# Minimal $p$-ary codes via the direct sum of functions, non-covering permutations and subspaces of derivatives

René Rodríguez* Enes Pasalic† Fengrong Zhang ‡ Yongzhuang Wei §

**Abstract**

In this article, we propose several generic methods for constructing minimal linear codes over the prime field $\mathbb{F}_p$. The first construction uses the direct sum of an arbitrary function $f : \mathbb{F}_{p^r} \to \mathbb{F}_p$ and a bent function $g : \mathbb{F}_{p^s} \to \mathbb{F}_p$ to induce minimal codes with parameters $[p^{r+s} - 1, r + s + 1]$ and minimum distance larger than $p^r(p-1)(p^{s-1} - p^{s/2-1})$. For the first time, we provide a general construction of linear codes from a subclass of non-weakly regular plateaued functions, which partially answers an open problem posed in [18]. The second construction deals with a bent function $g : \mathbb{F}_{p^m} \to \mathbb{F}_p$ and a suitable subspace of derivatives of $g$, i.e., functions of the form $g(y + a) - g(y)$ for some $a \in \mathbb{F}^*_{p^m}$. We also provide a sound generalization of the recently introduced concept of non-covering permutations [46]. Some important structural properties of this class of permutations are derived in this context. The most remarkable observation is that the class of non-covering permutations includes all APN power permutations (characterized by having two-to-one derivatives). Finally, the last construction combines the previous two methods (direct sum, non-covering permutations and subspaces of derivatives), using a bent function in the Maiorana-McFarland class, to construct minimal codes (even those violating the Ashikhmin-Barg bound) with larger dimensions. This last method proves to be highly flexible since it can lead to several non-equivalent codes, depending to a great extent on the choice of the underlying non-covering permutation.

**Keywords:** Minimal linear codes, $p$-ary functions, non-weakly regular functions, non-covering permutations, derivatives, direct sum.

## 1 Introduction

Minimal codes form a class of linear codes characterized by the property that none of the (non-zero) codewords are covered by any linearly independent codeword. These codes have been widely used in certain applications, such as secret sharing schemes [6, 13, 44] and secure two-party computation [9].

Ashikhmin and Barg [2] proved that a linear code over $\mathbb{F}_p$ is minimal whenever the minimum weight $w_{\min}$ and the maximum weight $w_{\max}$ are close to each other, precisely, $\frac{w_{\min}}{w_{\max}} > \frac{p-1}{p}$. Nevertheless, this condition is not necessary as shown by several constructions of infinite families of minimal linear codes for which $\frac{w_{\min}}{w_{\max}} \leq \frac{p-1}{p}$ [3, 4, 7, 12, 17, 25, 30, 36, 41, 47, 45, 46]. Minimal codes violating Ashikhmin and Barg's bound appear to be intrinsically harder to specify. These minimal codes, satisfying $\frac{w_{\min}}{w_{\max}} \leq \frac{p-1}{p}$, are called *wide* in this article.

Due to their important applications, an increasing interest in constructing minimal codes of different kinds has arisen. Several properties of these codes have been discovered, such as bounds, characterizations and asymptotic properties [1, 4, 9, 20].

There are a vast number of methods for constructing minimal codes—constructions based on $p$-ary functions are among the most renowned methods. In their pioneering work, Carlet, Charpin and Zinoviev [5] showed the first explicit connection between AB (and APN) functions and linear codes.

*University of Primorska, Famnit & IAM, Koper, Slovenia, e-mail: rene7ca@gmail.com

†University of Primorska, Famnit & IAM, Koper, Slovenia, and Guangxi Key Laboratory of Cryptography and Information Security, Guilin University of Electronic Technology, Guilin, P.R. China, e-mail: enes.pasalic6@gmail.com

‡State Key Laboratory of Integrated Services Networks, Xidian University, Xian 710071, P.R. China, e-mail: zhfl203@cumt.edu.cn

§Guangxi Key Laboratory of Cryptography and Information Security, Guilin University of Electronic Technology, Guilin, P.R. China, e-mail: walker_wyz@guet.edu.cn

Soon after, Carlet and Ding [6] constructed minimal codes based on perfect nonlinear mappings. Since then, many authors have addressed the construction of minimal linear codes using $p$-ary functions [3, 10, 13, 14, 17, 22, 23, 24, 25, 26, 28, 32, 34, 41, 42, 43].

In this work, we address the construction of (wide) minimal $p$-ary codes from general methods. These constructions can be seen as generalizations of the methods presented in [46], where the authors specified three generic methods for building minimal binary linear codes using the direct sum of Boolean functions (given in the form $h(x, y) = f(x) + g(y)$) and subspaces of derivatives of bent functions from the Maiorana-McFarland class. Nonetheless, unlike the binary case, explicit weight distributions are much harder to derive in the non-binary case. This is also evident from diverse works on this topic, e.g., the use of planar functions (whose all nonzero component functions are bent) by Carlet *et al.* in [6], where the codes associated to the planar function $x^2$ could be fully specified but the full specification of the weight distribution for another planar function of the form $x^{p^k+1}$ was left as an open problem.

Our first method (Theorem 2) uses the direct sum of functions and it provides a simple way to specify minimal codes. This method then allows us to readily obtain explicit minimal codes, namely, selecting an arbitrary $p$-ary function $f$ over $\mathbb{F}_{p^r}$ and a bent function $g$ over $\mathbb{F}_{p^s}$ is sufficient to specify a minimal linear code of dimension $n+1$, where $n = r+s$, based on their direct sum $h(x, y) = f(x)+g(y)$, whose minimum distance is larger than $p^r(p-1)(p^{s-1} - p^{s/2-1})$, see Corollary 1. Moreover, using this approach we provide the first explicit use of non-weakly regular plateaued functions to construct linear codes, whose weight distributions are fully derived. This partially answers an open problem posed in [18] (Problem 3.2).

The second method is based on subspaces of derivatives and the concept of *non-covering permutations* [46]. These permutations were used to construct non-equivalent (wide) minimal binary codes. The authors of [46] pointed out that a straightforward generalization of the definition of a non-covering permutation was doomed to fail due to the complications related to the involved conditions on the Walsh spectra of $p$-ary permutations. Providing a characterization of non-covering permutations through minimality of the code $\mathcal{C}_\phi$ (spanned by linear functions and the components of $\phi$), we propose a satisfactory definition of non-covering $p$-ary permutations and we then use them to construct minimal codes based on subspaces of derivatives, see Theorem 8. Moreover, we provide additional structural properties of non-covering permutations. In particular, we show that every APN power permutation and every 4-uniform power permutation are non-covering.

Finally, the third method introduces a generic construction of $p$-ary minimal linear codes having a larger dimension than $n+1$. This construction can be easily understood by following closely its binary counterpart [46]. It can be described as a merger between the two previously mentioned methods. Thus, the use of a $p$-ary function $f$ and its derivative, a suitable subspace of derivatives of dimension $\frac{m}{2}$ of a weakly regular bent function $g$ in the Maiorana-McFarland class and a non-covering $p$-ary permutation yields a (wide) minimal code of length $p^n - 1$ with dimension $n + \frac{m}{2} + 2$, see Theorem 9.

This paper is organized as follows. In Section 2, we introduce some basic definitions and results related to $p$-ary functions, cyclotomic fields, linear codes from functions and minimal codes. The first construction using the direct sum method for the purpose of constructing minimal linear codes is described in Section 3. In Section 4, we present a generalization of non-covering permutations to non-binary fields and study their properties. In Section 5.1, we provide the second construction employing non-covering permutations and the use of suitable subspaces of derivatives of weakly regular bent functions. Additionally, in Section 5.2, the third general class of minimal codes is introduced. Some concluding remarks are given in Section 6.

## 2 Preliminaries

### 2.1 $p$-ary functions

For any integer $m > 0$ and a prime number $p$, let $\mathbb{F}_{p^m}$ denote the finite field with $p^m$ elements. Denote by $\mathbb{F}_p^m$ an $m$-dimensional vector space over $\mathbb{F}_p$. These two algebraic structures can be identified by fixing a basis. A function $f$ from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p$ is called a *p-ary function.* When $p = 2$, a mapping $f$ from the the finite field $\mathbb{F}_{2^m}$ (or the vector space $\mathbb{F}_2^m$) to the binary field $\mathbb{F}_2$ is called a *Boolean function.* Given an ordering of $\mathbb{F}_{p^m}$, 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 $\mathbb{F}_p$. We then treat a function $f : \mathbb{F}_{p^m} \to \mathbb{F}_p$ and its truth table as the same object whenever there is no ambiguity. The *component functions* of $f : \mathbb{F}_{p^m} \to \mathbb{F}_p$ are the mappings $x \mapsto \mathrm{Tr}_1^m(af(x))$ for $a \in \mathbb{F}_{p^m}^*$, where the function $\mathrm{Tr}_1^m$ denotes the usual *absolute trace function* from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p$, i.e. $\mathrm{Tr}_1^m(x) = x + x^p + x^{p^2} + \cdots + x^{p^{(m-1)}}$.

The *Hamming weight* of a $p$-ary function $f$, denoted by $wt(f)$, is the number of non-zero entries in its truth table, or equivalently, the cardinality of its *support* $\mathsf{supp}(f) := \{x \in \mathbb{F}_{p^m} : f(x) \neq 0\}$. The *Hamming distance* $d(f, g)$ between $f$ and $g$, where $f, g : \mathbb{F}_{p^m} \to \mathbb{F}_p$, equals the size of the set $\{x \in \mathbb{F}_{p^m} : f(x) \neq g(x)\}$. Throughout this paper, we represent the cardinality of a set using the symbol $\#$, so that $\#S$ is the cardinality of $S$, whereas $|u|$ will denote the absolute value of a complex number $u$. For a vector $v = (v_1, v_2, \ldots, v_m) \in \mathbb{F}_p^m$, we will use the same notation as for functions to define its support and weight, namely, $\mathsf{supp}(v) = \{i \in \{1, 2, \ldots, m\} : v_i \neq 0\}$ and $wt(v) = \#\mathsf{supp}(v)$.

The *Walsh transform* of $f : \mathbb{F}_{p^m} \to \mathbb{F}_p$ at a point $b \in \mathbb{F}_{p^m}$ is the sum of characters given by

$$W_f(b) = \sum_{x \in \mathbb{F}_{p^m}} \xi_p^{f(x) + \mathrm{Tr}_1^m(bx)}, \tag{1}$$

where $\xi_p = e^{2\pi i/p}$ is the complex primitive $p$-th root of unity. The *inverse Walsh transform* of $f$ is then defined by

$$p^m \xi_p^{f(x)} = \sum_{b \in \mathbb{F}_{p^m}} W_f(b) \xi_p^{-\mathrm{Tr}_1^m(bx)}. \tag{2}$$

The set of linear functions over $\mathbb{F}_{p^m}$ will be denoted by $\mathcal{L}_m$, whereas the set of affine functions will be denoted by $\mathcal{A}_m$. The *nonlinearity* of a function $f : \mathbb{F}_{p^m} \to \mathbb{F}_p$ is the minimum Hamming distance between $f$ and the set $\mathcal{A}_m$, that is, $\mathcal{N}_f = \min_{g \in \mathcal{A}_m} d(f, g)$.

A function $f$ is said to be *p-ary bent* (or simply *bent*) if all its Walsh coefficients satisfy $|W_f(b)|^2 = p^m$. In the binary case, a Boolean function $f : \mathbb{F}_{2^m} \to \mathbb{F}_2$ is bent if and only if $W_f(b) = \pm 2^{\frac{m}{2}}$ for any $b \in \mathbb{F}_{2^m}$ and the Walsh transform of a Boolean function $f$ can be related to $\mathcal{N}_f$ using the equality

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

A bent function $f : \mathbb{F}_{p^m} \to \mathbb{F}_p$ is said to be *regular bent* if for every $b \in \mathbb{F}_{p^m}$, $p^{-m/2} W_f(b) = \xi_p^{f^*(b)}$ for some mapping $f^* : \mathbb{F}_{p^m} \to \mathbb{F}_p$. Such a function $f^*$ 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 $up^{-m/2} W_f(b) = \xi_p^{f^*(b)}$ for all $b \in \mathbb{F}_{p^m}$. 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.

A *p-ary k-plateaued* function $f : \mathbb{F}_{p^m} \to \mathbb{F}_p$ is characterized by the property $|W_f(b)|^2 = 0$ or $p^{m+k}$ for every $b \in \mathbb{F}_{p^m}$. When $k = 0$, this definition coincides with the definition of a $p$-ary bent function given above, thus without the zero spectral values.

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 the function

$$D_\gamma f(x) = f(x + \gamma) - f(x). \tag{3}$$

A function $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ is called *almost perfect nonlinear* or *APN* if its derivatives are two-to-one. For any $a \in \mathbb{F}_{2^m}^*$ and $b \in \mathbb{F}_{2^m}$, we define

$$\delta(a, b) = \#\{x \in \mathbb{F}_{2^m} : D_a f(x) = b\}.$$

The *differential uniformity* $\delta$ of $f$ is defined as $\delta = \max_{a \in \mathbb{F}_{2^m}^*, b \in \mathbb{F}_{2^m}} \delta(a, b)$. We also say that $f$ is *$\delta$-uniform*. Then, *APN* functions are exactly the 2-uniform functions.

