binom{\kappa}{i}+\binom{\kappa}{\kappa+1-i}$
$2^{r-1}-2^{\lambda-1}(\kappa+1-2i)$ $for\ 1 \leqslant i \leqslant (\kappa-2)/2\ and\ i\ even$	$\binom{\kappa}{i}+\binom{\kappa}{\kappa+1-i}$
$2^{r-1}+2^{\lambda-1}$	$(\kappa+1)2^{\kappa-1}+\binom{\kappa}{\kappa/2}+\binom{\kappa}{(\kappa+2)/2}$
$2^{r-1}-2^{\lambda-1}$	$(\kappa+1)2^{\kappa-1}$
2^{r-1}	$2^r-1+2^{\kappa}(2^{\lambda}-\kappa-2)$
0	1

The specification of weight distributions given in the above tables is obtained in a quite easy way using the Walsh spectrum of f given by (3.11). Nevertheless, for convenience of the reader, we briefly discuss how the weight distribution in Table 3.10 is obtained, the remaining cases being similar. The first and last entry in Table 3.10 are straightforward, the former weight corresponds to the value $W_f(0,0) = -(2^{\kappa}-\kappa-1)2^{\lambda}$, which gives the weight $2^{r-1}-\frac{1}{2}W_f(0,0) = 2^{r-1}+2^{\lambda-1}(2^{\kappa}-\kappa-1)$. To count the number of balanced codewords of weight 2^{r-1} (second to last row) we first notice that there are 2^r-1 non-zero linear functions. We also need to add those codewords that correspond to the spectral values $W_f(\nu_1,\nu_2)=0$. Their number is

$$|\{(\nu_1,\nu_2) \in \mathbb{F}_2^{\kappa} \times \mathbb{F}_2^{\lambda} : \nu_2 \notin Im(\phi)\}|$$

which is exactly $2^\kappa(2^\lambda - \kappa - 2)$. Thus, there are $2^r - 1 + 2^\kappa(2^\lambda - \kappa - 2)$ balanced codewords. The fourth row corresponds to the value $W_f(\nu_1, \nu_2) = -2^\lambda$. Their number is

$$|\{(\nu_1, \nu_2) \in \mathbb{F}_2^\kappa \times \mathbb{F}_2^\lambda : \nu_2 \in Im(\phi) \setminus \{0\}, \nu_1 \cdot \phi^{-1}(\nu_2) = 1\}|$$

which equals $(\kappa+1)2^{\kappa-1}$. The fifth row corresponds to the value $W_f(\nu_1, \nu_2) = 2^\lambda$. The frequency of this value equals to the sum of

$$|\{(\nu_1, \nu_2) \in \mathbb{F}_2^\kappa \times \mathbb{F}_2^\lambda : \nu_2 \in Im(\phi) \setminus \{0\}, \nu_1 \cdot \phi^{-1}(\nu_2) = 0\}|$$

and

$$|\{(\nu_1, \nu_2) \in \mathbb{F}_2^\kappa \times \mathbb{F}_2^\lambda : wt(\nu_1) \in \{\kappa/2, (\kappa+2)/2\}, \nu_2 = 0\}|,$$

in total $(\kappa + 1)2^{\kappa-1} + \binom{\kappa}{\kappa/2} + \binom{\kappa}{(\kappa+2)/2}$. Finally, the second and third row correspond to the Walsh values $(-1)^i(\kappa - 2i + 1)2^\lambda$. Since $1 \leqslant i \leqslant \kappa$, there are only $\kappa/2 - 1$ different non-zero values (the indices i and $\kappa + 1 - i$ give the same value), for each index i such that $1 \leqslant i \leqslant \kappa/2 - 1$ we have

$$|\{(\nu_1, \nu_2) \in \mathbb{F}_2^\kappa \times \mathbb{F}_2^\lambda : wt(\nu_1) \in \{i, \kappa + 1 - i\}, \nu_2 = 0\}|$$

codewords, i.e. $\binom{\kappa}{i} + \binom{\kappa}{\kappa+1-i}$.

Compared to the result in Theorem 3.4.1, the method in Theorem 3.4.2 achieves a larger minimum distance and fewer weights when the parameter κ is even. For instance, taking $r = 15$ gives that $\kappa = 8$ and our punctured code has parameters

$$[2^r - 1, r + 1, 2^{r-1} - 2^{\lambda-1}(\kappa - 3) - 1],$$

thus having minimum distance $2^{14} - 2^6 \cdot 5 - 1$. On the other hand, the code in Theorem 3.4.1 has minimum weight $2^{14} - 2^6 \cdot 7$ and the difference between the two is 127 (in general, the difference is $2^\lambda - 1$). In addition, when $r \equiv 3 \mod 4$, from Table 3.10 and 3.11, the punctured code $\mathcal{C}_f$ in Theorem 3.4.2 has $\frac{r+1}{4} + 4 = \frac{\kappa}{2} + 4$ non-zero different weights, whereas the code in Theorem 3.4.1 has $\frac{r+1}{2} + 2 = \kappa + 2$ non-zero different weights. We illustrate this discussion in the following example.

Example 3.4.3. *Let $r = 15$. This gives $\kappa = 8$ and $\lambda = 7$, so that $\kappa \equiv 0 \mod 4$. The minimum distance of $\mathcal{C}_f$ in this case, confirmed by computer-based simulations, equals $2^{14} - 2^6 \cdot 5$ which is in agreement with (3.13). Also, the maximum weight of the codewords equals 32192 which corresponds to $2^{r-1} + 2^{\lambda-1}(2^\kappa - \kappa - 1)$. Its enumerator polynomial is given by*

$$1 + 36z^{16064} + 1278z^{16320} + 62975z^{16384} + 1152^{16448} + 84z^{16576} + 9z^{16832} + z^{32192},$$

which is consistent with Table 3.10. *Note that when considering the punctured code over* $(\mathbb{F}_2^r)^*$ *the weight distribution changes slightly, namely, the weight enumerator in this case is given by*

$$1+36z^{16063}+1278z^{16319}+30208z^{16383}+32767z^{16384}+1152^{16447}+84z^{16575}+9z^{16831}+z^{32191}.$$

In contrast, the weight enumerator of the code in Theorem 3.4.1 for $r=15$ *is*

$$1+8z^{15936}+28z^{16064}+56z^{16192}+1350z^{16320}+62975z^{16384}+1080z^{16448}+28z^{16576}+8z^{16704}+z^{16382}+z^{32192}.$$

3.4.2 The second family of wide minimal codes from $\mathcal{GMM}$

Recently, a modification of Theorem 3.4.1 was presented in [40]. In this construction, the same hypotheses for the set U and $f\in\mathcal{B}_r$ are assumed, the only difference lies at the final step—the linear code $\mathcal{C}_{f+1}$ is considered instead.

Theorem 3.4.4. *[40] Let* $r\geqslant 7$ *be an odd integer,* $\kappa=(r+1)/2$ *and* $\lambda=(r-1)/2$. *Let* $U=\{x\in\mathbb{F}_2^\kappa : wt(x)\geqslant 2\}$ *and* f *be the Boolean function defined in (3.6), where* $\mu\equiv 1$ *and* ϕ *is an injection from* $\mathbb{F}_2^\kappa\setminus U$ *to* $(\mathbb{F}_2^\lambda)^*$ *such that* $\phi(x)=0$ *for any* $x\in U$. *The punctured code* $\mathcal{C}_{f+1}^\times$ *given by (2.12) considered over* $(\mathbb{F}_2^r)^*$ *is a wide minimal* $[2^r-1,r+1,2^{r-1}-2^{\lambda-1}(2^\kappa-\kappa-1)-1]$*-code.*

A similar approach as in Theorem 3.4.2 to modify the previous result provides codes with larger minimum distance.

Theorem 3.4.5 (The $\mathcal{GMM}$ method II)**.** *Let* $r\geqslant 7$ *be an odd integer,* $\kappa=(r+1)/2$ *and* $\lambda=(r-1)/2$. *Let* $U=\{x\in\mathbb{F}_2^\kappa : wt(x)\leqslant\kappa-2\}$ *and* $f\in\mathcal{B}_r$ *be the Boolean function defined in (3.6), where* $\mu\equiv 1$ *and* ϕ *is an injection from* $\mathbb{F}_2^\kappa\setminus U$ *to* $(\mathbb{F}_2^\lambda)^*$ *such that* $\phi(x)=0$ *for any* $x\in U$. *The code* $\mathcal{C}_{f+1}$ *is a wide minimal binary code with parameters* $[2^r,r+1,2^{r-1}-2^{\lambda-1}(2^\kappa-\kappa-3)]$.

Proof. The proof is quite similar to the proof of Theorem 3.4.2. In this case,

$$W_{f+1}(\nu_1,\nu_2)=\left\{\begin{array}{ll}(2^\kappa-\kappa-3)2^\lambda & if\ \nu_1=0,\nu_2=0;\\ ((-1)^{i+1}(\kappa-2i+1)-2)2^\lambda & if\ wt(\nu_1)=i,\nu_2=0;\\ (-1)^{\nu_1\cdot\phi^{-1}(\nu_2)}2^\lambda & if\ \nu_2\in Im(\phi)\setminus\{0\};\\ 0 & if\ \nu_2\notin Im(\phi),\end{array}\right. \tag{3.15}$$

where $i=1,2,\ldots,\kappa$. Again, from (3.15), we know that

$$W_f(\nu_1,\nu_2)\pm W_f(\omega_1,\omega_2)\neq 2^r,$$

for any pair of distinct $(\nu_1, \nu_2), (\omega_1, \omega_2) \in \mathbb{F}_2^{\kappa} \times \mathbb{F}_2^{\lambda}$. By Theorem 3.1.2, it follows that $\mathcal{C}_f$ is minimal. Observe that the minimum weight corresponds to

$$2^{r-1} - \frac{1}{2} W_{f+1}(0,0) = 2^{r-1} - 2^{\lambda-1}(2^{\kappa} - \kappa - 3).$$

To show wideness, compute the maximum weight according to the parity of κ. If κ is odd then the maximum weight corresponds to

$$2^{r-1} - \frac{1}{2} W_{f+1}(1_{\kappa}, 0) = 2^{r-1} + 2^{\lambda-1}(\kappa + 1),$$

where 1_{κ} denotes the all-one vector in $\mathbb{F}_2^{\kappa}$. This yields

$$\frac{w_{\min}}{w_{\max}} = \frac{2^{r-1} - 2^{\lambda-1}(2^{\kappa} - \kappa - 3)}{2^{r-1} + 2^{\lambda-1}(\kappa + 1)} \leqslant \frac{1}{2}.$$

If κ is even then the maximum weight is attained when $wt(\nu_1) = \kappa - 1$ or $wt(\nu_1) = 2$ and it corresponds to

$$2^{r-1} - \frac{1}{2} W_{f+1}(\nu_1, 0) = 2^{r-1} + 2^{\lambda-1}(\kappa - 1).$$

This implies

$$\frac{w_{\min}}{w_{\max}} = \frac{2^{r-1} - 2^{\lambda-1}(2^{\kappa} - \kappa - 3)}{2^{r-1} + 2^{\lambda-1}(\kappa - 1)} \leqslant \frac{1}{2}.$$

□

The weight distributions of the resulting codes in Theorem 3.4.5 are given in Tables 3.12-3.15 below, where the possible values of κ modulo four are considered.

Table 3.12: Weight distribution of $\mathcal{C}_f$ in Theorem 3.4.5 for $\kappa \equiv 0 \mod 4$

Weight w	Number of codewords A_w
$2^{r-1} - 2^{\lambda-1}(2^{\kappa} - \kappa - 3)$	1
$2^{r-1} + 2^{\lambda-1}((-1)^i(\kappa + 1 - 2i) + 2)$ $for\ 1 \leqslant i \leqslant \kappa, i \notin \{(\kappa-2)/2, (\kappa+4)/2\}$	$\binom{\kappa}{i} + \binom{\kappa}{\kappa-i+1}$
$2^{r-1} + 2^{\lambda-1}$	$(\kappa+1)2^{\kappa-1}$
$2^{r-1} - 2^{\lambda-1}$	$(\kappa+1)2^{\kappa-1} + \binom{\kappa}{(\kappa-2)/2} + \binom{\kappa}{(\kappa+4)/2}$
2^{r-1}	$2^r - 1 + 2^{\kappa}(2^{\lambda} - \kappa - 2)$
0	1

Table 3.13: Weight distribution of $\mathcal{C}_f$ in Theorem 3.4.5 for $\kappa \equiv 1 \mod 4$

Weight w	Number of codewords A_w
$2^{r-1} - 2^{\lambda-1}(2^\kappa - \kappa - 3)$	1
$2^{r-1} + 2^{\lambda-1}((-1)^i(\kappa + 1 - 2i) + 2)$ $for\ 1 \leqslant i \leq \kappa, i \neq (k+3)/2$	$\binom{\kappa}{i}$
$2^{r-1} + 2^{\lambda-1}$	$(\kappa+1)2^{\kappa-1}$
$2^{r-1} - 2^{\lambda-1}$	$(\kappa+1)2^{\kappa-1}$
2^{r-1}	$2^r - 1 + 2^\kappa(2^\lambda - \kappa - 2) + \binom{\kappa}{(k+3)/2}$
0	1

Table 3.14: Weight distribution of $\mathcal{C}_f$ in Theorem 3.4.5 for $\kappa \equiv 2 \mod 4$

Weight w	Number of codewords A_w
$2^{r-1} - 2^{\lambda-1}(2^\kappa - \kappa - 3)$	1
$2^{r-1} + 2^{\lambda-1}((-1)^i(\kappa + 1 - 2i) + 2)$ $for\ 1 \leqslant i \leq \kappa, i \notin \{\kappa/2, (\kappa+2)/2\}$	$\binom{\kappa}{i} + \binom{\kappa}{k-i+1}$
$2^{r-1} + 2^{\lambda-1}$	$(\kappa+1)2^{\kappa-1} + \binom{\kappa}{k/2} + \binom{\kappa}{(k+2)/2}$
$2^{r-1} - 2^{\lambda-1}$	$(\kappa+1)2^{\kappa-1}$
2^{r-1}	$2^r - 1 + 2^\kappa(2^\lambda - \kappa - 2)$
0	1

Table 3.15: Weight distribution of $\mathcal{C}_f$ in Theorem 3.4.5 for $\kappa \equiv 3 \mod 4$

Weight w	Number of codewords A_w
$2^{r-1} - 2^{\lambda-1}(2^\kappa - \kappa - 3)$	1
$2^{r-1} + 2^{\lambda-1}((-1)^i(\kappa + 1 - 2i) + 2)$ $for\ 1 \leqslant i \leq \kappa, i \neq (\kappa-1)/2$	$\binom{\kappa}{i}$
$2^{r-1} + 2^{\lambda-1}$	$(\kappa+1)2^{\kappa-1}$
$2^{r-1} - 2^{\lambda-1}$	$(\kappa+1)2^{\kappa-1}$
2^{r-1}	$2^r - 1 + 2^\kappa(2^\lambda - \kappa - 2) + \binom{\kappa}{(k-1)/2}$
0	1

Compared to the result in Theorem 3.4.4, the method shown in Theorem 3.4.5 achieves codes with larger minimum distance and fewer weights regardless of the parity of κ.

Example 3.4.6. *Let $r = 7$. This gives $\kappa = 4$ and $\lambda = 3$, so that $\kappa \equiv 0 \mod 4$. The code constructed in Theorem 3.4.5 is a wide minimal $[128, 8, 28]$-code whose* *enumerator polynomial is*

$$1 + z^{28} + 45z^{60} + 159z^{64} + 40z^{68} + 10z^{76}.$$

This is consistent with Table 3.12. The same code considered over $(\mathbb{F}_2^7)^*$ *has parameters* $[127, 8, 27]$*. On the other hand, the code in Theorem 3.4.4 has parameters* $[127, 8, 19]$*. Then the difference between minimum weights is* 8 *(in general, the difference equals* 2^λ*). The enumerator polynomial of the punctured code in Theorem 3.4.5 is*

$$1 + z^{27} + 45z^{59} + 32z^{63} + 127z^{64} + 40z^{67} + 10z^{75},$$

whereas the enumerator polynomial of the code in Theorem 3.4.4 is

$$1 + z^{19} + z^{51} + 36z^{59} + 32z^{63} + 127z^{64} + 54z^{67} + 4z^{75}.$$

Remark 3.4.7 (The wide bound)**.** *In general, a minimal code with parameters* $[n, k, d]$ *and maximum distance* $w_{\max}$ *satisfies* $w_{\max} \leqslant n - k + 1$ *(the Singleton bound for the maximum weight). Since a wide binary code satisfies* $2w_{\min} \leqslant w_{\max}$*, a wide minimal binary code must satisfy*

$$w_{\min} \leqslant \lfloor \frac{1}{2}(n - k + 1) \rfloor.$$

To the best of our knowledge, the best constructions in this regard (parameters $n = 2^m$*,* $k = m + 1$*) are given in Theorem 3.3.1. Theorem 3.4.2 and Theorem 3.4.5 provide codes with good parameters since their minimum distances are either* $2^{r-1} - 2^{\lambda-1}(\kappa - 1)$ *or* $2^{r-1} - 2^{\lambda-1}(\kappa - 3)$*, which are pretty close to* $\lfloor \frac{1}{2}(2^r - r) \rfloor$*.*

3.4.3 The third family of wide minimal codes from $\mathcal{GMM}$

The previous two sections illustrate the flexibility in the choice of a set U and the corresponding Boolean function in the generalized Maiorana-McFarcland class to define wide minimal linear codes. A refinement of these techniques is presented in this section. The method employs the derivative of a specific Boolean function instead.

In Theorem 3.4.2, the set U of vectors whose weight is at most $\kappa - 2$, i.e.

$$U = \{x \in \mathbb{F}_2^\kappa : wt(x) \leqslant \kappa - 2\},$$

is used as building block of f, whereas the set $U = \{x \in \mathbb{F}_2^\kappa : wt(x) \geqslant 2\}$ is used in Theorem 3.4.1. In what follows, we show that the same characteristic set as used in Theorem 3.4.1 can actually give rise to wide minimal codes for a suitable derivative of f, say $D_\gamma f$.

Theorem 3.4.8 (The $\mathcal{GMM}$ method III)**.** *Let $r \geqslant 9$ be an odd integer, $\kappa = (r+1)/2$ and $\lambda = (r-1)/2$. Let $U = \{x \in \mathbb{F}_2^\kappa : wt(x) \geqslant 2\}$ and f be the Boolean function defined in (3.6), where μ is the identically one function and ϕ is an injection from $\mathbb{F}_2^\kappa \setminus U$ to $(\mathbb{F}_2^\lambda)^*$ such that $\phi(x) = 0$ for any $x \in U$. Let $\gamma = (1_\kappa, 0) \in \mathbb{F}_2^\kappa \times \mathbb{F}_2^\lambda$, where 1_κ denotes the all-one vector in $\mathbb{F}_2^\kappa$. The code $\mathcal{C}_{D_\gamma f}$ given by (2.12) is a wide minimal code with parameters $[2^r, r+1, 2^\lambda(\kappa+1)]$.*

Proof. Set $U' = U + 1_\kappa$. From the proof of Theorem 3.4.1 in [20, Theorem 5.5], we know that

$$\sum_{x \in U} (-1)^{\nu_1 \cdot x} = \begin{cases} |U|, & if\ \nu_1 = 0, \\ P_1(i) + 1, & if\ wt(\nu_1) = i, \end{cases} \tag{3.16}$$

where $P_1(i) = \kappa - 2i$.

Working out the sums in the Walsh value $W_{D_\gamma f}(\nu_1, \nu_2)$ for $(\nu_1, \nu_2) \in \mathbb{F}_2^\kappa \times \mathbb{F}_2^\lambda$ by using (3.10) and (3.16), we get

$$\begin{aligned} W_{D_\gamma f}(\nu_1, \nu_2) &= \sum_{x \in \mathbb{F}_2^\kappa} \sum_{y \in \mathbb{F}_2^\lambda} (-1)^{\phi(x)\cdot y + \phi(x+1_\kappa)\cdot y + \nu_1 \cdot x + \nu_2 \cdot y} \\ &= \sum_{x \in (\mathbb{F}_2^\kappa \setminus U)} \sum_{y \in \mathbb{F}_2^\lambda} (-1)^{\phi(x)\cdot y + \nu_1 \cdot x + \nu_2 \cdot y} + \sum_{x \in (\mathbb{F}_2^\kappa \setminus U')} \sum_{y \in \mathbb{F}_2^\lambda} (-1)^{\phi(x+1_\kappa)\cdot y + \nu_1 \cdot x + \nu_2 \cdot y} \\ &+ \sum_{x \in (U \cap U')} \sum_{y \in \mathbb{F}_2^\lambda} (-1)^{\nu_1 \cdot x + \nu_2 \cdot y}. \end{aligned}$$

Therefore the Walsh coefficients satisfy

$$W_{D_\gamma f}(\nu_1, \nu_2) = \begin{cases} (2^\kappa - 2\kappa - 2)2^\lambda & if\ \nu_1 = 0, \nu_2 = 0; \\ -\left(\kappa - 2i + 1 + (-1)^i(\kappa - 2i + 1)\right)2^\lambda & if\ wt(\nu_1) = i, \nu_2 = 0; \\ (1 + (-1)^{\nu_1 \cdot 1_\kappa})(-1)^{\nu_1 \cdot \phi^{-1}(\nu_2)} 2^\lambda & if\ \nu_2 \in Im(\phi) \setminus \{0\}; \\ 0 & if\ \nu_2 \notin Im(\phi), \end{cases} \tag{3.17}$$

where $i = 1, 2, \ldots, \kappa$. From (3.17), observe that

$$W_{D_\gamma f}(\nu_1, \nu_2) \pm W_{D_\gamma f}(\omega_1, \omega_2) \neq 2^r$$

for any pair of distinct $(\nu_1, \nu_2), (\omega_1, \omega_2) \in \mathbb{F}_2^\kappa \times \mathbb{F}_2^\lambda$, hence $\mathcal{C}_{D_\gamma f}$ is minimal.

Using (3.17), the parameters and weight distribution of $\mathcal{C}_{D_\gamma f}$ can be inferred, see Tables 3.16 - 3.19. In this case, a codeword of minimal non-zero weight is attained when $wt(\nu_1) = 0, wt(\nu_2) = 0$ (corresponding to the first row in Tables 3.16 - 3.19) so that the minimum distance $w_{\min}$ is equal to

$$wt(\phi(x) \cdot y + \phi(x + 1_\kappa) \cdot y) = 2^{r-1} - \frac{1}{2} W_{D_\gamma f}(0, 0) = 2^\lambda(\kappa + 1), \tag{3.18}$$

where the last equality comes from the fact that $W_{D_\gamma f}(0,0) = 2^r - 2^\lambda(2\kappa+2)$. Similarly, a codeword of maximal weight is attained when $wt(\nu_1) = 2, wt(\nu_2) = 0$ (corresponding to the second row in Tables 3.16 - 3.19), so that

$$w_{\max} = 2^{r-1} + 2^\lambda(\kappa - 3). \tag{3.19}$$

Combining (3.18) and (3.19), we obtain $\frac{w_{\min}}{w_{\max}} \leqslant \frac{1}{2}$ for $\kappa \geqslant 5$. □

The weight distributions of the linear codes $\mathcal{C}_{D_\gamma f}$ is given below in Tables 3.16 - 3.19) for different values of κ modulo four.

Table 3.16: Weight distribution of $\mathcal{C}_{D_\gamma f}$ in Theorem 3.4.8 for $\kappa \equiv 1 \mod 4$

Weight w	Number of codewords A_w
$2^\lambda(\kappa+1)$	1
$2^{r-1} + 2^\lambda(\kappa+1-2i)$ *for* $1 \leqslant i \leqslant \kappa,$ *and* i *even*	$\binom{\kappa}{i}$
$2^{r-1} + 2^\lambda$	$\kappa 2^{\kappa-2}$
$2^{r-1} - 2^\lambda$	$2^{\kappa-1} + \kappa 2^{\kappa-2}$
2^{r-1}	$2^r - 1 + 2^\kappa(2^\lambda - \kappa - 2) + (k+1)2^{\kappa-1} + \sum\limits_{i=1}^{(\kappa+1)/2} \binom{\kappa}{2i-1}$
0	1

Table 3.17: Weight distribution of $\mathcal{C}_{D_\gamma f}$ in Theorem 3.4.8 for $\kappa \equiv 3 \mod 4$

Weight w	Number of codewords A_w
$2^\lambda(\kappa+1)$	1
$2^{r-1} + 2^\lambda(\kappa+1-2i)$ *for* $1 \leqslant i \leqslant \kappa, i \neq (\kappa+1)/2$ *and* i *even*	$\binom{\kappa}{i}$
$2^{r-1} + 2^\lambda$	$\kappa 2^{\kappa-2}$
$2^{r-1} - 2^\lambda$	$2^{\kappa-1} + \kappa 2^{\kappa-2}$
2^{r-1}	$2^r - 1 + 2^\kappa(2^\lambda - \kappa - 2) + (k+1)2^{\kappa-1}$ $+ \sum\limits_{i=1}^{(\kappa+1)/2} \binom{\kappa}{2i-1} + \binom{\kappa}{(\kappa+1)/2}$
0	1

Table 3.18: Weight distribution of $\mathcal{C}_{D_\gamma f}$ in Theorem 3.4.8 for $\kappa \equiv 0 \mod 4$

Weight w	Number of codewords A_w
$2^\lambda(\kappa+1)$	1
$2^{r-1}+2^\lambda(\kappa+1-2i)$ $for\ 1 \leqslant i \leqslant \kappa,\ and\ i\ even, i \neq \kappa/2$	$\binom{\kappa}{i}$
$2^{r-1}+2^\lambda$	$\kappa 2^{\kappa-2}+\binom{\kappa}{\kappa/2}$
$2^{r-1}-2^\lambda$	$2^{\kappa-1}+\kappa 2^{\kappa-2}$
2^{r-1}	$2^r-1+2^\kappa(2^\lambda-\kappa-2)+(k+1)2^{\kappa-1}+\sum_{i=1}^{\kappa/2}\binom{\kappa}{2i-1}$
0	1

Table 3.19: Weight distribution of $\mathcal{C}_{D_\gamma f}$ in Theorem 3.4.8 for $\kappa \equiv 2 \mod 4$

Weight w	Number of codewords A_w
$2^\lambda(\kappa+1)$	1
$2^{r-1}+2^\lambda(\kappa+1-2i)$ $for\ 1 \leqslant i \leqslant \kappa,\ i \neq (\kappa+2)/2,\ and\ i\ even$	$\binom{\kappa}{i}$
$2^{r-1}+2^\lambda$	$\kappa 2^{\kappa-2}$
$2^{r-1}-2^\lambda$	$2^{\kappa-1}+\kappa 2^{\kappa-2}+\binom{\kappa}{(\kappa+2)/2}$
2^{r-1}	$2^r-1+2^\kappa(2^\lambda-\kappa-2)+(k+1)2^{\kappa-1}+\sum_{i=1}^{\kappa/2}\binom{\kappa}{2i-1}$
0	1

The weight distribution tables above, referring to Theorem 3.4.8, have been confirmed both through computer-based simulations and theoretically. A similar reasoning used to specify the weight distribution in Table 3.2 can be applied here.

The codes specified by Theorem 3.4.8 have a smaller minimal distance than those defined in Theorem 3.4.2. Nevertheless, we will show later that the codewords of both codes can be simultaneously used resulting in codes with larger dimension.

Chapter 4

Minimal codes with larger dimensions

A minimal code is well-suited for the current practical two-party computation protocols when their information rate is high. Similar to the case of (extended) simplex codes $\mathcal{S}_m$, the presented codes derived from Boolean functions $\mathcal{C}_f$ have a rather bad information rate, namely, $\frac{m+1}{2^m}$. This motivates the quest of secondary constructions or, in general, any method, that allow us to increase the dimension of resulting codes. Since our main goal in this thesis is the study of wide minimal codes, the proposed methods in this chapter will be tailored to increase the dimension of the codes $\mathcal{C}_f$ while preserving both properties.

In this chapter, we present essentially three constructions of minimal codes. As a first step, a secondary construction of minimal codes based on bent-concatenation is introduced. Then, some derivatives of a bent function g are adjoined to the associated code $\mathcal{C}_g$ to produce wide minimal codes with larger dimensions. Finally, these two methods will be put together into a more general framework to produce codes with better dimensions, which are both wide and minimal. Most of the results presented in this chapter are based on the results proved in [65].