### 2.2 Legendre symbol and cyclotomic fields

The field $\mathbb{Q}$ can be extended by adjoining the $p$-th root of unity $\xi_p$. Since $\xi_p$ is a root of the polynomial $1+x+\ldots+x^{p-1}=\sum_{i=0}^{p-1}x^i$, this is a Galois extension of degree $p-1$ denoted by $\mathbb{Q}(\xi_p)$. The ring of integers of $\mathbb{Q}(\xi_p)$, denoted by $\mathbb{Z}(\xi_p)$, is the ring of elements $x$ in $\mathbb{Q}(\xi_p)$ for which there is an $n \in \mathbb{N}$ and there are integers $a_0,\ldots,a_{n-1} \in \mathbb{Z}$ such that $a_0+\cdots+a_{n-1}x^{n-1}+x^n=0$. Moreover, the set $\{\xi_p,\ldots,\xi_p^{p-1}\}$ is an integral basis for $\mathbb{Q}(\xi_p)$.

For an odd prime $p$ and $c \in \mathbb{F}_p$, the *Legendre symbol* is defined as

$$\left(\frac{c}{p}\right)=\begin{cases}0 & c=0;\\ 1 & c\neq 0, c \text{ is a quadratic residue modulo } p;\\ -1 & c \neq 0, c \text{ is a quadratic non-residue modulo } p.\end{cases}$$

The Legendre symbol is multiplicative, meaning that for any $a,b\in\mathbb{F}_p$, $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)=\left(\frac{ab}{p}\right)$. Additionally, $\sum_{c\in\mathbb{F}_p^*}\left(\frac{c}{p}\right)=0$ and

$$\left(\frac{-1}{p}\right)=\begin{cases}1 & p\equiv 1 \pmod 4;\\ -1 & p \equiv 3 \pmod 4).\end{cases}$$

Let $k$ be an integer, it can be proved [19] that there exist unique coefficients $a_i$ in $\mathbb{Q}$ that satisfy the equation

$$a_1\xi_p+\cdots+a_{p-1}\xi_p^{p-1}=\begin{cases}\sqrt{p}p^k & p\equiv 1 \pmod 4;\\ i\sqrt{p}p^k & p\equiv 3 \pmod 4),\end{cases} \tag{4}$$

where $a_i=\left(\frac{i}{p}\right)p^k$. For more on cyclotomic fields and field extensions, we refer the interest reader to [19].

### 2.3 Linear codes from functions

A *linear* $[n,k,d]$*-code* $\mathcal{C}$ over the alphabet $\mathbb{F}_p$ is a $k$-dimensional linear subspace of $\mathbb{F}_p^n$, whose minimum Hamming distance (equivalently, the minimum weight of its non-zero codewords) is $d$. Every code considered in this paper is a linear code, thus we will not distinguish between the terms linear code and code. The code $\mathcal{S}_m$ spanned by all linear functionals over $\mathbb{F}_{p^m}^*$ is a $[p^m-1,m,p^m-p^{m-1}]$-code, called the *(affine) m-simplex code*, i.e., $\mathcal{S}_m=\{(L(x))_{x\in\mathbb{F}_{p^m}^*} : L\in\mathcal{L}_m\}$.

Let $a_i$ be the number of codewords with Hamming weight $i$ in $\mathcal{C}$. The *weight distribution* of a code $\mathcal{C}$ is the vector $(1,a_1,\ldots,a_n)$ and it is fully specified by its *weight enumerator polynomial*, which is the polynomial $1+a_1z+\cdots+a_nz^n$. We say that a code with parameters $[n,k,d]$ is *distance-optimal*, or simply *optimal*, provided that there does not exist an $[n,k,d']$ linear code with $d<d'$.

A generic method to specify linear codes from a mapping $F:\mathbb{F}_{p^m}\to\mathbb{F}_{p^m}$ with $F(0)=0$ is described as follows. For a positive integer $m$, the linear code $\mathcal{C}_F\subset\mathbb{F}_p^{p^m-1}$ is defined by

$$\mathcal{C}_F=\left\{\mathbf{c}_{a,u}:=\left(\mathrm{Tr}_1^l(aF(x))+\mathrm{Tr}_1^m(ux)\right)_{x\in\mathbb{F}_{p^m}^*} : a\in\mathbb{F}_{p^l}, u\in\mathbb{F}_{p^m}\right\}, \tag{5}$$

where $l=1$ if the image of $F$ is contained in $\mathbb{F}_p$ and otherwise $l=m$. The dimension of $\mathcal{C}_F$ is at most $2m$ and its length is $p^m-1$. For $p=2$, the code $\mathcal{C}_F$ can be used to characterize AB functions and APN functions [5]. To avoid ambiguity, we will use capital letters to denote functions from $\mathbb{F}_{p^m}$ to $\mathbb{F}_{p^m}$ whose image is not contained in the base field $\mathbb{F}_p$ (so that $l=m$ in (5)), whereas lowercase letters will denote functions from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p$ (so that $l=t$ in (5)), whenever we are dealing with both types of functions.

This generic construction has been widely used (see, for instance [5, 6, 12, 13]). Codes with good error-correcting parameters have been reported in the literature [6, 11] by using special classes of vectorial mappings from $\mathbb{F}_p^m$ to $\mathbb{F}_p^m$. If $F:\mathbb{F}_{p^m}\to\mathbb{F}_{p^m}$ has no linear components, the linear code $\mathcal{C}_F$ derived from the generic construction in (5) has dimension $2m$. Moreover, its weights can be expressed by the Walsh transform of absolute trace functions of the map $F:\mathbb{F}_{p^m}\to\mathbb{F}_{p^m}$ as shown by the following theorem.

**Theorem 1.** *[22] Let $F$ be a function from $\mathbb{F}_{p^m}$ to $\mathbb{F}_{p^m}$ with $F(0) = 0$. Consider the linear code $\mathcal{C}_F$ defined in (5), where $l = m$. If $F$ has no linear component, then $\mathcal{C}_F$ has dimension $2m$. Moreover, for every $a \in \mathbb{F}_{p^m}, u \in \mathbb{F}_{p^m}$, we have*

$$wt(c_{a,u}) = p^m - \frac{1}{p} \sum_{\omega \in \mathbb{F}_p} W_{\psi_{\omega a}}(\omega u), \tag{6}$$

*where $\psi_\alpha : \mathbb{F}_{p^m} \to \mathbb{F}_p$ is defined by $x \mapsto \mathrm{Tr}_1^m(\alpha F(x))$ for $\alpha \in \mathbb{F}_{p^m}$. Additionally, let $f = \mathrm{Tr}_1^m(F(x))$. The linear code $\mathcal{C}_f$ (where we consider $l = 1$) defined in (5) has dimension $m+1$ when $f$ is not linear. Moreover, for every $a \in \mathbb{F}_p^*, u \in \mathbb{F}_{p^m}$, we have*

$$wt(c_{a,u}) = p^m - p^{m-1} - \frac{1}{p} \sum_{\omega \in \mathbb{F}_p^*} \sigma_\omega(\sigma_a(W_f(a^{-1}u))), \tag{7}$$

*where $\sigma_\alpha : \mathbb{Q}(\xi_p) \to \mathbb{Q}(\xi_p)$ denotes the automorphism $\sigma_\alpha(\xi_p) = \xi_p^\alpha$.*

In particular, for $p = 2$, the non-zero weights of $\mathcal{C}_F$ are $2^{m-1}$ and $2^{m-1} - \frac{1}{2} W_{\psi_\alpha}(\lambda)$ for $\alpha \in \mathbb{F}_{2^m}^*, \lambda \in \mathbb{F}_{2^m}$ [11]. For a survey on the known construction of linear codes from cryptographically significant functions we refer the reader to [18].

### 2.4 Minimal linear codes

For every $\mathbf{u}, \mathbf{v} \in \mathbb{F}_p^n$, we say that $\mathbf{u}$ *covers* $\mathbf{v}$ if and only if $\mathsf{supp}(\mathbf{v}) \subseteq \mathsf{supp}(\mathbf{u})$. We denote this relation by $\mathbf{v} \preceq \mathbf{u}$. Given an $[n, k, d]$-code $\mathcal{C} \subseteq \mathbb{F}_p^n$, a codeword $\mathbf{u} \in \mathcal{C}$ is called *minimal* if for every $\mathbf{v} \in \mathcal{C}$, the condition $\mathbf{v} \preceq \mathbf{u}$ implies that there exists $a \in \mathbb{F}_p$ such that $\mathbf{v} = a\mathbf{u}$. The code $\mathcal{C}$ is said to be *minimal* if every element $\mathbf{c} \in \mathcal{C}$ is minimal.

A sufficient condition for a code to be minimal over $\mathbb{F}_p$ was given by Ashikhmin and Barg [2]. This condition states that if the minimum weight and the maximum weight of a code are sufficiently close to each other, then the code must be minimal. More precisely, we have the following theorem.

**Lemma 1.** *Let $\mathcal{C}$ be a linear code over $\mathbb{F}_p$. Denote by $w_{\min}$ and $w_{\max}$ the minimum and maximum nonzero Hamming weights in $\mathcal{C}$, respectively. If it holds that $\frac{w_{\min}}{w_{\max}} > \frac{p-1}{p}$, then $\mathcal{C}$ is minimal.*

In this article, a linear code will be called *narrow* if it satisfies the condition of Lemma 1, namely, if $\frac{w_{\min}}{w_{\max}} > \frac{p-1}{p}$. Lemma 1 can thus be rephrased as "narrow linear codes are minimal". The above condition is not necessary and the codes satisfying $\frac{w_{\min}}{w_{\max}} \leqslant \frac{p-1}{p}$ are called *wide*.

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 and it is the content of the following lemma.

**Proposition 1.** *[17] Let $\mathcal{C} \subset \mathbb{F}_p^n$ be a linear code. The code $\mathcal{C}$ is minimal if and only if for each pair of nonzero linearly independent (over $\mathbb{F}_p$) codewords $\mathbf{a}$ and $\mathbf{b}$ in $\mathcal{C}$, we have*

$$\sum_{c \in \mathbb{F}_p^*} wt(\mathbf{a} + c\mathbf{b}) \neq (p-1)wt(\mathbf{a}) - wt(\mathbf{b}).$$

## 3 Minimal codes from the direct sum of functions

In this section, we present the direct sum method that describes a simple way to construct minimal linear codes using the bent concatenation of functions, due to the so-called $\mathcal{L}_m$-surjectivity of bent functions. Moreover, we will employ both weakly regular and non-weakly regular plateaued functions in the direct sum and specify exactly the weight distribution of the resulting minimal codes.

Note that, in general, the exact weight distributions of these codes are harder to specify than in the binary setting presented in [46]. Given two functions $f : \mathbb{F}_{p^r} \to \mathbb{F}_p$ and $g : \mathbb{F}_{p^s} \to \mathbb{F}_p$, their *direct sum* is the $p$-ary function $h : \mathbb{F}_{p^r} \times \mathbb{F}_{p^s} \to \mathbb{F}_p$ defined by $h(x, y) = f(x) + g(y)$. For any $(a, b) \in \mathbb{F}_{p^r} \times \mathbb{F}_{p^s}$, we can write

$$W_h(a,b) = \sum_{(x,y)\in\mathbb{F}_{p^r}\times\mathbb{F}_{p^s}} \xi_p^{f(x)+g(y)+\mathrm{Tr}_1^r(ax)+\mathrm{Tr}_1^s(by)} = \sum_{x\in\mathbb{F}_{p^r}} \xi_p^{f(x)+\mathrm{Tr}_1^r(ax)} \sum_{y\in\mathbb{F}_{p^s}} \xi_p^{g(y)+\mathrm{Tr}_1^s(by)} = W_f(a)W_g(b). \quad (8)$$

Thus, the Walsh spectrum of the direct sum is completely determined by the spectra of the summands. To state the main theorem in this section we will need one more concept, which describes a particular class of $p$-ary functions. Hereinafter, the symbol $l_v(x)$ will be used interchangeably with $\mathrm{Tr}_1^m(vx)$ (or its vector space counterpart) to denote the linear function defined by $v \in \mathbb{F}_{p^m}$ (or $v \in \mathbb{F}_p^m$), whenever the ambient space is clear from the context.

**Definition 1.** *A surjective function $f : \mathbb{F}_{p^m} \to \mathbb{F}_p$ is called $\mathcal{L}_m$-*surjective *if the function remains surjective after the addition of an element in $\mathcal{L}_m$. Equivalently, if, for each $v \in \mathbb{F}_{p^m}$ and $a \in \mathbb{F}_p$, there exists $x \in \mathbb{F}_{p^m}$ such that $f(x) + l_v(x) = a$.*

In characteristic two, every non-affine function is $\mathcal{L}_m$-surjective. In fact, it is not so hard to construct $\mathcal{L}_m$-surjective functions over $\mathbb{F}_{p^m}$, as illustrated by the following example.