To ease notation, the set of n-variable linear functions will be denoted by $\mathcal{L}_n$. The elements of $\mathcal{L}_n$ are then functions of the form $l_v : \mathbb{F}_p^n \to \mathbb{F}_p$ defined by $l_v(x) = v \cdot x$ for $v \in \mathbb{F}_p^n$. Again, we will take no notice of whether these functions are defined in $\mathbb{F}_p^n$ or in $\mathbb{F}_{p^n}$.

Since at least two functions will be involved in the constructions of this chapter, it will be useful to emphasize the function itself in the notation $\mathcal{W}_{\max}, \mathcal{W}_{\min}$ so that for any p-ary function f, we will denote by $\mathcal{W}_{\max}^{(f)}$ (resp. $\mathcal{W}_{\min}^{(f)}$) the maximal (resp. minimal) value in the Walsh spectrum of f.

4.1 Direct sum method

As pointed out in the introduction, it is well-known [15] that the Kronecker product of two minimal codes is a minimal code. However, little is known about some other secondary constructions of minimal linear codes. This lack of methods prompts us to provide a more suitable framework to study the construction of minimal codes from other minimal codes or, at least, to obtain minimal codes with a larger dimension from other mathematical objects under weak assumptions.

The approach presented in this section will be based on the so-called *direct sum* or *bent concatenation* of Boolean functions: let r, s and n be three positive integers such that $r + s = n$[1]. Let $f : \mathbb{F}_p^r \to \mathbb{F}_p$ and $g : \mathbb{F}_p^s \to \mathbb{F}_p$ be two p-ary functions. The *direct sum* of f and g is the n-variable p-ary function h defined by

$$h(x, y) = f(x) + g(y) \text{ for } (x, y) \in \mathbb{F}_p^r \times \mathbb{F}_p^s. \tag{4.1}$$

In this context, the following well-known result in the binary setting will be proved useful in the sequel. The proof of this theorem is omitted, the interested reader can track down a proof in [49].

Lemma 4.1.1. *[9, 49] Let r, s and n be three positive integers such that $r + s = n$. Let $f \in \mathcal{B}_r$ and $g \in \mathcal{B}_s$. Consider the direct sum h of f and g, i.e. $h(x, y) = f(x) + g(y)$. The following hold:*

(i) The Walsh spectrum of h is completely determined by the Walsh spectra of f and g, more precisely,

$$W_h(\alpha, \beta) = W_f(\alpha)W_g(\beta) \tag{4.2}$$

for each $(\alpha, \beta) \in \mathbb{F}_2^r \times \mathbb{F}_2^s$.

(ii) Let $(u, v) \in \mathbb{F}_2^n$ be a pair of vectors such that $u = (u_1, \ldots, u_r)$ and $v = (v_1, \ldots, v_s)$. The weight of $h + l_{(u,v)}$ satisfies

$$wt\left(h + l_{(u,v)}\right) = 2^r wt\left(g + l_v\right) + 2^s wt\left(f + l_u\right) - 2wt\left(f + l_u\right) wt\left(g + l_v\right). \tag{4.3}$$

[1] Throughout this chapter, typically, the variable m will denote the length of a linear code, whereas n will be used to denote the input space of Boolean functions and the space $\mathbb{F}_p^n$ will be identified with $\mathbb{F}_p^r \times \mathbb{F}_p^s$ without further mentioning.

Another concept will be presented before embarking in the main result of this section. For any subset $S \subset \{1, \ldots, m\}$, define the *S-puncturing* of an $[m, k, d]$-code $C \subseteq \mathbb{F}_q^m$ as the function $p_S : C \to \mathbb{F}_q^m$ given by

$$p_S(c)_i = \begin{cases} c_i & \text{if } i \notin S; \\ 0 & \text{otherwise,} \end{cases}$$

where subindexes i indicate the coordinates of the corresponding vector.

The following lemma, whose proof is omitted, is a slight rephrasing of the definition of minimality and it emphasizes that minimality is a local property that depends on each coordinate.

Proposition 4.1.2. *Let C be a p-ary linear code with parameters $[m, k, d]$. The code C is minimal if and only if for every two linearly independent codewords $c, c' \in C$, there exists $S \subset \{1, \ldots, m\}$ such that*

$$p_S(c) \npreceq p_S(c'),$$

where p_S denotes the S-puncturing of C.

We are now ready to state and prove the main result of this section. The idea is simple—consider the associated code of the direct sum of two p-ary functions f, g in such a way that the associated code of g is minimal.

Theorem 4.1.3 (The direct sum method)**.** *Let n, r, s be three integers such that $r + s = n$. Let $f : \mathbb{F}_p^r \to \mathbb{F}_p$ be any function with $f(0) = 0$ and $g : \mathbb{F}_p^s \to \mathbb{F}_p$ be a non-affine function such that $\mathcal{C}_g$ is minimal. Consider their direct sum h. If, for each $v \in \mathbb{F}_p^s$ and $a \in \mathbb{F}_p$, there exists a non-zero $y \in \mathbb{F}_p^s$ such that $g(y) + l_v(y) = a$, then the code $\mathcal{C}_h$, defined by (2.12), is a minimal p-ary linear code. Moreover, for $p = 2$, if we define*

$$\delta := \max\{\mathcal{W}_{\max}^{(f)} \mathcal{W}_{\max}^{(g)}, \mathcal{W}_{\min}^{(f)} \mathcal{W}_{\min}^{(g)}\},$$

then the parameters of $\mathcal{C}_h$ are $[2^n, n+1, 2^{n-1} - \frac{1}{2}\delta]$.

Proof. First we will prove that if two codewords c_1, c_2 in $\mathcal{C}_h$ are linearly independent and $c_1 \preceq c_2$, then the induced codewords in $\mathcal{C}_g$ are linearly independent unless either is zero. Let

$$c = (ag(y) + l_v(y))_{y \in \mathbb{F}_p^s}, c' = (a'g(y) + l_{v'}(y))_{y \in \mathbb{F}_p^s} \in \mathcal{C}_g$$

be two linearly dependent non-zero codewords, i.e. $c' = \lambda c$ for some $\lambda \in \mathbb{F}_p^*$, $c \neq 0$. This easily implies $v' = \lambda v$ and $a' = \lambda a$ since g is non-affine. Consider two codewords in $\mathcal{C}_h$ of the form

$$c_1 = af(x) + ag(y) + l_w(x) + l_v(y) \text{ and } c_2 = \lambda af(x) + \lambda ag(y) + l_{w'}(x) + l_{\lambda v}(y).$$

By assumption, for every $x \in \mathbb{F}_p^r$, there exists a non-zero y_x such that

$$\lambda a(f(x) + g(y_x)) + \lambda l_v(y_x) + l_{w'}(x) = 0,$$

equivalently, $l_{w'}(x) = -\lambda(a(f(x) + g(y_x)) + l_v(y_x))$. Since $c_1 \preceq c_2$, $l_w(x) = a(f(x) + g(y_x)) + l_v(y_x)$ for every $x \in \mathbb{F}_p^r$. Thus, the function $l_{w'}(x)$ is equal to $\lambda l_w(x)$. This implies that $c_2 = \lambda c_1$. Let $c_1, c_2 \in \mathcal{C}_h$ be two linearly independent codewords in $\mathcal{C}_h$. By the previous paragraph and by minimality of $\mathcal{C}_g$, $c_1 \preceq c_2$ unless either of the induced codewords in $\mathcal{C}_g$ is the zero codeword. In this case, either c_1 or c_2 is a linear function depending on the variable x only. It cannot happen that $c_1 \preceq c_2$ and both codewords are linear depending on x only since the simplex code is minimal. Without loss of generality, suppose that

$$c_1 = (l_{w'}(x))_{(x,y) \in \mathbb{F}_p^r \times \mathbb{F}_p^s} \text{ and } c_2 = (a(f(x) + g(y)) + l_w(x) + l_v(y))_{(x,y) \in \mathbb{F}_p^r \times \mathbb{F}_p^s}.$$

To prove that $c_1 \not\preceq c_2$, if $a \neq 0$, then let $x_0 \in \mathbb{F}_p^r$ be such that $l_{w'}(x_0) \neq 0$ and $y_{x_0} \in \mathbb{F}_p^s$ be such that $g(y_{x_0}) + l_{a^{-1}v}(y_{x_0}) = -a^{-1}(af(x_0) + l_w(x_0))$. If $a = 0$, then take $x_0 \in \mathbb{F}_p^r$ such that $l_{w'}(x_0) \neq 0$ and $y_{x_0} \in \mathbb{F}_p^s$ such that $l_v(y_{x_0}) = -l_w(x_0)$. Analogously, we can prove that $c_2 \not\preceq c_1$. This shows that $\mathcal{C}_h$ is minimal. The second part of the statement, related to the minimum distance of $\mathcal{C}_h$, follows at once from Lemma 4.1.1. □

An immediate consequence of Theorem 4.1.3 is that a bent function g together with any other function f give rise to minimal linear codes.

Corollary 4.1.4. *Let n, r, s be three integers such that $r \geqslant 2, s > 2$ and $r+s = n$ (when $p = 2$, let s be even). Let $f : \mathbb{F}_p^r \to \mathbb{F}_p$ be a function with $f(0) = 0$ and $g : \mathbb{F}_p^s \to \mathbb{F}_p$ be bent. Consider the direct sum $h(x, y) = f(x) + g(y)$. The code $\mathcal{C}_h$ is a minimal linear code with parameters $[p^n, n + 1, d]$ where $d > p^r(p-1)(p^{s-1} - p^{s/2-1})$.*

Proof. According to Theorem 4 in [11], the minimum weight $w_{\min}$ of $\mathcal{C}_g$ satisfies

$$w_{\min} \geqslant (p-1)(p^{s-1} - p^{s/2-1})$$

and every nonzero weight is at most $(p-1)(p^{s-1} + p^{s/2-1})$. This tells us that the ratio $w_{\min}/w_{\max}$ is at least

$$\frac{p^{s-1} - p^{s/2-1}}{p^{s-1} + p^{s/2-1}},$$

which is larger than $\frac{p-1}{p}$ because either $p > 2$ and $s \geqslant 3$ or $p = 2$ and $s \geqslant 4$. By Ashikhmin-Barg's condition, the code $\mathcal{C}_g$ is minimal. Moreover, for every

$a \in \mathbb{F}_p$ and $v \in \mathbb{F}_p^s$, there are at least $p^{s-1} - (p-1)p^{s/2-1} - 1$ values y such that $g(y) + l_v(y) = a$ since $g + l_v$ is bent. Theorem 4.1.3 implies that $\mathcal{C}_h$ is a minimal linear code. For every $z \in \mathbb{F}_p^r$ and every two linear functions $u : \mathbb{F}_p^r \to \mathbb{F}_p$, $v : \mathbb{F}_p^s \to \mathbb{F}_p$, the set $\{y \in \mathbb{F}_p^s : g(y) + l_v(y) \neq f(z) + l_u(z)\}$ has cardinality at least $(p-1)(p^{s-1} - p^{s/2-1}) + 1$ thus any codeword in $\mathcal{C}_h$ has weight strictly greater than $p^r(p-1)(p^{s-1} - p^{s/2-1})$. □

As suggested by Lemma 4.1.1, the Walsh spectrum of the direct sum of p-ary functions is well-understood and it entirely depends on the Walsh spectra of each summand. In particular, when $g : \mathbb{F}_p^s \to \mathbb{F}_p$ is bent, the Walsh spectrum of the direct sum $h(x, y) = f(x) + g(y)$ can be completely determined using the Walsh spectrum of f. For simplicity, we will consider the case $p = 2$ since our main results are given for the binary case. However, a similar analysis can be, in principle, carried out for the case $p > 2$.

Consider the set (not multi-set) W_f^{abs} of distinct absolute values of non-zero elements in the Walsh spectrum $W_f = \{\{W_f(\lambda) : \lambda \in \mathbb{F}_2^r\}\}$ of an arbitrary Boolean function $f \in \mathcal{B}_r$, i.e.,

$$W_f^{\text{abs}} = \{|z| : z \in W_f, z \neq 0\} = \{|W_f(\lambda)| : \lambda \in \mathbb{F}_2^n, W_f(\lambda) \neq 0\}, \tag{4.4}$$

where $a \neq b$ for any $a, b \in W_f^{\text{abs}}$. For every element ρ in W_f^{abs}, define $\mathfrak{m}_\rho^+$ as the multiplicity of ρ in W_f and define $\mathfrak{m}_\rho^-$ as the multiplicity of $-\rho$ in W_f. Let also $\mathfrak{m}_0$ denote the multiplicity of 0 in W_f. For any bent function $g \in \mathcal{B}_s$, denote its dual bent function by $\tilde{g}$, i.e. $(-1)^{\tilde{g}(\lambda)} = 2^{-s/2} W_g(\lambda)$ for any $\lambda \in \mathbb{F}_2^s$.

Corollary 4.1.5. *Let n, r, s be three integers such that $r \geqslant 2, s > 2$ is even and $r + s = n$. Let $f \in \mathcal{B}_r$ be such that $f(0) = 0$ and $g \in \mathcal{B}_s$ be bent. Consider $h(x, y) = f(x) + g(y)$. The code $\mathcal{C}_h$ is a minimal binary linear code with parameters $[2^n, n+1, \mathcal{N}_h]$ and it has $2|W_f^{\text{abs}}| + 1$ different non-zero weights, where W_f^{abs} is given by (4.4). The weight distributions of $\mathcal{C}_h$, depending on the weight of the dual $\tilde{g}$, are displayed in Table 4.1 and Table 4.2.*

Proof. Since $g \in \mathcal{B}_s$ is bent, the code $\mathcal{C}_g$ is minimal. Theorem 4.1.3 implies that $\mathcal{C}_h$ is minimal with parameters $[2^n, n + 1, 2^{n-1} - \frac{1}{2}\delta]$, where

$$\delta = \max\{\mathcal{W}_{\max}^{(f)} \mathcal{W}_{\max}^{(g)}, \mathcal{W}_{\min}^{(f)} \mathcal{W}_{\min}^{(g)}\}.$$

Replacing the corresponding values for $\pm 2^{s/2}$,

$$\delta = 2^{s/2} \max\{\mathcal{W}_{\max}^{(f)}, -\mathcal{W}_{\min}^{(f)}\} = 2^{s/2} \max_{w \in \mathbb{F}_2^r} |W_f(w)|.$$

Thus, the minimum distance of $\mathcal{C}_h$ equals the minimum distance $\mathcal{N}_h$ of h. For every $\lambda = (\lambda_1, \lambda_2) \in \mathbb{F}_2^n$, the weight of the codeword corresponding to $c_{1,(\lambda_1,\lambda_2)}$ in $\mathcal{C}_h$ equals

$$2^{n-1} - \frac{1}{2} W_f(\lambda_1) W_g(\lambda_2) = 2^{n-1} \pm 2^{s/2-1} W_f(\lambda_1).$$

By definition, the dual $\tilde{g}$ of g has weight $2^{s-1} - 2^{s/2-1}$ when $|\{w \in \mathbb{F}_2^s : W_g(w) = -2^{s/2}\}| = 2^{s-1} - 2^{s/2-1}$. Hence, for every $\rho \in W_f^{\text{abs}}$, the weight $2^{n-1} - 2^{s/2-1}\rho$ of $\mathcal{C}_h$ is attained

$$(2^{s-1} + 2^{s/2-1})\mathfrak{m}_\rho^+ + (2^{s-1} - 2^{s/2-1})\mathfrak{m}_\rho^- \text{ times,}$$

since it is attained by the pair of Walsh values $(2^{s/2}, \rho)$ or by the pair $(-2^{s/2}, -\rho)$. Similarly, the weight $2^{n-1} + 2^{s/2-1}\rho$ is attained

$$(2^{s-1} - 2^{s/2-1})\mathfrak{m}_\rho^+ + (2^{s-1} + 2^{s/2-1})\mathfrak{m}_\rho^- \text{ times.}$$

A similar analysis can be done when the dual of g has weight $2^{s-1} + 2^{s/2-1}$. Finally, note that for every $\rho \in W_f^{\text{abs}}$, either $\mathfrak{m}_\rho^+ \neq 0$ or $\mathfrak{m}_\rho^- \neq 0$, this implies that both weights $2^{n-1} - 2^{s/2-1}\rho$ and $2^{n-1} + 2^{s/2-1}\rho$ are always attained. Additionally, distinct values in W_f^{abs} yield distinct values of the corresponding weights, thus there are $2||W_f^{\text{abs}}|| + 1$ non-zero weights including the weight 2^{n-1}. □

Table 4.1: Weight distribution of $\mathcal{C}_h$ when f is a Boolean function with $f(0) = 0$ and g is a bent function whose dual has weight $2^{s-1} - 2^{s/2-1}$ and $h(x, y) = f(x) + g(y)$, where ρ runs over the set W_f^{abs}.

Weight w	Number of codewords A_w
$2^{n-1} - 2^{s/2-1}\rho$	$(2^{s-1} + 2^{s/2-1})\mathfrak{m}_\rho^+ + (2^{s-1} - 2^{s/2-1})\mathfrak{m}_\rho^-$
$2^{n-1} + 2^{s/2-1}\rho$	$(2^{s-1} - 2^{s/2-1})\mathfrak{m}_\rho^+ + (2^{s-1} + 2^{s/2-1})\mathfrak{m}_\rho^-$
2^{n-1}	$2^n + 2^s\mathfrak{m}_0 - 1$
0	1

Table 4.2: Weight distribution of $\mathcal{C}_h$ when f is a Boolean function with $f(0) = 0$ and g is a bent function whose dual has weight $2^{s-1} + 2^{s/2-1}$ and $h(x, y) = f(x) + g(y)$, where ρ runs over the set W_f^{abs}.

Weight w	Number of codewords A_w
$2^{n-1} - 2^{s/2-1}\rho$	$(2^{s-1} - 2^{s/2-1})\mathfrak{m}_\rho^+ + (2^{s-1} + 2^{s/2-1})\mathfrak{m}_\rho^-$
$2^{n-1} + 2^{s/2-1}\rho$	$(2^{s-1} + 2^{s/2-1})\mathfrak{m}_\rho^+ + (2^{s-1} - 2^{s/2-1})\mathfrak{m}_\rho^-$
2^{n-1}	$2^n + 2^s\mathfrak{m}_0 - 1$
0	1

Once we know the Walsh spectrum of f, the weight distribution of the code $\mathcal{C}_h$ is easily obtained. A simple instance is when r is an odd integer and f is a semi-bent Boolean function with $f(0) = 0$. The weight distributions of $\mathcal{C}_h$ in this case are displayed in Tables 4.3 and 4.4.

Table 4.3: Weight distribution of $\mathcal{C}_h$ when f is semi-bent, g is a bent function whose dual has weight $2^{s-1} - 2^{s/2-1}$ and $h(x, y) = f(x) + g(y)$.

Weight w	Number of codewords A_w
$2^{n-1} - 2^{s/2-1}2^{(r+1)/2}$	$(2^{s-1} + 2^{s/2-1})(2^{r-2} + 2^{\frac{r-3}{2}}) + (2^{s-1} - 2^{s/2-1})(2^{r-2} - 2^{\frac{r-3}{2}})$
$2^{n-1} + 2^{s/2-1}2^{(r+1)/2}$	$(2^{s-1} + 2^{s/2-1})(2^{r-2} - 2^{\frac{r-3}{2}}) + (2^{s-1} - 2^{s/2-1})(2^{r-2} + 2^{\frac{r-3}{2}})$
2^{n-1}	$2^n + 2^{n-1} - 1$
0	1

Table 4.4: Weight distribution of $\mathcal{C}_h$ when f is semi-bent, g is a bent function whose dual has weight $2^{s-1} + 2^{s/2-1}$ and $h(x, y) = f(x) + g(y)$.

Weight w	Number of codewords A_w
$2^{n-1} - 2^{s/2-1}2^{(r+1)/2}$	$(2^{s-1} - 2^{s/2-1})(2^{r-2} + 2^{\frac{r-3}{2}}) + (2^{s-1} + 2^{s/2-1})(2^{r-2} - 2^{\frac{r-3}{2}})$
$2^{n-1} + 2^{s/2-1}2^{(r+1)/2}$	$(2^{s-1} - 2^{s/2-1})(2^{r-2} - 2^{\frac{r-3}{2}}) + (2^{s-1} + 2^{s/2-1})(2^{r-2} + 2^{\frac{r-3}{2}})$
2^{n-1}	$2^n + 2^{n-1} - 1$
0	1

For the subsequent examples, it will be convenient to represent $\mathbb{F}_2^r$ ordered lexicographically as $\mathbb{F}_2^r = \{v_0, \ldots, v_{2^r-1}\}$, where the vectors $v_i \in \mathbb{F}_2^r$ can be thought as the r-length binary representation of the integer i for $0 \leqslant i \leqslant r - 1$.

Example 4.1.6. *Let $r = 3, s = 4$. Consider the functions $f \in \mathcal{B}_3$ and $g \in \mathcal{B}_4$ given by $f(x_1, x_2, x_3) = x_1x_2 + x_3$ and $g(y_1, y_2, y_3, y_4) = y_1y_3 + y_2y_4$. The function g is bent and f is semi-bent whose Walsh spectrum is given Table 4.5 below. By computer-based simulations, we have verified that the linear code $\mathcal{C}_h$ is a minimal code with minimum weight $w_{\min} = \mathcal{N}_h = 56$ and $w_{\max} = 72$. It is therefore a $[128, 8, 56]$-code. Moreover, its weight enumerator is*

$$1 + 36z^{56} + 191z^{64} + 28z^{72},$$

i.e., $\mathcal{C}_h$ is a three-weight code.

Table 4.5: Walsh spectrum of the semi-bent function f in Example 4.1.6 given by $f(x_1, x_2, x_3) = x_1x_2 + x_3$.

λ	v_0	v_1	v_2	v_3	v_4	v_5	v_6	v_7
$W_f(\lambda)$	0	4	0	4	0	4	0	-4

Example 4.1.7. *Let $r = 4, s = 4$. Consider the functions $f \in \mathcal{B}_4$ and $g \in \mathcal{B}_4$ given by $f(x_1, x_2, x_3, x_4) = x_1x_2x_3+x_4$ and $g(y_1, y_2, y_3, y_4) = y_1y_3+y_2y_4+1$. The function g is a bent function and the Walsh spectrum of f is displayed in Table 4.6 below. It can be verified that the linear code $\mathcal{C}_h$ is a minimal $[256, 9, 104]$-code with $w_{\min} = \mathcal{N}_h = 104$ and $w_{\max} = 152$. Moreover, its weight enumerator is*

$$1 + 6z^{104} + 54z^{120} + 383z^{128} + 58z^{136} + 10z^{152},$$

i.e., $\mathcal{C}_h$ is a five-weight code.

Table 4.6: Walsh spectrum of the semi-bent function f in Example 4.1.7 given by $f(x_1, x_2, x_3, x_4) = x_1x_2x_3 + x_4$.

λ	v_1	v_2	v_3	v_4	v_5	v_6	v_7	v_8	v_9	v_{10}	v_{11}	v_{12}	v_{13}	v_{14}	v_{15}	v_{16}
$W_f(\lambda)$	0	12	0	4	0	4	0	-4	0	4	0	-4	0	-4	0	4

The largest minimum distance which can be achieved for a bent function $g \in \mathcal{B}_s$ by means of Corollary 4.1.5, depends on the Walsh spectrum of $f \in \mathcal{B}_r$. When n is even, choosing a bent function $f \in \mathcal{B}_r$ gives the largest minimum distance $2^{n-1} - 2^{n/2-1}$. When n is odd, a semi-bent function $f \in \mathcal{B}_r$ will provide the largest minimum distance of $\mathcal{C}_h$, which is $2^{n-1} - 2^{s/2+\frac{r+1}{2}-1}$. The codes constructed in either Theorem 4.1.3 or Corollary 4.1.5 cannot be optimal (nor almost optimal) since optimal codes with length 2^n and dimension $n+1$ have minimum distance 2^{n-1} (the *extended first order Reed-Muller code*, which is however not a minimal code). Nevertheless, the direct sum method gives an extremely large family of minimal codes (with different weight distributions) due to the arbitrary selection of f and g.

4.2 Subspaces of derivatives and non-covering permutations

In this section, we propose a different approach to obtaining (wide) minimal binary codes by employing a suitable subspace of derivatives of a bent function g

which is taken from the $\mathcal{MM}$ class of bent functions. To achieve the minimality of the resulting codes, it will be required that the underlying permutation ϕ used to define g satisfies certain covering properties. The proposed class of permutations is much harder to specify for $p > 2$ and therefore we almost exclusively focus on the binary case in this section. Nonetheless, we deal with the general case in Subsection 4.2.1 and in Section 4.4.

For s even, let $g \in \mathcal{B}_s$ be a bent function in the $\mathcal{MM}$ class defined as

$$g(y_1, y_2) = y_1 \cdot \phi(y_2);\ (y_1, y_2) \in \mathbb{F}_2^{s/2} \times \mathbb{F}_2^{s/2}, \tag{4.5}$$

where ϕ is a permutation on $\mathbb{F}_2^{s/2}$ such that the algebraic degree of each component function $a \cdot \phi$ is at least two.

The following lemmas identify useful non-covering properties of the codewords related to derivatives of the bent function g at directions which affect only the linear parts of g.

Lemma 4.2.1. *Let g be a bent function on $\mathbb{F}_2^s$ (s even) in the $\mathcal{MM}$ class, as specified in (4.5). For any two different vectors $\alpha, \beta \in \mathbb{F}_2^{s/2} \times \{0\}$, the corresponding derivatives $D_\alpha g$ and $D_\beta g$ are different and*

$$D_\alpha g + D_\beta g = D_{(\alpha+\beta)} g. \tag{4.6}$$

Moreover, for every non-zero $v = (v_1, v_2) \in \mathbb{F}_2^{s/2} \times \mathbb{F}_2^{s/2}, \gamma \in \mathbb{F}_2^{s/2}$ and $\epsilon \in \mathbb{F}_2$,

$$wt(D_{(\gamma,0)} g + l_v + \epsilon) = \begin{cases} 2^{s-1} - 2^{s/2-1}(-1)^\epsilon W_{\gamma\cdot\phi}(v_2) & \textit{if } \gamma \neq 0, v_1 = 0 \\ 2^{s-1} & \textit{otherwise.} \end{cases} \tag{4.7}$$

Proof. Compute, for every $y = (y_1, y_2) \in \mathbb{F}_2^{s/2} \times \mathbb{F}_2^{s/2}$ and $\gamma \in \mathbb{F}_2^{s/2}$,

$$D_{(\gamma,0)} g(y) = \phi(y_2) \cdot y_1 + \phi(y_2) \cdot (y_1 + \gamma) = \phi(y_2) \cdot \gamma.$$

Consider a pair of vectors $\alpha = (\alpha_1, 0), \beta = (\beta_1, 0) \in \mathbb{F}_2^{s/2} \times \{0\}$. The sum of the corresponding derivatives satisfies

$$D_\alpha g(y) + D_\beta g(y) = \phi(y_2) \cdot \alpha + \phi(y_2) \cdot \beta = \phi(y_2) \cdot (\alpha + \beta) = D_{\alpha+\beta} g(y),$$

for every $y \in \mathbb{F}_2^s$. Thus, equation (4.6) holds. Since g is bent, $D_{(\alpha+\beta)} g$ is a balanced function, hence $D_\alpha g$ and $D_\beta g$ are different.

To prove (4.7), suppose first that $\gamma \neq 0$ and $v_1 = 0$. In this case, the function $D_{(\gamma,0)} g + l_v + \epsilon$ evaluated at an element $y = (y_1, y_2)$ equals $\phi(y_2) \cdot \gamma + v_2 \cdot y_2 + \epsilon$, thus it has weight

$$2^{s/2}(2^{s/2-1} - \frac{1}{2}(-1)^\epsilon W_{\gamma\cdot\phi}(v_2)).$$

Now, if either $\gamma = 0$ or $v_1 \neq 0$, then the function $D_{(\gamma,0)}g + l_v + \epsilon$ is either affine (non-constant) or equals $\phi(y_2) \cdot \gamma + v_2 \cdot y_2 + v_1 \cdot y_1 + \epsilon$ when evaluated at $y = (y_1, y_2)$, in both cases, $wt(D_{(\gamma,0)}g + l_v + \epsilon) = 2^{s-1}$. □

Following the notation used for codewords in the linear code $\mathcal{C}_g$, for a Boolean function $g \in \mathcal{B}_s$, denote by $c_{\alpha,v,\epsilon}$ the vector

$$(g(y+\alpha) + v \cdot y + \epsilon)_{y \in \mathbb{F}_2^s},$$

where $\alpha, v \in \mathbb{F}_2^s$ and $\epsilon \in \mathbb{F}_2$. Additionally, denote by $c'_{\alpha,v,\epsilon}$ the vector corresponding to the derivative $D_\alpha g$, i.e.

$$(g(y) + g(y+\alpha) + v \cdot y + \epsilon)_{y \in \mathbb{F}_2^s},$$

where $\alpha, v \in \mathbb{F}_2^s$ and $\epsilon \in \mathbb{F}_2$. The next result specifies the non-covering property among vectors that stem from a bent function g.