**Example 1.** *For $m > 1$, let $\{l_1, \dots, l_m\}$ be a basis for $\mathcal{L}_m$. Take any subset $I = \{x_1, \dots, x_{p-1}\} \subset \ker(l_m)$. Let $\pi : I \to \mathbb{F}_p^*$ be a bijective function. Define the function $f : \mathbb{F}_{p^m} \to \mathbb{F}_p$ as follows:*

$$f(x) := \begin{cases} \pi(x) & x \in I; \\ -l_m(x) & \textit{otherwise}. \end{cases}$$

*Let $l = c_1 l_1 + \cdots + c_m l_m$, where $c_i \in \mathbb{F}_p$. We claim that the function $f + l$ is surjective. Indeed, let $a \in \mathbb{F}_p$. If $l = l_m$, then $x = \pi^{-1}(a)$ yields the result when $a \neq 0$, otherwise any element $x \notin I$ satisfies $f(x) + l_m(x) = 0$. If $l \neq l_m$, then take any element $x \notin I$ such that $l_m(x) - l(x) = -a$ (there are at least $p^{m-1} - p + 1$ such elements), so that $f(x) + l(x) = a$.*

An undesirable property of the class of functions presented in the previous example is that they possess a very low nonlinearity, namely, $p - 1$. On the other hand, the class of bent functions and the class of weakly regular plateaued functions are some important classes of $\mathcal{L}_m$-surjective functions in odd characteristic.

The following theorem was first stated in [46] and essentially proved for the binary case. Here, we present a complete proof for any prime $p$.

**Theorem 2.** *Let $n, r, s$ be three positive 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 an $\mathcal{L}_s$-surjective function with $g(0) = 0$ such that the code $\mathcal{C}_g = \{(ag(y) + \mathrm{Tr}_1^s(vy))_{y\in\mathbb{F}_{p^s}^*} : a \in \mathbb{F}_p, v \in \mathbb{F}_{p^s}\}$ is minimal. Consider their direct sum $h(x, y) = f(x) + g(y)$. Then the code*

$$\mathcal{C}_h = \left\{ \left(ah(x,y) + \mathrm{Tr}_1^r(ux) + \mathrm{Tr}_1^s(vy)\right)_{(x,y)\in\mathbb{F}_{p^r}\times\mathbb{F}_{p^s}\setminus\{(0,0)\}} : a \in \mathbb{F}_p, (u,v) \in \mathbb{F}_{p^r} \times \mathbb{F}_{p^s} \right\}, \quad (9)$$

*is a minimal $p$-ary linear code of length $p^n - 1$ and dimension $n + 1$.*

*Proof.* The length and dimension of $\mathcal{C}_h$ are obviously $p^n - 1$ and $n + 1$, respectively. To show that $\mathcal{C}_h$ is minimal, we will prove first that if two codewords $\mathbf{c}_1, \mathbf{c}_2$ in $\mathcal{C}_h$ are linearly independent and $\mathbf{c}_1 \preceq \mathbf{c}_2$, then the induced codewords in $\mathcal{C}_g$ are linearly independent unless one of them is zero. Let

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

be two linearly dependent non-zero codewords, i.e. $\mathbf{c}' = \lambda c$ for some $\lambda \in \mathbb{F}_p^*$, $\mathbf{c} \neq 0$. 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

$$\mathbf{c}_1 = af(x) + ag(y) + l_w(x) + l_v(y) \text{ and } \mathbf{c}_2 = \lambda af(x) + \lambda ag(y) + l_{w'}(x) + l_{\lambda v}(y).$$

Since $g$ is $\mathcal{L}_s$-surjective, for every $x \in \mathbb{F}_{p^r}$, there exists at least one $y_x$ such that $\lambda a(f(x) + g(y_x)) + \lambda l_v(y_x) + l_{w'}(x) = 0$, equivalently, $l_{w'}(x) = -\lambda(a(f(x) + g(y_x)) + l_v(y_x))$. If $\mathbf{c}_1 \preceq \mathbf{c}_2$, then $l_w(x) =$

$a(f(x)+g(y_x))+l_v(y_x)$ for every $x \in \mathbb{F}_{p^r}$. Thus, the function $l_{w'}(x)$ is equal to $\lambda l_w(x)$. This implies that $\mathbf{c}_2 = \lambda \mathbf{c}_1$. Let $\mathbf{c}_1, \mathbf{c}_2 \in \mathcal{C}_h$ be two linearly independent codewords in $\mathcal{C}_h$. By the previous paragraph and by minimality of $\mathcal{C}_g$, $\mathbf{c}_1 \not\preceq \mathbf{c}_2$ unless either of the induced codewords in $\mathcal{C}_g$ is the zero codeword. In this case, either $\mathbf{c}_1$ or $\mathbf{c}_2$ is a linear function depending on the variable $x$ only. It cannot happen that $\mathbf{c}_1 \preceq \mathbf{c}_2$ and both codewords depend linearly on $x$ only, since the simplex code is minimal. Without loss of generality, suppose that

$$\mathbf{c}_1 = (l_{w'}(x))_{(x,y)\in\mathbb{F}_{p^r}\times\mathbb{F}_{p^s}} \text{ and } \mathbf{c}_2 = (a(f(x)+g(y))+l_w(x)+l_v(y))_{(x,y)\in\mathbb{F}_{p^r}\times\mathbb{F}_{p^s}}.$$

To prove that $\mathbf{c}_1 \not\preceq \mathbf{c}_2$, 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 $\mathbf{c}_2 \not\preceq \mathbf{c}_1$. This shows that $\mathcal{C}_h$ is minimal. □

**Example 2.** *Let $p = 3$ and $m = 5$. Consider the function $g : \mathbb{F}_{3^5} \to \mathbb{F}_3$ given by $y \mapsto \mathrm{Tr}_1^5(y^{25})$. Using* MAGMA*, we have verified that $g$ is an $\mathcal{L}_5$-surjective function and that the code $\mathcal{C}_g$ is a wide minimal $[242, 6, 120]$-code with weight enumerator polynomial equal to*

$$1 + 2z^{120} + 2z^{132} + 30z^{144} + 60z^{150} + 120z^{156} + 344z^{162} + 90z^{168} + 40z^{174} + 30z^{180} + 10z^{186}.$$

*Let $f : \mathbb{F}_{3^2} \to \mathbb{F}_3$ be defined by $f(x) = \mathrm{Tr}_1^2(x)$. Theorem 2 then ensures the minimality of $\mathcal{C}_h$ for $h = f + g$. The weight enumerator polynomial of $\mathcal{C}_h$ can be easily computed (since $f$ is linear) as*

$$1 + 2z^{1080} + 2z^{1188} + 30z^{1296} + 60z^{1350} + 120z^{1404} + 6176z^{1458} + 90z^{1512} + 40z^{1566} + 30z^{1620} + 10z^{1674}.$$

*In this case, the wideness of $\mathcal{C}_g$ implies that $\mathcal{C}_h$ is also wide.*

**Remark 1.** *Note that Example 2 illustrates the generality of our method. Namely, one can obtain wide minimal linear codes from the direct sum of functions even using the simplest function (i.e., a linear function $\mathrm{Tr}_1^2(x)$) as a building block. Surprisingly, this method yields wide minimal linear codes with a larger minimum distance than some wide minimal codes obtained previously in the literature, see for instance [3, 41].*

An immediate consequence of Theorem 2 is that a bent function $g$ together with any other function $f$ give rise to minimal linear codes.

**Corollary 1.** *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 $f(0) = 0$, $g : \mathbb{F}_{p^s} \to \mathbb{F}_p$ be bent with $g(0) = 0$. Consider the direct sum $h(x, y) = f(x) + g(y)$. The code $\mathcal{C}_h$, defined by (9), is a minimal code with parameters $[p^n - 1, n + 1, d]$ where $d > (p-1)(p^{n-1} - p^{r+\frac{s}{2}-1})$.*

*Proof.* Since $g$ is bent, the minimum weight $w_{\min}$ of $\mathcal{C}_g$ satisfies $w_{\min} \geqslant (p-1)(p^{s-1} - p^{\frac{s}{2}-1})$ and every weight is at most $(p-1)(p^{s-1} + p^{\frac{s}{2}-1})$ (for a proof of these facts, see for instance [6, Theorem 2]). This tells us that the ratio $\frac{w_{\min}}{w_{\max}}$ is at least $\frac{p^{s-1}-p^{\frac{s}{2}-1}}{p^{s-1}+p^{\frac{s}{2}-1}}$, which is larger than $\frac{p-1}{p}$ because either $p > 2$ and $s \geqslant 3$ or $p = 2$ and $s \geqslant 4$. By Lemma 1, the code $\mathcal{C}_g$ is minimal. Since bent functions are $\mathcal{L}_s$-surjective, $\mathcal{C}_h$ is a minimal code by Theorem 2. For every $z \in \mathbb{F}_{p^r}$ and every two linear functions $l_u : \mathbb{F}_{p^r} \to \mathbb{F}_p$, $l_v : \mathbb{F}_{p^s} \to \mathbb{F}_p$, the set $\{y \in \mathbb{F}_{p^s} : g(y) + l_v(y) \neq f(z) + l_u(z)\}$ has cardinality at least

$$(p-1)(p^{s-1} - p^{\frac{s}{2}-1}) + 1$$

since $g(y)+l_v(y)$ is bent. Thus, any codeword in $\mathcal{C}_h$ has weight greater than $p^r(p-1)(p^{s-1}-p^{\frac{s}{2}-1})$. □

Unlike the binary linear codes derived from bent and plateaued functions used in the direct sum whose weight distributions are relatively easy to derive (see [46]), in the non-binary case more regularity is required as demonstrated in [22] and [24], where in the first reference weakly regular bent functions are employed whereas in [24] the authors considered weakly regular plateaued functions for the purpose of specifying $p$-ary linear codes with few weights. Notice that these cases of using entirely weakly regular bent or plateaued functions are intrinsically less complicated than mixing two (possibly) different structures in the direct sum $h = f + g$.

### 3.1 The weight distribution of $\mathcal{C}_h$ for (weakly regular) plateaued functions

As remarked above, the weight distribution of $p$-ary codes is in general hard to derive and can behave quite unexpectedly if no structure on the direct sum functions is imposed. To deal with this, we will consider plateaued functions in order to get additional information on the weight distribution of the codes obtained using the direct sum method.

It can be shown [24] that the Walsh values of a $p$-ary $k$-plateaued function $f : \mathbb{F}_{p^m} \to \mathbb{F}_p$ can be expressed as $u_b p^{-(m+k)/2} W_f(b) = \xi_p^{f^*(b)}$ for a complex number $u_b$ with $|u_b| = 1$ and a $p$-ary function $f^*$, where $f^* : \mathbb{F}_{p^m} \to \mathbb{F}_p$ is such that $f^*(a) = 0$ for all $a \in \mathbb{F}_{p^m} \setminus \mathsf{supp}(W_f)$, where

$$\mathsf{supp}(W_f) = \{a \in \mathbb{F}_{p^m} : |W_f(a)|^2 = p^{m+k}\}.$$

If the value of $u_b$ does not depend on $b$, then the function $f$ is called *$p$-ary weakly regular $k$-plateaued*, and *non-weakly regular $k$-plateaued* otherwise. The function $f^*(x)$ is called the *dual* of $f(x)$. Furthermore, it was shown [24] that a weakly regular $k$-plateaued function $f$ satisfies $W_f(b) = \epsilon_f \sqrt{p^*}^{m+k} \xi_p^{f^*(b)}$, where $\epsilon_f = \pm 1$ is called the *sign of the Walsh transform of $f(x)$* and $p^* = (-\frac{1}{p})p$. Similarly, one can easily show that a non-weakly regular $k$-plateaued function $f$ satisfies $W_f(b) = \epsilon_f(b)\sqrt{p^*}^{m+k} \xi_p^{f^*(b)}$, where $\epsilon_f(b) = \pm 1$ will be called *the sign of the Walsh transform of $f(x)$ at $b \in \mathbb{F}_{p^m}$*. Note that the direct sum of two plateaued functions is again a plateaued function, which is weakly regular only if both functions are weakly regular. This fact can be easily verified using Equation (8).

The following example specifies two weakly regular 1-plateaued functions, when $p = 3$ and $p = 5$.