Lemma 4.2.2. *Let s be even and $y = (y_1, y_2) \in \mathbb{F}_2^{s/2} \times \mathbb{F}_2^{s/2}$. Let g be a bent function in $\mathcal{B}_s$ as specified in (4.5). For $\alpha, \beta \in \mathbb{F}_2^{s/2} \times \{0\}$, $u, v \in \mathbb{F}_2^s$ and $\epsilon_1, \epsilon_2 \in \mathbb{F}_2$, the following hold:*

(i) If $\alpha \neq \beta$ or $l_v + \epsilon_1 \neq l_u + \epsilon_2$, then $c_{\alpha,v,\epsilon_1} \not\preceq c_{\beta,u,\epsilon_2}$.

(ii) If $\beta \neq 0$ or $l_u + \epsilon_2 \neq 1$, then $c_{\alpha,v,\epsilon_1} \not\preceq c'_{\beta,u,\epsilon_2}$

Proof. The statements are proved separately.

(i) Since g is a bent function, the difference $wt(c_{\beta,u,\epsilon_2}) - wt(c_{\alpha,v,\epsilon_1})$ equals either $\pm 2^{s/2}$ or 0. On the other hand,

$$c_{\alpha,v,\epsilon_1} + c_{\beta,u,\epsilon_2} = (D_{\alpha+\beta}g(y) + (v+u) \cdot y + \epsilon_1 + \epsilon_2)_{y \in \mathbb{F}_2^s} = c'_{\alpha+\beta, v+u, \epsilon_1+\epsilon_2}.$$

Using Lemma 4.2.1, we get $wt(c_{\alpha,v,\epsilon_1} + c_{\beta,u,\epsilon_2}) \neq 2^{s/2}$. Hence, if $c_{\alpha,v,\epsilon_1} \preceq c_{\beta,u,\epsilon_2}$, then $c_{\alpha,v,\epsilon_1} = c_{\beta,u,\epsilon_2}$. Equivalently, $\alpha = \beta$ and $l_v + \epsilon_1 = l_u + \epsilon_2$.

(ii) The function corresponding to c_{α,v,ϵ_1} and $c_{\alpha,v,\epsilon_1} + c'_{\beta,u,\epsilon_2}$ is the sum of a bent function and an affine function. Specifically, using the definition of g,

$$c_{\alpha,v,\epsilon_1} + c'_{\beta,u,\epsilon_2} = (g(y+\alpha+\beta) + (v+u) \cdot y + \epsilon_1 + \epsilon_2)_{y \in \mathbb{F}_2^s}.$$

From this, the weights of these vectors can be computed as $wt(c_{\alpha,v,\epsilon_1}) = 2^{s-1} \pm 2^{s/2-1}$ and $wt(c_{\alpha,v,\epsilon_1} + c'_{\beta,u,\epsilon_2}) = 2^{s-1} \pm 2^{s/2-1}$, thus

$$wt(c'_{\beta,u,\epsilon_2} + c_{\alpha,v,\epsilon_1}) + wt(c_{\alpha,v,\epsilon_1}) = 2^s + 2^{s/2} \quad or \quad 2^s - 2^{s/2} \quad or \quad 2^s.$$

If $c_{\alpha,v,\epsilon_1} \preceq c'_{\beta,u,\epsilon_2}$, then $wt(c'_{\beta,u,\epsilon_2}) = wt(c'_{\beta,u,\epsilon_2} + c_{\alpha,v,\epsilon_1}) + wt(c_{\alpha,v,\epsilon_1})$, which implies that $wt(c'_{\beta,u,\epsilon_2})$ must be equal to either $2^s - 2^{s/2}$ or 2^s (the weight of a vector cannot be larger than 2^s). By Lemma 4.2.1, $wt(c'_{\beta,u,\epsilon_2}) \neq 2^s - 2^{s/2}$. Consequently, if $c_{\alpha,v,\epsilon_1} \preceq c'_{\beta,u,\epsilon_2}$, then c'_{β,u,ϵ_2} is the all-one vector, i.e. $\beta = 0$ and $l_u + \epsilon_2$ is the identically one function.

□

Consider a basis $\mathscr{B} = \{v_1, \ldots, v_{s+1}\} \subset \mathbb{F}_2^{2^s}$ for $\mathcal{C}_g$. Let $D_{\hat{e}_1}g, \ldots, D_{\hat{e}_{s/2}}g$ be the derivatives of g at respective direction $\hat{e}_i$, where $\hat{e}_i \in \mathbb{F}_2^{s/2} \times \mathbb{F}_2^{s/2}$ is the canonical vector with all zero co-ordinates except for the i-th coordinate in which there is a one. Note that for $(y_1, y_2) \in \mathbb{F}_2^{s/2} \times \mathbb{F}_2^{s/2}$,

$$D_{\hat{e}_i}g(y_1, y_2) = y_1 \cdot \phi(y_2) + (y_1 + e_i) \cdot \phi(y_2) = e_i \cdot \phi(y_2),$$

where we tacitly use the canonical vectors $e_i \in \mathbb{F}_2^{s/2}$. The previous lemmas suggest that if the vectors

$$D_{\hat{e}_1}g, \ldots, D_{\hat{e}_{s/2}}g$$

are added to the basis $\mathscr{B}$, then one may obtain a minimal code with larger dimension. Unfortunately, this is not always true since the covering properties in Lemma 4.2.2 does not necessarily hold for the derivatives of g, i.e. Lemma 4.2.2 does not address the (non-)covering property of two vectors that stem from the derivative of g.

Before providing a sound solution for the issue mentioned in the previous paragraph, let us introduce a concept to elaborate on our discussion. The key idea for the first construction method given in (2.12), is to adjoin non-affine functions to the extended simplex code. Adjoining two linearly independent non-affine functions $f_1, f_2 \in \mathcal{B}_n$ whose sum is non-affine gives a $[2^n, n+2, d]$-code that will be denoted by $\mathcal{C}_{f_1} \oplus \mathcal{C}_{f_2}$, formally,

$$\mathcal{C}_{f_1} \oplus \mathcal{C}_{f_2} := \{(a_1 f_1(x) + a_2 f_2(x) + \lambda \cdot x)_{x \in \mathbb{F}_2^n} : a_i \in \mathbb{F}_2, \lambda \in \mathbb{F}_2^n\}, \qquad (4.8)$$

which can be seen to be equal to $\mathcal{C}_{f_1} \cup \mathcal{C}_{f_2} \cup \mathcal{C}_{f_1+f_2}$. Recursively, we can define $\bigoplus_{i \in I} \mathcal{C}_{f_i}$ for more than two functions. The minmiality of $\mathcal{C}_{f_1} \oplus \mathcal{C}_{f_2}$ can be expressed in terms of the minimality of each individual code and an additional non-covering property as stated in the following lemma.

Lemma 4.2.3. *Let f_1, f_2 be two distinct non-affine Boolean functions such that $f_1 + f_2$ is non-affine. Then, the code $\mathcal{C}_{f_1} \oplus \mathcal{C}_{f_2}$ is minimal if and only if $\mathcal{C}_{f_1}$, $\mathcal{C}_{f_2}, \mathcal{C}_{f_1+f_2}$ are minimal and the following condition holds:*

For every two vectors $\lambda_1, \lambda_2 \in \mathbb{F}_2^n$ and elements $\epsilon_1, \epsilon_2, \epsilon_3 \in \mathbb{F}_2$ such that $\epsilon_1 + \epsilon_2 + \epsilon_3 = 1$ (over $\mathbb{Z}$), we have

$$(-1)^{\epsilon_1} W_{f_1}(\lambda_1) + (-1)^{\epsilon_2} W_{f_2}(\lambda_2) + (-1)^{\epsilon_3} W_{f_1+f_2}(\lambda_1 + \lambda_2) \neq 2^n. \tag{4.9}$$

Proof. Let $\mathcal{C} := \mathcal{C}_{f_1} \oplus \mathcal{C}_{f_2}$. Suppose that $\mathcal{C}$ is minimal. Since $\mathcal{C}_{f_1}$, $\mathcal{C}_{f_2}, \mathcal{C}_{f_1+f_2}$ are subcodes of $\mathcal{C}$, they are minimal too. Let $\lambda_1, \lambda_2 \in \mathbb{F}_2^n$ be arbitrary. We show (4.9) only for the case $\epsilon_1 = 1, \epsilon_2 = \epsilon_3 = 0$, since the other two cases are similar (symmetric). Consider two distinct non-zero codewords $c_1 = (f_1(x) + \lambda_1 \cdot x)_{x \in \mathbb{F}_2^n}$ and $c_2 = (f_2(x) + \lambda_2 \cdot x)_{x \in \mathbb{F}_2^n}$. Since $\mathcal{C}$ is minimal, $c_2 \not\preceq c_1$. This implies that

$$wt(c_1) - wt(c_2) \neq wt(c_1 + c_2),$$

which is equivalent to

$$-W_{f_1}(\lambda_1) + W_{f_2}(\lambda_2) \neq 2^n - W_{f_1+f_2}(\lambda_1 + \lambda_2).$$

In other words, $-W_{f_1}(\lambda_1) + W_{f_2}(\lambda_2) + W_{f_1+f_2}(\lambda_1 + \lambda_2) \neq 2^n$. Conversely, suppose that $\mathcal{C}_{f_1}$, $\mathcal{C}_{f_2}, \mathcal{C}_{f_1+f_2}$ are minimal and (4.9) holds. It suffices to prove that the codewords stemming from different codes do not cover each other. There are several cases to consider but we only treat the case of (non-linear) $c_1 \in \mathcal{C}_{f_1}$ and $c_2 \in \mathcal{C}_{f_2}$, since the other cases are similar. Let $c_1 = (f_1(x) + \lambda_1 \cdot x)_{x \in \mathbb{F}_2^n}$ and $c_2 = (f_2(x) + \lambda_2 \cdot x)_{x \in \mathbb{F}_2^n}$. The statement $c_2 \preceq c_1$ is equivalent to

$$2^{n-1} - \frac{1}{2} W_{f_1}(\lambda_1) - 2^{n-1} + \frac{1}{2} W_{f_2}(\lambda_2) = 2^{n-1} - \frac{1}{2} W_{f_1+f_2}(\lambda_1 + \lambda_2),$$

which, in turn, is equivalent to

$$-W_{f_1}(\lambda_1) + W_{f_2}(\lambda_2) + W_{f_1+f_2}(\lambda_1 + \lambda_2) = 2^n.$$

Therefore $c_2 \preceq c_1$ is incompatible with (4.9). □

Let us now go back to the construction of minimal codes adjoining some vectors to a basis for $\mathcal{C}_g$. Define the functions $g_0 := g$ and $g_i := D_{(e_i,0)} g$ for $i \in \{0, \ldots, \frac{s}{2}\}$, where $\{e_1, \ldots, e_{s/2}\}$ is the canonical basis for $\mathbb{F}_2^{s/2}$. As pointed out earlier, Lemma 4.2.2 suggests that the code

$$\mathcal{C} = \bigoplus_{i \in \{0, \ldots, \frac{s}{2}\}} \mathcal{C}_{g_i}, \tag{4.10}$$

may be minimal. We now introduce a special subclass of permutations ϕ over $\mathbb{F}_2^m$ that allows us to assure minimality of the aforementioned code.

Definition 4.2.4. *A permutation ϕ on $\mathbb{F}_2^m$ such that $\phi(0) = 0$ is a* non-covering permutation *if for every $(a_1, b) \neq (a_2, b) \in \mathbb{F}_2^m \times (\mathbb{F}_2^m)^*$ we have*

$$W_{b\cdot\phi}(a_1) \pm W_{b\cdot\phi}(a_2) \neq 2^m, \tag{4.11}$$

and furthermore for every pair $(a_1, b_1), (a_2, b_2) \in \mathbb{F}_2^m \times (\mathbb{F}_2^m)^*$ with $b_1 \neq b_2$, the following is satisfied

$$W_{b_1\cdot\phi}(a_1) - W_{b_2\cdot\phi}(a_2) + W_{(b_1+b_2)\cdot\phi}(a_1 + a_2) \neq 2^m. \tag{4.12}$$

Definition 4.2.4 implies that the degree of $a \cdot \phi$ is at least 2 for any $a \in (\mathbb{F}_2^m)^*$, thus a non-covering permutation has no affine components. A particular class of non-covering permutations stem from AB permutations: For odd $m > 3$, any AB permutation ϕ satisfies

$$W_{b\cdot\phi}(a_1) \pm W_{b\cdot\phi}(a_2) \leqslant 2 \cdot 2^{\frac{m+1}{2}} < 2^m,$$

for $(a_1, b) \neq (a_2, b) \in \mathbb{F}_2^m \times (\mathbb{F}_2^m)^*$ and

$$W_{b_1\cdot\phi}(a_1) - W_{b_2\cdot\phi}(a_2) + W_{(b_1+b_2)\cdot\phi}(a_1 + a_2) \leqslant 3 \cdot 2^{\frac{m+1}{2}} < 2^m,$$

for $(a_1, b_1), (a_2, b_2) \in \mathbb{F}_2^m \times (\mathbb{F}_2^m)^*$ such that $b_1 \neq b_2$. Therefore, an AB permutation ϕ is non-covering for odd $m > 3$.

Similarly, another class of non-covering permutations is the *multiplicative inverse* given by $\phi(y) = y^{2^m-2}$ on $\mathbb{F}_{2^m}$, as shown in the following lemma.

Lemma 4.2.5. *Let m be any integer such that $m \geqslant 5$. The multiplicative inverse permutation $\phi(y) = y^{2^m-2}$ is a non-covering permutation on $\mathbb{F}_{2^m}$.*

Proof. For this proof, we identify the space $\mathbb{F}_2^m$ with $\mathbb{F}_{2^m}$. It is well-known [57] that the Walsh values of any component $\phi_b := \mathrm{Tr}(by^{2^m-2})$ of the inverse permutation ϕ, for $b \in \mathbb{F}_{2^m}^*$, are given by the integers congruent to 0 mod 4 in the interval $[-2^{m/2+1}, 2^{m/2+1}]$. This implies $|W_{\phi_b}| \leqslant 2^{m/2+1}$, for any $b \in \mathbb{F}_{2^m}^*$. For $m \geqslant 5$, we then have

$$W_{\phi_b}(a_1) \pm W_{\phi_b}(a_2) \leqslant 2 \cdot 2^{m/2+1} < 2^m,$$

for $(a_1, b) \neq (a_2, b) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}^*$. This shows that (4.11) is satisfied. For $m > 5$, we also have

$$W_{\phi_{b_1}}(a_1) - W_{\phi_{b_2}}(a_2) + W_{\phi_{b_1+b_2}}(a_1 + a_2) \leqslant 3 \cdot 2^{\frac{m+1}{2}} < 2^m,$$

for $(a_1, b_1), (a_2, b_2) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}^*$ with $b_1 \neq b_2$. Hence (4.12) is satisfied for $m > 5$. The equation (4.12) holds also for $m = 5$, which can be confirmed by computer simulations (see also Example 4.2.12). □

With the notion of non-covering permutations, we are now able to prove the following lemma, which shows that the desired (non-)covering property applies also to vectors that stem from some derivatives of a bent function g in the $\mathcal{MM}$ class as defined in (4.5).

Lemma 4.2.6. *Let s be even. Let $g \in \mathcal{B}_s$ be a bent function in $\mathcal{MM}$ as defined in (4.5, i.e.*

$$g(y_1, y_2) = y_1 \cdot \phi(y_2)$$

for $(y_1, y_2) \in \mathbb{F}_2^{s/2} \times \mathbb{F}_2^{s/2}$. Assume that ϕ is a non-covering permutation. For $\alpha, \beta \in \mathbb{F}_2^{s/2} \times \{0\}$, $u, v \in \mathbb{F}_2^s$ and $\epsilon \in \mathbb{F}_2$, suppose that the vectors $c'_{\alpha,v,0}$ and $c'_{\beta,u,\epsilon}$ are different from each other. It holds that $c'_{\alpha,v,0} \not\preceq c'_{\beta,u,\epsilon}$ unless $c'_{\alpha,v,0}$ is null or $c'_{\beta,u,\epsilon}$ is the all-one vector.

Proof. Let $g, \phi, \alpha, \beta, u, v$ and ϵ be as in the statement. Using the definition of g, the sum of its derivatives satisfies

$$g(y) + g(y + \alpha) + g(y) + g(y + \beta) = g(y) + g(y + \alpha + \beta)$$

for each $y \in \mathbb{F}_2^s$, hence

$$c'_{\alpha,v,0} + c'_{\beta,u,\epsilon} = (D_{\alpha+\beta}g(y) + (v + u) \cdot y + \epsilon)_{y \in \mathbb{F}_2^s} = c'_{\alpha+\beta,v+u,\epsilon}.$$

Assume that $c'_{\beta,u,\epsilon}$ is not the all-one vector. If either $c'_{\alpha,v,0}$ or $c'_{\beta,u,\epsilon}$ depend on y_1, then exactly two vectors amongst $c'_{\alpha,v,0}, c'_{\beta,u,\epsilon}, c'_{\alpha+\beta,v+u,\epsilon}$ are balanced since the only terms that depend on y_1 are affine. In this case $c'_{\alpha,v,0} \not\preceq c'_{\beta,u,\epsilon}$ unless $c'_{\alpha,v,0}$ is the zero vector.

Let us represent with a superscript (i) the restriction of an element in $\mathbb{F}_2^{s/2} \times \mathbb{F}_2^{s/2}$ to the coordinate y_i where $i \in \{1, 2\}$, e.g., $v^{(2)}$ is the restriction of v to the coordinate y_2.

Suppose that neither $c'_{\alpha,v,0}$ nor $c'_{\beta,u,\epsilon}$ depend on the first variable y_1 and $c'_{\alpha,v,0} \preceq c'_{\beta,u,\epsilon}$, i.e.,

$$wt(c'_{\beta,u,\epsilon}) - wt(c'_{\alpha,v,0}) = wt(c'_{\alpha+\beta,v+u,\epsilon}).$$

Let $c_1 = {c'_{\alpha,v,0}}^{(2)}$ and $c_2 = {c'_{\beta,u,\epsilon}}^{(2)}$. In this case,

$$2^{s/2}wt(c_1) - 2^{s/2}wt(c_2) = 2^{s/2}wt(c_1 + c_2)$$

since none of the vectors depend on y_2. Factor out to get

$$wt(c_2) - wt(c_1) = wt(c_1 + c_2). \tag{4.13}$$

Note that c_1 and c_2 can be expressed as

$$c_1 = \left(\phi(y_2)\cdot\alpha^{(1)} + v^{(2)}\cdot y_2\right)_{y_2\in\mathbb{F}_2^{s/2}}, \quad c_2 = \left(\phi(y_2)\cdot\beta^{(1)} + u^{(2)}\cdot y_2 + \epsilon\right)_{y_2\in\mathbb{F}_2^{s/2}}.$$

If $\alpha^{(1)} \neq 0, \beta^{(1)} \neq 0$ and $\alpha^{(1)} \neq \beta^{(1)}$, then

$$wt(c_1) = 2^{s/2-1} - \frac{1}{2}W_{\alpha^{(1)}\cdot\phi}(v^{(2)}), \quad wt(c_2) = 2^{s/2-1} - \frac{1}{2}(-1)^{\epsilon}W_{\beta^{(1)}\cdot\phi}(u^{(2)}),$$

and

$$wt(c_1+c_2) = 2^{s/2-1} - \frac{1}{2}(-1)^{\epsilon}W_{(\alpha^{(1)}+\beta^{(1)})\cdot\phi}(v^{(2)}+u^{(2)}).$$

Using (4.13) and rearranging,

$$W_{\alpha^{(1)}\cdot\phi}(v^{(2)}) - (-1)^{\epsilon}W_{\beta^{(1)}\cdot\phi}(u^{(2)}) + (-1)^{\epsilon}W_{(\alpha^{(1)}+\beta^{(1)})\cdot\phi}(v^{(2)}+u^{(2)}) = 2^{s/2},$$

which contradicts (4.12) in the definition of a non-covering permutation.

Now, if $\alpha^{(1)} \neq 0, \beta^{(1)} \neq 0$ and $\alpha^{(1)} = \beta^{(1)}$, then

$$wt(c_1) = 2^{s/2-1} - \frac{1}{2}W_{\alpha^{(1)}\cdot\phi}(v^{(2)}), \quad wt(c_2) = 2^{s/2-1} - \frac{1}{2}(-1)^{\epsilon}W_{\alpha^{(1)}\cdot\phi}(u^{(2)}),$$

and $wt(c_1+c_2) = 2^{s/2-1}$. Using (4.13),

$$W_{\alpha^{(1)}\cdot\phi}(v^{(2)}) - (-1)^{\epsilon}W_{\alpha^{(1)}\cdot\phi}(u^{(2)}) = 2^{s/2},$$

which contradicts (4.11) in the definition of a non-covering permutation. A similar argument rules out the possibility that $\alpha^{(1)} \neq 0, \beta^{(1)} = 0$. This forces $\alpha^{(1)} = 0$. Finally, using similar arguments and the fact that c_2 is not the all-one vector in $\mathbb{F}_2^s$, we get $v^{(2)} = 0$. Therefore c_1 is null, thus $v = 0$ and $\alpha = (0,0)$, in other words, c_1 is the zero vector. □

Now we are in a position to claim the minimality of the linear code in (4.10) using a bent function g defined by (4.5) and its suitable derivatives in accordance to Lemma 4.2.6.

Theorem 4.2.7 (The derivative method)**.** *Let s be an even integer at least four. Let $g \in \mathcal{B}_s$ be a bent function in the $\mathcal{MM}$ class defined as in (4.5), i.e. $g(y_1,y_2) = y_1\cdot\phi(y_2)$ for $(y_1,y_2) \in \mathbb{F}_2^{s/2}\times\mathbb{F}_2^{s/2}$. Let $\mathcal{C}$ be the linear code defined in* (4.10)*, namely,*

$$\mathcal{C} = \bigoplus_{i\in\{0,\ldots,\frac{s}{2}\}} \mathcal{C}_{g_i}, \tag{4.14}$$

where $g_0 = g$ and $g_i = g + D_{(e_i,0)}$ for $i = 1,\ldots,s/2$. The linear code $\mathcal{C}$ is a $[2^s, s+\frac{s}{2}+1, 2^{s/2}\theta]$-code with $\theta \geqslant \mathcal{N}_\phi$. Moreover, if ϕ is non-covering, then $\mathcal{C}$ is minimal.

Proof. Clearly, the length of $\mathcal{C}$ is 2^s and its dimension is $s+\frac{s}{2}+1$ since the set $\{g_0, g_1, \dots, g_{s/2}\}$ is linearly independent. For the minimum distance, note that, for every $y \in \mathbb{F}_2^s$, $\mu \in \mathbb{F}_2, v \in \mathbb{F}_2^s$ and every non-negative integer k with $k \leqslant s/2$,

$$\mu g(y)+g(y+e_{i_1})+\dots+g(y+e_{i_k})+v\cdot y = (\mu+\delta)g(y)+g(y+e_{i_0}+\dots+e_{i_k})+v\cdot y,$$

where δ is equal to k (mod 2). Hence, the minimum distance can be deduced using Lemma 4.2.1 and expressing each codeword $c \in \mathcal{C}$ in the form

$$c = ((\mu+\delta)g(y) + g(y+e_{i_0}+\dots+e_{i_k}) + v\cdot y)_{y\in\mathbb{F}_2^s}.$$

Let us now consider two distinct codewords $c_1, c_2 \in \mathcal{C}$, whose parameters are indexed accordingly, so that k_i, μ_i, δ_i correspond to c_i, for $i = 1, 2$. Suppose that $c_1 \preceq c_2$. Lemma 4.2.2 implies that c_1 is the zero codeword when $\mu_1 + \delta_1 = 0$ or $\mu_2 + \delta_2 = 0$. If $\mu_1 + \delta_1 = \mu_2 + \delta_2 = 1$, then Lemma 4.2.6 implies that c_1 is the zero codeword since ϕ is non-covering. Therefore, $\mathcal{C}$ is minimal. □

Corollary 4.2.8. *Let the notation of Theorem 4.2.7 hold. Suppose that* $s \equiv 2 \mod 4$ *and* $s/2 > 3$. *If* ϕ *is an AB permutation over* $\mathbb{F}_2^{s/2}$ *with* $\phi(0) = 0$, *then* $\mathcal{C}$, *defined by (4.14), is a five-valued minimal code with parameters* $[2^s, s+\frac{s}{2}+1, 2^{s-1}-2^{\frac{s+s/2-1}{2}}]$ *whose weight distribution is displayed in Table 4.7.*

Proof. Theorem 4.2.7 implies that the code $\mathcal{C}$ has parameters $[2^s, s+s/2+1, d]$, where

$$d \geqslant 2^{s/2}\mathcal{N}_\phi = 2^{s/2}(2^{s/2-1} - 2^{\frac{s/2-1}{2}}).$$

The minimality of $\mathcal{C}$ can also be inferred from Theorem 4.2.7, as AB permutations are non-covering for $s/2 > 3$. For any $\beta \in (\mathbb{F}_2^{s/2})^*, \lambda \in \mathbb{F}_2^{s/2}$ such that $W_{\beta\cdot\phi}(\lambda) = 2^{\frac{s/2+1}{2}}$, the codeword corresponding to the function $D_{(\beta,0)}g + (\lambda, 0)\cdot y$ has weight $2^{s/2}(2^{s/2-1}-2^{(s/2-1)/2})$. This implies that $d = 2^{s/2}(2^{s/2-1}-2^{(s/2-1)/2})$. Since ϕ is an AB permutation with $\phi(0) = 0$, the number of occurrences of $2^{\frac{s/2+1}{2}}$ in the Walsh spectra of every component $\beta\cdot\phi$ is $2^{s/2-2}+2^{(s/2-3)/2}$. This means that there are $(2^{s/2}-1)(2^{s/2-2}+2^{(s/2-3)/2})$ codewords of minimum weight. In a similar fashion, the other weights in the weight distribution of $\mathcal{C}$ can be obtained. □

Table 4.7: Weight distribution of $\mathcal{C}$ in Corollary 4.2.8.

Weight w	Number of codewords A_w
$2^{s-1}-2^{\frac{s+s/2-1}{2}}$	$(2^{s/2}-1)(2^{s/2-2}+2^{(s/2-3)/2})$
$2^{s-1}-2^{s/2-1}$	$2^{s/2}(2^{s-1}+2^{s/2-1})$
2^{s-1}	$2^{s/2-1}(2^{s/2}-1)+(2^s-2^{s/2})(2^{s/2}-1)+(2^s-1)$
$2^{s-1}+2^{s/2-1}$	$2^{s/2}(2^{s-1}-2^{s/2-1})$
$2^{s-1}+2^{\frac{s+s/2-1}{2}}$	$(2^{s/2}-1)(2^{s/2-2}-2^{(s/2-3)/2})$
0	1

Note that when ϕ is an AB permutation, the code $\mathcal{C}$ is actually narrow since the ratio

$$\frac{w_{\min}}{w_{\max}}=\frac{2^{s-1}-2^{\frac{s+s/2-1}{2}}}{2^{s-1}+2^{\frac{s+s/2-1}{2}}}$$

is larger than $1/2$ when $s/2>3$. On the other hand, the use of a non-covering permutation ϕ which is not AB may give rise to wide minimal codes, thus violating the Ashikhmin-Barg bound.

Corollary 4.2.9. *Let the notation of Theorem 4.2.7 hold. Suppose that $s/2\geqslant 5$ and let ϕ be the inverse permutation over $\mathbb{F}_{2^{s/2}}$ given by $\phi(y)=y^{2^{s/2}-2}$. The linear code $\mathcal{C}$ defined by (4.14) is an $(s-2)$-valued minimal code with parameters $[2^s, s+\frac{s}{2}+1, 2^{s/2}\theta]$, where $\theta=2^{s/2}(2^{s/2-1}-2^{s/4})$ when $s/2$ is even and θ equals the highest even integer bounded above by $2^{s/2-1}-2^{s/4}$ when $s/2$ is odd.*

Proof. It is well-known [57] that $\mathcal{N}_\phi=\min_{b\in\mathbb{F}_{2^s}^*}\mathcal{N}_{Tr(b\phi)}$ is equal to $\theta=(2^{s/2-1}-2^{s/4})$ when $s/2$ is even, and θ equals the highest even integer bounded above by $2^{s/2-1}-2^{s/4}$ when $s/2$ is odd. Theorem 4.2.7 implies that the code $\mathcal{C}$ has parameters $[2^n, s+s/2+1, d]$, where $d\geqslant 2^{s/2}\theta$. The minimality of $\mathcal{C}$ follows from Theorem 4.2.7, as the inverse permutations are non-covering for $s/2\geqslant 5$. Since the Walsh spectrum of any component of ϕ is given by the integers congruent to 0 mod 4 in the (real) range $[-2^{s/4+1}+1, 2^{s/4+1}+1]$, selecting $\beta\in(\mathbb{F}_2^{s/2})^*$, $\lambda\in\mathbb{F}_2^{s/2}$ such that $2^{s/2-1}-\frac{1}{2}W_{\beta\cdot\phi}(\lambda)=\mathcal{N}_\phi$ yields a codeword of weight $2^{s/2}\mathcal{N}_\phi$. This then implies that $d=2^{s/2}\mathcal{N}_\phi$. □

Example 4.2.10. *Set $s=10$. Let ϕ be the multiplicative inverse permutation on $\mathbb{F}_{2^5}$ given by $\phi(y)=y^{2^5-2}=y^{30}$. Let g be a bent function in $\mathcal{MM}$ as in (4.5) given by $g(y_1,y_2)=\phi(y_2)\cdot y_1$. The linear code*

$$\mathcal{C}=\bigoplus_{i\in\{0,\dots,5\}}\mathcal{C}_{g_i}$$

is an eight-valued minimal code with parameters $[1024, 16, 320]$. *Moreover, its weight enumerator is*

$$1+31z^{320}+155z^{384}+310z^{448}+16896z^{496}+31961z^{512}+15872z^{528}+155z^{576}+155z^{640},$$

hence $w_{\min}/w_{\max} = \frac{1}{2}$, *so that* $\mathcal{C}$ *is also wide.*

4.2.1 Non-covering permutations

In this section, we will take a closer look at the concept of non-covering permutations introduced in the previous section, which proved to be useful to construct (wide) minimal codes with a larger dimension.

Using simple Walsh spectrum arguments and known bounds on the nonlinearity of ϕ, one can show that there are no non-covering permutations ϕ over $\mathbb{F}_2^m$ for $m \leqslant 4$. However, there are 32! permutations over $\mathbb{F}_2^5$ and many of these permutations are non-covering.

In general, if a permutation $\phi : \mathbb{F}_2^m \to \mathbb{F}_2^m$ satisfies $\max_{(a,b)\in\mathbb{F}_2^m\times(\mathbb{F}_2^m)^*} |W_{b\cdot\phi(a)}| < 2^m/3$, then ϕ is a non-covering permutation. In other words, if the nonlinearity $\mathcal{N}_\phi$ of a class of permutations is at least $2^m/3$, then the permutations in this class are non-covering. For instance, when $m = 2t$ is even and t is odd, it can be checked by computer-based simulations that a class of permutation binomials of the form

$$F(x) = x^{\frac{2^n-1}{2^t-1}+1} + ax,$$

for moderately large t's, studied in [4], are non-covering. Hence, non-covering permutations are easily obtained.

Due to the form of the defining conditions in Definition 4.2.4, it can be foreseen that the concept of a non-covering permutation is somehow related to minimality of the associated code $\mathcal{C}_\phi$. This is indeed the case and these two properties are in fact equivalent. Throughout this section, it will be more convenient to work in the finite field $\mathbb{F}_{2^m}$ instead of in its vectorial counterpart $\mathbb{F}_2^m$.

Theorem 4.2.11. *Let* $\phi : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ *be a permutation without affine components such that* $\phi(0) = 0$. *Consider the code* $\mathcal{C}_\phi$ *defined by equation (2.12). The permutation* ϕ *is non-covering if and only if* $\mathcal{C}_\phi$ *is minimal.*

Proof. Assume that ϕ is a non-covering permutation. Let $c_{b_1,a_1}, c_{b_2,a_2} \in \mathcal{C}_\phi$ be two different non-zero codewords. Suppose that $c_{b_1,a_1} \preceq c_{b_2,a_2}$. Note that at most one out of the three relations $c_{b_1,a_1} \in \mathcal{S}_m^{\text{ext}}$, $c_{b_2,a_2} \in \mathcal{S}_m^{\text{ext}}$ and $c_{b_1+b_2,a_1+a_2} \in \mathcal{S}_m^{\text{ext}}$ can be true, as the simplex code is minimal. By Proposition 3.1.1, we have got

$$wt(c_{b_1+b_2,a_1+a_2}) = wt(c_{b_2,a_2}) - wt(c_{b_1,a_1}). \tag{4.15}$$

We consider now a few cases according to the values of b_1 and b_2. If $b_1 = b_2$ (so that $a_1 \neq a_2$), then the LHS of (4.15) is equal to 2^{m-1} since c_{0,a_1+a_2} is a non-zero linear function. Thus (4.15) becomes

$$2^{m-1} = 2^m - \frac{1}{2}W_{\mathrm{Tr}(b_1\phi)}(a_2) - 2^m + \frac{1}{2}W_{\mathrm{Tr}(b_1\phi)}(a_1).$$

Multiplying by two and rearranging, we obtain

$$2^m = W_{\mathrm{Tr}(b_1\phi)}(a_1) - W_{\mathrm{Tr}(b_1\phi)}(a_2),$$

which is a contradiction to (4.11) in the definition of a non-covering permutation. A similar argument works when either $b_1 = 0$ and $b_2 \neq 0$ or $b_1 \neq 0$ and $b_2 = 0$. If $b_1 \neq b_2$ and $b_1 \neq 0, b_2 \neq 0$, then (4.15) becomes

$$2^m - \frac{1}{2}W_{\mathrm{Tr}((b_1+b_2)\phi)}(a_1 + a_2) = 2^m - \frac{1}{2}W_{\mathrm{Tr}(b_2\phi)}(a_2) - 2^m + \frac{1}{2}W_{\mathrm{Tr}(b_1\phi)}(a_1).$$

Again, multiplying by two and rearranging, we obtain

$$2^m = W_{\mathrm{Tr}(b_1\phi)}(a_1) - W_{\mathrm{Tr}(b_2\phi)}(a_2) + W_{\mathrm{Tr}((b_1+b_2)\phi)}(a_1 + a_2),$$

which is a contradiction to (4.12) in the definition of a non-covering permutation. This yields that every two different non-zero codewords in $\mathcal{C}_\phi$ do not cover each other, thus $\mathcal{C}_\phi$ is minimal. Conversely, assume that $\mathcal{C}_\phi$ is minimal. Take $a_1, a_2 \in \mathbb{F}_{2^m}$ with $a_1 \neq a_2$ and $b \in \mathbb{F}_{2^m}^*$. Consider the codewords $c_{b,a_1}, c_{b,a_2} \in \mathcal{C}_\phi$, which are non-zero since ϕ does not have affine components. Now, as $\mathcal{C}_\phi$ is minimal, we know that

$$2^{m-1} \neq wt(c_{b,a_2}) - wt(c_{b,a_1}) \text{ and } wt(c_{b,a_2}) \neq 2^{m-1} - wt(c_{b,a_1}).$$

This readily implies that

$$2^m \neq W_{\mathrm{Tr}(b\phi)}(a_1) \pm W_{\mathrm{Tr}(b\phi)}(a_2).$$

Similarly, minimality of $\mathcal{C}_\phi$ applied to the codewords c_{b_1,a_1}, c_{b_2,a_2} for $a_1, a_2, \in \mathbb{F}_{2^m}$ and $b_1, b_2 \in \mathbb{F}_{2^m}^*$ with $b_1 \neq b_2$, gives

$$2^m \neq W_{\mathrm{Tr}(b_1\phi)}(a_1) - W_{\mathrm{Tr}(b_2\phi)}(a_2) + W_{\mathrm{Tr}((b_1+b_2)\phi)}(a_1 + a_2).$$

We have thus proved that ϕ is a non-covering permutation on $\mathbb{F}_{2^m}$. □

In the particular case of power permutations, the non-covering property (4.12) can be reduced to $b_1 = b_2 = 1$, namely, for $\phi : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ given by $\phi(x) = x^d$ with $\gcd(d, n) = 1$,

$$W_{\mathrm{Tr}(b\phi)}(a) = \textstyle\sum_{y\in\mathbb{F}_{2^m}}(-1)^{\mathrm{Tr}(by^d+ay)} = \sum_{x\in\mathbb{F}_{2^m}}(-1)^{\mathrm{Tr}(x^d+a\phi^{-1}(b)^{-1}x)} = W_{\mathrm{Tr}(\phi)}(a\phi^{-1}(b)^{-1}).$$

Thus, for a power permutation is enough to verify (4.11) and, that for every $a_1, a_2 \in \mathbb{F}_{2^m}, b_1, b_2 \in \mathbb{F}_{2^m}^*$ with $b_1 \neq b_2$, we have

$$W_{\mathrm{Tr}(\phi)}(a_1\phi^{-1}(b_1)^{-1}) - W_{\mathrm{Tr}(\phi)}(a_2\phi^{-1}(b_2)^{-1}) + W_{\mathrm{Tr}(\phi)}((a_1+a_2)\phi^{-1}(b_1+b_2)^{-1}) \neq 2^m. \tag{4.16}$$

Example 4.2.12 (Dobbertin's APN permutation). *In $\mathbb{F}_{2^5}$, the permutation ϕ given by $x \mapsto x^{29}$ is an APN permutation since $2^4 + 2^3 + 2^2 + 2 - 1 = 29$ [23]. Moreover, ϕ is also a non-covering permutation. The Walsh spectrum of the component defined by $x \mapsto \mathrm{Tr}(\phi(x))$ is displayed in Table 4.8 The condition (4.11) readily follows since the maximum spectral value is 12. Using computer-based simulations, we have verified that if*

$$W_{\mathrm{Tr}(\phi)}(a_1\phi^{-1}(b_1)^{-1}) = W_{\mathrm{Tr}(\phi)}((a_1 + a_2)\phi^{-1}(b_1 + b_2)^{-1}) = 12$$

for some $a_1, a_2 \in \mathbb{F}_{2^5}, b_1, b_2 \in (\mathbb{F}_{2^5})^*$ then, necessarily, $W_{\mathrm{Tr}(\phi)}(a_2\phi^{-1}(b_2)^{-1})$ is positive and its values belong to $\{0, 4, 8\}$. Hence the left hand side in (4.16) is at most 28, so (4.16) is satisfied. We conclude that ϕ is a non-covering permutation.

Table 4.8: Walsh spectrum of the component $x \mapsto \mathrm{Tr}(\phi(x))$ of Dobbertin's APN permutation $x \mapsto x^{29}$ in $\mathbb{F}_{2^5} = \{v_0, \ldots, v_{31}\}$ ordered lexicographically.

v_0	0	v_8	0	v_{16}	12	v_{24}	-4
v_1	0	v_9	8	v_{17}	-4	v_{25}	4
v_2	4	v_{10}	4	v_{18}	8	v_{26}	8
v_3	4	v_{11}	-4	v_{19}	-8	v_{27}	0
v_4	0	v_{12}	-8	v_{20}	-4	v_{28}	4
v_5	-8	v_{13}	-8	v_{21}	4	v_{29}	4
v_6	-4	v_{14}	4	v_{22}	0	v_{30}	8
v_7	4	v_{15}	4	v_{23}	-8	v_{31}	8

For $m = 5$, non-affine power permutations are either AB or they have the same Walsh spectra of Dobbertin's permuation. As we proved earlier, the former class of permutations is non-covering. The previous example shows that Dobbertin's permuation is non-covering. Thus every non-affine power permutation over $m = 5$ is non-covering.

For small dimensions, one can perform an exhaustive search over all possible exponents d to find non-covering permutations. In $\mathbb{F}_{2^6}$, all power permutations have nonlinearity larger than $\frac{2^6}{3} = 21.333\ldots$ (thus non-covering) except for power permutation with Walsh values in $\{-8, 0, 8, 16, 24\}$ attained, for instance, by $d = 2^5 + 2^4 + 2^3 + 2$. However, the code $\mathcal{C}_\phi$ satisfies $w_{\min} = 20, w_{\max} = 36$, hence $\frac{w_{\min}}{w_{\max}} > 1/2$ and the code is narrow.

For $m = 7$, the nonlinearity of every power permutation is larger than $128/3 = 42.666\ldots$, thus they are non-covering. In $\mathbb{F}_{2^8}$, all power permutations have nonlinearity larger than $2^8/3 = 85.33\ldots$, except for a class of permutations whose Walsh values belong to $\{-32, -16, 0, 16, 96\}$ attained by, for instance, $d = 202$. In this case the code $\mathcal{C}_\phi$ is narrow as $w_{\min} = 80, w_{\max} = 144$.

For $m > 8$, the following results show that low differentially uniform power permutations are non-covering since their nonlinearity is high.

Theorem 4.2.13. *[14] Let ϕ be a power permutation over $\mathbb{F}_{2^m}$ with differential uniformity δ. The nonlinearity $\mathcal{N}_\phi$ of the permutation ϕ satisfies*

$$\mathcal{N}_\phi \geqslant 2^{m-1} - 2^{\frac{3m-4}{4}} \sqrt[4]{\delta}.$$

Corollary 4.2.14. *Let $m > 8$ be an arbitrary integer and $d > 1$ be a non-power of two such that $(d, 2^m - 1) = 1$. Every δ-differentially uniform power permutation ϕ over $\mathbb{F}_{2^m}$ defined by $\phi(x) = x^d$ is non-covering for $\delta \in \{2, 4\}$.*

Proof. By Theorem 4.2.13, it is enough to prove that $2^{m-1} - 2^{\frac{3m-4}{4}} \sqrt[4]{\delta}$ is strictly larger than $2^m/3$ when $m > 8$ and $\delta = 2$ or $\delta = 4$. Note that

$$2^{m-1} - 2^{\frac{3m-4}{4}} \sqrt[4]{\delta} \geqslant 2^{m-1} - 2^{\frac{3m-4}{4}} \sqrt{2}.$$

Now, the number $2^{m-1} - 2^{\frac{3m-4}{4}} \sqrt{2}$ is strictly larger than $2^m/3$ if and only if

$$3 \cdot 2^{m-1} - 3 \cdot 2^{\frac{3m-4}{4}} \sqrt{2} > 2^m. \tag{4.17}$$

Rearranging equation (4.17), this happens if and only if $2^m - 3 \cdot 2^{\frac{3m-4}{4}} \sqrt{2} > 2^{m-1}$, equivalently, $3 \cdot 2^{\frac{3m-4}{4}} \sqrt{2} < 2^{m-1}$. Hence, the assertion is true provided that $3\sqrt{2} < 2^{m/4}$, or, equivalently, $2^m > 3^4 \cdot 2^2$, which is true for $m > 8$. □

For $m \geqslant 6$, all known examples of APN permutations have high nonlinearity, namely, strictly larger than $2^m/3$, thus they are non-covering. So are 4-differentially uniform permutations (without affine components), since most known examples have high nonlinearity over $\mathbb{F}_{2^m}$ (m necessarily even). A particular instance of this fact is the case of quadratic 4-differentially uniform permutations, which attain the best nonlinearity $2^{m-1} - 2^{m/2}$ [14]. A known example of a class of 4-differentially uniform permutations that does not attain an optimal nonlinearity in general [46] is given by permutations of the form

$$x^{2^m-2} + \mathrm{Tr}(x^{(2^m-2)d} + (x^{2^m-2}+1)^d),$$

where $d = 3(2^t+1)$, $2 \leqslant t \leqslant m/2-1$. These permutations have algebraic degree $m-1$ and nonlinearity at least $2^{m-2} - 2^{m/2-1} - 1$. Nevertheless, their nonlinearity is still larger than $2^m/3$ except for some sporadic examples over $\mathbb{F}_{2^6}$, which are however non-covering as verified by computer simulations. This leads to a natural question regarding non-covering permutations, namely, we state the following conjecture.

Conjecture 1. *For $\delta = 2$ or $\delta = 4$, every δ-uniform permutation over $\mathbb{F}_2^m$ without affine components is a non-covering permutation.*

This conjecture is closely related to the question "does every APN and 4-differentially uniform permutation without affine components have good nonlinearity?" If the answer to this question is positive, then Conjecture 1 is true. However, if the answer is negative, then it may happen that Conjecture 1 is still true.

With the characterization of non-covering permutations in terms of the minimality of the associated code $\mathcal{C}_\phi$ given in Theorem 4.2.11, we can now formulate a satisfactory generalization of this concept to non-binary alphabets.

Definition 4.2.15. *A permutation ϕ on $\mathbb{F}_{p^m}$ with $\phi(0) = 0$ is called a* p-ary non-covering permutation *or, simply,* non-covering permutation *provided that the associated linear code $\mathcal{C}_\phi$ is a $2m$-dimensional minimal code.*

The following examples corroborate the existence of non-covering permutations in odd characteristics.

Example 4.2.16. *Working in $\mathbb{F}_{3^4}$, consider the mapping ϕ defined by $\phi(x) = x^{11}$. Note that ϕ is a permutation since $\gcd(11, 3^4-1) = 1$. Since ϕ has no affine components, $\mathcal{C}_\phi$ has dimension 8. Using computer-based simulations, we observed that the minimum weight in $\mathcal{C}_\phi$ is 42, whereas the maximum weight is 60. This yields*

$$\frac{w_{\min}}{w_{\max}} = \frac{7}{10},$$

which is larger than $\frac{2}{3}$, hence the ternary code $\mathcal{C}_\phi$ is minimal. This implies that ϕ is a non-covering permutation.

By computer simulations, it can be observed that several (non-affine) power permutations of the form $\phi(x) = x^d$ over $\mathbb{F}_{3^4}$ give rise to narrow codes $\mathcal{C}_\phi$. Hence, we know that for $d \in \{11, 17, 19, 33, 51, 57, 59, 73\}$, the power permutation x^d is non-covering. Some other non-affine power permutations yield wide minimal codes, for instance, $d = 53, 79$. Nonetheless, this is in general harder to verify computationally.

Similar conclusions are inferred for power permutations on $\mathbb{F}_{3^5}$, namely, we have the following.

Example 4.2.17. *Working in $\mathbb{F}_{3^5}$, consider the mapping ϕ defined by $\phi(x) = x^5$. Note that ϕ is a permutation since $\gcd(5, 3^5 - 1) = 1$. Moreover, ϕ has no affine components, so $\mathcal{C}_\phi$ is 10-dimensional. By computer-based simulations, we observed that the minimum weight in $\mathcal{C}_\phi$ is 144, whereas the maximum weight is 180. This yields*

$$\frac{w_{\min}}{w_{\max}} = \frac{4}{5},$$

which is larger than $\frac{2}{3}$, hence the ternary code $\mathcal{C}_\phi$ is minimal. This implies that ϕ is a non-covering permutation.

By computer simulations, one can observe that almost all (non-affine) power permutations of the form $\phi(x) = x^d$ over $\mathbb{F}_{3^5}$ give rise to narrow codes $\mathcal{C}_\phi$. Indeed, for a non-power of three d such that $1 < d < 242$, $\gcd(d, 242) = 1$ and

$$d \notin \{25, 71, 75, 89, 155, 185, 191, 213, 223, 225\},$$

the power permutation x^d is non-covering.

4.2.2 Revised techniques for $\mathcal{GMM}$

To take up the pursuit of wide minimal codes with larger dimensions, we build on the techniques introduced in Section 3.4, where Boolean functions in the general Maiorana-McFarland class were considered, and apply the tools presented in 4.2. More specifically, adding a function f_2 to a basis of the code $\mathcal{C}_{f_1}$, see (4.8). Thus, we combine codewords associated to functions specified in Theorem 3.4.2 with those given in Theorem 3.4.8 and consider the linear code $\mathcal{C}_f \oplus \mathcal{C}_{D_\gamma f}$, which under certain conditions is a wide minimal code.

Theorem 4.2.18. *Let $r \geqslant 9$ be an odd integer such that $r \neq 11$. Let $\kappa = (r+1)/2$ and $\lambda = (r-1)/2$. Let $U = \{x \in \mathbb{F}_2^\kappa : wt(x) \geqslant 2\}$ and $f \in \mathcal{B}_r$ be the Boolean function defined in (3.6), where μ is the identically one function and ϕ is an injection from $\mathbb{F}_2^\kappa \setminus U$ to $\mathbb{F}_2^\lambda \setminus \{0\}$ such that $\phi(x) = 0$ for any $x \in U$. Let $\gamma = (1_\kappa, 0) \in \mathbb{F}_2^r$, where 1_κ denotes the all-one vector in $\mathbb{F}_2^\kappa$. The code $\mathcal{C}_f \oplus \mathcal{C}_{D_\gamma f}$ is a wide minimal code with parameters $[2^r, r+2, 2^\lambda(\kappa+1)]$.*

Proof. We will only prove the special case when $\kappa \equiv 1 \mod 4$ since the remaining case are quite similar.

For odd κ (see [20, Table II]), the weight of any codeword in $\mathcal{C}_f$ belongs to $S_f = A \cup B$, where A, B are the sets of integers defined by

$$A = \left\{0,\ 2^{r-1},\ 2^{r-1} + 2^{\lambda-1},\ 2^{r-1} - 2^{\lambda-1},\ 2^{r-1} + 2^{\lambda-1}(2^{\kappa} - \kappa - 1)\right\},$$

$$B = \{2^{r-1} + 2^{\lambda-1}(1 + \kappa - 2i) : 1 \leqslant i \leqslant \kappa, i \neq (\kappa + 1)/2\}.$$

For $\kappa \equiv 1 \mod 4$ (see Table 3.16), the weight of any code in $\mathcal{C}_{D_\gamma f}$ belongs to $S_{D_\gamma f} = A' \cup B'$, where A', B' are the sets of integers defined by

$$A' = \{0,\ 2^{r-1},\ 2^{r-1} + 2^{\lambda},\ 2^{r-1} - 2^{\lambda},\ 2^{\lambda}(\kappa + 1)\},$$

$$B' = \{2^{r-1} + 2^{\lambda}(1 + \kappa - 2i) : 1 \leqslant i \leqslant \kappa, i\ even\}.$$

Since $f(x) + D_\gamma f(x) = f(x + \gamma)$ for each $x \in \mathbb{F}_2^r$, the function $f + D_\gamma f$ satisfies the hypotheses in Theorem 3.4.2. Thus for $\kappa \equiv 1 \mod 4$ (see Table 3.8), the weight of any codeword in $\mathcal{C}_{f+D_\gamma f}$ belongs to $S_{f+D_\gamma f} = A'' \cup B'' \cup C''$, where A'', B'', C'' are given by

$$A'' = \{0,\ 2^{r-1},\ 2^{r-1} + 2^{\lambda-1},\ 2^{r-1} - 2^{\lambda-1},\ 2^{r-1} + 2^{\lambda-1}(2^{\kappa} - \kappa - 1)\}$$

$$B'' = \{2^{r-1} + 2^{\lambda-1}(1 + \kappa - 2i) : 1 \leqslant i \leqslant \kappa, i \neq (\kappa + 1)/2,\ i\ odd\}$$

$$C'' = \{2^{r-1} - 2^{\lambda-1}(1 + \kappa - 2i) : 1 \leqslant i \leqslant \kappa,\ i\ even\}.$$

To prove minimality, there are three different cases to consider depending on the possible codewords.

1. Consider the codewords of the form

$$c_1 := (f(x) + v \cdot x)_{x \in \mathbb{F}_2^r} \text{ and } c_2 := (f(x) + f(x + \gamma) + u \cdot x)_{x \in \mathbb{F}_2^r}.$$

   Assume that $c_1 \preceq c_2$ or $c_2 \preceq c_1$, it must be that either

$$wt\,(c_1 + c_2) = wt(c_2) - wt(c_1) \in S_{f+D_\gamma f}$$

   or

$$wt\,(c_1 + c_2) = wt(c_1) - wt(c_2) \in S_{f+D_\gamma f}.$$

   However, from the above discussion on weights

$$wt(c_2) - wt(c_1) \notin S_{f+D_\gamma f} \text{ and } wt(c_1) - wt(c_2) \notin S_{f+D_\gamma f}.$$

   It then holds that $c_1 \npreceq c_2$ and $c_2 \npreceq c_1$ in this case.

2. Consider the codewords

$$c_1 := (f(x+\gamma) + v \cdot x)_{x \in \mathbb{F}_2^r} \text{ and } c_2 := (f(x) + f(x+\gamma) + u \cdot x)_{x \in \mathbb{F}_2^r}.$$

In this case $c_1 + c_2$ belongs to $\mathcal{C}_f$, however,

$$wt(c_2) - wt(c_1) \notin S_f \setminus \{0\} \text{ and } wt(c_1) - wt(c_2) \notin S_f \setminus \{0\},$$

which is possible only if $c_1 \npreceq c_2$ and $c_2 \npreceq c_1$.

3. Lastly, consider the codewords

$$c_1 := (f(x) + v \cdot x)_{x \in \mathbb{F}_2^r} \text{ and } c_2 := (f(x+\gamma) + u \cdot x)_{y \in \mathbb{F}_2^r}.$$

Observe that the sum $c_1 + c_2$ belongs to $\mathcal{C}_{D_\gamma f}$, but

$$wt(c_2) - wt(c_1) \notin S_{D_\gamma f} \setminus \{0\} \text{ and } wt(c_1) - wt(c_2) \notin S_{D_\gamma f} \setminus \{0\},$$

which implies that $c_1 \npreceq c_2$ and $c_2 \npreceq c_1$.

Similarly, we can prove that $c_1 \npreceq c_2$ and $c_2 \npreceq c_1$ when $\kappa \equiv 3 \mod 4$, $\kappa \equiv 0 \mod 4$ and $\kappa \equiv 2 \mod 4$. Thus, the code $\mathcal{C}_f \oplus \mathcal{C}_{D_\gamma f}$ is a minimal code.

By Theorem 3.4.1, $\mathcal{C}_f$ is wide. Clearly, the minimum weight $w_{\min}$ of $\mathcal{C}_f \oplus \mathcal{C}_{D_\gamma f}$ is smaller than or equal to the minimum weight in $\mathcal{C}_f$. Likewise, the maximum weight $w_{\max}$ of $\mathcal{C}_f \oplus \mathcal{C}_{D_\gamma f}$ is at least the maximum weight of $\mathcal{C}_f$. Therefore $\mathcal{C}_f \oplus \mathcal{C}_{D_\gamma f}$ is wide.

Since f and $D_\gamma f$ are two non-affine linearly independent functions whose sum is non-affine, $|\mathcal{C}_f \oplus \mathcal{C}_{D_\gamma f}| = 2^{r+2}$. Moreover, the minimum weight $w_{\min}$ in $\mathcal{C}_f \oplus \mathcal{C}_{D_\gamma f}$ equals the minimum element in $(S_f \cup S_{D_\gamma f} \cup S_{f+D_\gamma f}) \setminus \{0\}$, which is clearly $2^\lambda(\kappa+1)$. Therefore the code $\mathcal{C}_f \oplus \mathcal{C}_{D_\gamma f}$ is a wide minimal binary $[2^r, r+2, 2^\lambda(\kappa+1)]$-code. □

4.3 A generic construction of minimal codes

For the same purpose in mind, that is, the increasing of the dimension of wide minimal codes while preserving both wideness and minimality, we introduce a general construction, denoted by $\mathcal{C}_h^{(\gamma)}$ (see 4.19 below), based on the direct-sum method (Section 4.1), which also connects the techniques introduced in Section 4.2. To achieve minimality of the construction $\mathcal{C}_h^{(\gamma)}$ for a given Boolean function $h = f + g$, the function $f \in \mathcal{B}_r$ will be selected so that it has at least one non-affine derivative $D_\gamma f$ such that $\mathcal{C}_f \oplus \mathcal{C}_{D_\gamma f}$ is a minimal code. The increase in dimension is a consequence of additionally employing (suitable) derivatives of h. The construction of wide minimal codes given in this section will heavily rely on non-covering permutations, which are easily specified in the binary case, so we will focus on the binary case first. The general treatment and observations about this technique for $p > 2$ are discussed in Section 4.4.