**Example 3.** *For $p = 3$, the function $f : \mathbb{F}_{3^5} \to \mathbb{F}_3$ defined by $f(x) = \mathrm{Tr}_1^5(x^2 + 2x^4)$ is a weakly regular 1-plateaued function satisfying $\{W_f(a) : a \in \mathbb{F}_{3^5}^*\} = \{-27, -27\xi_3, -27\xi_3^2\}$. This implies that the dual $f^* : \mathbb{F}_{3^5} \to \mathbb{F}_3$ is surjective, as $f^*$ takes on all the values in $\mathbb{F}_p$. Since $(-\frac{1}{3}) = -1$, we get $\sqrt{3^*}^6 = -27$, thus $\epsilon_f = 1$. For $p = 5$, the function $f : \mathbb{F}_{5^2} \to \mathbb{F}_5$ given by $f(x) = \mathrm{Tr}_1^2(x^2 + x^6)$ is a weakly regular 1-plateaued function satisfying $\{W_f(a) : a \in \mathbb{F}_{5^2}^*\} = \{\sqrt{5}^3, \sqrt{5}^3\xi_5, \sqrt{5}^3\xi_5^4\}$. Since $(-\frac{1}{5}) = 1$, we get $\sqrt{5^*}^3 = \sqrt{5}^3$, thus $\epsilon_f = 1$.*

**Theorem 3.** *Let $f$ be $k_1$-plateaued defined over $\mathbb{F}_{p^r}$ and $g$ be $k_2$-plateaued over $\mathbb{F}_{p^s}$, with $f(0) = 0$ and $g(0) = 0$. Let $n = r + s$ and $k = k_1 + k_2$. For $a \in \mathbb{F}_p^*, \beta = (u, v) \in \mathbb{F}_{p^r} \times \mathbb{F}_{p^s}$, the weight of the vector (codeword) in $\mathcal{C}_h$ defined by (9), where $h(x, y) = f(x) + g(y)$,*

$$\mathbf{c}_{a,\beta} = \big(a(f(x) + g(y)) + \mathrm{Tr}_1^r(ux) + \mathrm{Tr}_1^s(vy)\big)_{(x,y)\in\mathbb{F}_{p^r}\times\mathbb{F}_{p^s}}$$

*is given by*

$$wt(\mathbf{c}_{a,\beta}) = p^n - p^{n-1} - \frac{1}{p}\epsilon_f(u)\epsilon_g(v)\eta_0(a^{n+k})\sqrt{p^*}^{n+k} \sum_{b\in\mathbb{F}_p^*} \eta_0(b^{n+k})\xi_p^{ba(f^*(a^{-1}u)+g^*(a^{-1}v))}, \tag{10}$$

*where $\eta_0(c) = \left(\frac{c}{p}\right)$ denotes the Legendre symbol of $c \in \mathbb{F}_p$.*

*Proof.* By plugging $h$ into Equation (7) in Theorem 1, the weight $wt(\mathbf{c}_{a,\beta})$ equals

$$p^n - p^{n-1} - \frac{1}{p}\epsilon_f(u)\epsilon_g(v) \sum_{b\in\mathbb{F}_p^*} \sigma_b(\sigma_a(\sqrt{p^*}^{n+k}\xi_p^{f^*(a^{-1}u)+g^*(a^{-1}v)})),$$

by using the corresponding values of $W_{f+g}$ in (7), where it can be easily verified that

$$W_{f+g}(u, v) = W_f(u)W_g(v) = \epsilon_f(u)\sqrt{p^*}^{r+k_1}\xi_p^{f^*(u)}\epsilon_g(v)\sqrt{p^*}^{s+k_2}\xi_p^{g^*(v)} = \epsilon_f(u)\epsilon_g(v)\sqrt{p^*}^{n+k}\xi_p^{f^*(u)+g^*(v)}.$$

Using the fact that $\sigma_z(\sqrt{p^*}^{n+k}) = \left(\frac{z^{n+k}}{p}\right)\sqrt{p^*}^{n+k}$, for each $z \in \mathbb{F}_p^*$, gives

$$\sum_{b\in\mathbb{F}_p^*} \left(\frac{a^{n+k}}{p}\right)\left(\frac{b^{n+k}}{p}\right)\sqrt{p^*}^{n+k}\xi_p^{ba(f^*(a^{-1}u)+g^*(a^{-1}v))},$$

which establishes the result. ∎

**Example 4.** *Let us illustrate how to apply Theorem 3, when two weakly regular plateaued functions are employed. Let $f : \mathbb{F}_{3^3} \to \mathbb{F}_3$ be the weakly regular 1-plateaued function defined by $x \mapsto \mathrm{Tr}_1^3(\omega x^{13} + \omega^7 x^4 + \omega^7 x^3 + \omega x^2)$, where $\omega$ is a generator of $\mathbb{F}_{3^3}^*$, and let $g : \mathbb{F}_{3^4} \to \mathbb{F}_3$ be the weakly regular 1-plateaued function defined by $g(y) = \mathrm{Tr}_1^4(y^2 + 2y^4)$. One can check that $\epsilon_f = -1$ and $\epsilon_g = 1$. For $\beta = (u, v) = (0, 0) \in \mathbb{F}_{3^3} \times \mathbb{F}_{3^4}$ and $a = 2 \in \mathbb{F}_3^*$, the duals of $f$ and $g$ satisfy $f^*(a^{-1}u) = f^*(0) = 1$ and $g^*(a^{-1}v) = 0$. Therefore, for instance, the codeword $\boldsymbol{c}_{2,(0,0)}$ has weight*

$$3^7 - 3^6 + \left(\frac{-1}{3}\right) i 3^{7/2} \sum_{b \in \mathbb{F}_3^*} \eta(b) \xi_3^{2b}.$$

*This equals $3^7 - 3^6 - 3^4 = 1377$, since $(\frac{-1}{3}) = -1$ and $\sum_{b \in \mathbb{F}_3^*} \eta(b)\xi_3^{2b} = -i\sqrt{3}$.*

Since the direct sum of two weakly regular plateaued functions is weakly regular, we can derive the weight distribution of the code $\mathcal{C}_h$ given in (9) by adapting the results of Mesnager et. al. [24] for the direct sum method. However, their results only apply to a subclass of weakly regular plateaued functions (see Remark 2), that is why we restrict our discussion to the use of a mixed structure considering a weakly regular plateaued function and a weakly regular bent function.

In order to explicitly compute the weights of the derived codes $\mathcal{C}_h$, defined by Equation (9), where $h(x, y) = f(x) + g(y)$, $f$ is a weakly regular $k$-plateaued function and $g$ is a weakly regular bent function, we must count the number of elements in the preimage of a given function. More precisely, using a similar notation than in [24], given $f_1 : \mathbb{F}_{p^m} \to \mathbb{F}_p$ and any function $f_2 : \mathsf{supp}(W_{f_1}) \to \mathbb{F}_p$, define the sets

$$N_{f_2}(j) = \{x \in \mathsf{supp}(W_{f_1}) : f_2(x) = j\} \tag{11}$$

and the numbers $n_{f_2}(j) = \#N_{f_2}(j)$, for $j \in \mathbb{F}_p$.

**Remark 2.** *The authors in [24] considered general weakly regular plateaued functions $f$, however, their results (Proposition 4 and its consequences) apply only to the case when the dual $f^*$ fulfills the condition $N_{f^*}(j) \neq \emptyset$ for each $j$, i.e., $f^*$ is surjective. Nevertheless, there exist weakly regular plateaued functions whose dual $f^*$ is not surjective. On the other hand, the direct sum $h$ of any weakly regular plateaued function with a weakly bent function always satisfies $N_{h^*}(j) \neq \emptyset$, which can then be used in Corollary 1 to obtain 3-weight minimal codes (see Example 5 below).*

**Example 5.** *Let $p = r = s = 3$. The ternary function $f(x) = \mathrm{Tr}_1^3(2x^4 + x^2)$ is a weakly regular 2-plateaued function with $W_f(b) \in \{0, i3^{5/2}, i3^{5/2}\xi_3^2\}$. Moreover, $\mathsf{supp}(W_f) = \mathbb{F}_3$ and $f^* : \mathsf{supp}(W_f) \to \mathbb{F}_3$ satisfies $n_{f^*}(0) = 1, n_{f^*}(1) = 0$, and $n_{f^*}(2) = 2$. The code $\mathcal{C}_f$ has two non-zero weights and its weight enumerator is $1 + 4z^9 + 76z^{18}$. Furthermore, take any weakly regular bent function $g : \mathbb{F}_{p^s} \to \mathbb{F}_p$. The direct sum*

$$h(x, y) = f(x) + g(y) = \mathrm{Tr}_1^3(2x^4 + x^2) + g(y)$$

*will yield a 3-weight code (with weight distribution displayed in Table 2) since $h$ is weakly regular 2-plateaued, whose dual $h^* = f^* + g^*$ satisfies $N_{h^*}(j) = \sum_{i \in \mathbb{F}_p} N_{f^*}(i) N_{g^*}(j - i) \neq \emptyset$ for each $j$.*

As mentioned above, using the same technique as in [24], we can derive the weight distribution of $\mathcal{C}_h$, defined by Equation (9), where $h(x, y) = f(x) + g(y)$, $f$ is a weakly regular $k$-plateaued function and $g$ is a weakly regular bent function (recall that we treat it as a 0-plateaued function). Then, the weight distribution is displayed in Table 1 when $n + k := r + s + k$ is even and in Table 2 when $n + k$ is odd (referring to Theorem 3, we are setting $k_2 = 0$ so that $k = k_1$).

Table 1: Weight distribution of $\mathcal{C}_h$ for $h(x, y) = f(x) + g(y)$ with $f : \mathbb{F}_p^r \to \mathbb{F}_p$ a weakly regular $k$-plateaued function and $g : \mathbb{F}_p^s \to \mathbb{F}_p$ a weakly regular bent function, when $n + k$ is even.

| Weight $w$ | Number of codewords |
|---|---|
| $p^n - p^{n-1}$ | $p^n - 1 + (p-1)(p^n - p^{n-k})$ |
| $p^n - p^{n-1} - \epsilon_f \epsilon_g \left(\frac{-1}{p}\right)^{\frac{n+k}{2}} p^{(n+k-2)/2}(p-1)$ | $(p-1)p^{n-k-1} + \left(\frac{-1}{p}\right)^{\frac{n+k}{2}} (p-1)^2(\epsilon_f \epsilon_g p^{\frac{n-k-2}{2}})$ |
| $p^n - p^{n-1} + \epsilon_f \epsilon_g \left(\frac{-1}{p}\right)^{\frac{n+k}{2}} p^{(n+k-2)/2}$ | $(p-1)(p^{n-k} - p^{n-k-1}) - \left(\frac{-1}{p}\right)^{\frac{n+k}{2}} (p-1)^2(\epsilon_f \epsilon_g p^{\frac{n-k-2}{2}})$ |

Table 2: Weight distribution of $\mathcal{C}_h$ for $h(x,y) = f(x) + g(y)$ with $f : \mathbb{F}_p^r \to \mathbb{F}_p$ a weakly regular $k$-plateaued function and $g : \mathbb{F}_p^s \to \mathbb{F}_p$ a weakly regular bent function, when $n+k$ is odd.

| Weight $w$ | Number of codewords |
|---|---|
| $p^n - p^{n-1}$ | $p^{n+1} - p^{n-k-1}(p-1)^2 - 1$ |
| $p^n - p^{n-1} - \epsilon_f\epsilon_g \left(\frac{-1}{p}\right)^{\frac{n+k+1}{2}} p^{(n+k-1)/2}$ | $\frac{(p-1)^2}{2}(p^{n-k-1} + \epsilon_f\epsilon_g \left(\frac{-1}{p}\right)^{\frac{n+k+1}{2}} p^{\frac{n-k-1}{2}})$. |
| $p^n - p^{n-1} + \epsilon_f\epsilon_g \left(\frac{-1}{p}\right)^{\frac{n+k+1}{2}} p^{(n+k-1)/2}$ | $\frac{(p-1)^2}{2}(p^{n-k-1} - \epsilon_f\epsilon_g \left(\frac{-1}{p}\right)^{\frac{n+k+1}{2}} p^{\frac{n-k-1}{2}})$. |

**Example 6.** *Let $f : \mathbb{F}_{3^3} \to \mathbb{F}_3$ be the weakly regular 1-plateaued function defined by $x \mapsto \mathrm{Tr}_1^3(\omega x^{13} + \omega^7 x^4 + \omega^7 x^3 + \omega x^2)$, where $\omega$ is a generator of $\mathbb{F}_{3^3}^*$ with $\omega^3 + 2\omega + 1 = 0$, whose sign is $\epsilon_f = -1$. Let $g : \mathbb{F}_{3^2} \to \mathbb{F}_3$ be the weakly regular bent function defined by $g(y) = \mathrm{Tr}_1^2(y^2)$, whose sign is $\epsilon_g = -1$. Since $\left(\frac{-1}{3}\right) = -1$ and $n+k = 6$, we have*

$$\epsilon_f\epsilon_g \left(\frac{-1}{p}\right)^{\frac{n+k}{2}} = (-1)(-1)\left(\frac{-1}{3}\right)^3 = -1.$$

*Let $h(x,y) = f(x) + g(y)$ be their direct sum. Computer simulations show that the enumerator polynomial of the linear code $\mathcal{C}_h$, given in (9), is $1 + 120z^{153} + 566z^{162} + 42z^{180}$, which is in accordance with Table 1. Similarly, using the same function $f$ together with the weakly regular bent function $g : \mathbb{F}_{3^3} \to \mathbb{F}_3$ given by $g(y) = \mathrm{Tr}_1^3(y^2)$ (in this case $\epsilon_g = 1$). The enumerator polynomial of $\mathcal{C}_h$ is $1 + 180z^{459} + 1862z^{486} + 144z^{513}$, where $h(x,y) = f(x) + g(y)$. This is in accordance with Table 2.*

A very similar description of the weight distribution of $\mathcal{C}_h$ can be carried out when either $f$ or $g$ is non-weakly regular and the other function is weakly regular, assuming that the dual of the non-weakly constituent has additional symmetry. In the next section, we will discuss the case when $g$ is a weakly regular bent function and $f$ is a non-weakly regular $k$-plateaued function.

### 3.2 Minimal codes from non-weakly regular plateaued functions

Unlike the weakly regular case, little is known about non-weakly regular functions. To the best of our knowledge, the only constructions of linear codes from non-weakly regular functions are given in [29, 31], where the use of non-weakly regular bent functions was considered. In this section, for the first time, we propose a method of constructing linear codes from non-weakly regular plateaued functions. More precisely, we will first specify the weight distributions of the codes derived from a non-weakly regular plateaued function $f$ satisfying certain conditions (given in Lemma 3). Then, we employ the direct sum method whose constituent functions are a non-weakly regular plateaued function and a weakly regular bent function.