Let s be an even integer. Let $f \in \mathcal{B}_r$ be an arbitrary Boolean function[2] and and $g \in \mathcal{B}_s$ be a bent function in $\mathcal{MM}$ as given in (4.5). Consider the direct sum $h = f + g$ and a non-zero element $\gamma \in (\mathbb{F}_2^r)^*$. Define the vectors $c_{u,\alpha,\beta,v} \in \mathbb{F}_2^{2^n}$ as

$$c_{u,\alpha,\beta,v} := (uh(x,y) + h(x+\alpha, y+\beta) + v \cdot (x,y))_{(x,y)\in\mathbb{F}_2^r\times\mathbb{F}_2^s} \tag{4.18}$$

for $u \in \mathbb{F}_2, \alpha \in \{0,\gamma\}, \beta \in \mathbb{F}_2^{s/2} \times \{0\}$, and $v \in \mathbb{F}_2^n$. The set of all of these vectors will be denoted by $\mathcal{C}_h^{(\gamma)}$, namely,

$$\mathcal{C}_h^{(\gamma)} := \left\{ c_{u,\alpha,\beta,v} : u \in \mathbb{F}_2, \alpha \in \{0,\gamma\}, \beta \in \mathbb{F}_2^{s/2} \times \{0\}, v \in \mathbb{F}_2^n \right\}. \tag{4.19}$$

Lemma 4.3.1. *Let $f \in \mathcal{B}_r$ be a non-affine function and $\gamma \in (\mathbb{F}_2^r)^*$ such that $D_\gamma f$ is nonaffine. Let g be a bent function in $\mathcal{B}_s$ defined by (4.5). If h is the direct sum of f and g, then the set $\mathcal{C}_h^{(\gamma)}$ defined in (4.19) is a binary linear code with parameters $[2^n, n + \frac{s}{2} + 2]$.*

Proof. To prove that $\mathcal{C}_h^{(\gamma)}$ is a linear subspace of $\mathbb{F}_2^{2^n}$, take two different vectors in $\mathcal{C}_h^{(\gamma)}$, say, $c_{u_1,\alpha_1,\beta_1,v_1}$ and $c_{u_2,\alpha_2,\beta_2,v_2}$ Using the definition of g, note that the sum $g(y+\beta_1) + g(y+\beta_2)$ equals $g(y) + g(y+\beta_1+\beta_2)$. Moreover, given that $\alpha_1, \alpha_2 \in \{0,\gamma\}$, the sum $f(x+\alpha_1) + f(x+\alpha_2)$ is equal to $f(x) + f(x+\alpha_1+\alpha_2)$. These two facts imply that

$$h(x+\alpha_1, y+\beta_1) + h(x+\alpha_2, y+\beta_2) = f(x) + g(y) + f(x+\alpha_1+\alpha_2) + g(y+\beta_1+\beta_2).$$

Replacing the corresponding values of $f + g$ by h, we get

$$h(x+\alpha_1, y+\beta_1) + h(x+\alpha_2, y+\beta_2) = h(x,y) + h(x+\alpha_1+\alpha_2, y+\beta_1+\beta_2).$$

From the last equality, the sum of the vectors $c_{u_1,\alpha_1,\beta_1,v_1}$ and $c_{u_2,\alpha_2,\beta_2,v_2}$ is equal to

$$(u_1+u_2+1)h(x,y) + h(x+\alpha_1+\alpha_2, y+\beta_1+\beta_2) + (v_1+v_2)\cdot(x,y),$$

[2] As before, the space $\mathbb{F}_2^r \times \mathbb{F}_2^s$ will be identified with $\mathbb{F}_2^n$ so that $n = r + s$.

i.e. $c_{u_1,\alpha_1,\beta_1,v_1} + c_{u_2,\alpha_2,\beta_2,v_2} = c_{u_1+u_2+1,\alpha_1+\alpha_2,\beta_1+\beta_2,v_1+v_2}$. Thus, the sum of the corresponding vectors lies in $\mathcal{C}_h^{(\gamma)}$. This proves that $\mathcal{C}_h^{(\gamma)}$ is a linear subspace of $\mathbb{F}_2^{2^n}$.

The function h is clearly non-affine since it is the direct sum of non-affine functions. In general, for $\alpha \in \{0,\gamma\}$ and $\beta \in \mathbb{F}_2^{s/2} \times \{0\}$,

$$D_{(\alpha,\beta)}h \text{ is affine if and only if } \alpha = 0 \text{ and } \beta = 0. \tag{4.20}$$

To prove this, observe that

$$h(x,y) + h(x+\alpha, y+\beta) = f(x) + f(x+\alpha) + g(y) + g(y+\beta),$$

hence $D_{(\alpha,\beta)}h$ is affine if and only if both $f(x) + f(x+\alpha)$ and $g(y) + g(y+\beta)$ are affine. Since $D_\gamma f$ is non-affine by hypothesis and $D_\beta g = \phi(y^{(2)}) \cdot \beta$ is a non-affine Boolean function as ϕ does not have affine components, the only possible way that these two functions are affine, arises when $\alpha = 0$ and $\beta = 0$. Considering again the sum of two elements in $\mathcal{C}_h^{(\gamma)}$ and plugging the values $\alpha = \alpha_1+\alpha_2, \beta = \beta_1+\beta_2$ into (4.20), we conclude that $c_{u_1+u_2+1,\alpha_1+\alpha_2,\beta_1+\beta_2,v_1+v_2}$ is the zero codeword if and only if $u_1+u_2 = 0$, $\alpha_1+\alpha_2 = 0$, $\beta_1+\beta_2 = 0$ and $v_1+v_2 = 0$. Thus, there are $2^{n+\frac{s}{2}+2}$ many different elements, i.e., $\dim(\mathcal{C}_h^{(\gamma)}) = n + \frac{s}{2} + 2$. □

Theorem 4.3.2 (The generic construction)**.** *Let n, r, s be three integers such that $s > 2$ is even and $r + s = n$. Let $f \in \mathcal{B}_r$ be a non-affine function and $\gamma \in (\mathbb{F}_2^r)^*$ with $D_\gamma f$ non-affine such that $\mathcal{C}_f \oplus \mathcal{C}_{D_\gamma f}$ is a minimal code. Let $g \in \mathcal{B}_s$ be a bent function in $\mathcal{MM}$, defined in (4.5) so that $g(y_1, y_2) = y_1 \cdot \phi(y_2)$, where ϕ is a non-covering permutation on $\mathbb{F}_2^{s/2}$. Consider the direct sum h of the functions f and g. The code $\mathcal{C}_h^{(\gamma)}$ defined in (4.19) is a minimal linear code with parameters $[2^n, n + \frac{s}{2} + 2]$. Moreover, if $\mathcal{C}_{D_\gamma f}$ is wide, then so is $\mathcal{C}_h^{(\gamma)}$.*

Proof. Lemma 4.4.7 implies that $\mathcal{C}_h^{(\gamma)}$ is a linear binary code with parameters $[2^n, n + \frac{s}{2} + 2]$. Since $\phi(0)$ is null, the image of $\beta \in \mathbb{F}_2^{s/2} \times \{0\}$ under g is null, too. We will use this fact throughout the proof without further mentioning it.

For functions $\mathfrak{h} : \mathbb{F}_2^n \to \mathbb{F}_2$, corresponding to codewords in $\mathcal{C}_h^{(\gamma)}$, let $A_\mathfrak{h} : \mathbb{F}_2^r \to \mathbb{F}_2$ and $B_\mathfrak{h} : \mathbb{F}_2^s \to \mathbb{F}_2$ denote the restrictions of $\mathfrak{h}$ to the x and y coordinates, respectively. That is, for a function

$$\mathfrak{h}(x,y) = uh(x,y) + h(x+\alpha, y+\beta) + v \cdot (x,y),$$

$A_\mathfrak{h}(x) = uf(x) + f(x+\alpha) + v \cdot (x,0)$ and $B_\mathfrak{h}(y) = ug(y) + g(y+\beta) + v \cdot (0,y)$. Consider two distinct non-zero codewords in $\mathcal{C}_h^{(\gamma)}$, say,

$$\mathbf{c}_1 := c_{u_1,\alpha_1,\beta_1,v_1} = (\mathfrak{h}_1(x,y))_{(x,y)\in\mathbb{F}_2^n}$$

and

$$\mathbf{c}_2 := c_{u_2,\alpha_2,\beta_2,u_2} = (\mathfrak{h}_2(x,y))_{(x,y)\in\mathbb{F}_2^n}.$$

If $A_{\mathfrak{h}_1}$ and $A_{\mathfrak{h}_2}$ are non-zero and distinct, then puncturing at the y-coordinates gives two non-zero distinct codewords in $\mathcal{C}_f \oplus \mathcal{C}_{D_\gamma f}$, which is minimal by hypothesis. Thus, neither $\mathbf{c}_1 \preceq \mathbf{c}_2$ nor $\mathbf{c}_2 \preceq \mathbf{c}_1$. Similarly, if $B_{\mathfrak{h}_1}$ and $B_{\mathfrak{h}_2}$ are non-zero and distinct, then puncturing at x-coordinates yields distinct non-zero vectors of the form

$$(u_1 g(x) + g(y+\beta_1) + v_1 \cdot (0,y) + u_1 f(0) + f(\alpha_1))_{y\in\mathbb{F}_2^s}$$

and

$$(u_2 g(x) + g(y+\beta_2) + v_2 \cdot (0,y) + u_2 f(0) + f(\alpha_2))_{y\in\mathbb{F}_2^s}.$$

The fact that $\phi(y)$ is non-covering implies that these (nonzero) vectors do not cover each other by Lemmas 4.2.2 and 4.2.6. Thus, neither $\mathbf{c}_1 \preceq \mathbf{c}_2$ nor $\mathbf{c}_2 \preceq \mathbf{c}_1$, in this case.

Using the assumption that $\mathbf{c}_1, \mathbf{c}_2$ are distinct non-zero codewords and the above paragraph, there are only two cases to be considered:

- $A_{\mathfrak{h}_1} = A_{\mathfrak{h}_2}$ (non-zero), $B_{\mathfrak{h}_i} = 0$ and $B_{\mathfrak{h}_{(i \bmod 2)+1}} \neq 0$ for exactly one $i \in \{1,2\}$, or
- $B_{\mathfrak{h}_1} = B_{\mathfrak{h}_2}$ (non-zero), $A_{\mathfrak{h}_i} = 0$ and $A_{\mathfrak{h}_{(i \bmod 2)+1}} \neq 0$ for exactly one $i \in \{1,2\}$.

Let us prove the first item only since the other case can be proved *mutatis mutandis*. Suppose then that $A_{\mathfrak{h}_1} = A_{\mathfrak{h}_2}$ with $A_{\mathfrak{h}_1} \neq 0$, $B_{\mathfrak{h}_i} = 0$ and $B_{\mathfrak{h}_{(i \bmod 2)+1}} \neq 0$ for exactly one $i \in \{1,2\}$. Without loss of generality, assume that $i = 1$. Take $x_0, x_0' \in \mathbb{F}_2^r$ and $y_0 \in \mathbb{F}_2^s$ with $A_{\mathfrak{h}_1}(x_0) = 1$, $A_{\mathfrak{h}_1}(x_0') = 0$ and $B_{\mathfrak{h}_2}(y_0) = 1$, which exist as $A_{\mathfrak{h}_1}, B_{\mathfrak{h}_2}$ are non-constant. Now, the (x_0, y_0) coordinate of $\mathbf{c}_1$ equals

$$A_{\mathfrak{h}_1}(x_0) + B_{\mathfrak{h}_1}(y_0) = A_{\mathfrak{h}_1}(x_0) = 1$$

whereas the (x_0, y_0) coordinate of $\mathbf{c}_2$ equals $A_{\mathfrak{h}_1}(x_0) + B_{\mathfrak{h}_2}(y_0) = 0$, this gives $\mathbf{c}_1 \not\preceq \mathbf{c}_2$. The (x_0', y_0) coordinate of $\mathbf{c}_1$ equals

$$A_{\mathfrak{h}_1}(x_0') + B_{\mathfrak{h}_1}(y_0) = A_{\mathfrak{h}_1}(x_0') = 0$$

whereas the (x_0', y_0) coordinate of $\mathbf{c}_2$ equals $A_{\mathfrak{h}_1}(x_0') + B_{\mathfrak{h}_2}(y_0) = 1$. This means that $\mathbf{c}_2 \not\preceq \mathbf{c}_1$. We have proved that distinct non-zero codewords in $\mathcal{C}_h^{(\gamma)}$ do not cover each other, i.e., $\mathcal{C}_h^{(\gamma)}$ is minimal.

To show the wideness of $\mathcal{C}_h^{(\gamma)}$, suppose that $\mathcal{C}_{D_\gamma f}$ is wide. Note that a codeword corresponding to a function

$$\mathfrak{h}(x,y) = uh(x,y) + h(x+\alpha, y+\beta) + v \cdot (x,y)$$

such that $B_\mathfrak{h}(y)$ is identically zero has weight $2^s wt(A_\mathfrak{h}(x))$. Moreover, there is a natural correspondence between the codewords of $\mathcal{C}_{D_\gamma f}$ and the codewords of $\mathcal{C}_h^{(\gamma)}$ with $u \neq 0$ and $B_\mathfrak{h}(y)$ identically zero. If $\mathcal{C}_{D_\gamma f}$ is wide, then it readily follows that $\frac{w_{\min}}{w_{\max}} \leqslant \frac{1}{2}$ for $\mathcal{C}_h^{(\gamma)}$. □

4.3.1 Explicit wide minimal codes

At this point, it is not clear that there are functions $f \in \mathcal{B}_r$ and $g \in \mathcal{B}_s$ satisfying the conditions in Theorem 4.3.2. To get explicit families of wide minimal codes thereby, we must study the existence of suitable functions f and its derivatives as well as the specification of non-covering permutations.

A priori, these initial conditions may seem hard to satisfy, however, the results given in Theorem 3.2.7 essentially provide classes of Boolean functions suitable for this purpose. In fact, it can be proved that the functions given in Example 3.2.8 and 3.2.9 are instances of functions such that $\mathcal{C}_f \oplus \mathcal{C}_{D_\gamma f}$ is a minimal code and $\mathcal{C}_{D_\gamma f}$ is wide.

The importance of Theorem 4.3.2 lies in the fact that once a suitable function f and the corresponding $D_\gamma f$ are specified, we can define a bent function g in the $\mathcal{MM}$ class using an arbitrary non-covering permutation ϕ. Therefore, a huge class of wide binary linear codes can be derived from a single Boolean function f. These codes are not necessarily equivalent since one can, for instance, employ permutations ϕ of different algebraic degree (or Walsh spectrum). The following example illustrates the possibility of getting non-equivalent codes using different permutations ϕ. Conversely, for a fixed non-covering permutation, the use of different functions f gives rise to several wide minimal codes.

For a positive integer r, let us identify the vectors in $\mathbb{F}_2^r$ with the integers $0, \ldots, 2^r - 1$, via their binary representation lexicographically ordered, e.g., for $r = 6$, $(0,0,0,0,0,1) \in \mathbb{F}_2^6$ is identified with 1.

Fact 1. The function f in $\mathcal{B}_6$, whose support is given by

$$\Delta = \{4, 7, 8, 18, 21, 22, 24, 28, 35, 36, 42, 51, 54, 60\},$$

together with its derivative $D_\gamma f$ at direction $\gamma = (1,0,1,1,0,1)$ have the property that $\mathcal{C}_f \oplus \mathcal{C}_{D_\gamma f}$ is minimal and $\mathcal{C}_{D_\gamma f}$ is wide.

Proposition 4.3.3. *Let $f \in \mathcal{B}_6$ and its derivative $D_\gamma f$ be as in Fact 1. Consider any bent function $g \in \mathcal{B}_{10}$ of the form (4.5) whose underlying permutation ϕ is non-covering. Then, the associated code $\mathcal{C}_h^{(\gamma)}$ is a wide minimal linear code with parameters $[2^{16}, 23]$.*

Proof. The result follows immediately from Theorem 4.4.8. □

To compute the minimum distance in the resulting code of the previous proposition, the permutation ϕ must be specified. We do so in the following example.

Example 4.3.4. *In Proposition 4.3.3, if we consider the cubic AB permutation $\phi : \mathbb{F}_{2^5} \to \mathbb{F}_{2^5}$ given by $\phi(y) = y^7$ as the underlying permutation for g, then $\mathcal{C}_h^{(\gamma)}$ is a wide minimal code with minimum distance $w_{\min} = 24576 = 3 \cdot 2^{13}$ and $w_{\max} = 49152 = 3 \cdot 2^{14}$. Thus, $\mathcal{C}_h^{(\gamma)}$ has parameters $[2^{16}, 23, 3 \cdot 2^{13}]$ and ratio $w_{\min}/w_{\max} = 1/2$. On the other hand, if we consider the inverse permutation $\phi : \mathbb{F}_{2^5} \to \mathbb{F}_{2^5}$ given by $\phi(y) = y^{30}$ to define g, then $\mathcal{C}_h^{(\gamma)}$ is a wide minimal linear code with parameters $[2^{16}, 23, 5 \cdot 2^{12}]$, $w_{\max} = 49152 = 3 \cdot 2^{14}$ and ratio $w_{\min}/w_{\max} = 5/12$.*

Generally speaking, since AB permutations (m odd) and the inverse permutation are non-covering for $m \geqslant 5$, non-covering permutations exist for every integer m with $m \geqslant 5$. Employing a fixed function $f \in \mathcal{B}_r$ and a fixed derivative $D_\gamma f$ such that $\mathcal{C}_f \oplus \mathcal{C}_{D_\gamma f}$ is minimal and $\mathcal{C}_{D_\gamma f}$ is wide (e.g., the functions in Example 3.2.8, Example 3.2.9, Fact 1, or, Fact 2 below), each of these permutations specifies a wide minimal $[2^{r+10}, 17 + r]$- code $\mathcal{C}_h^{(\gamma)}$.

If the non-covering permutation ϕ has a simple Walsh spectrum (for instance AB permutations), then the weight distribution of $\mathcal{C}_h^{(\gamma)}$ can be obtained once we know the Walsh spectra of the underlying functions f and $D_\gamma f$. To precisely describe it, we will use the notation introduced for describing the weight distributions of the direct sum method presented in Section 4.1, namely, the notation introduced in (4.4) and the paragraph following it.

Since we will be dealing with two Walsh spectra, corresponding to f and $D_\gamma f$, we will reserve the symbols W_f, W_f^{abs}, $\mathfrak{m}_\rho^+$, $\mathfrak{m}_\rho^-$ and $\mathfrak{m}_0$, to refer to the values associated to f and the symbols $W_{D_\gamma f}$, $W_{D_\gamma f}^{\text{abs}}$, $\mathfrak{n}_{\rho'}^+$, $\mathfrak{n}_{\rho'}^-$ and $\mathfrak{n}_0$, to refer to the values attached to $D_\gamma f$.

Theorem 4.3.5. *Use the same notation as in Theorem 4.3.2. Suppose that $s/2$ is an odd integer and $\phi : \mathbb{F}_2^{s/2} \to \mathbb{F}_2^{s/2}$ is an AB permutation. If the maximum value $\mathcal{W}_{\max}$ in the Walsh spectrum of $D_\gamma f$ is at at least $2^{(2r-s/2+1)/2}$, then the minimum distance of $\mathcal{C}_h^{(\gamma)}$ is equal to $2^s w_{\min}^\gamma$, where $w_{\min}^\gamma$ is the minimum weight* *in* $\mathcal{C}_{D_\gamma f}$. *In particular, if* $\mathcal{C}_f \oplus \mathcal{C}_{D_\gamma f}$ *is minimal and* $\mathcal{C}_{D_\gamma f}$ *is wide, then the code* $\mathcal{C}_h^{(\gamma)}$ *is also a wide minimal linear code with parameters* $[2^n, n+s/2+2, 2^s w_{min}^{\gamma}]$.

Proof. To prove the claim on the minimum distance, we will derive the possible weights of codewords in $\mathcal{C}_h^{(\gamma)}$. For simplicity, consider only codewords in $\mathcal{C}_h^{(\gamma)}$ whose underlying Boolean function is not linear. Note that each such codeword $c_{u,\alpha,\beta,v}$ corresponds to any of the following four types:

$$u = 1, \beta = 0, \alpha \neq 0;\ \ u = 1, \beta \neq 0, \alpha = 0;\ \ u = 1, \beta \neq 0, \alpha \neq 0;\ \ u = 0.$$

The weights of these codewords can be easily computed using known properties of the direct sum. These weights belong, respectively, to the sets

$$\{2^{n-1} \pm 2^{s-1} w : w \in W_{D_\gamma f}\},\ \{2^{n-1} \pm 2^{\frac{s+s/2-1}{2}+r}\},\ \{2^{n-1} \pm 2^{\frac{s+s/2-1}{2}} \rho' : \rho' \in W_{D_\gamma f}^{\text{abs}}\},$$

$$\{2^{n-1} \pm 2^{\frac{s}{2}-1} \rho : \rho \in W_f^{\text{abs}}\}.$$

Within these sets, consider the elements smaller than 2^{n-1}, that is, $2^{n-1} - 2^{\frac{s+s/2-1}{2}+r}$ together with

$$2^{n-1} - 2^{s-1} w,\ 2^{n-1} - 2^{\frac{s+s/2-1}{2}} \rho',\ 2^{n-1} - 2^{s/2-1} \rho,$$

for each positive element $w \in W_{D_\gamma f}$, $\rho \in W_f^{\text{abs}}$ and $\rho' \in W_{D_\gamma f}^{\text{abs}}$. Since ρ, ρ' are both smaller than 2^r, we have that for every $\rho \in W_f^{\text{abs}}$ and $\rho' \in W_{D_\gamma f}^{\text{abs}}$

$$2^{s/2-1} \rho < 2^{s/2-1+r} < 2^{(s+s/2-1)/2+r} \text{ and } 2^{(s+s/2-1)/2} \rho' < 2^{(s+s/2-1)/2+r}.$$

By hypothesis, $2^{(s+s/2-1)/2+r} \leqslant 2^{s-1} \mathcal{W}_{\max}$, so the minimum weight of $\mathcal{C}_h^{(\gamma)}$ is $2^{n-1} - 2^{s-1} W_{D_\gamma f}(u_M) = 2^s w_{\min}^{\gamma}$. The last part of the statement follows directly from Theorem 4.3.2. □

A simple description of the weight distribution of the code $\mathcal{C}_h^{(\gamma)}$ in Theorem 4.3.5 can be specified knowing that the possible values for weights are distinct from each other (otherwise, frequencies of the repeated entries in the left column in Table 4.9 must be summed). That is, if for every $w \in W_{D_\gamma f}, \rho' \in W_{D_\gamma f}^{\text{abs}}$, $\rho \in W_f^{\text{abs}}$ we have $2^{(s/2-1)/2} w \neq \rho'$, $\rho' \neq 2^{(2r-s/2+1)/2}$, $2^{(s/2+1)/2} \rho' \neq \rho$ and $\rho \neq 2^{s/2} w$, then the weight distribution of the code $\mathcal{C}_h^{(\gamma)}$ can be fully determined and is given in Table 4.9.

Note that the number of non-zero weights given in Table 4.9 (left column) depends on the cardinalities of W_f^{abs} and $W_{D_\gamma f}^{\text{abs}}$. In particular, the code $\mathcal{C}_h^{(\gamma)}$ in Theorem 4.3.5 has at most $4|W_{D_\gamma f}^{\text{abs}}| + 2|W_f^{\text{abs}}| + 3$ non-zero weights.

Table 4.9: Weight distribution of $\mathcal{C}_h^{(\gamma)}$ in Theorem 4.3.5 for $s/2$ odd and an AB permutation $\phi : \mathbb{F}_2^{s/2} \to \mathbb{F}_2^{s/2}$, where ρ runs over W_f^{abs} and ρ' runs over $W_{D_\gamma f}^{\text{abs}}$.

Weight w	Number of codewords
$2^{n-1} - 2^{s-1}\rho'$	$\mathfrak{n}_{\rho'}^{+}$
$2^{n-1} - 2^{\frac{s+s/2-1}{2}+r}$	$(2^{s/2}-1)(2^{s/2-2} + 2^{(s/2-3)/2})$
$2^{n-1} - 2^{\frac{s+s/2-1}{2}}\rho'$	$(2^{s/2}-1)((2^{s/2-2} + 2^{(s/2-3)/2})\mathfrak{n}_{\rho'}^{+} + (2^{s/2-2} - 2^{(s/2-3)/2})\mathfrak{n}_{\rho'}^{-})$
$2^{n-1} - 2^{s/2-1}\rho$	$2^{s/2+1}((2^{s-1} + 2^{s/2-1})\mathfrak{m}_{\rho}^{+} + (2^{s-1} - 2^{s/2-1})\mathfrak{m}_{\rho}^{-})$
2^{n-1}	$2^n + 2^{n-1} + 2^{s/2+1}\mathfrak{m}_0 + (2^{s/2}-1)2^{s/2-1} + (2^{s/2-1}+1)\mathfrak{n}_0 - 1$
$2^{n-1} + 2^{s/2-1}\rho$	$2^{s/2+1}((2^{s-1} - 2^{s/2-1})\mathfrak{m}_{\rho}^{+} + (2^{s-1} + 2^{s/2-1})\mathfrak{m}_{\rho}^{-})$
$2^{n-1} + 2^{\frac{s+s/2-1}{2}}\rho'$	$(2^{s/2}-1)((2^{s/2-2} - 2^{(s/2-3)/2})\mathfrak{n}_{\rho'}^{+} + (2^{s/2-2} + 2^{(s/2-3)/2})\mathfrak{n}_{\rho'}^{-})$
$2^{n-1} + 2^{\frac{s+s/2-1}{2}+r}$	$(2^{s/2}-1)(2^{s/2-2} - 2^{(s/2-3)/2})$
$2^{n-1} + 2^{s-1}\rho'$	$\mathfrak{n}_{\rho'}^{-}$
0	1

Fact 2. The function $f \in \mathcal{B}_6$ whose support is given by

$$\Delta = \{3, 5, 7, 11, 12, 24, 27, 31, 34, 37, 51, 52\}$$

and its derivative $D_\gamma f$ at direction $\gamma = (0, 1, 1, 0, 1, 0)$ are such that the associated codes $\mathcal{C}_{D_\gamma f}$ and $\mathcal{C}_f \oplus \mathcal{C}_{D_\gamma f}$ are wide and minimal. Moreover, the Walsh spectra of f and $D_\gamma f$ satisfy

$$W_f(b) \in \{-16, -12, -8, -4, 0, 4, 8, 12, 40\}, W_{D_\gamma f}(b) \in \{-24, -8, 0, 8, 24\},$$

for every $b \in \mathbb{F}_2^6$.

Proposition 4.3.6. *Let $f \in \mathcal{B}_6$ and $D_\gamma f$ be as in Fact 2. Consider any bent function $g \in \mathcal{B}_{10}$ as in (4.5) whose underlying permutation is non-covering. The code $\mathcal{C}_h^{(\gamma)}$ is a wide minimal linear code with parameters $[2^{16}, 23]$. Moreover, if ϕ is an AB permutation on $\mathbb{F}_2^5$, then $\mathcal{C}_h^{(\gamma)}$ has parameters $[2^{16}, 23, 2^{10} \cdot 20]$ and its weight distribution is displayed in Table 4.10.*

Proof. The result follows at once from Theorem 4.3.2, Theorem 4.3.5 and Table 4.9. □

Note that for the function f in Fact 2, the cardinalities of $W_{D_\gamma f}^{\text{abs}}$ and W_f^{abs} are 2 and 5, respectively. Thus, there are at most $4|W_{D_\gamma f}^{\text{abs}}| + 2|W_f^{\text{abs}}| + 3 = 21$ distinct weights in $\mathcal{C}_h^{(\gamma)}$ when ϕ is an AB on $\mathbb{F}_2^5$ (see Table 4.9). In this case, it can be

Table 4.10: Weight distribution of $\mathcal{C}_h^{(\gamma)}$ in Theorem 4.3.6 for any AB permutation $\phi : \mathbb{F}_2^5 \to \mathbb{F}_2^5$.

Weight w	Number of codewords A_w
$2^{15} - 2^{10} + 2^5 \cdot 26$	$2^{16} \cdot 3$
$2^{15} - 2^{10} + 2^5 \cdot 28$	$2^{16} \cdot 10$
$2^{15} - 2^{10} + 2^5 \cdot 30$	$2^{16} \cdot 13$
$2^{15} - 2^{10} + 2^5 \cdot 34$	$2^{16} \cdot 13$
$2^{15} - 2^{10} + 2^5 \cdot 36$	$2^{16} \cdot 5$
$2^{15} - 2^{10} + 2^5 \cdot 38$	$2^{16} \cdot 3$
$2^{15} - 2^{10} + 2^5 \cdot 12$	$2^6(2^9 + 2^4)$
$2^{15} - 2^{10} + 2^5 \cdot 40$	$2^6(2^9 + 2^4)$
$2^{15} + 2^{10} - 2^5 \cdot 12$	$2^6(2^9 - 2^4)$
$2^{15} + 2^{10} - 2^5 \cdot 40$	$2^6(2^9 - 2^4)$
$2^{15} + 2^8 \cdot 20 - 2^{13}$	$(2^5 - 1)((2^3 + 2) + (2^3 - 2) \cdot 3)$
$2^{15} + 2^8 \cdot 28 - 2^{13}$	$(2^5 - 1)((2^3 + 2) \cdot 21 + (2^3 - 2) \cdot 7)$
$2^{15} + 2^8 \cdot 36 - 2^{13}$	$(2^5 - 1)((2^3 + 2) \cdot 7 + (2^3 - 2) \cdot 21)$
$2^{15} + 2^8 \cdot 44 - 2^{13}$	$(2^5 - 1)((2^3 + 2) \cdot 3 + (2^3 - 2))$
$2^{10} \cdot 20$	1
$2^{10} \cdot 28$	21
$2^{10} \cdot 36$	7
$2^{10} \cdot 44$	3
$2^{15} - 2^{13}$	$(2^5 - 1)(2^3 + 2)$
$2^{15} + 2^{13}$	$(2^5 - 1)(2^3 - 2)$
2^{15}	5160943
0	1

proved that all of these weights are distinct, so there are exactly 21 non-zero weights, which is in accordance with Table 4.10.

The minimum distance of the codes built using the construction in Theorem 4.3.5 is subjected to the minimum distance of the corresponding derivative code $\mathcal{C}_{D_\gamma f}$. In the following theorems, this constraint is removed by considering the functions in $\mathcal{GMM}$ from Theorem 3.4.1 together with a suitable non-covering ϕ with high non-linearity.

Theorem 4.3.7. *Let r, s be three positive integers such that $r \geqslant 9$ is odd and $r \neq 11$, s is even with $s \geqslant 6$. For $\kappa = (r+1)/2$ and $\lambda = (r-1)/2$, let $f \in \mathcal{B}_r$ be defined as in Theorem 3.4.1. Let $g \in \mathcal{B}_s$ be a bent function in $\mathcal{MM}$, as in (4.2.4), whose underlying permutation ϕ is non-covering and it satisfies*

$$\mathcal{N}_\phi \geqslant 2^{\frac{s}{2}-\frac{(r+1)}{2}}(\frac{r+1}{2}+1).$$

Let $\mathcal{C}_h^{(\gamma)}$ be as in (4.19), where h is the direct sum of f and g and $\gamma = (1_\kappa, 0) \in \mathbb{F}_2^r$. The linear code $\mathcal{C}_h^{(\gamma)}$ is a wide minimal code with parameters

$$\left[2^n,\ n+\frac{s}{2}+2,\ 2^{s+\frac{r-1}{2}}\left(\frac{r+1}{2}+1\right)\right].$$

Proof. Since f is defined as in Theorem 3.4.1, the derivative $D_\gamma f$ is nonaffine. By Theorem 4.2.18, $\mathcal{C}_f \oplus \mathcal{C}_{D_\gamma f}$ is a minimal code. Furthermore, by Theorem 3.4.8, we have that $\mathcal{C}_{D_\gamma f}$ is wide. Therefore, combining this and Theorem 4.3.2, the linear code $\mathcal{C}_h^{(\gamma)}$ is a wide and minimal.

For the minimum weight of $\mathcal{C}_h^{(\gamma)}$, there are five cases to consider according to the possible values of a non-zero codeword $c_{u,\alpha,\beta,v}$ in $\mathcal{C}_h^{(\gamma)}$. Let us represent each vector v in $\mathbb{F}_2^n = \mathbb{F}_2^r \times \mathbb{F}_2^s$ by $v = (v^x, v^y) \in \mathbb{F}_2^r \times \mathbb{F}_2^s$.

Case $u = 0$. Since g is a bent function in $\mathbb{F}_2^s$, Lemma 4.1.1 implies that $\mathcal{N}_h > 2^{n-2}$. Hence, $wt(c_{u,\alpha,\beta,v}) \geqslant \mathcal{N}_h > 2^{n-2} > 2^{s+(r-1)/2}((r+1)/2+1)$ for each $v \in \mathbb{F}_2^n$, where the last inequality holds due to $r \geqslant 9$.

Case $u = 1, \alpha = 0, \beta = 0$. In this case, the underlying function of the codeword is a non-zero linear function so that its weight is 2^{n-1}.

Case $u = 1, \alpha = 0, \beta \neq 0$. There are two sub-cases to analyze.

(i) If $v^x \neq 0$, then the codeword $c_{u,\alpha,\beta,v}$ can be written as

$$(g(y) + g(y+\beta) + v^x \cdot x + v^y \cdot y)_{(x,y)\in\mathbb{F}_2^n},$$

hence its weight is 2^{n-1}.

(ii) If $v^x = 0$, then the weight of $c_{u,\alpha,\beta,v}$ can be expressed as

$$wt((g(y) + g(y + \beta) + v^y \cdot y)_{(x,y)\in\mathbb{F}_2^n}),$$

which is equal to

$$2^r wt((g(y) + g(y + \beta) + v^y \cdot y)_{y\in\mathbb{F}_2^s})$$

since there is no dependence on the variable x. This can be turned into

$$2^r wt((\phi(y_2) \cdot \beta + v^y \cdot y)_{y\in\mathbb{F}_2^s}),$$

hence $wt(c_{u,\alpha,\beta,v}) \geqslant 2^{r+s/2}\mathcal{N}_\phi$. By hypothesis, $\mathcal{N}_\phi \geqslant 2^{\frac{s}{2}-\frac{(r+1)}{2}}(\frac{r+1}{2}+1)$. This yields

$$wt(c_{u,\alpha,\beta,v}) \geqslant 2^{r+s/2}(2^{\frac{s}{2}-\frac{(r+1)}{2}}(\frac{r+1}{2}+1)) = 2^{s+(r-1)/2}((r+1)/2+1).$$

Case $u = 1, \alpha \neq 0, \beta = 0$**.** Again, there are two sub-cases to consider.

(i) If $v^y \neq 0$, then the codeword $c_{u,\alpha,\beta,v}$ is balanced since it equals

$$(f(x) + f(x + \alpha) + v^x \cdot x + v^y \cdot y)_{(x,y)\in\mathbb{F}_2^n}.$$

(ii) If $v^y = 0$, then the weight of $c_{u,\alpha,\beta,v}$ is equal to $2^s wt((f(x) + f(x + \alpha) + v^x \cdot x)_{x\in\mathbb{F}_2^r})$ so

$$wt(c_{u,\alpha,\beta,v}) \geqslant 2^{s+(r-1)/2}((r+1)/2+1)$$

since the code $\mathcal{C}_{D_\gamma f}$ has minimum distance $2^\lambda(\kappa+1)$ by Theorem 3.4.8. Equality holds if and only if $(f(x) + f(x + \alpha) + v^x \cdot x)_{x\in\mathbb{F}_2^r}$ is a minimum weight codeword in $\mathcal{C}_{D_\gamma f}$.

Case $u = 1, \alpha \neq 0, \beta \neq 0$**.** From Lemma 4.1.1, the weight of $c_{u,\alpha,\beta,v}$ can be split into the sum

$$2^r wt(D_\beta g + l_{v^y}) + 2^s wt(D_\alpha f + l_{v^x}) - 2wt(D_\alpha f + l_{v^x})wt(D_\beta g + l_{v^y}).$$

Depending on the weight of $D_\beta g + l_{v^y}$, there are three further sub-cases to investigate. For this last part, we will denote by $w^\gamma_{\min}$ the number $2^\lambda(\kappa+1)$, which is the minimum distance in $\mathcal{C}_{D_\gamma f}$

(i) If $wt(D_\beta g + l_{v^y}) = 2^{s-1}$, then the codeword $c_{u,\alpha,\beta,v}$ is balanced, so that $wt(c_{u,\alpha,\beta,v}) = 2^{r+s-1}$.

(ii) If $wt(D_\beta g + l_{v^y}) < 2^{s-1}$, then the weight of the codeword $c_{u,\alpha,\beta,v}$, which equals

$$2^r wt(D_\beta g + l_{v^y}) + wt(D_\alpha f + l_{v^x})(2^s - 2wt(D_\beta g + l_{v^y})),$$

is strictly larger than $2^r wt(D_\beta g + l_{v^y})$. Using the assumption

$$\mathcal{N}_\phi \geqslant 2^{\frac{s}{2} - \frac{(r+1)}{2}}(\frac{r+1}{2} + 1),$$

we get $wt(c_{u,\alpha,\beta,v}) > 2^{s+(r-1)/2}((r+1)/2+1)$.

(iii) If $wt(D_\beta g + l_{v^y}) > 2^{s-1}$, then the weight of the codeword $c_{u,\alpha,\beta,v}$, which equals

$$wt(D_\beta g + l_{v^y})(2^r - 2wt(D_\alpha f + l_{v^x})) + 2^s wt(D_\alpha f + l_{v^x}),$$

is strictly larger than $2^{s+r-1} = 2^{n-1}$. Therefore, $wt(c_{u,\alpha,\beta,v}) > 2^{s+(r-1)/2}((r+1)/2+1)$.

Putting everything together, we can conclude that the minimum weight $w_{\min}$ in $\mathcal{C}_h^{(\gamma)}$ equals $2^{s+(r-1)/2}((r+1)/2+1)$. □

Corollary 4.3.8. *Let the notation of Theorem 4.3.7 hold. If $\phi : \mathbb{F}_2^{s/2} \to \mathbb{F}_2^{s/2}$ is an AB permutation, where $s/2$ is odd, then the code $\mathcal{C}_h^{(\gamma)}$ in Theorem 4.3.7 is a wide minimal linear code with parameters $[2^n, n+\frac{s}{2}+2, 2^{s+(r-1)/2}((r+1)/2+1)]$.*

Proof. The proof follows immediately from Theorem 4.3.7 using the fact that $\mathcal{N}_\phi = 2^{s/2-1} - 2^{(s/2-1)/2} > 2^{\frac{s}{2}-\frac{(r+1)}{2}}(\frac{r+1}{2}+1)$. □

The above result covers the case when $s \equiv 2 \mod 4$, which enables the use of AB permutations. For $s \equiv 0 \mod 4$ (which forces $s/2$ even) there are no AB permutations. In this case, we consider the inverse function over $\mathbb{F}_2^{s/2}$ even though many other permutations satisfy the condition

$$\mathcal{N}_\phi \geqslant 2^{\frac{s}{2} - \frac{(r+1)}{2}}(\frac{r+1}{2} + 1).$$

Corollary 4.3.9. *Let the notation of Theorem 4.3.7 hold. If $\phi : \mathbb{F}_{2^{s/2}} \to \mathbb{F}_{2^{s/2}}$ is the inverse permutation $\phi(x) = x^{-1}$, where $s/2$ is even, then the code $\mathcal{C}_h^{(\gamma)}$ in Theorem 4.3.7 is a $[2^n, n+\frac{s}{2}+2, 2^{s+(r-1)/2}((r+1)/2+1)]$-wide minimal linear code.*

Proof. The result follows by an application of Theorem 4.3.7 using the fact that $\mathcal{N}_\phi = 2^{s/2-1} - 2^{s/4} > 2^{\frac{s}{2}-\frac{(r+1)}{2}}(\frac{r+1}{2}+1)$. □

From the proof of Theorem 4.3.7, the minimum distance of $\mathcal{C}_h^{(\gamma)}$ is governed by the choice of f and in particular by the minimum distance of $\mathcal{C}_{D_\gamma f}$, which must be a wide minimal linear code. Thus, increasing the minimum distance of this family of codes is directly related to the possibility of finding f such that $\mathcal{C}_{D_\gamma f}$ is wide minimal code with a better minimum distance than $2^\lambda(\kappa+1)$ (the minimum distance induced by functions derived in Theorem 3.4.8). This is an interesting open problem that leads towards future research challenges.

4.4 The p-ary case

In this section, we will provide two constructions of minimal codes using bent functions, non-covering permutations and suitable subspaces of derivatives. The results can be seen as generalizations of the corresponding results in Chapter 4.

Definition 4.4.1. *Let m be an even integer and k be a positive integer smaller than m. We will say that a bent function $g : \mathbb{F}_{p^m} \to \mathbb{F}_p$ with $g(0) = 0$ and a non-covering permutation $\phi : \mathbb{F}_{p^k} \to \mathbb{F}_{p^k}$ form a k-*minimal pair* if there exist a k-dimensional subspace U whose non-zero elements are nonaffine derivatives of g, and a linear mapping $\Psi : U + \mathcal{L}_m \to \mathcal{C}_\phi$ such that the following hold.*

(i) (Coherence) The restriction of Ψ to $\mathcal{L}_m$ is a p^{m-k}-to-one map onto $\mathcal{L}_k$ and the restriction of Ψ to U is an isomorphism between U and Comp_ϕ, where $\mathrm{Comp}_\phi = \{\mathrm{Tr}(v\phi(x)) : v \in \mathbb{F}_{p^k}\}$ denotes the linear space of components of ϕ.

(ii) (Weight-preserving) For each $w \in \mathcal{L}_k$, there exists a unique $v_w \in \mathcal{L}_m$ with $\Psi(v_w) = w$ such that, for every $u \in U$,

$$p^{m-k} wt(\Psi(u) + w) = wt(u + v_w)$$

and $wt(u + v') = p^m - p^{m-1}$ for every other $v' \in \mathcal{L}_m$ with $v' \neq v_w$ and $\Psi(v') = w$.

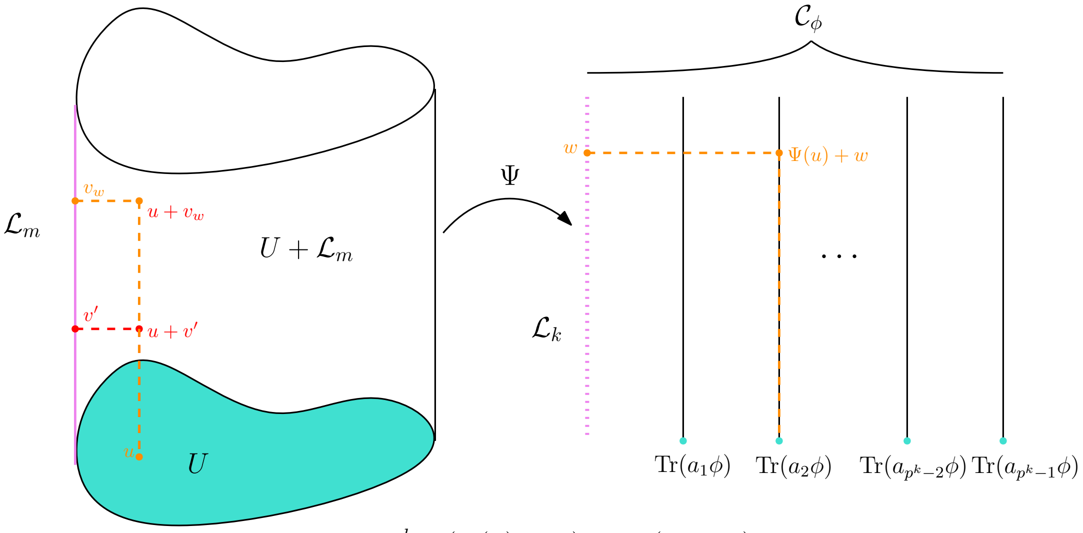
(iii) (Closure) Denote $\Lambda_0 = \{v_w : w \in \mathcal{L}_k\}$ and $\Lambda_1 = \mathcal{L}_m \setminus \Lambda_0$.

(a) The assignation $\iota : \mathcal{L}_k \to \Lambda_0$ given by $\iota(w) = v_w$ is a linear isomorphism;

(b) For each $v \in \Lambda_0$, $v' \in \Lambda_1$ and $c \in \mathbb{F}_p^*$, $cv + v', v + cv' \in \Lambda_1$;

(c) If $v, v' \in \Lambda_1$, then there exists at most one $c \in \mathbb{F}_p^*$ such that $v + cv' \in \Lambda_0$.

The concept introduced in the previous definition identifies a subspace of derivatives of a bent function and the components of a non-covering permutation. This identification is carried out in such a way that, when adding linear functions, the preimages of linear parts are tacitly partitioned into two groups. The idea of Definition 4.4.1 is depicted in Figure 4.1 and it will be helpful to construct examples of minimal codes. As a particular instance, we have the following $\frac{m}{2}$-minimal pair using the $\mathcal{MM}$ class.



$$p^{m-k} wt(\Psi(u) + w) = wt(u + v_w)$$

$$wt(u + v') = p^m - p^{m-1}$$

Figure 4.1: A k-minimal pair given by a subspace of derivatives U of g and a non-covering permutation ϕ.

Proposition 4.4.2. *Consider an even integer m and the simplest bent functions $g : \mathbb{F}_{p^{m/2}} \times \mathbb{F}_{p^{m/2}} \to \mathbb{F}_p$ in the Maiorana-McFarland class ($\mathcal{MM}$), defined as follows:*

$$g(x, y) = \mathrm{Tr}(x\phi(y)) \text{ for } (x, y) \in \mathbb{F}_{p^{m/2}} \times \mathbb{F}_{p^{m/2}}, \tag{4.21}$$

where $\phi : \mathbb{F}_{p^{m/2}} \to \mathbb{F}_{p^{m/2}}$ is a permutation. If ϕ is a non-covering permutation, then g and ϕ form an $\frac{m}{2}$-minimal pair.

Proof. We will prove that the subspace of derivatives

$$U := \{D_{(\gamma,0)}g : \gamma \in \mathbb{F}_{p^{m/2}}\}, \tag{4.22}$$

and the mapping $\Psi : U + \mathcal{L}_m \to \mathcal{C}_\phi$ given by

$$\Psi(D_{(\gamma,0)}g(x,y) + \mathrm{Tr}(ux + vy)) = (\mathrm{Tr}(\phi(y)\gamma) + \mathrm{Tr}(vy))_{y\in\mathbb{F}_{p^{m/2}}}$$

satisfy the conditions in Definition 4.4.1. Condition (i) is easily checked—for the restriction $\gamma = 0$, the mapping is $p^{m/2}$-to-one, whereas for $u = v = 0$, the mapping is clearly an isomorphism. For condition (ii), take $u = 0$, so that $v_w = (\mathrm{Tr}(vy))_{(x,y)\in\mathbb{F}_{p^m}}$ for $w = (\mathrm{Tr}(vy))_{y\in\mathbb{F}_{p^{m/2}}}$. For every derivative $D_{(\gamma,0)}g(x,y) \in U$,

$$wt((D_{(\gamma,0)}g(x,y) + \mathrm{Tr}(vy))_{(x,y)\in\mathbb{F}_{p^m}}) = p^{m/2}wt((\phi(y)\gamma + \mathrm{Tr}(vy))_{y\in\mathbb{F}_{p^{m/2}}})$$

since the vector $\phi(y)\gamma + \mathrm{Tr}(vy)$ does not depend on x. For any other $u \neq 0$, the vector $(D_{(\gamma,0)}g(x,y) + \mathrm{Tr}(ux + vy))_{(x,y)\in\mathbb{F}_{p^m}}$ is balanced. Condition $(iii).(a)$ is trivially satisfied as the function $w \mapsto v_w$ is essentially an inclusion. Let Λ_0, Λ_1 be as in Definition 4.4.1. For each $\mathrm{Tr}(vy) \in \Lambda_0, \mathrm{Tr}(u'x + v'y) \in \Lambda_1$ $(u' \neq 0)$ and $c \in \mathbb{F}_p^*$, it holds that $\mathrm{Tr}(cu'x + (v + cv')y), \mathrm{Tr}(u'x + (cv + v')y) \in \Lambda_1$, hence $(iii).(b)$ holds. Finally, if $\mathrm{Tr}(ux + vy), \mathrm{Tr}(u'x + v'y) \in \Lambda_1$ (thus $u \neq 0$ and $u' \neq 0$), there is at most one $c \in \mathbb{F}_{p^m}^*$ such that $\mathrm{Tr}((u + cu')x + (v + cv')y) \in \Lambda_0$, namely, if u, u' are $\mathbb{F}_p$-linearly independent, then there is no such c. Moreover, if they are $\mathbb{F}_p$-linearly dependent, this c is unique. □

Theorem 4.4.3. *Let $g : \mathbb{F}_{p^m} \to \mathbb{F}_p$ be a bent function with $g(0) = 0$ and $\phi : \mathbb{F}_{p^k} \to \mathbb{F}_{p^k}$ be a non-covering permutation such that they form a k-minimal pair. Assume that*

$$U = \{D_\gamma g : \gamma \in I\} \cup \{0\},$$

where $I = \{\gamma_1, \dots, \gamma_{p^k-1}\} \subseteq \mathbb{F}_{p^m}$. Let $\mathcal{B}$ be a basis for U and $\mathcal{B}'$ be a basis for $\mathcal{L}_m$. Suppose that the following conditions hold.

- *For each $v \in \mathbb{F}_{p^m}$ and for each $f(x) \in U$, the function $f(x) + \mathrm{Tr}(vx)$ has weight strictly smaller than $p^m - p^k$ and strictly larger than $2(p-1)(p^{m/2} - p^{m/2-1})$;*
- *The function $f(x) + cg(x+\gamma)$ is bent for every $f(x) \in U, c \in \mathbb{F}_p^*$ and $\gamma \in I$.*

Then, the code spanned by $\mathcal{B} \cup \mathcal{B}' \cup \{g\}$ punctured at zero is a $[p^m - 1, m + k + 1]$-minimal code.

Proof. Let $C^* = \langle \mathcal{B} \cup \mathcal{B}' \cup \{g\}\rangle$ and let C be the code obtained from C^* by puncturing the $x = 0$ coordinate. Note that every codeword in C can be expressed as

$$\mathbf{c}_{v,\gamma,\delta} := (\mathrm{Tr}(vx) + g(x+\gamma) + (\delta - 1)g(x))_{x\in\mathbb{F}_{p^m}^*}$$

for some $v, \gamma \in \mathbb{F}_{p^m}, \delta \in \mathbb{F}_p$. Consider two linearly independent codewords $\mathbf{c}_1 := \mathbf{c}_{v,\gamma,\delta}, \mathbf{c}_2 := \mathbf{c}_{v',\gamma',\delta'}$ in C. We will show that

$$\sum_{c \in \mathbb{F}_p^*} wt(\mathbf{c}_1 + c\mathbf{c}_2) \neq (p-1)wt(\mathbf{c}_1) - wt(\mathbf{c}_2),$$

for all the choices of parameters v, γ, δ and v', γ', δ'. For this, we will break down the proof into several cases according to the possible values of the indices. Throughout the proof, we will denote by η the number $(p-1)(p^{m-1} - p^{m/2-1})$ and $\theta = (p-1)(p^{m-1} + p^{m/2-1})$.

Case $\gamma = 0, \delta = 1$ and $\delta' \neq 0$: In this case, the weight $wt(\mathbf{c}_1)$ equals $p^m - p^{m-1}$. Since $g(x+\gamma') + (\delta' - 1)g(x)$ is bent, the codewords $\mathbf{c}_1 + c\mathbf{c}_2$ and $\mathbf{c}_2$ have weight at least η for every $c \in \mathbb{F}_p^*$. Hence

$$\sum_{c \in \mathbb{F}_p^*} wt(\mathbf{c}_1 + c\mathbf{c}_2) \geqslant (p-1)\eta.$$

On the other hand,

$$(p-1)wt(\mathbf{c}_1) - wt(\mathbf{c}_2) \leqslant (p-1)(p^m - p^{m-1}) - \eta < p\eta - \eta = (p-1)\eta.$$

Case $\gamma' = 0, \delta' = 1$ and $\delta \neq 0$: The weight $wt(\mathbf{c}_2)$ equals $p^m - p^{m-1}$. Since $g(x+\gamma) + (\delta - 1)g(x)$ is bent, the codewords $\mathbf{c}_1 + c\mathbf{c}_2$ and $\mathbf{c}_1$ have weight at least η for every $c \in \mathbb{F}_p^*$. Hence

$$\sum_{c \in \mathbb{F}_p^*} wt(\mathbf{c}_1 + c\mathbf{c}_2) \geqslant (p-1)\eta.$$

On the other hand,

$$(p-1)wt(\mathbf{c}_1) - wt(\mathbf{c}_2) \leqslant (p-1)\theta - p^m + p^{m-1} = (p-1)p^{m/2-1} < (p-1)\eta.$$

The latter inequality holds as $p^{m/2-1} < p^{m-1} - p^{m/2-1}$ for $m > 2$.

Case $\gamma' \neq 0 \vee \delta' \neq 1$ and $\delta \neq 0$: Since $g(x+\gamma') + (\delta' - 1)g(x)$ and $g(x+\gamma) + cg(x+\gamma') + (\delta - 1 + c(\delta' - 1))g(x)$ are bent for every $c \in \mathbb{F}_p$, the weights $wt(\mathbf{c}_2)$, $wt(\mathbf{c}_1 + c\mathbf{c}_2)$ are at least η for every $c \in \mathbb{F}_p^*$. Hence

$$\sum_{c \in \mathbb{F}_p^*} wt(\mathbf{c}_1 + c\mathbf{c}_2) \geqslant (p-1)\eta.$$

On the other hand,

$$(p-1)wt(\mathbf{c}_1) - wt(\mathbf{c}_2) \leqslant (p-1)wt(\mathbf{c}_1) - \eta.$$

By assumption, $wt(\mathbf{c}_1) < (p^m - p^k)$. Then, we have

$$(p-1)wt(\mathbf{c}_1)-\eta < (p-1)(p^m-p^k)-\eta = (p-1)(p^m-p^k-p^{m-1}+p^{m/2-1}) \leqslant (p-1)\eta.$$

Case $\gamma \neq 0 \vee \delta \neq 1$ and $\delta' \neq 0$: Since $g(x+\gamma)+(\delta-1)g(x)$ and $cg(x+\gamma)+g(x+\gamma')+(c(\delta-1)+\delta'-1))g(x)$ are bent for every $c \in \mathbb{F}_p$, the weights $wt(\mathbf{c}_1)$, $wt(\mathbf{c}_1+c\mathbf{c}_2)$ are at least η for every $c \in \mathbb{F}_p^*$. Hence

$$\sum_{c\in\mathbb{F}_p^*} wt(\mathbf{c}_1+c\mathbf{c}_2) \geqslant (p-1)\eta.$$

On the other hand,

$$(p-1)wt(\mathbf{c}_1) - wt(\mathbf{c}_2) \leqslant (p-1)\theta - wt(\mathbf{c}_2).$$

By assumption, $wt(\mathbf{c}_2) > 2(p-1)(p^{m/2}-p^{m/2-1})$. Then, we have

$$(p-1)\theta-wt(\mathbf{c}_2) < (p-1)(p^m-p^{m-1}+p^{m/2}-p^{m/2-1}-2p^{m/2}+2p^{m/2-1}) \leqslant (p-1)\eta.$$

Case $\delta = \delta' = 0$: Let $\Psi : U + \mathcal{L}_m \to \mathcal{C}_\phi$ be a linear map as in Definition 4.4.1. Let Λ_0, Λ_1 be as in Condition (iii) of Definition 4.4.1. Set $\mathfrak{v} := \mathrm{Tr}(vx) \in \mathcal{L}_m$ and $\mathfrak{v}' := \mathrm{Tr}(v'x) \in \mathcal{L}_m$. We will consider three additional subcases according to the possible memberships in Λ_1 or Λ_0.

Subcase $\mathfrak{v} \in \Lambda_1 \wedge \mathfrak{v}' \in \Lambda_0$ or $\mathfrak{v} \in \Lambda_0 \wedge \mathfrak{v}' \in \Lambda_1$: In any of these cases, for any $c \in \mathbb{F}_p^*$, $\mathfrak{v}+c\mathfrak{v}' \in \Lambda_1$, thus $\mathbf{c}_1+c\mathbf{c}_2$ is balanced. Hence,

$$S_1 := \sum_{c\in\mathbb{F}_p^*} wt(\mathbf{c}_1+c\mathbf{c}_2) = (p-1)(p^m-p^{m-1}).$$

In the first case, we have

$$S_2 := (p-1)wt(\mathbf{c}_1) - wt(\mathbf{c}_2) = (p-1)(p^m-p^{m-1}) - wt(\mathbf{c}_2).$$

This implies that $S_1 > S_2$ since $\mathbf{c}_2$ is not zero. In the second case,

$$S_2 := (p-1)wt(\mathbf{c}_1) - wt(\mathbf{c}_2) = (p-1)wt(\mathbf{c}_1) - (p^m-p^{m-1}).$$

If $S_1 = S_2$, then $wt(\mathbf{c}_1) = p^m$, which is impossible as $\mathbf{c}_1$ has weight strictly smaller than $p^m - p^k$. We conclude that $S_1 \neq S_2$ in both cases.