Following the terminology introduced in [29, 31], for a given set $S \subseteq \mathbb{F}_{p^m}$, we say that a function $f : S \to \mathbb{F}_p$ is *bent relative to* $S$ if $|W_f(\alpha)| = \#S^{1/2}$ for all $\alpha \in \mathbb{F}_{p^m}$, where $W_f(\alpha)$ is considered as the restriction to $S$ of the Walsh transform of $f$, i.e.,

$$W_f(\alpha) = \sum_{x \in S} \xi_p^{f(x) + \mathrm{Tr}_1^m(\alpha x)}. \tag{12}$$

For weakly regular plateaued functions, the dual function $f^*$ is bent relative to $\mathsf{supp}(W_f)$. For non-weakly regular plateaued functions, the dual may or may not be bent relative to $\mathsf{supp}(W_f)$. There are infinitely many examples of both cases.

Let $S \subseteq \mathbb{F}_{p^m}$ be such that $|S|$ is a positive divisor of $p^m$. Let $f : S \to \mathbb{F}_p$ be a function such that

$$W_f(0) = \sum_{x \in S} \xi_p^{f(x)} = t(f)\nu p^{\frac{\mu}{2}} \xi_p^j,$$

where $t(f) = \pm 1$ or 0, $\nu \in \{1, i\}$, $j \in \mathbb{F}_p$ and $\mu = m + k$ or $\mu = m - k$ for some $0 \leq k \leq m$. The number $t(f)$ will be called the *type of* $f$.

For a $k$-plateaued function $f : \mathbb{F}_{p^m} \to \mathbb{F}_p$ with $0 \leq k \leq m$, let $\Gamma^+(f)$ and $\Gamma^-(f)$ be the sets that partition $S = \mathsf{supp}(W_f)$ and are given by

$$\Gamma^+(f) = \{w \in S : W_f(w) = \nu p^{\frac{m+k}{2}} \xi_p^{f^*(w)}\},\ \Gamma^-(f) = \{w \in S : W_f(w) = -\nu p^{\frac{m+k}{2}} \xi_p^{f^*(w)}\}, \tag{13}$$

where $\nu \in \{1, i\}$. Note that in this case $t(f) = \epsilon_f(0) \left(\frac{-1}{p}\right)^{\mu}$, where $\epsilon_f(0)$ denotes the sign of $W_f$ at 0.

**Lemma 2.** *[24, 31] Let $f : \mathbb{F}_{p^m} \to \mathbb{F}_p$ be a $k$-plateaued function such that its dual $f^*$ is bent relative to* $\mathsf{supp}(f)$*, and it satisfies $N_{f^*}(j) \neq \emptyset$ for each $j$ and $f^{**}(0) = i_0$, where $f^{**}$ denotes the dual of $f^*$. When $m - k$ is odd, for $1 \leq j \leq p - 1$,*

$$n_{f^*}(i_0) = p^{m-k-1}, n_{f^*}(i_0 + j) = p^{m-k-1} + t(f^*) \left(\frac{j}{p}\right) p^{\frac{m-k-1}{2}}.$$

*When $m - k$ is even,*

$$n_{f^*}(i_0) = p^{m-k-1} + t(f^*)p^{\frac{m-k}{2}} - t(f^*)p^{\frac{m-k}{2}-1}, n_{f^*}(j) = p^{m-k-1} - t(f^*)p^{\frac{m-k}{2}-1}$$

*for $j \neq i_0$.*

For a $k$-plateaued function $f : \mathbb{F}_{p^m} \to \mathbb{F}_p$, define the numbers $A_j := \#(N_{f^*}(j) \cap \Gamma^+(f))$ and $B_j := \#(N_{f^*}(j) \cap \Gamma^-(f))$ for $j \in \mathbb{F}_p$. Employing Lemma 2, we will now determine the exact values of $A_j, B_j$ for certain non-weakly regular plateaued functions.

**Lemma 3.** *Let $f$ be a non-weakly regular $k$-plateaued over $\mathbb{F}_{p^r}$ such that $f(0) = 0$. If the dual $f^*$ is the constant zero function, then $A_0 = \#\Gamma^+(f) = \frac{p^{r-k}+p^{\frac{r-k}{2}}}{2}$ and $B_0 = \#\Gamma^-(f) = \frac{p^{r-k}-p^{\frac{r-k}{2}}}{2}$. If $f^*$ is bent relative to* $\mathsf{supp}(f)$ *and it satisfies $N_{f^*}(j) \neq \emptyset$ for every $j \in \mathbb{F}_p$, define $\theta_a = t(f^*) + a \left(\frac{-1}{p}\right)^{r+k}$ for $a \in \{-1, 0, 1\}$. Then, setting $Z_0 := A_0 - B_0$, we have:*

- *For $r - k$ odd, $\#\Gamma^+(f) = \frac{p^{r-k}+pZ_0}{2}$, $\#\Gamma^-(f) = \frac{p^{r-k}-pZ_0}{2}$ and*

$$A_j = \frac{p^{r-k-1} + \theta_1 \left(\frac{j}{p}\right) p^{\frac{r-k-1}{2}} + Z_0}{2}, B_j = \frac{p^{r-k-1} + \theta_{-1} \left(\frac{j}{p}\right) p^{\frac{r-k-1}{2}} - Z_0}{2},$$

  *for $j \in \mathbb{F}_p^*$.*

- *For $r - k$ even, $\#\Gamma^+(f) = \frac{p^{r-k}-p^{\frac{r-k}{2}}(p-1)+pZ_0}{2}$, $\#\Gamma^-(f) = \frac{p^{r-k}-pZ_0+p^{\frac{r-k}{2}}(p-1)}{2}$ and*

$$A_j = \frac{p^{r-k-1} - p^{\frac{r-k}{2}} - \theta_0 p^{\frac{r-k}{2}-1} + Z_0}{2}, B_j = \frac{p^{r-k-1} + p^{\frac{r-k}{2}} - \theta_0 p^{\frac{r-k}{2}-1} - Z_0}{2},$$

  *for $j \in \mathbb{F}_p^*$.*

*Proof.* For this proof, set $A = \#\Gamma^+(f)$ and $B = \#\Gamma^-(f)$. If $f^*$ is the zero function, then only $A_0$ and $B_0$ are non-zero. In the other case, $A_j, B_j$ are non-zero for each $j$. By the inverse Walsh transform and $f(0) = 0$,

$$\sum_{j=0}^{p-1} \Big( \sum_{x \in \Gamma^+(f)} \nu p^{\frac{r+k}{2}} \xi_p^j - \sum_{x \in \Gamma^-(f)} \nu p^{\frac{r+k}{2}} \xi_p^j \Big) = p^r. \tag{14}$$

Suppose that $f^*$ is the zero function. In this case, Equation (14) yields $A - B = Z_0 = \nu^{-1} p^{\frac{r-k}{2}}$ which implies that $\nu = 1$ and $r - k$ is even. Moreover, since $A + B = p^{r-k}$, we get $A = \frac{p^{r-k}+p^{\frac{r-k}{2}}}{2}$ and

$B = \frac{p^{r-k}-p^{\frac{r-k}{2}}}{2}$. Suppose that $f^*$ is bent relative to $\mathsf{supp}(W_f)$ and $N_{f^*}(j) \neq \emptyset$ for each $j$. For $r-k$ odd, working out Equation (14), we get

$$\sum_{j=1}^{p-1} \xi_p^j (A_j - B_j - Z_0) = \nu^{-1} p^{\frac{r-k}{2}} = \left(\frac{-1}{p}\right)^{r+k} \nu \sqrt{p} p^{\frac{r-k-1}{2}}.$$

Now, as $\xi_p, \ldots, \xi_p^{p-1}$ form a basis for $\mathbb{Q}(\xi_p)$ over $\mathbb{Q}$, then $\left(\frac{-1}{p}\right)^{r+k} (A_j - B_j - Z_0) = \left(\frac{j}{p}\right) p^{\frac{r-k-1}{2}}$. Then $\left(\frac{-1}{p}\right)(A-B) = \left(\frac{-1}{p}\right) \sum_{j=0}^{p-1}(A_j - B_j) = \left(\frac{-1}{p}\right) pZ_0$ so $A - B = pZ_0$. On the other hand, $A + B = p^{r-k}$. Therefore, $A = \frac{p^{r-k}+pZ_0}{2}$ and $B = \frac{p^{r-k}-pZ_0}{2}$. For the case $r-k$ even, rearrange Equation (14) to obtain

$$\sum_{j=1}^{p-1} \xi_p^j (A_j - B_j - Z_0 + p^{\frac{r-k}{2}}) = 0,$$

then $A_j - B_j - Z_0 + p^{\frac{r-k}{2}} = 0$ by linear independence of $\{\xi_p, \ldots, \xi_p^{p-1}\}$, so that $(A-B) = pZ_0 - p^{\frac{r-k}{2}}(p-1)$. On the other hand, $A+B = p^{r-k}$. Therefore, $A = \frac{p^{r-k}-p^{\frac{r-k}{2}}(p-1)+pZ_0}{2}$ and $B = \frac{p^{r-k}-pZ_0+p^{\frac{r-k}{2}}(p-1)}{2}$. Finally, by combining the obtained values for $A_j - B_j$ with Lemma 2, we get the result. $\square$

**Remark 3.** *Lemma 3 gives the full description of the Walsh spectrum of a subclass of non-weakly regular plateaued functions in terms of $Z_0$. Therefore, it provides an efficient computation of Walsh values from the knowledge of $A_0$ and $B_0$. Moreover, we highlight the possibility of extending this result to a broader class of non-weakly regular plateaued functions, e.g., when exactly one of the sets $N_{f^*}(j), j \neq 0$, is empty.*

We are now able to get the weight distributions of the codes $\mathcal{C}_f$ in (5) (with $l = t = 1$), when $f$ is a non-weakly regular plateaued function satisfying the conditions of Lemma 3.

**Theorem 4.** *Let $f = \mathrm{Tr}_1^r(F(x))$ be a non-weakly regular $k$-plateaued defined over $\mathbb{F}_{p^r}$, whose dual is bent relative to $\mathsf{supp}(W_f)$ and $N_{f^*}(j) \neq \emptyset$ for each $j \in \mathbb{F}_p$, where $F : \mathbb{F}_{p^r} \to \mathbb{F}_{p^r}$ and $F(0) = 0$. The code $\mathcal{C}_f$ in (5) (with $l = t = 1$) is a $[p^r - 1, r+1, d]$-code that is either five-valued or three-valued depending on the parity of $r+k$, whose weight distribution is displayed in Table 3 and Table 4 for $r+k$ even and $r+k$ odd, respectively.*

*Proof.* We will only prove the case $r+k$ odd since the even case is similar. The weights of $\mathcal{C}_f$ are easily derived from Theorem 1, which are $p^r - p^{r-1} - p^{(r+k-1)/2}, p^r - p^{r-1}$ and $p^r - p^{r-1} + p^{(r+k-1)/2}$. To count the number of codewords that attain the weight $p^r - p^{r-1} - p^{(r+k-1)/2}$, we must count the number of pairs $(\alpha, \beta) \in \mathbb{F}_{p^r}^* \times \mathbb{F}_{p^r}$ such that $f^*(\alpha^{-1}\beta) \neq 0$ and make $\left(\frac{-1}{p}\right)^{r+k} \epsilon_f(\alpha^{-1}\beta) \left(\frac{f^*(\alpha^{-1}\beta)}{p}\right)$ positive. That is to say, we must compute the number

$$\sum_{j \in \mathbb{F}_p^*, \left(\frac{j}{p}\right) = \left(\frac{-1}{p}\right)^{r+k}} (p-1)A_j + \sum_{j \in \mathbb{F}_p^*, \left(\frac{j}{p}\right) = -\left(\frac{-1}{p}\right)^{r+k}} (p-1)B_j.$$

By Lemma 3, this sum equals $\frac{1}{2}(p-1)^2(p^{r-k-1} + \left(\frac{-1}{p}\right)^{r+k} p^{\frac{r-k-1}{2}})$. Similarly, the number of codewords for the weight $p^r - p^{r-1} + p^{(r+k-1)/2}$ is $\frac{1}{2}(p-1)^2(p^{r-k-1} - \left(\frac{-1}{p}\right)^{r+k} p^{\frac{r-k-1}{2}})$. Finally, the number of balanced codewords equals

$$p^r - 1 + \#\{(\alpha, \beta) \in \mathbb{F}_{p^r}^* \times \mathbb{F}_{p^r} : W_f(\alpha^{-1}\beta) = 0\} + \#\{(\alpha, \beta) \in \mathbb{F}_{p^r}^* \times \mathbb{F}_{p^r} : f^*(\alpha^{-1}\beta) = 0\},$$

which is, by Lemma 2 and using the fact that $\#\mathsf{supp}(W_f) = p^{r-k}$, $p^r - 1 + (p-1)(p^r - p^{r-k}) + (p-1)p^{r-k-1} = p^{r+1} - p^{r-k+1} + 2p^{r-k} - p^{r-k-1} - 1$, equivalently, $p^{r+1} - (p-1)^2 p^{r-k-1} - 1$. $\square$

Table 3: Weight distribution of the code $\mathcal{C}_f$, derived in Theorem 4, for a non-weakly regular $k$-plateaued function $f : \mathbb{F}_{p^r} \to \mathbb{F}_p$, whose dual is bent relative to $\mathsf{supp}(W_f)$, when $r+k$ is even.