Subcase $\mathfrak{v} \in \Lambda_1 \wedge \mathfrak{v}' \in \Lambda_1$: By Condition $(iii).(c)$, there is at most one $c_0 \in \mathbb{F}_p^*$ such that $\mathfrak{v}+c_0\mathfrak{v}' \in \Lambda_0$. This implies that

$$\sum_{c\in\mathbb{F}_p^*} wt(\mathbf{c}_1+c\mathbf{c}_2) = (p-2)(p^m-p^{m-1}) + wt(\mathbf{c}_1+c_0\mathbf{c}_2).$$

On the other hand, $(p-1)wt(\mathbf{c}_1) - wt(\mathbf{c}_2) = (p-2)(p^m - p^{m-1})$. Putting everything together, we conclude that $S_1 \neq S_2$ since $\mathbf{c}_1 + c_0\mathbf{c}_2$ is not the zero codeword (by linear independence).

Subcase $\mathfrak{v} \in \Lambda_0 \wedge \mathfrak{v}' \in \Lambda_0$: By Condition $(iii).(a)$, for each $c \in \mathbb{F}_p^*$, $\mathfrak{v} + c\mathfrak{v}' \in \Lambda_0$. First we will prove that the codewords $\Psi(\mathbf{c}_1), \Psi(\mathbf{c}_2)$ in $\mathcal{C}_\phi$ are linearly independent. Suppose not, that is, there exists $\lambda \in \mathbb{F}_p$ such that $\Psi(\mathbf{c}_1) = \lambda\Psi(\mathbf{c}_2)$. Note that $\lambda \neq 0$ as $\mathbf{c}_1 \neq 0$ and Ψ is linear. From this, it is easy to see that $D_\gamma g = \lambda D_{\gamma'} g$ and $\Psi(\mathfrak{v} - \lambda\mathfrak{v}') = 0$. By uniqueness of $v_0 = 0$, it must be that $\mathfrak{v} = \lambda\mathfrak{v}'$ since $\mathfrak{v} - \lambda\mathfrak{v}' \in \Lambda_0$. This yields that $\mathbf{c}_1$ and $\mathbf{c}_2$ are linearly dependent, a contradiction. Thus we know that $\Psi(\mathbf{c}_1), \Psi(\mathbf{c}_2)$ are linearly independent, therefore they cannot cover each other since ϕ is non-covering. Hence,

$$\sum_{c \in \mathbb{F}_p^*} wt(\mathbf{c}_1 + c\mathbf{c}_2) = p^{m-k} \sum_{c \in \mathbb{F}_p^*} wt(\Psi(\mathbf{c}_1) + c\Psi(\mathbf{c}_2))$$

is different from $p^{m-k}(p-1)wt(\Psi(\mathbf{c}_1)) - p^{m-k}wt(\Psi(\mathbf{c}_2)) = (p-1)wt(\mathbf{c}_1) - wt(\mathbf{c}_2)$. □

Within this setting, the non-binary version of the derivative method (Theorem 4.2.7) is now easily obtained as a corollary.

Corollary 4.4.4 (The p-ary derivative method)**.** *For s even, let $g : \mathbb{F}_{p^{s/2}} \times \mathbb{F}_{p^{s/2}} \to \mathbb{F}_p$ be a bent function in the $\mathcal{MM}$ class defined as in (4.21) and $\phi : \mathbb{F}_{p^{s/2}} \to \mathbb{F}_{p^{s/2}}$ be a non-covering permutation. Define*

$$U := \{D_{(\gamma,0)}g : \gamma \in \mathbb{F}_{p^{s/2}}\}. \tag{4.23}$$

Let $\mathcal{B}$ be a basis for U and $\mathcal{B}'$ be a basis for the linear functions on $\mathbb{F}_{p^s}$. Then, the code spanned by $\mathcal{B} \cup \mathcal{B}' \cup \{g\}$ punctured at zero is a minimal $[p^s - 1, s + s/2 + 1]$-code.

Proof. The result follows immediately from Theorem 4.4.3 and Proposition 4.4.2. □

Example 4.4.5. *Let $s = 8$. The power permutation $\phi : \mathbb{F}_{3^4} \to \mathbb{F}_{3^4}$ defined by $\phi(y) = y^{17}$ is non-covering since the code $\mathcal{C}_\phi$ is an 8-dimensional narrow code with minimum weight 42 and maximum weight 60. Using computer simulations, we verified that the code C described in Corollary 4.4.4 derived from $g(x,y) = \mathrm{Tr}(x\phi(y))$ and the subspace of derivatives*

$$U = \{D_{(\gamma,0)}g : \gamma \in \mathbb{F}_{3^4}\},$$

is a minimal ternary $[6560, 13, 3402]$*-code, which is in accordance with Corollary 4.4.4. Moreover, its weight enumerator polynomial is*

$$1 + 960z^{3402} + 720z^{3888} + 363042z^{4320} + 527840z^{4374} + 699840z^{4401} + 1920z^{4860},$$

so that C is six-valued and narrow.

The code presented in the previous example is a narrow code, thus its minimality can be deduced by simply looking at the weight distribution. However, an interesting feature of Corollary 4.4.4 is that wide minimal codes can be produced as shown by the following example (cf. Example 4.2.10).

Example 4.4.6. *Let $s = 8$. Let $\phi : \mathbb{F}_{3^4} \to \mathbb{F}_{3^4}$ be the power permutation defined by $\phi(y) = y^{79}$. It can be verified that the code $\mathcal{C}_\phi$ is an 8-dimensional wide minimal code with minimum weight 42 and maximum weight 64, thus ϕ is a non-covering permutation. Using computer simulations, we verified that the code C described in Corollary 4.4.4 derived from $g(x, y) = \mathrm{Tr}(x\phi(y))$ and the subspace of derivatives*

$$U = \{D_{(\gamma,0)}g : \gamma \in \mathbb{F}_{3^4}\},$$

is a minimal ternary $[6560, 13, 3402]$*-code, which is in accordance with Corollary 4.4.4. Moreover, its weight distribution is displayed in Table 4.11 so that C is fourteen-valued and also* wide *since $\frac{3402}{5184} = \frac{21}{32} < \frac{2}{3}$.*

Table 4.11: Weight distribution of the ternary code in Example 4.4.6 shown in ascending order.

Weight w	Number of codewords A_w
3402	160
3564	560
3726	320
3888	640
4050	640
4212	1120
4320	363042
4374	525360
4401	699840
4536	640
4698	400
4860	960
5022	320
5184	320

Finally, we consider one more approach to designing minimal linear codes. In order to avoid unnecessary notation, we will identify the elements in $\mathbb{F}_{p^{s/2}} \times \{0\}$ with the elements in $\mathbb{F}_{p^{s/2}}$ without further mentioning whenever there is no room for ambiguity.

Lemma 4.4.7. *Let $f : \mathbb{F}_{p^r} \to \mathbb{F}_p$ be a non-affine function, $\gamma \in \mathbb{F}_{p^r}^*$ be such that f and $D_\gamma f$ are linearly independent and $g(y_1, y_2) = \mathrm{Tr}(y_1\phi(y_2))$ be a bent function, where ϕ is a permutation on $\mathbb{F}_{p^{s/2}}$ without affine components. Consider the direct sum $h(x, y) = f(x) + g(y)$. Denote by $\mathcal{C}_h^{(\gamma)}$ the p-ary linear code spanned by the linear functions on $\mathbb{F}_{p^n}$ and the functions $h_{\alpha,\beta}$, defined by $h_{\alpha,\beta}(x, y) = h(x + \alpha, y + \beta)$ for $\alpha \in \{0, \gamma\}, \beta \in \mathbb{F}_{p^{s/2}} \times \{0\}$. Then the set $\mathcal{C}_h^{(\gamma)}$ is a linear code with parameters $[p^n, n + \frac{s}{2} + 2]$.*

Proof. Set $\beta_0 := 0$. Let $\mathscr{B} = \{\beta_1, \ldots, \beta_{s/2}\}$ be a basis of $\mathbb{F}_{p^{s/2}} \times \{0\}$. Define $\mathcal{B} = \mathscr{B} \cup \{\beta_0\}$. We claim that the set $\{h_{0,\beta} : \beta \in \mathcal{B}\} \cup \{h_{\gamma,0}\}$ is linearly independent. Suppose that $\varsigma := \sum_{i=0}^{s/2} \lambda_i h_{0,\beta_i}(x, y) + \lambda_{s/2+1} h_{\gamma,0} = 0$ for some scalars $\lambda_0, \ldots, \lambda_{s/2}, \lambda_{s/2+1} \in \mathbb{F}_p$. Since the sum ς is the direct sum of the functions

$$(\sum_{i=0}^{s/2} \lambda_i) f(x) + \lambda_{s/2+1} f(x + \gamma) \text{ and } \sum_{i=1}^{s/2} \lambda_i g(y + \beta_i) + (\lambda_0 + \lambda_{s/2+1}) g(y),$$

ς equals zero if and only if $\sum_{i=0}^{s/2} \lambda_i g(y + \beta_i) + (\lambda_0 + \lambda_{s/2+1}) g(y) = 0$, $\sum_{i=0}^{s/2} \lambda_i = 0$ and $\lambda_{s/2+1} = 0$. The latter can be inferred from the linear independence of f and $D_\gamma f$. By definition, the sum $\sum_{i=0}^{s/2} \lambda_i g(y + \beta_i)$ can be rewritten as

$$\mathrm{Tr}(\phi(y_2)(y_1(\sum_{i=0}^{s/2} \lambda_i) + \sum_{i=0}^{s/2} \lambda_i \beta_i)).$$

Since $\sum_{i=0}^{s/2} \lambda_i = 0$, it holds that $\sum_{i=0}^{s/2} \lambda_i g(y + \beta_i) = 0$ if and only if $\sum_{i=0}^{s/2} \lambda_i \beta_i = 0$. This last condition implies that $\lambda_i = 0$ for each $1 \leqslant i \leqslant s/2$ by linear independence of $\mathscr{B}$. Thus, $\lambda_0 = 0$, too. Finally, note that the code $\mathcal{C}_h^{(\gamma)}$ is equal to the direct sum of the subspace of linear functions over $\mathbb{F}_{p^n}$ and the span $\langle h_{0,\beta}, h_{\gamma,0} \rangle$, hence its dimension is $n + s/2 + 2$. □

Theorem 4.4.8. *Let r be any positive integer and s be an even integer larger than two. Let $f : \mathbb{F}_{p^r} \to \mathbb{F}_p$ be a non-affine function with $f(0) = 0$ and $\gamma \in \mathbb{F}_{p^r}^*$ be such that $\{f, D_\gamma f\}$ is linearly independent. Let $g : \mathbb{F}_{p^{s/2}} \times \mathbb{F}_{p^{s/2}} \to \mathbb{F}_p$ be a bent function in $\mathcal{MM}$ of the form $g(y_1, y_2) = \mathrm{Tr}(y_1\phi(y_2))$, where ϕ is a non-covering permutation on $\mathbb{F}_{p^{s/2}}$. Suppose that the following two conditions hold:*

(i) For each $v \in \mathbb{F}_{p^s}$, $\beta \in \mathbb{F}_{p^{s/2}}$ and $a, b, c \in \mathbb{F}_p$ such that the tuple (v, β, a, b, c) is not zero, there exists $y = (y_1, y_2) \in \mathbb{F}_{p^s}^*$ that satisfies

$$ag(y_1, y_2) + g(by_1 + \beta, y_2) + l_v(y) = c.$$

(ii) The code $\mathcal{C}_f \oplus \mathcal{C}_{D_\gamma f}$ is an $(r+2)$-dimensional minimal code.

Then, the code $\mathcal{C}_h^{(\gamma)}$ is a minimal linear code with parameters $[p^n, n + \frac{s}{2} + 2]$. Moreover, if $\mathcal{C}_{D_\gamma f}$ is wide, then so is $\mathcal{C}_h^{(\gamma)}$.

Proof. The parameters of $\mathcal{C}_h^{(\gamma)}$ can be deduced from Lemma 4.4.7. Let $\mathscr{B} = \{\beta_1, \dots, \beta_{s/2}\}$ be a basis of $\mathbb{F}_{p^{s/2}}$. Note that each codeword in $\mathcal{C}_h^{(\gamma)}$ can be expressed as

$$\lambda(f(x)+g(y_1,y_2))+\mu f(x)+g(\mu y_1+\beta,y_2)+\nu(f(x+\gamma)+g(y_1,y_2))+L(x,y_1,y_2) \tag{4.24}$$

for some $\lambda, \nu \in \mathbb{F}_p$, $L \in \mathcal{L}_n$, $\beta = \sum_{i=1}^{s/2} \mu_i \beta_i \in \mathbb{F}_{p^{s/2}}$ and $\mu = \sum_{i=1}^{s/2} \mu_i$. First we will show that if the underlying functions that depend on y are linearly dependent then the corresponding codewords are linearly dependent provided they cover each other. Let $c, c' \in \mathcal{C}_h^{(\gamma)}$ be two non-zero codewords such that $c' \preceq c$, where the defining parameters of c and c' are $\lambda, \mu, \beta, \nu, L$ and $\lambda', \mu', \beta', \nu', L'$. Assume that

$$(\lambda' + \nu')g(y_1, y_2) + g(\mu' y_1 + \beta', y_2) + L'^y(y_1, y_2)$$

is equal to

$$\xi((\lambda + \nu)g(y_1, y_2) + g(\mu y_1 + \beta, y_2) + L^y)$$

for some $\xi \in \mathbb{F}_p$, where L^y denotes the restriction of L to the (y_1, y_2) coordinates. Rearranging this equality, we get that

$$\mathrm{Tr}(\phi(y_2)((\lambda' - \xi\lambda + \nu' - \xi\nu + \mu' - \xi\mu)y_1 + \beta' - \xi\beta))$$

is a linear function. This is possible only if $\beta' - \xi\beta = 0$ and $\lambda' - \xi\lambda + \nu' - \xi\nu + \mu' - \xi\mu = 0$, so that $\beta' = \xi\beta$. This implies $\mu' = \xi\mu$ by linear independence of the β_i's. We also have $\lambda' + \nu' = \xi(\lambda + \nu)$ and $L' = \xi L$. By condition (i), for each $x \in \mathbb{F}_{p^r}$, there exists a non-zero $y^{(x)} = (y_1^{(x)}, y_2^{(x)})$ such that

$$\lambda f(x) + \mu f(x) + \nu f(x + \gamma) + L^x(x)$$

is equal to

$$-((\lambda + \nu)g(y_1^{(x)}, y_2^{(x)}) + g(\mu y_1^{(x)} + \beta) + L^y(y_1^{(x)}, y_2^{(x)})).$$

Since $c' \preceq c$, for every $x \in \mathbb{F}_{p^r}$,

$$\lambda' f(x) + \xi\mu f(x) + \nu' f(x+\gamma) + L'^x(x)$$

is equal to $-\xi((\lambda+\nu)g(y_1^{(x)}, y_2^{(x)}) + g(\mu y_1^{(x)} + \beta) + L^y(y_1^{(x)}, y_2^{(x)}))$. In other words, for every $x \in \mathbb{F}_{p^r}$,

$$(\lambda' - \xi\lambda)f(x) + (\nu' - \xi\nu)f(x+\gamma) + (L' - \xi L^x)(x) = 0.$$

Since $C_f \oplus C_{D_\gamma f}$ is $(r+2)$-dimensional, we infer that $\lambda' = \xi\lambda$, $\nu' = \xi\nu$ and $L'^x = \xi L^x$. Suppose that $c, c' \in \mathcal{C}_h^{(\gamma)}$ are linearly independent and $c' \preceq c$. By the above discussion and Lemma 4.4.4, the function corresponding to the coordinate y of either c or c' is zero. Both of these functions cannot be zero simultaneously by minimality of $\mathcal{C}_f \oplus \mathcal{C}_{D_\gamma f}$. W.L.O.G, assume that the underlying function of c' that depends on y is zero. In this case, using condition (i), take an element $(x, y) \in \mathbb{F}_{p^r} \times \mathbb{F}_{p^s}$ such that (the underlying function of) c evaluated at this point is zero but c' evaluated at x is non-zero. This contradicts $c' \preceq c$. Analogously, we can rule out the case when the underlying function of c that depends on y is zero. Hence, if c, c' are linearly independent, then they cannot cover each other. This proves that $\mathcal{C}_h^{(\gamma)}$ is minimal. To prove the last part of the statement, note that each element in $\mathcal{C}_{D_\gamma f}$ can be identified (up to weight-scaling) with a codeword in $\mathcal{C}_h^{(\gamma)}$ (take $\mu = 0$, $\beta = 0$, $\nu = -\lambda$ and $L^y = 0$ in Equation 4.24). □

Chapter 5

Conclusions

The construction of minimal codes, which are suitable for secret sharing schemes or two-party computation protocols, has recently become one of the most active and important research lines in Cryptography/Coding Theory. This thesis has addressed two major mathematical and cryptographically significant problems regarding minimal codes—the construction of minimal codes that violate the Ashikhmin-Barg's bound and the introduction of general frameworks of constructing minimal codes from special classes of functions over finite fields. The results presented in Chapter 3 have provided a solution to the first problem, whereas the contents of Chapter 4 have given a solution to the second one.

In Chapter 3, four methods for obtaining wide minimal codes in the binary settings were presented, which we have referred as the basis method (Subsection 3.2.2), the affine subspace method (Subsection 3.2.3), the hyperplane method (Section 3.3) and the general Maiorana-McFarland method (Section 3.4).

The use of affine subspaces and bases allowed us to exploit the geometry of $\mathbb{F}_2^m$ in order to obtain wide minimal codes. Employing the characterization of minimal codes in terms of cutting vectorial blocking sets, these two methods rely on characteristic sets which serve as blocking sets. To construct characteristic sets that induce wide minimal codes, some algebraic and combinatorial properties were imposed on these sets. As we have shown, the inclusion of a basis and a linear combination of basis vectors, as well as a suitable punctured $(m-2)$-affine subspace take care efficiently of the algebraic properties. On the other hand, the size of the characteristic sets played an important role as a combinatorial property. These two features were conveniently merged to induce the desired wide minimal codes from Boolean functions.

A thorough analysis of the possible weight distributions of the resulting codes was given in Subsection 3.2.2 and Subsection 3.2.3, respectively. Their minimum distance depends on the size of the employed characteristic set Δ. When using affine subspaces, we were able to provide explicit weight distributions when the set Γ used in the construction of Δ has size two, see Tables 3.1-3.3.

Unlike the previous approach, the hyperplane method (Section 3.3) was not derived, *a priori*, from the vectorial blocking set framework. Theorem 3.3.1 and Theorem 3.3.2 were proved using a purely set theoretical/combinatorial argument on the possible weights of codewords. As a particular case, root functions turned out to be suitable examples to plug into this setting. We provided a complete description of the weight distribution and asymptotic behaviour of the weight ratios of the codes based on root functions in Subsection 3.3.2.

The general Maiorana-McFarland method is based on the well-established approaches used in [20] and in [40]. The main difference between these approaches and our method lies in the fact that the set U, that serves as a building block of the function in $\mathcal{GMM}$, was slightly modified. This modification allowed us to introduce wide minimal codes with a larger minimum distance, whose full weight distributions were given in Tables 3.8 - 3.15. Moreover, we were able to provide another construction, based on the same principles, using a derivative of a function f. These results played a crucial role for the generic construction given in Section 4.3.

These four methods share the attribute of having an ample range of possible initial inputs, thus leading to several wide minimal codes whose full specifications can be derived. Thus, a common exhibited feature is the flexibility of inputs and resulting weight distributions. As far as we know, for the first time, this property is achieved in the construction of infinite families of wide minimal binary linear codes.

As a second step, secondary constructions and the increase of dimension were considered in Chapter 4. Essentially, three methods for constructing (wide) minimal codes were devised. These approaches are based on typical operations of Boolean functions, namely, direct sums and derivatives. Additionally, a novel concept of non-covering permutations was introduced.

The first strategy, termed the direct sum method, employed an arbitrary Boolean function f and a non-affine function g whose associated code is minimal. These conditions proved to be enough to construct minimal codes. The use of bent functions and semi-bent functions as constituent blocks was discussed, and a deep analysis of the possible weight distributions was given in Section 4.1.

The second technique relies on a subspace of derivatives of a bent function g in $\mathcal{MM}$. Certain non-covering properties of vectors associated to g and its derivatives are inherited from the bentness of g, thus adjoining a basis for this subspace of derivatives to a basis for the space of linear functions was almost sufficient to produce minimal codes. However, derivatives of g do not necessarily satisfy the non-covering property. Here is where non-covering permutations came into play—using a non-covering permutation suffices to give rise to minimal codes and, sometimes, to wide minimal codes. The gist of this approach is that one can use any non-covering permutation to construct minimal linear codes. As shown in Subsection 4.2.1, this is a very vast class of permutations and several examples of such permutations were provided.

The last approach that was presented in this thesis is what we called the generic method to obtain wide minimal codes. This approach can be thought of as a combination of the direct sum method and the derivative method. The ingredients for this construction are simple, roughly, one needs a non-covering permutation ϕ and a function f with a suitable derivative $D_\gamma f$. We have proved that a linear code with length $n = r + s$ can be defined using the direct sum of two functions, whose dimension is $n + s/2 + 2$ (Lemma 4.3.1). To obtain wide minimal codes using this generic framework, we employed a bent function g in $\mathcal{MM}$ with a non-covering permutation as underlying permutation (cf. the derivative method) and a function f with a non-affine derivative $D_\gamma f$ such that the linear code $C_f \oplus C_{D_\gamma f}$ is minimal. Moreover, a way to ensure wideness of the resulting code is to require $C_{D_\gamma f}$ be wide. These results were shown in Theorem 4.3.2. Naturally, some concrete examples of wide minimal codes using this general framework were presented and their weight distributions completely specified (see Subsection 4.3.1). To round off the presented results, we studied more in detail the p-ary case, thus generalizing the results in Chapter 4 to the non-binary setting.

Many questions, open problems and research directions have arisen from the work in this thesis.

To start with, one could investigate how to obtain minimal codes that are more suitable for practical applications using well-known operations on linear codes such as puncturing, shortening, concatenating, etc. We proposed some techniques to increase the dimension of the obtained codes, however, their rates seem to be still quite bad, hence a natural question is how to increase the dimension and decrease the length while preserving minimality in such a way that the approaches are generic and flexible. Of course, an alternative approach could be used in order to fix some of these issues, e.g., the defining set method given in Equation (2.14).

In a similar fashion, the author is intrigued about knowing how all the constructions interact with each other. For instance, is it possible that, say, the affine subspace method and the hyperplane method are a particular case of a more general construction? We know that minimal codes and cutting vectorial blocking sets are equivalent objects, so, in principle, we can trace back these objects from one another. The question is then which blocking sets correspond to the presented constructions.

Another interesting problem is to find a practical application of wide minimal codes. Thus, how can we use the fact that weights are far from each other in real life? At this point, the interest is purely mathematical—the construction of infinite families of wide minimal codes has been a mathematical challenge which essentially motivated this work.

Needless to say, generalizations of our methods to the non-binary case would provide insight on the above questions and would give a systematic way to construct infinite families of non-binary minimal codes. We have successfully stepped a bit forward in this direction with the results given in Section 4.4. Nevertheless, we clearly expect that quite more can be said, even about the techniques given in Chapter 3.

Non-covering permutations are interesting by their own right in both the p-ary and the binary case. As any other class of permutations, non-covering permutations deserve a deeper analysis in terms of their cryptographic properties and their relations with other mathematical objects. Conjecture 1 is an example of this type of properties. We have observed that low-differential power permutations are non-covering due to its high nonlinearity, however, we do not know anything about general low-differentially uniform permutations without affine components. Even if there exist low-differentially uniform permutations with a not-so-high nonlinearity, then these permutations could be non-covering and give rise to wide minimal codes. This is in fact a hard problem to solve since it includes the challenge of identifying the nonlinearity of arbitrary APN permutations and 4-differentially uniform permutations without affine components, which is a well-known open problem.

Bibliography

[1] Alfarano, G. N., Borello, M., Neri, A.: A geometric characterization of minimal codes and their asymptotic performance. Adv. Math. Commun. (2020). https://doi.org/10.3934/amc.2020104

[2] Ashikhmin, A., Barg, A.: Minimal vectors in linear codes. IEEE Trans. Inf. Theory 44 (5), 2010–2017 (1998)

[3] Bartoli, D., Bonini, M.: Minimal linear codes in odd characteristic. IEEE Trans. Inf. Theory 65 (7), 4152–4155 (2019)

[4] Bhattacharya, S., Sarkar, S.: On some permutation binomials and trinomials over $\mathbb{F}_{2^n}$. Des. Codes Cryptogr. 82, 149–160 (2017)

[5] Blakley, G. R.: Safeguarding cryptographic keys. Manag. Requir. Knowl., Int. Workshop (AFIPS). 48: 313–317 (1979)

[6] Bonini, M., Borello, M.: Minimal linear codes arising from blocking sets. J. Algebr. Comb. 53, 327–341 (2021)

[7] Browning, K., Dillon, J., Kibler, R., McQuistan, M.: APN polynomials and related codes. J. Comb. Inf. Syst. Sci. 34, 135–159 (2009)

[8] Browning, K., Dillon, J., McQuistan, M., Wolfe, A.: An APN permutation in dimension six. In: Post-proc 9-th Int. Conf. Finite Fields Their Appl., vol. 518, pp. 33-–42. Amer. Math. Soc. (2010)

[9] Carlet, C.: Boolean functions for cryptography and coding theory. Cambridge University Press, Cambridge (2021). https://doi.org/10.1017/9781108606806

[10] Carlet, C., Charpin, P., Zinoviev, V.: Codes, bent functions and permutations suitable for DES-like cryptosystems. Des. Codes Cryptogr. 15, 125–156 (1998)

[11] Carlet, C., Ding, C., Yuan, J.: Linear codes from highly nonlinear functions and their secret sharing schemes. IEEE Trans. Inf. Theory 51 (6), 2089–2102 (2005)

[12] Chabanne, H., Cohen, G., Patey, A.: Towards secure two-party computation from the wire-tap channel. In: Lee, H.-S., Han, D.-G. (eds.) Proc. ICISC 2013 (Lecture Notes in Computer Science), vol. 8565, pp 34–46. Springer-Verlag, Berlin (2014)

[13] Chang, S., Hyun, J.: Linear codes from simplicial complexes. Des. Codes Cryptogr. 86, 2167–2181 (2018)

[14] Charpin, P., Peng, J.: New links between nonlinearity and differential uniformity. Finite Fields Appl. 56, p. 188–208 (2019). https://doi.org/10.1016/j.ffa.2018.12.001

[15] Cohen, G., Mesnager, S., Patey, A.: On minimal and quasi-minimal linear codes. In: Stam, M. (eds.) Proc. IMACC (Lect. Notes Comput. Sci., vol. 8308), pp. 85–98. Springer-Verlag, Berlin (2013)

[16] Ding, C.: A construction of binary linear codes from Boolean functions. Discrete Math. 339 (9), 2288—2303 (2016)

[17] Ding, C. A class of three-weight and four-weight codes. In: Proc. Int. Conf. Coding Crypt., Lecture Notes Comput. Sci. 5557 (Springer Verlag, Heidelberg), pp. 34-42 (2009)

[18] Ding, C: Linear codes from some 2-designs. IEEE Trans. Inf. Theory 61 (6), 3265–3275 (2015)

[19] Ding, C.: A construction of binary linear codes from Boolean functions. Discrete Math. 339 (9), 2288–2303 (2016)

[20] Ding, C., Heng, Z., Zhou, Z.: Minimal binary linear codes. IEEE Trans. Inf. Theory 64 (10), 6536–6545 (2018)

[21] Ding, C., Yuan, J.: Covering and secret sharing with linear codes. In: Calude, C., Dinneen M., Vajnovszki V. (eds) Discrete Math. Theor. Comput. Sci. (Lect. Notes Comput. Sci., vol. 2731), pp. 11–25. Springer, Berlin, Heidelberg (2003)

[22] Ding, K., Ding, C.: A class of two-weight and three-weight codes and their applications in secret sharing. IEEE Trans. Inf. Theory 64 (11), 5835–5842 (2015)

[23] Dobbertin, H.: Almost perfect nonlinear power functions on $GF(2^n)$: a new case for n divisible by 5. In: Jungnickel, D., Niederreiter, H., (eds.) Finite Fields Appl., pp. 113—121. Springer, Berlin, Heidelberg (2001). https://doi.org/10.1007/978-3-642-56755-1_11

[24] Goldreich, O., Micali, S., Wigderson, A.: How to play any mental game. Proc. 19th Ann. ACM Symp. Theory Comput. (STOC 1987), 218–229 (1987)

[25] Heng, Z., Ding, C., Wang, W.: Optimal binary linear codes from maximal arcs. IEEE Trans. Inf. Theory 66 (9), 5387–5394 (2020)

[26] Heng, Z., Ding, C., Zhou, Z.: Minimal linear codes over finite fields. Finite Fields Appl. 54, 176–196 (2018)

[27] Jaffe, D.: Optimal binary linear codes of length ≤ 30. Discrete Math. 223 (1), 135–155 (2000)

[28] Langevin, P., Saygi, Z., Saygi, E.: Classification of APN cubics in dimension 6 over GF(2). http://langevin.univ-tln.fr/project/apn-6/apn-6.html (2022)

[29] Li, X., Yue, Q.: Four classes of minimal binary linear codes with $w_{min}/w_{max} < 1/2$ derived from Boolean functions. Des. Codes Cryptogr. 88, 257–271 (2020)

[30] Lidl, R., Niederreiter, H.: Finite fields (2nd ed.) Encyclopedia of Mathematics and its Applications. Cambridge: Cambridge University Press (1996). https://doi.org/10.1017/CBO9780511525926

[31] Lint, J.: Introduction to coding theory. Graduate Texts in Mathematics, vol. 86. Springer Berlin, Heidelberg (1982). https://doi.org/10.1007/978-3-662-07998-0

[32] Lu, W., Wu, X., Cao, X: The parameters of minimal codes. Finite Fields Appl. 71 (2021). https://doi.org/10.1016/j.ffa.2020.101799

[33] MacWilliams, F., Sloane, N.: The theory of error-correcting codes. North Holland, Amsterdam (1977)

[34] Massey, J. L.: Minimal codewords and secret sharing. Proc. 6th Jt. Swed. Russ. Workshop Inf. Theory, August 22–27, 276–279 (1993)

[35] McFarland, R.: A family of difference sets in non-cyclic groups. J. Comb. Theory (series A) 15, 1–10 (1973)

[36] Mesnager, S.: Bent functions. Springer Cham, Switzerland (2016). https://doi.org/10.1007/978-3-319-32595-8

[37] Mesnager, S.: Linear codes with few weights from weakly regular bent functions based on a generic construction. Cryptogr. Commun. 9, 71–84 (2017)

[38] Mesnager, S.: Linear codes from functions. In: Huffman, W. C., Kim, J., Solé, P., (eds.) Concise Encycl. Coding Theory, pp. 463–526. Chapman and Hall/CRC, London, New York (2021)

[39] Mesnager, S., Özbudak, F., Sinak, A.: Linear codes from weakly regular plateaued functions and their secret sharing schemes. Des. Codes Cryptogr. 87 (2-3), 463–480 (2019)

[40] Mesnager, S., Qi, Y., Ru, H., Tang, C.: Minimal linear codes from characteristic functions. IEEE Trans. Inf. Theory 66 (9), 5404–5413 (2020)

[41] Mesnager, S., Sinak, A.: Several classes of minimal linear codes with few weights from weakly regular plateaued functions. IEEE Trans. Inf. Theory 66 (4), 2296–2310 (2020)

[42] Mesnager, S., Sinak, A., Yayla, O.: Minimal linear codes with few weights and their secret sharing. Int. J. Inf. Secur. Sci. 8 (4), 77–87 (2019)

[43] Pasalic, E., Chattopadhyay, A., Chowdhury, D.: An analysis of root functions—a subclass of the impossible class of faulty functions (ICFF). Discrete Appl. Math. 222, 1–13 (2017)

[44] Pasalic, E., Rodríguez, R., Zhang, F., Wei, Y.: Several classes of minimal binary linear codes violating the Ashikhmin-Barg bound. Cryptogr. Commun. 13, 637–659 (2021). https://doi.org/10.1007/s12095-021-00491-1

[45] Qi, Y., Yang, T., Dai, B.: Minimal linear codes from vectors with given weights. IEEE Commun. Lett. 24 (12), 2674–2677 (2020)

[46] Qu, L., Tan, Y., Tan, C., Li, C.: Constructing differentially 4-uniform permutations over $\mathbb{F}_2^{2k}$ via the switching method. IEEE Trans. Inf. Theory 59 (7), 4675–4686 (2013). https://doi.org/10.1109/TIT.2013.2252420

[47] Rabin, M.: How to exchange secrets with oblivious transfer. Technical Report TR-81, Aiken Computation Lab, Harvard University (1981)

[48] Rodríguez, R., Pasalic, E., Zhang, F., Wei. Y.: Minimal p-ary linear codes from non-covering permutations. In preparation.

[49] Rothaus, O.: On bent functions. J. Comb. Theory (series A) 20, 300–305 (1976)

[50] Shamir, A.: How to share a secret. Commun. ACM 22 (11): 612–613 (1979)

[51] Shannon, C.: A mathematical theory of communication. Bell Syst. Tech. J. 27, 379–423 (1948)

[52] Sinak, A.: Minimal linear codes from weakly regular plateaued balanced functions. Discrete Math. 344 (3), 112215 (2021)

[53] Tang, D., Carlet, C., Zhou, Z.: Binary linear codes from vectorial Boolean functions and their weight distribution. Discrete Math. 340 (12), 3055–3072 (2017)

[54] Tang, D., Li, X.: A note on the minimal binary linear code. Cryptogr. Commun. 12, 375–388 (2020)

[55] Tang, C., Qiu, Y., Liao, Q., Zhou, Z.: Full characterization of minimal linear codes as cutting blocking sets. IEEE Trans. Inf. Theory 67 (6), 3690–3700 (2021)

[56] Wolfmann, J: Codes projectifs à deux ou trois poids associés aux hyperquadriques d'une géométrie finie. Discrete Math. 13 (2), 185–211 (1975)

[57] Wolfmann, J.: The weights of the orthogonal of certain cyclic codes or extended Goppa codes. In: Mora T. (eds) Appl. Algebra Algebr. Algorithms Error-Correcting Codes. AAECC 1988 (Lect. Notes Comput. Sci., vol 357), pp. 476–480. Springer, Berlin, Heidelberg (1989). https://doi.org/10.1007/3-540-51083-4_84

[58] Xu, G., Qu, L.: Three classes of minimal linear codes over the finite fields of odd characteristic. IEEE Trans. Inf. Theory 65 (11), 7067–7078 (2019)

[59] Xu, G., Qu, L., Cao, X.: Minimal linear codes from Maiorana-McFarland functions. Finite Fields Appl. 65 (2020). https://doi.org/10.1016/j.ffa.2020.101688

[60] Xu, G., Qu, L., Luo, G.: Minimal linear codes from weakly regular bent functions. The 11th Int. Conf. Seq. Appl. (SETA 2020), September 22–25, Saint Petersburg, Russia (2020)

[61] Yao, A.: Protocols for secure computations. 23rd Ann. Symp. Found. Comput. Sci. (sfcs 1982). November 3–5, Chicago, USA (1982)

[62] Yao, A.: How to generate and exchange secrets. 27th Ann. Symp. Found. Comput. Sci. (sfcs 1986), October 27–29, Toronto, Canada (1986)

[63] Yuan, J., Ding, C.: Secret sharing schemes from three classes of linear codes. IEEE Trans. Inf. Theory 52 (1), 206–212 (2006)

[64] Zhang, F., Pasalic, E., Rodríguez, R., Wei, Y.: Wide minimal binary linear codes from the general Maiorana–McFarland class. Des. Codes Cryptogr. 89, 1485–1507 (2021). `https://doi.org/10.1007/s10623-021-00883-7`

[65] Zhang, F., Pasalic, E., Rodríguez, R., Wei, Y.: Minimal binary linear codes: a general framework based on bent concatenation. Des. Codes Cryptogr. 90, 1289–1318 (2022). `https://doi.org/10.1007/s10623-022-01037-z`

[66] Zhang, W., Yan, H., Wei, H.: Four families of minimal binary linear codes with $w_{min}/w_{max} \leqslant 1/2$. Appl. Algebra Eng. Commun. Comput. 30, 75–184 (2019)

Index

Povzetek v slovenskem jeziku

Koda je algoritem, ki spremeni vir informacij (besede) v drugo obliko (kodne besede). Običajno je vir informacij podan s pomočjo niza simbolov, imenovanega *abeceda*. *Koda za odpravljanje napak* je koda, ki lahko zaznava in odpravlja napake. Glavni namen kodiranja informacij je obnoviti izvorno sporočilo, ki je bilo poslano prejemniku preko hrupnega komunikacijskega kanala. Proučevanja kod za odpravljanje napak sodi v matematično področje *teorije kodiranja*. Teorija kodiranja sega v leto 1948, ko je Claude E. Shannon objavil svoje pomembno delo *A Mathematical Theory of Communication* [51], v katerem je predstavil koncept informacijske entropije kot merila informacijske vsebine v sporočilu.

Kode za odpravljanje napak, še posebej linearne kode, so bile široko raziskane zaradi pomembnih aplikacij v potrošniški elektroniki, varnem dvostranskem računanju [15], shemah za skupno rabo skrivnosti [11, 22, 63], avtentikaciji, sistemih za shranjevanje podatkov, asociativnih shemah in krepko regularnih grafih.

V zadnjih desetletjih so minimalne kode bile deležne veliko pozornosti kriptografske skupnosti zaradi svojih pomembnih aplikacij v varnostnih protokolih, kot so sheme deljenja skrivnosti [5, 50] in varno dvostransko računanje [24], ki so bistvenega pomena v današnjem digitalnem svetu. Za ta razred linearnih kod je značilna pokrivna lastnost, in sicer je linearna koda minimalna pod pogojem, da nobena od njenih neničelnih kodnih besed ni pokrita z nobeno drugo linearno neodvisno kodno besedo.

Z matematičnega vidika so lastnosti in konstrukcije neskončnih družin minimalnih kod postale temeljna tema na tem področju. Veliko dela je bilo opravljenega za popolno razumevanje kombinatoričnih in geometrijskih lastnosti teh kod [1, 3, 6, 11, 15, 20]. Kar zadeva konstrukcije, jih je večina temeljila na zadostnem Ashikhmin-Bargovem pogoju, ki povezuje najmanjšo in največjo težo kode [2], natančneje, če je količnik najmanjše teže q-arne kode nad njeno največjo težo strogo večji od $\frac{q-1}{q}$, potem je koda minimalna. Z drugimi besedami, ta pogoj zahteva, da so uteži blizu druga drugi. Linearne kode, ki izpolnjujejo pogoj Ashikhmin-Barg, imenujemo ozke, kode, ki tega ne izpolnjujejo, pa široke.

Konstruirati neskončne družine širokih minimalnih kod, tudi v binarnem okviru, je bil izziv, saj do pionirskega dela Dinga et. al. [20] nismo imeli nobenega primera. V omenjnem članku so nato predstavili tri neskončne družine širokih minimalnih binarnih kod z uporabo nekaterih konstrukcij, ki temeljijo na Boolovih funkcijah. Kmalu zatem je bilo uvedenih več metod za konstruiranje širokih minimalnih kod z uporabo velikega števila tehnik: simplicialni kompleksi [13], karakteristične funkcije [20, 29, 40], projektivne ravnine [3], rezane bločne množice [6, 55], maksimalni loki [25], šibko regularne ukrivljene funkcije [37, 60] in šibko regularne platojske funkcije [39, 40, 41, 42, 52], itd.

Ker je lastnost minimalnosti povezana s podporami kodnih besed, je naravno razmišljati o karakterizaciji minimalnosti v smislu uteži kodnih besed znotraj dane linearne kode. Da je to smiselno, je bilo pokazano v [26]. Koda C je minimalna, če in samo če za vsak par neničelnih linearno neodvisnih kodnih besed a in b v C velja

$$\sum_{c\in\mathbb{F}_q^*} wt(a+cb) \neq (q-1)wt(a) - wt(b). \tag{5.1}$$

Vse konstrukcije v doktorski disertaciji temeljijo na p-arnih funkcijah nad končnimi polji. Za praštevilo p lahko vektorski prostor $\mathbb{F}_p^m$ identificiramo s končnim poljem $\mathbb{F}_{p^m}$ tako, da določimo takšno bazo, da imata ta dva objekta enake linearne lastnosti. Preslikava f iz $\mathbb{F}_p^m$ v $\mathbb{F}_p$ se imenuje *p-arna funkcija.* 2-arno funkcijo imenujemo preprosto *Boolova funkcija.* Ko je vrstni red elementov $\mathbb{F}_{p^m}$ fiksiran, na primer $\mathbb{F}_{p^m} = \{\alpha_0 = 0, \alpha_1, \dots, \alpha_{p^m-1}\}$, katera koli p-arna funkcija $f : \mathbb{F}_{p^m} \to \mathbb{F}_p$ enolično določi zaporedje izhodnih vrednosti (imenovano *tabela resnice*), podano kot

$$[f(\alpha_0), f(\alpha_1), \dots, f(\alpha_{p^m-1})],$$

na katerega lahko gledamo kot na vektor dolžine p^m z vrednostmi iz polja $\mathbb{F}_p$. Funkcija $f : \mathbb{F}_{p^m} \to \mathbb{F}_p$ in njena tabela resnice sta nato obravnavani kot ekvivalenten objekt, ko ni dvoumnosti.

Dve standardni metodi za definiranje linearnih kod, ki izhajajo iz p-arnih funkcij, sta dobro raziskani v literaturi [19]. Prva splošna metoda določa linearne kode z uporabo preslikave $f : \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$. Linearno kodo $\mathcal{C}_f \subset \mathbb{F}_p^{p^m}$ namreč definira

$$\mathcal{C}_f = \{c_{a,u} := (\mathrm{Tr}(af(x)) + \mathrm{Tr}(ux))_{x\in\mathbb{F}_{p^m}} : a, u \in \mathbb{F}_{p^m}\}. \tag{5.2}$$

Ekvivalentno definicijo kode $\mathcal{C}_f$ je mogoče dobiti z uporabo vektorske prostorske predstavitve polja $\mathbb{F}_{p^m}$ in s standardnim direktnim produktom. Dimenzija kode $\mathcal{C}_f$ je največ $2m$ in njena dolžina je p^m.

Druga splošna konstrukcija linearnih kod iz funkcij fiksira množico

$$D = \{d_1, d_2, \ldots, d_s\} \subset \mathbb{F}_{p^m}$$

tako imenovano *definirno množico* tako, da je

$$\mathcal{C}_D = \{(\mathrm{Tr}(d_1x), \mathrm{Tr}(d_2x), \ldots, \mathrm{Tr}(d_sx)) : x \in \mathbb{F}_{p^m}\}. \tag{5.3}$$

Dimenzija linearnih kod, podanih v (5.2), je $2m$ pod pogojem, da funkcija f nima linearnih komponent. Poleg tega je mogoče njihove uteži izraziti z Walshevo transformacijo funkcije $f : \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$ kot

$$wt(\mathbf{c}_{a,u}) = p^m - \frac{1}{p} \sum_{\omega \in \mathbb{F}_p} W_{\mathrm{Tr}(\omega a)}(\omega u). \tag{5.4}$$

Namen disertacije je dvojen. Prvič, nadaljevanje raziskovalne smeri prejšnjih del [6, 20, 38] in iskanje več konstrukcij širokih minimalnih binarnih kod z uporabo teorije Boolovih funkcij, s čimer pridobimo linearne kode, primerne za sheme deljenja skrivnosti ali protokole za dvostransko računanje. Te družine imajo značilnost, da imajo takšne prilagodljive parametre, da pokrivajo širok razpon možnih minimalnih uteži.

Prve neskončne družine širokih minimalnih kod temeljijo na geometrijskem pristopu za konstrukcijo minimalnih kod, predstavljen v [6], kjer so avtorji pokazali močno povezavo med rezanimi vektorskimi bločnimi množicami in minimalnimi kodami. Presenetljivo se izkaže, da sta ta dva predmeta enaka [55] (glej izrek 3.2.2). Z uporabo preluknjanih hiperravnin predlagamo novo metodo za pridobivanje širokih minimalnih kod iz generične konstrukcije, ki jo je mogoče uporabiti skupaj s tako imenovanimi korenskimi funkcijami, da bi dobili določene neskončne družine širokih minimalnih kod, katerih porazdelitve teže je mogoče eksplicitno podati. Družina širokih minimalnih binarnih linearnih kod, ki uporabljajo Boolove funkcije, ki pripadajo splošnemu Maiorana-McFarland razredu, je bila podana v [20]. Predlagamo podobne metode konstrukcije in zagotavljamo dva eksplicitna razreda širokih minimalnih kod, ki dosegajo boljše parametre za odpravljanje napak v primerjavi s tistimi metodami, obravnavanimi v [20].

Kot drugi rezultat bodo predstavljene nekatere splošne konstrukcije minimalnih kod, ki temeljijo na različnih dobro znanih tehnikah funkcij nad končnimi polji, skupaj z nekaterimi novimi koncepti, prilagojenimi konstrukciji minimalnih kod (npr. nepokrivajoče permutacije). Cilj teh konstrukcij je zagotoviti splošen okvir za generacijo minimalnih kod, ki so široke, ali tudi ne, na tak način, da imajo večjo dimenzijo glede na svojo dolžino. To je še posebej pomembno pri obravnavi aplikacij, saj mora biti praktičen varen dvostranski računski protokol (ki temelji na linearnih kodah) sestavljen iz minimalne kode z visokim razmerjem.

Te splošne okvire je mogoče videti tudi kot sekundarne konstrukcije minimalnih kod, kar je lahko še ena motivacija za njihovo študije: dobro znano je [15], da je Kroneckerjev produkt dveh minimalnih kod minimalna koda. Vendar pa je malo znanega o nekaterih drugih sekundarnih konstrukcijah minimalnih linearnih kod.

Direktna vsota funkcij je zelo primeren kandidat za konstrukcijo minimalnih kod, saj je njen Walshev spekter v celoti določen z Walshevimi spektri njenih sestavnih seštevnikov. Predlagamo preprosto metodo z uporabo direkntih vsot, ki poda minimalne kode. Zaradi svoje preprostosti je to metodo mogoče prilagoditi za pridobitev več neenakovrednih minimalnih kod. Odvodi ukrivljene funkcije g (ker so uravnotežene) se prav tako izkažejo za združljive z lastnostjo minimalnosti kod $\mathcal{C}_g$, saj dodajati bazo določenih odvodov inducira minimalno kodo z večjo dimenzijo. Končno sta ti dve metodi združeni za rešitev predlaganega problema pridobivanja kod z večjimi dimenzijami.

Kot stranski produkt teh konstrukcij je predstaven in podrobneje preučen koncept nepokrivajočih permutacij. Ta razred permutacij vsebuje razred AB permutacij, APN potenčnih permutacij, 4-diferencialno enakomernih permutacij in na splošno zelo nelinearnih permutacij.

Doktorska disertacija v splošnem ponuja več konstrukcij (širokih) minimalnih kod iz generičnih konstrukcij, ki se opirajo na teorijo Boolovih in p-arnih funkcij. Te konstrukcije so generične v smislu, da lahko kot vhodni podatek vnesemo poljubno funkcijo, ki izpolnjuje določene šibke predpostavke, in pridobimo različne minimalne kode, ki niso ekvivalentne.

Preostali del dokumenta je organiziran na sledeči način. V poglavju 1 so podane teoretične osnove naših rezultatov skupaj z nekaj motivacije. Predstavljen je koncept minimalne kode in poudarjen je njen pomen v kontekstu shem deljenja skrivnosti in večstranskih računskih protokolov. Potrebne definicije in preliminarni rezultati o funkcijah, linearnih kodah in minimalnih kodah so predstavljeni v poglavju 2.

Glavni rezultati so v poglavjih 3 in 4. V poglavju 3 predstavljamo štiri konstrukcije širokih minimalnih binarnih linearnih kod s splošnimi konstrukcijami z uporabo Boolovih funkcij. Za več primerov teh konstrukcij podajamo popolno specifikacijo njihove porazdelitve uteži. Te tehnike so poimenovane z besedo »metoda« in dodanim opisom najpomembnejšega predmeta. Tako uvajamo metodo baze (Poglavje 3.2.2), metodo afinega podprostora (Poglavje 3.2.3), metodo hiperravnine (Poglavje 3.3) in metodo splošne Maiorana-McFarland funkcije (Poglavje 3.4).

Nazadnje so v poglavju 4 predstavljene tri metode za pridobitev širokih minimalnih kod z večjo dimenzijo. Ti pristopi temeljijo na standardnem delovanju funkcij, kot so direktna vsota ali odvodi. V poglavju 4.1 so minimalne kode sestavljene iz direktne vsote dveh Boolovih funkcij pod določenimi šibkimi predpostavkami, in sicer, da je ena od povezanih kod minimalna. Za isti namen konstruiranja (širokih) minimalnih kod je v poglavju 4.2 predstavljen nov koncept »nepokrivajoče permutacije«. Te permutacije so uporabne pri določanju linearnih kod, povezanih z ukrivljenimi funkcijami v razredu Maiorana-McFarland. Zadnja konstrukcija, imenovana »splošna konstrukcija«, je kombinirana različica metode direktne vsote in metode odvodov. Podana je v poglavju 4.3 in njeni eksplicitni primeri so podani v poglavju 4.3.1. Posplošitev rezultatov na p-arni primer je obravnavana v poglavju 4.4.

Plod raziskave, opravljene v doktorskem delu, so štiri strokovni članki. Trije od štirih so že objavljeni v uglednih revijah, četrti pa je še v pripravi. Ti članki so v referencah navedeni kot [44, 48, 64, 65].

Spodaj naštejemo in povzamemo glavne matematične prispevke:

- Izrek 3.2.5 (Metoda baze). Konstrukcija širokih minimalnih kod iz baz s parametri $[2^m, m+1, d]$ z $d \in \{m+1, \dots, 2^{m-2}\}$.

- Izrek 3.2.7. Zadostni pogoji za dokaz minimalnosti in širokosti odvodov kod $\mathcal{C}_{D_\gamma f}$

- Izrek 3.2.12 (Metoda afinega podprostora). Konstrukcija širokih minimalnih kod iz preluknjanega $(m-2)$-dimenzionalnega afinega podprostora s parametri $[2^m, m+1, d]$, kjer je $d \in \{2^{m-3}+1, \dots, 2^{m-2}+2^{m-3}-1\}$.

- Izrek 3.3.1 (Metoda hiperravnine). Konstrukcija širokih minimalnih kod iz preklunjanih hiperravnin s parametri $[2^m, m+1, d]$, kjer je $d \in \{2^{m-2}+1, \dots, 2^{m-1}\}$.

- Izrek 3.3.2 (Metoda hiperravnine, komplementarna konstrukcija). Konstrukcija širokih minimalnih kod iz preluknjanih hiperravnin s parametri $[2^m, m+1, d]$, kjer je $d \in \{m+1, \ldots, 2^{m-2}+1\}$.
- Izrek 3.3.4. Široke minimalne kode, povezane s korenskimi funkcijami.
- Posledica 3.3.6. Asimptotično obnašanje kod, povezanih s korenskimi funkcijami.
- Izrek 3.4.2 (Metoda $\mathcal{GMM}$ I). Za liho celo število $m \geqslant 9$ in $m \neq 11$, konstrukcija širokih minimalnih kod iz splošnega $\mathcal{MM}$ razreda s parametri
$$[2^m, m+1, 2^{m-1} - 2^{\frac{m-5}{2}}(m-1)] \text{ ali } [2^m, m+1, 2^{m-1} - 2^{\frac{m-5}{2}}(m-5)],$$
v odvisnosti od parnosti vrednosti $(m+1)/2$.
- Izrek 3.4.5 (Metoda $\mathcal{GMM}$ II). Za liho celo število $m \geqslant 7$, konstrukcija širokih minimalnih kod iz splošnega $\mathcal{MM}$ razreda s parametri
$$[2^m, m+1, 2^{m-1} - 2^{\frac{m-5}{2}}(2^{\frac{m-1}{2}} - m + 5)].$$
- Izrek 3.4.8 (Metoda $\mathcal{GMM}$ III). Za liho celo število $m \geqslant 9$, konstrukcija širokih minimalnih kod iz odvodov funkcij iz splošnega $\mathcal{MM}$ razreda s parametri
$$[2^m, m+1, 2^{m-1} - 2^{\frac{m-3}{2}}(m+3)].$$
- Izrek 4.1.3 (Metoda direktne vsote). Splošen okvir za pridobivanje minimalnih kod, ki temelji na direktni vsoti p-arnih funkcij in poda kode dolžine p^m in dimenzije $m+1$.
- Posledica 4.1.4. Konstrukcija minimalnih kod z uporabo metode direktne vsote ukrivljene funkcije s s spremenljivkami in neafine funkcije z r spremenljivkami, ki poda kode s parametri $[p^m, m+1, d]$, kjer je
$$d > p^m - p^{m-1} - p^{r+s/2} + p^{r+s/2-1}.$$
- Lema 4.2.3. Karakterizacija minimalnosti kode $\mathcal{C}_{f_1} \oplus \mathcal{C}_{f_2}$ v smislu minimalnosti svojih gradnikov.
- Definicija 4.2.4. Predstavljen koncept nepokrivajoče permutacije.
- Izrek 4.2.7 (Metoda odvodov). Konstrukcija minimalnih kod iz ukrivljenih funkcij z m spremenljivkami v $\mathcal{MM}$ razredu z nepokrivajočo permutacijo ϕ kot temeljno permutacijo. Parametri so $[2^m, m+\frac{m}{2}+1, 2^{m/2}\theta]$, kjer je θ večji od nelinearnosti funkcije ϕ.

- Posledica 4.2.8. Konstrukcija minimalnih kod iz ukrivljenih funkcij z m spremenljivkami iz $\mathcal{MM}$ razreda in AB permutacijo kot temeljno permutacijo. Parametri so
$$[2^m, m + \frac{m}{2} + 1, 2^{m-1} - 2^{\frac{m+m/2-1}{2}}].$$

- Posledica 4.2.9. Konstrukcija minimalnih kod iz ukrivljenih funkcij z m spremenljivkami iz $\mathcal{MM}$ razreda z multiplikativno inverzno permutacijo kot temeljno permutacijo. Parametri so $[2^m, m + \frac{m}{2} + 1, 2^{m/2}\theta]$, kjer je $\theta = 2^{m/2}(2^{m/2-1} - 2^{m/4})$, ko je $m/2$ sod in je θ enaka najvišjemu sodemu celemu številu navzgor omejenem z $2^{m/2-1} - 2^{m/4}$, ko je $m/2$ lih.

- Posledica 4.2.14. Vsaka nizko diferencialno ($\delta = 2$ ali $\delta = 4$) enakomerna potenčna permutacija je nepokrivajoča.

- Izrek 4.2.18. Konstrukcija širokih minimalnih kod z uporabo funkcije v $\mathcal{GMM}$ in njenega odvoda. Parametri so
$$[2^m, m + 1, 2^{m-1} - 2^{\frac{m-3}{2}}(m + 3)].$$

- Izrek 4.3.2. Splošen okvir za konstrukcijo širokih minimalnih kod iz podprostorov odvodov funkcije $f : \mathbb{F}_2^r \to \mathbb{F}_2$ in nepokrivajočih permutacij $\phi : \mathbb{F}_2^{s/2} \to \mathbb{F}_2^{s/2}$, ki inducirajo kode s parametri $[2^{r+s}, r + s + \frac{s}{2} + 2]$.

- Izrek 4.3.7. Primer izreka 4.3.2, pri katerem je najmanjša razdalja induciranih kod eksplicitno izračunana kot $2^{s+(r-1)/2}((r + 1)/2 + 1)$.

- Definicija 4.4.1. Predstavljen koncept k-minimalnega para, ki je sestavljen iz ukrivljene funkcije in nepokirvajoče permutacije.

- Izrek 4.4.3. Konstrukcija minimalnih kod, ki temelji na k-minimalnem paru s parametri $[p^m - 1, m + k + 1]$.

- Posledica 4.4.4 (p-arna metoda odvodov). Primer izreka 4.4.3, kjer je podprostor U sestavljen iz odvodov funkcije g v smereh, ki vplivajo samo na linearni del funkcije g.

- Izrek 4.4.8. Generična konstrukcija minimalnih p-arnih kod, ki temelji na metodi direktne vsote in nepokrivajočih permutacjiah in poda kode s parametri $[p^n, n + \frac{s}{2} + 2]$.