| Weight $w$ | Number of codewords |
|---|---|
| $p^r - p^{r-1} - p^{(r+k-2)/2}(p-1)$ | $\frac{(p-1)}{2}(p^{r-k-1} + t(f^*)p^{\frac{r-k}{2}} - t(f^*)p^{\frac{r-k}{2}-1} + Z_0)$ |
| $p^r - p^{r-1} - p^{(r+k-2)/2}$ | $\frac{(p-1)^2}{2}(p^{r-k-1} + p^{\frac{r-k}{2}} - t(f^*)p^{\frac{r-k}{2}-1} - Z_0)$ |
| $p^r - p^{r-1}$ | $p^{r+1} - (p-1)p^{r-k} - 1$ |
| $p^r - p^{r-1} + p^{(r+k-2)/2}$ | $\frac{(p-1)^2}{2}(p^{r-k-1} - p^{\frac{r-k}{2}} - t(f^*)p^{\frac{r-k}{2}-1} + Z_0)$ |
| $p^r - p^{r-1} + p^{(r+k-2)/2}(p-1)$ | $\frac{(p-1)}{2}(p^{r-k-1} + t(f^*)p^{\frac{r-k}{2}} - t(f^*)p^{\frac{r-k}{2}-1} - Z_0)$ |

Table 4: Weight distribution of the code $\mathcal{C}_f$, derived in Theorem 4, for a non-weakly regular $k$-plateaued function $f : \mathbb{F}_{p^r} \to \mathbb{F}_p$, whose dual is bent relative to $\mathsf{supp}(W_f)$, when $r+k$ is odd.

| Weight $w$ | Number of codewords |
|---|---|
| $p^r - p^{r-1} - p^{(r+k-1)/2}$ | $\frac{(p-1)^2}{2}(p^{r-k-1} + \left(\frac{-1}{p}\right)^{r+k} p^{\frac{r-k-1}{2}})$ |
| $p^r - p^{r-1}$ | $p^{r+1} - (p-1)^2 p^{r-k-1} - 1$ |
| $p^r - p^{r-1} + p^{(r+k-1)/2}$ | $\frac{(p-1)^2}{2}(p^{r-k-1} - \left(\frac{-1}{p}\right)^{r+k} p^{\frac{r-k-1}{2}})$ |

**Example 7.** *Let $f : \mathbb{F}_{3^2} \to \mathbb{F}_3$ and $g : \mathbb{F}_{3^3} \to \mathbb{F}_3$ be given by $f(x) = \mathrm{Tr}_1^2(x^2 + 2x^4)$ and $g(y) = \mathrm{Tr}_1^3(y^8 + y^{14})$. The function $f$ is a weakly regular 1-plateaued function and $g$ is a non-weakly regular bent function. Their Walsh spectra are*

$$\{W_f(b) : b \in \mathbb{F}_{3^2}\} = \{0, -i3^{3/2}, -i3^{3/2}\xi_3\} \text{ and } \{W_g(b) : b \in \mathbb{F}_{3^3}\} = \{\pm i3^{3/2}, -i3^{3/2}\xi_3, \pm i3^{3/2}\xi_3^2\}$$

*Let $\omega_1$ be a generator of $\mathbb{F}_{3^2}$ such that $\omega_1^2 + 2\omega_1 + 2 = 0$ and $\omega_2$ be a generator of $\mathbb{F}_{3^3}$ such that $\omega_2^3 + 2\omega_2 + 1 = 0$. The dual function $f^*$ is defined on $\mathsf{supp}(W_f) = \{0, \omega_1^2, \omega_1^6\}$ and it is given by $f^*(0) = 0$, $f^*(\omega_1^2) = 1$ and $f^*(\omega_1^6) = 1$. The truth table of $g^*$ is*

$$(0, 2, 1, 2, 2, 1, 1, 0, 0, 2, 2, 0, 2, 0, 2, 1, 2, 2, 1, 1, 0, 0, 2, 2, 0, 2, 0),$$

*where we use the ordering $1, \omega_2, \omega_2^2, \ldots, \omega_2^{25}, 0$ of $\mathbb{F}_{3^3}$. Moreover, it can be verified that $g^*$ is a non-weakly regular bent function and $f^*$ is bent relative to $\mathsf{supp}(W_f)$, and*

$$W_{f^*}(0) = \sum_{x \in \mathsf{supp}(W_f)} \xi_3^{f^*(x)} = 2\xi_3 + 1 = \sqrt{3}i, \text{ and } W_{g^*}(0) = \sum_{y \in \mathbb{F}_{3^3}} \xi_3^{g^*(y)} = -6\xi_3 - 3 = -\sqrt{3}^3 i,$$

*hence $t(f^*) = 1$ and $t(g^*) = -1$. Consider the function $h : \mathbb{F}_{3^2} \times \mathbb{F}_{3^3} \to \mathbb{F}_3$ given by $h(x,y) = f(x) + g(y)$. Then $h$ is a non-weakly regular 1-plateaued function, whose Walsh spectrum satisfies*

$$\{W_h(u,v) : (u,v) \in \mathbb{F}_{3^2} \times \mathbb{F}_{3^3}\} = \{0, \pm 27, \pm 27\xi_3, \pm 27\xi_3^2\}.$$

*This implies that its dual $h^*$ is surjective (equivalently, $N_{h^*}(j) \neq \emptyset$ for each $j$). Moreover, $h^*$ is bent relative to $\mathsf{supp}(W_h)$ and*

$$W_{h^*}(0,0) = \sum_{(x,y) \in \mathsf{supp}(W_h)} \xi_3^{h^*(x,y)} = W_{f^*}(0)W_{g^*}(0) = 9,$$

*hence $t(h^*) = 1$. In this case, we have $A_0 = 15$ and $B_0 = 18$, thus $Z_0 = -3$. The weight enumerator polynomial of the code $\mathcal{C}_h$, defined in (9), is*

$$1 + 30z^{144} + 72z^{153} + 566z^{162} + 24z^{171} + 36z^{180},$$

*which is in accordance with Theorem 4 and Table 3.*

Note that if $f=\mathrm{Tr}_1^r(F(x))$ is a non-weakly regular $k$-plateaued defined over $\mathbb{F}_{p^r}$ such that $F:\mathbb{F}_{p^r}\to\mathbb{F}_{p^r}$ and $F(0)=0$, whose dual $f^*$ is bent relative to $\mathsf{supp}(W_f)$ and $N_{f^*}(j)\neq\emptyset$, and $g=\mathrm{Tr}_1^s(G(x))$ is a weakly regular bent function over $\mathbb{F}_{p^s}$, where $G:\mathbb{F}_{p^s}\to\mathbb{F}_{p^s}$ and $G(0)=0$. Then the function $h(x,y)=f(x)+g(y)$ is a non-weakly regular $k$-plateaued function whose dual $h^*=f^*+g^*$ is bent relative to $\mathsf{supp}(W_h)$, $N_{h^*}(j)\neq\emptyset$ for each $j$ and it has type $t(h^*)=t(f^*)\epsilon_g\left(\frac{-1}{p}\right)^s$. Thus, the code $\mathcal{C}_h$, where $h(x,y)=f(x)+g(y)$, is a minimal code. The weight distribution can then be obtained by applying Theorem 4 (thus inferred from Table 3 and Table 4).

Moreover, we can deduce a similar result when the dual of $f$ is the zero function.

**Theorem 5.** *Let $f=\mathrm{Tr}_1^r(F(x))$ be a non-weakly regular $k$-plateaued over $\mathbb{F}_{p^r}$, where $F:\mathbb{F}_{p^r}\to\mathbb{F}_{p^r}$ and $F(0)=0$, whose dual $f^*$ is the constant zero function (hence $r+k$ is even). Let $g=\mathrm{Tr}_1^s(G(x))$ be a weakly regular bent function over $\mathbb{F}_{p^s}$, where $G:\mathbb{F}_{p^s}\to\mathbb{F}_{p^s}$ and $G(0)=0$. Let $n=r+s$. For $\alpha\in\mathbb{F}_p,\beta=(a,b)\in\mathbb{F}_{p^r}\times\mathbb{F}_{p^s}$, the code $\mathcal{C}_h$ in (9), where $h(x,y)=f(x)+g(y)$, is a minimal $[p^n-1,n+1,d]$-code that is either five-valued or three-valued depending on the parity of $n+k$. Its weight distribution is displayed in Tables 5 and Table 6 for $n+k$ even and $n+k$ odd, respectively.*

*Proof.* The function $h(x,y)=f(x)+g(y)$ is clearly a non-weakly regular $k$-plateaued function. The weights are easily derived from Theorem 3. Let us find their distribution only for the case when $s$ is even since the other case is similar. Using Lemma 2, we see that the number of $(\alpha,\beta)\in\mathbb{F}_{p^n}^*\times\mathbb{F}_{p^n}$ such that $\alpha^{-1}\beta\in\mathsf{supp}(W_h)$ and $h^*(\alpha^{-1}\beta)=0$, which lead to a positive sign in $W_h$ equals

$$\frac{(1+t(g^*))}{2}(p-1)A_0(p^{s-1}+t(g^*)p^{\frac{s}{2}}-t(g^*)p^{\frac{s}{2}-1})+\frac{(1-t(g^*))}{2}(p-1)B_0(p^{s-1}+t(g^*)p^{\frac{s}{2}}-t(g^*)p^{\frac{s}{2}-1}).$$

According to Theorem 3, $A_0=\frac{p^{r-k}+p^{\frac{r-k}{2}}}{2}, B_0=\frac{p^{r-k}-p^{\frac{r-k}{2}}}{2}$, so that the number of codewords with weight $p^n-p^{n-1}-p^{(n+k-2)/2}(p-1)$ is

$$\frac{1}{2}(p-1)(p^{s-1}+t(g^*)p^{\frac{s}{2}}-t(g^*)p^{\frac{s}{2}-1})(p^{r-k}+t(g^*)p^{\frac{r-k}{2}}),$$

where $t(g^*)=\left(\frac{-1}{p}\right)^s\epsilon_g$ as $g$ is weakly regular. Similarly, the weight $p^n-p^{n-1}+p^{(n+k-2)/2}(p-1)$ is attained $\frac{1}{2}(p-1)(p^{s-1}+t(g^*)p^{\frac{s}{2}}-t(g^*)p^{\frac{s}{2}-1})(p^{r-k}-t(g^*)p^{\frac{r-k}{2}})$ times. Again using Lemma 2, the number of times that $h^*(\alpha^{-1}\beta)\neq 0$, which lead to a positive sign in $W_h$ and to a negative sign in $W_h$, equal to $\frac{1}{2}(p-1)(p^{s-1}-t(g^*)p^{\frac{s}{2}-1})(p^{r-k}+t(g^*)p^{\frac{r-k}{2}})$ and $\frac{1}{2}(p-1)(p^{s-1}-t(g^*)p^{\frac{s}{2}-1})(p^{r-k}-t(g^*)p^{\frac{r-k}{2}})$, which correspond to the number of occurrences of $p^n-p^{n-1}-p^{(n+k-2)/2}$ and $p^n-p^{n-1}+p^{(n+k-2)/2}$, respectively. Finally, the number of balanced codewords is equal to $p^n-1+\#\{(\alpha,\beta)\in\mathbb{F}_{p^n}^*\times\mathbb{F}_{p^n}: W_h(\alpha^{-1}\beta)=0\}$, which is $p^n-1+(p-1)(p^n-p^{n-k})=p^{n+1}-p^{n-k+1}+p^{n-k}-1$. $\square$

Table 5: Weight distribution of $\mathcal{C}_h$ in Theorem 5 for $h(x,y)=f(x)+g(y)$ with $f:\mathbb{F}_{p^r}\to\mathbb{F}_p$ a non-weakly regular $k$-plateaued function with zero dual $f^*$ and $g:\mathbb{F}_{p^s}\to\mathbb{F}_p$ a weakly regular bent function, when $n+k$ is even.

| Weight $w$ | Number of codewords |
|---|---|
| $p^n-p^{n-1}-p^{(n+k-2)/2}(p-1)$ | $\frac{p-1}{2}(p^{s-1}+t(g^*)p^{\frac{s}{2}}-t(g^*)p^{\frac{s}{2}-1})(p^{r-k}+t(g^*)p^{\frac{r-k}{2}})$ |
| $p^n-p^{n-1}-p^{(n+k-2)/2}$ | $\frac{p-1}{2}(p^{s-1}-t(g^*)p^{\frac{s}{2}-1})(p^{r-k}+t(g^*)p^{\frac{r-k}{2}})$ |
| $p^n-p^{n-1}$ | $p^{n+1}-p^{n-k+1}+p^{n-k}-1$ |
| $p^n-p^{n-1}+p^{(n+k-2)/2}$ | $\frac{p-1}{2}(p^{s-1}-t(g^*)p^{\frac{s}{2}-1})(p^{r-k}-t(g^*)p^{\frac{r-k}{2}})$ |
| $p^n-p^{n-1}+p^{(n+k-2)/2}(p-1)$ | $\frac{p-1}{2}(p^{s-1}+t(g^*)p^{\frac{s}{2}}-t(g^*)p^{\frac{s}{2}-1})(p^{r-k}-t(g^*)p^{\frac{r-k}{2}})$ |

Table 6: Weight distribution of $\mathcal{C}_h$ in Theorem 5 for $h(x,y)=f(x)+g(y)$ with $f:\mathbb{F}_{p^r}\to\mathbb{F}_p$ a non-weakly regular $k$-plateaued function with zero dual $f^*$ and $g:\mathbb{F}_{p^s}\to\mathbb{F}_p$ a weakly regular bent function, when $n+k$ is odd.

| Weight $w$ | Number of codewords |
|---|---|
| $p^n-p^{n-1}-t(g^*)p^{(n+k-1)/2}$ | $\frac{(p-1)^2}{2}(p^{n-k-1}+t(g^*)p^{\frac{n-k-1}{2}})$ |
| $p^n-p^{n-1}$ | $p^{n+1}-p^{n-k-1}(p-1)^2-1$ |
| $p^n-p^{n-1}+t(g^*)p^{(n+k-1)/2}$ | $\frac{(p-1)^2}{2}(p^{n-k-1}-t(g^*)p^{\frac{n-k-1}{2}})$ |

**Example 8.** *Set $p=3$ and $r=s=3$. Consider the function $f:\mathbb{F}_{3^3}\to\mathbb{F}_3$ given by $f(x)=\mathrm{Tr}_1^3(x^7)$, whose Walsh values are $W_f(b)\in\{-9,0,9\}$ for each $b$, thus it is a non-weakly regular 1-plateaued function with zero dual $f^*$ (recalling that $W_f(b)=\epsilon_f(b)\sqrt{p^*}^{m+k}\xi_p^{f^*(b)}$ so that $f^*(b)=0$ for all $b\in\mathbb{F}_{3^3}$). Let also $g:\mathbb{F}_{3^3}\to\mathbb{F}_3$ be the weakly regular bent function given by $g(y)=\mathrm{Tr}(y^2)$ for which $t(g^*)=1$. The code $\mathcal{C}_h$ specified in Theorem 5, where $h(x,y)=f(x)+g(y)$, is a 3-valued minimal ternary $[728,7,459]$-code whose weight enumerator polynomial is*

$$1+180z^{459}+1862z^{486}+144z^{513}.$$

*Similarly, if $r=3$ and $s=4$, then the function $f:\mathbb{F}_{3^3}\to\mathbb{F}_3$ given by $f(x)=\mathrm{Tr}_1^3(x^7)$ and the bent function $g:\mathbb{F}_{3^4}\to\mathbb{F}_3$ given by $g(y)=\mathrm{Tr}_1^4(y^2)$ for which $t(g^*)=-1$, induce a 5-valued ternary minimal code $\mathcal{C}_h$ with parameters $[2186,8,1404]$, whose weight enumerator polynomial is*

$$1+126z^{1404}+720z^{1431}+5102z^{1458}+360z^{1485}+252z^{1512}.$$

**Remark 4.** *To the best of our knowledge, Theorem 4 and Theorem 5 give the first construction of linear codes from non-weakly regular plateaued functions. Moreover, these constructions partially solve an open problem (Problem 3.2) proposed in [22].*

**Remark 5.** *Note that the codes constructed from the direct sum of (non-)weakly regular functions are in general narrow, thus minimality can be inferred from Ashikhmin-Barg's condition. However, the importance of Theorem 2 lies in the possibility of specifying minimal codes from wide minimal codes or even, using exactly one non-minimal constituent. In general, the weight distributions of the codes from Theorem 2 are hard to derive. Hence, more structure is needed to specify such distributions, as illustrated by the codes constructed in Theorem 4 and Theorem 5.*

### 3.3 A brief comparison to known constructions

In this section, we provide a short comparison of our constructions to other known constructions of $p$-ary minimal described previously in the literature. For this purpose, we will focus on infinite families of minimal linear codes with parameters $[p^n-1,n+1]$ whose minimum distance has been determined.

Recall the well-known Griesmer bound [16, 21]: for a $p$-ary code $C$ with parameters $[n,k,d]$, where $k\ge 1$, it holds that $\sum_{i=0}^{k-1}\lceil \frac{d}{p^i}\rceil\le n$. This yields that the minimum distance $d$ of a code with parameters $[p^n-1,n+1]$ satisfies

$$d\le p^n-p^{n-1}-1.$$

Moreover, a minimal code with such parameters satisfies $n+p-1\le w_{\min}\le w_{\max}\le p^n-n-1$ [9]. Hence $w_{\min}\le\frac{p-1}{p}(p^n-n-1)$ for a wide minimal code.

In Table 7, we summarize the properties of some known constructions of (wide) minimal $p$-ary linear codes presented in the literature. From Table 7, we can see that Theorem 2 and Corollary 1 lead to new infinite families of minimal codes with few weights (see Theorem 4 and Theorem 5), which may have large minimum distance. For instance, the codes in Example 8 have minimum distance 459 and 1404, respectively. Comparing these values to the best possible minimum distance for a $[3^6-1,7]$-code and a $[3^7-1,8]$-code, we get the ratios

$$\frac{459}{485}\approx 0.946392 \text{ and } \frac{1404}{1457}\approx 0.963624.$$

Moreover, using our approach, one can obtain infinite families of new wide minimal linear codes as illustrated by Example 2 (see Remark 1).

Table 7: Properties of some known (wide) minimal $p$-ary codes ($p > 2$) with length $p^n - 1$ and dimension $n + 1$.

| Minimum distance $d$ | # Weights | Notes | Wide | Reference |
|---|---|---|---|---|
| $a(p^{n-s} - p^{n-s-1})(p^{s/2} - 1)$ | 6 | $s \geq 4$ even, $2 \leq a \leq (p-1)p^{s/2-2}$ | Yes | [42] |
| $(p-1)(p^{n-2} \pm (p-1)p^{\frac{n}{2}+\frac{n+2s}{4}-2})$ | 6 | $n$ even, $\frac{n}{2} + s$ even, $0 \leq s \leq \frac{n}{2} - 4$ | Yes | [27, 43] |
| $(p-1)p^{n-2}$ | 6 | $n$ even, $\frac{n}{2} + s$ odd, $0 \leq s \leq \frac{n}{2} - 3$ | Yes | [27, 43] |
| $p^n - 1 - p^{n-t} - p^t + 2$ | 5 | $2 \leq t \leq n-2$ | Yes | [25] |
| $p^{n-t} + p^t - 2$ | 5 | $2 \leq t \leq n-2$ | Yes | [25] |
| $p^n - 1 - sp^{n/2} + s$ | 4 | $n$ even, $s > p^{n/2-1} + 1$ | $s > 2p^{n/2-1} - p^{n/2-2}$ | [25] |
| $s(p^{n/2} - 1)$ | 4 | $n$ even, $p - 2 < s < p^{n/2} - p^{n/2-1}$ | $s \leq p^{n/2} - 2p^{n/2-1} + p^{n/2-2}$ | [25] |
| $(p-1)(p^{n-1} - p^{\frac{n-1}{2}})$ | 3 | $n$ odd | No | [40] |
| $(p-1)(p^{n-1} - p^{\frac{n-2}{2}})$ | 3 | $n$ even | No | [35, 40, 48] |
| $p^n - p^{n-1} - p^{\frac{n+s}{2}-1}(p-1)$ | 3 | $n + s$ even, $0 \leq s \leq n-4$ | No | [22, 24] |
| $p^n - p^{n-1} - p^{\frac{n+s}{2}-1}$ | 3 | $n + s$ even, $0 \leq s \leq n-4$ | No | [22, 24] |
| $p^n - p^{n-1} - p^{\frac{n+s-1}{2}}$ | 3 | $n + s$ odd, $0 \leq s \leq n-3$ | No | [22, 24] |
| $p^{n-s-1}(p-1)(s(p-1)+1)$ | $\leq s + 4$ | $(p-1)(p^{s-2} - s) > 1$ | Yes | [42] |
| $\leq \sum_{i=1}^{k} \binom{n}{i}(p-1)^i$ | $-$ | $2 \leq k \leq n-2$ | $\sum_{i=1}^{k} \binom{n}{i}(p-1)^{i-1} < p^{n-1} - p^{n-2}$ | [3, 12] |

# 4 Non-covering permutations

Non-covering permutations were introduced in [46] to construct infinite families of minimal binary linear codes. In this section, we generalize this concept to the non-binary setting and provide similar results as in the binary case together with additional observations. Throughout this section, for a given function $F : \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$ and $b \in \mathbb{F}_{p^m}^*$, we will denote the $b$-component of $F$ by $\psi_b^{(F)}$, that is $\psi_b^{(F)} : \mathbb{F}_{p^m} \to \mathbb{F}_p$ is the $p$-ary function defined by $\psi_b^{(F)}(x) = \mathrm{Tr}_1^m(bF(x))$. Whenever there is no ambiguity, we will omit the super index $(F)$.

In the binary case, a permutation $\phi$ on $\mathbb{F}_{2^m}$ such that $\phi(0) = 0$ is *non-covering* if the following two conditions are satisfied:

- For every $b \in \mathbb{F}_{2^m}^*$ and $a_1, a_2 \in \mathbb{F}_{2^m}$ with $a_1 \neq a_2$,

$$W_{\psi_b}(a_1) \pm W_{\psi_b}(a_2) \neq 2^m, \tag{15}$$

- 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

$$W_{\psi_{b_1}}(a_1) - W_{\psi_{b_2}}(a_2) + W_{\psi_{b_1+b_2}}(a_1 + a_2) \neq 2^m. \tag{16}$$

One could try to generalize this definition directly, however, it seems to be a difficult task if one requires the definition to be useful (allowing to compute weights of codewords). That is why, an equivalent property is more suitable for our purposes. Due to the form of the above defining conditions, it can be foreseen that the concept of a non-covering permutation is somehow related to minimality of the associated code $\mathcal{C}_\phi$, defined in (5) (thus $t = 1$ and $l = m$). This is indeed the case and these two properties are in fact equivalent. Note that this equivalence was already pointed out (without a proof) in ([46], Remark 2).

**Theorem 6.** *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 (5). The permutation $\phi$ is non-covering if and only if $\mathcal{C}_\phi$ is minimal.*

*Proof.* Assume that $\phi$ is a non-covering permutation. Let $\mathbf{c}_{b_1,a_1}, \mathbf{c}_{b_2,a_2} \in \mathcal{C}_\phi$ be two different non-zero codewords. Suppose that $\mathbf{c}_{b_1,a_1} \preceq \mathbf{c}_{b_2,a_2}$. Note that at most one out of the three relations $\mathbf{c}_{b_1,a_1} \in \mathcal{S}_m$, $\mathbf{c}_{b_2,a_2} \in \mathcal{S}_m$ and $\mathbf{c}_{b_1+b_2,a_1+a_2} \in \mathcal{S}_m$ can be true, as the $m$-simplex code is minimal. By Proposition 1, we have

$$wt(\mathbf{c}_{b_1+b_2,a_1+a_2}) = wt(\mathbf{c}_{b_2,a_2}) - wt(\mathbf{c}_{b_1,a_1}). \tag{17}$$

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 left hand side of (17) is equal to $2^{m-1}$ since $\mathbf{c}_{0,a_1+a_2}$ is a non-zero linear function. Thus (17) becomes

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

Multiplying by two and rearranging, we obtain $2^m = W_{\psi_{b_1}}(a_1) - W_{\psi_{b_1}}(a_2)$, which is a contradiction to (15) 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 (17) becomes

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

Again, multiplying by two and rearranging, we obtain

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

which is a contradiction to (16) 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 $\mathbf{c}_{b,a_1}, \mathbf{c}_{b,a_2} \in \mathcal{C}_\phi$, which are non-zero since $\phi$ does not have affine components. Now, as $\mathcal{C}_\phi$ is minimal, we know that $2^{m-1} \neq wt(\mathbf{c}_{b,a_2}) - wt(\mathbf{c}_{b,a_1})$ and $wt(\mathbf{c}_{b,a_2}) \neq 2^{m-1} - wt(\mathbf{c}_{b,a_1})$. This readily implies that $2^m \neq W_{\psi_b}(a_1) \pm W_{\psi_b}(a_2)$. Similarly, minimality of $\mathcal{C}_\phi$ applied to the codewords $\mathbf{c}_{b_1,a_1}, \mathbf{c}_{b_2,a_2}$ 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 $2^m \neq W_{\psi_{b_1}}(a_1) - W_{\psi_{b_2}}(a_2) + W_{\psi_{b_1+b_2}}(a_1 + a_2)$. We have thus proved that $\phi$ is a non-covering permutation on $\mathbb{F}_{2^m}$. □

If the absolute Walsh values of a permutation $\phi$ are strictly bounded above by $\frac{2^m}{3}$, i.e.,

$$\max_{a\in\mathbb{F}_{2^m}, b\in\mathbb{F}_{2^m}^*} |W_{\psi_b}(a)| < \frac{2^m}{3},$$

then Equations (15) and (16) are satisfied, thus $\phi$ is non-covering. Equivalently, if the nonlinearity of $\phi$ satisfies $\mathcal{N}_\phi = 2^m - \frac{1}{2}\max_{b\in\mathbb{F}_{2^m}^*, a\in\mathbb{F}_{2^m}} |W_{\psi_b}(a)| > 2^m - \frac{2^{m-1}}{3} = \frac{2^m}{3}$, then $\phi$ is non-covering. We state this in the following proposition to further refer to it.

**Proposition 2.** *Any permutation $\phi : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ with $\phi(0) = 0$ whose nonlinearity $\mathcal{N}_\phi$ is strictly larger than $\frac{2^m}{3}$ is a non-covering permutation.*

In the particular case of power permutations, the non-covering property (16) can be reduced to $b_1 = b_2 = 1$, namely, for $\phi : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ given by $\phi(x) \mapsto x^d$ with $\gcd(d, n) = 1$,

$$W_{\psi_b}(a) = \textstyle\sum_{y\in\mathbb{F}_{2^m}}(-1)^{\mathrm{Tr}_1^m(by^d+ay)} = \sum_{x\in\mathbb{F}_{2^m}}(-1)^{\mathrm{Tr}_1^m(x^d+a\phi^{-1}(b)^{-1}x)} = W_{\psi_1}(a\phi^{-1}(b)^{-1}).$$

Thus, for a power permutation it is enough to verify (15) 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

$$W_{\psi_1}(a_1\phi^{-1}(b_1)^{-1}) - W_{\psi_1}(a_2\phi^{-1}(b_2)^{-1}) + W_{\psi_1}((a_1 + a_2)\phi^{-1}(b_1 + b_2)^{-1}) \neq 2^m. \qquad (18)$$

**Example 9** (Dobbertin's APN permutation)**.** *In $\mathbb{F}_{2^5}$, the permutation $\phi$ given by $x \mapsto x^{29}$ is an APN permutation since $2^4 + 2^3 + 2^2 + 2 - 1 = 29$ [15]. The Walsh spectrum of the component $\psi_1$ defined by $x \mapsto \mathrm{Tr}_1^5(\phi(x))$ is displayed in Table 8. Condition (15) readily follows since the maximum spectral value is 12. It can also be verified that if $W_{\psi_1}(a_1\phi^{-1}(b_1)^{-1}) = W_{\psi_1}((a_1 + a_2)\phi^{-1}(b_1 + b_2)^{-1}) = 12$ for some $a_1, a_2 \in \mathbb{F}_{2^5}, b_1, b_2 \in \mathbb{F}_{2^5}^*$ then, necessarily, $W_{\psi_1}(a_2\phi^{-1}(b_2)^{-1})$ is non-negative and its values belong to $\{0, 4, 8\}$. Hence the left hand side of (18) is at most 28, so (18) is satisfied. We conclude that $\phi$ is a non-covering permutation.*

Table 8: Walsh spectrum of the component $x \mapsto \mathrm{Tr}_1^5(\phi(x))$ 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 permutation. As it was observed in [46], the former class of permutations is non-covering. The previous example shows that Dobbertin's permutation is non-covering. Thus every non-affine power permutation over $m = 5$ is non-covering.

**Remark 6.** *When $m \in \{6, 7, 8\}$, performing an exhaustive search over all possible exponents $d$ for permutations $\phi(x) = x^d$ over $\mathbb{F}_{2^m}$ leads to the conclusion that all power permutations give rise to minimal linear codes, even though in few cases $\mathcal{N}_\phi \leq \frac{2^m}{3}$ which is only a sufficient condition.*

For $m > 8$, the following results show that a power permutation $\phi$ on $\mathbb{F}_2^m$ with low differential uniformity $\delta = \max_{a \in \mathbb{F}_{2^m}^*, b \in \mathbb{F}_{2^m}} \#\{x \in \mathbb{F}_{2^m} : \phi(x) + \phi(x+a) = b\}$ is non-covering since its nonlinearity is high.

**Theorem 7.** *[8] Let $\phi$ be a power permutation over $\mathbb{F}_{2^m}$ with differential uniformity $\delta$. The nonlinearity $\mathcal{N}_\phi$ of the permutation $\phi$ satisfies*

$$\mathcal{N}_\phi \geqslant 2^{m-1} - 2^{\frac{3m-4}{4}} \sqrt[4]{\delta}.$$

**Corollary 2.** *Let $m > 8$ be an arbitrary integer and $d > 1$ be a non-power of two such that $(d, 2^m - 1) = 1$. Every $\delta$-differentially uniform power permutation $\phi$ over $\mathbb{F}_{2^m}$ defined by $\phi(x) = x^d$ is non-covering for $\delta \in \{2, 4\}$.*

*Proof.* By Theorem 7, 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 $3 \cdot 2^{m-1} - 3 \cdot 2^{\frac{3m-4}{4}} \sqrt{2} > 2^m$. Rearranging this equation, we see that the inequality is true 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. The same applies to 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 $2^{m-1} - 2^{\frac{m}{2}}$ [8]. A known example of a class of 4-differentially uniform permutations that does not attain an optimal nonlinearity in general [33] is given by permutations of the form

$$x^{2^m-2} + \mathrm{Tr}_1^m(x^{(2^m-2)d} + (x^{2^m-2} + 1)^d),$$

where $d = 3(2^t + 1)$, $2 \leqslant t \leqslant \frac{m}{2} - 1$. These permutations have algebraic degree $m - 1$ and nonlinearity at least $2^{m-2} - 2^{\frac{m}{2}-1} - 1$. Nevertheless, their nonlinearity is still larger than $2^m/3$ except for some sporadic examples over $\mathbb{F}_{2^6}$. 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 $\delta$-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?", where here by good nonlinearity we mean strictly larger than $\frac{2^m}{3}$. 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.

**Remark 7.** *By Proposition 2, any permutation $\phi$ over $\mathbb{F}_{2^m}$ with nonlinearity $\mathcal{N}_\phi$ larger than $\frac{2^m}{3}$ allows us to construct a minimal code $\mathcal{C}_\phi$ with parameters $[2^m - 1, 2m, d]$, where $d > \frac{2^m}{3}$. Moreover, as shown in [46], any such permutation can also be used to construct (wide) minimal codes with parameters $[2^{2m} - 1, 2m + m + 1, d]$, where $d \geq 2^m \mathcal{N}_\phi > \frac{2^{2m}}{3}$ from a generic construction using bent functions and subspaces of derivatives. An interesting open problem is then to specify an infinite class of non-covering permutations with $\mathcal{N}_\phi \leq \frac{2^m}{3}$. Another related problem is to describe an infinite class of non-covering permutations for which $\mathcal{C}_\phi$ is minimal and wide.*

### 4.1 $p$-ary non-covering permutations

With the characterization of non-covering permutations in terms of the minimality of the associated code $\mathcal{C}_\phi$ given in Theorem 6, we can now formulate a satisfactory generalization of this concept to non-binary alphabets.

**Definition 2.** *A permutation $\phi$ 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 code $\mathcal{C}_\phi$ defined in* (5) *is a $2m$-dimensional minimal code (hence $\phi$ does not have any affine components).*

The following examples corroborate the existence of non-covering permutations in odd characteristics.

**Example 10.** *Working in $\mathbb{F}_{3^4}$, consider the mapping $\phi$ defined by $\phi(x) = x^{11}$. Note that $\phi$ is a permutation since* $\gcd(11, 3^4 - 1) = 1$. *Since $\phi$ 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 $\phi$ is a non-covering permutation. Similarly, we can consider the mapping $\phi$ defined by $\phi(x) = x^5$ on $\mathbb{F}_{3^5}$ for which the associated code $\mathcal{C}_\phi$ is also minimal.*

**Open Problem 1.** *It turns out (based on computer simulations) that power monomials $\phi = x^d$ over $\mathbb{F}_{p^m}$ induce minimal linear codes $\mathcal{C}_\phi$ and are therefore non-covering. We leave a formal proof of this observation as an open problem. Similarly, one can conjecture that permutations over $\mathbb{F}_{p^m}$ with low differential uniformity also give rise to minimal codes.*

## 5 Increasing the dimension of codes

In this section, we will provide two constructions of minimal codes using bent functions, non-covering permutations and suitable subspaces of derivatives in characteristic $p > 2$. The results can be seen as a generalization of the corresponding results in [46], even though, the $p$-ary case appears to be more involved requiring more complicated conditions on the building blocks.

In Section 5.1, we will introduce the concept of $k$-minimal pairs, which involve a bent function $g$ and a non-covering permutation. These pairs are defined by abstracting certain properties of bent functions in the Maiorana-McFarland class. They will serve us to construct (wide) minimal linear codes from general classes of bent functions through suitable subspaces of derivatives. Afterwards, in Section 5.2, we combine the approaches introduced in Section 3 and in Section 5.1 to present a generic method that induces (wide) minimal linear codes with larger dimensions.

### 5.1 Minimal linear codes through derivative subspaces

Recall that the code $C_\phi$ in Equation (5), for a given permutation $\phi : \mathbb{F}_{p^k} \to \mathbb{F}_{p^k}$, is defined as

$$\mathcal{C}_\phi = \left\{ \left( \mathrm{Tr}_1^k(a\phi(x)) + \mathrm{Tr}_1^k(ux) \right)_{x \in \mathbb{F}_{p^k}^*} : a \in \mathbb{F}_{p^k}, u \in \mathbb{F}_{p^k} \right\}. \tag{19}$$

**Definition 3.** *Let $m$ be an 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 exists a $k$-dimensional subspace $U$ of $\mathbb{F}_p^{p^m}$, whose non-zero elements are vectors corresponding to the evaluations of non-affine 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 $\Psi$ to $\mathcal{L}_m$ is a $p^{m-k}$-to-one map onto $\mathcal{S}_k$ and the restriction of $\Psi$ to $U$ is an isomorphism between $U$ and $\mathrm{Comp}_\phi = \{(\mathrm{Tr}_1^k(\phi(y)\gamma))_{y \in \mathbb{F}_{p^k}^*} : \gamma \in \mathbb{F}_{p^k}\}$.*

*(ii) (Weight-preserving) For each $w \in \mathcal{S}_k$, 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 $\Lambda_0 = \{v_w : w \in \mathcal{S}_k\}$ and $\Lambda_1 = \mathcal{L}_m \setminus \Lambda_0$.*

*(a) The assignation $w \mapsto v_w$ (described in (ii)) 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. This idea will help to construct examples of minimal codes.

**Proposition 3.** *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:*

$$g(x, y) = \mathrm{Tr}_1^{m/2}(x\phi(y)) \text{ for } (x, y) \in \mathbb{F}_{p^{m/2}} \times \mathbb{F}_{p^{m/2}}, \tag{20}$$

*where $\phi : \mathbb{F}_{p^{m/2}} \to \mathbb{F}_{p^{m/2}}$ is a permutation. If $\phi$ is a non-covering permutation, then $g$ and $\phi$ form an $\frac{m}{2}$-minimal pair.*

*Proof.* We will prove that the subspace of derivatives

$$U := \{D_{(\gamma,0)}g : \gamma \in \mathbb{F}_{p^{m/2}}^*\} \cup \{0\}, \tag{21}$$

and the mapping $\Psi : U + \mathcal{L}_{m/2}^2 \to \mathcal{C}_\phi$ given by

$$\Psi(D_{(\gamma,0)}g(x, y) + \mathrm{Tr}_1^{m/2}(ux) + \mathrm{Tr}_1^{m/2}(vy)) = (\mathrm{Tr}_1^{m/2}(\phi(y)\gamma) + \mathrm{Tr}_1^{m/2}(vy))_{y \in \mathbb{F}_{p^{m/2}}^*} \tag{22}$$

satisfy the conditions in Definition 3. 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 $u = 0$ in (22), so that $v_w = \mathrm{Tr}_1^{m/2}(vy)$ for $w = (\mathrm{Tr}_1^{m/2}(vy))_{y \in \mathbb{F}_{p^{m/2}}^*}$. For every derivative $D_{(\gamma,0)}g(x, y) \in U$,

$$wt(D_{(\gamma,0)}g(x, y) + \mathrm{Tr}_1^{m/2}(vy)) = p^{m/2} wt((\phi(y)\gamma + \mathrm{Tr}_1^{m/2}(vy))_{y \in \mathbb{F}_{p^{m/2}}^*})$$

since $\phi(y)\gamma + \mathrm{Tr}_1^{m/2}(vy)$ does not depend on $x$. For any other $u \neq 0$, the function $D_{(\gamma,0)}g(x, y) + \mathrm{Tr}_1^{m/2}(ux) + \mathrm{Tr}_1^{m/2}(vy)$ is balanced.

Condition $(iii)(a)$ is trivially satisfied as the function $w \mapsto v_w$ is essentially an inclusion. Let $\Lambda_0, \Lambda_1$ be as in Definition 3. For each $\mathrm{Tr}_1^{m/2}(vy) \in \Lambda_0, \mathrm{Tr}_1^{m/2}(u'x) + \mathrm{Tr}_1^{m/2}(v'y) \in \Lambda_1$ $(u' \neq 0)$ and $c \in \mathbb{F}_p^*$, it holds that $\mathrm{Tr}_1^{m/2}(cu'x) + \mathrm{Tr}_1^{m/2}((v+cv')y), \mathrm{Tr}_1^{m/2}(u'x) + \mathrm{Tr}_1^{m/2}((cv+v')y) \in \Lambda_1$, hence $(iii)(b)$ holds. Finally, if $\mathrm{Tr}_1^{m/2}(ux) + \mathrm{Tr}_1^{m/2}(vy), \mathrm{Tr}_1^{m/2}(u'x) + \mathrm{Tr}_1^{m/2}(v'y) \in \Lambda_1$ (thus $u \neq 0$ and $u' \neq 0$), there is exactly one $c \in \mathbb{F}_{p^m}^*$ such that $\mathrm{Tr}_1^{m/2}((u+cu')x) + \mathrm{Tr}_1^{m/2}((v+cv')y) \in \Lambda_0$, when $u, u'$ are $\mathbb{F}_p$-linearly dependent, otherwise there is no such $c$.

□

**Open Problem 2.** *We leave it as an open problem to find $k$-minimal pairs for $k > m/2$ for arbitrary bent functions $g$.*

**Theorem 8.** *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 $U = \{D_\gamma g : \gamma \in I\}$, where $I = \{0, \gamma_1, \dots, \gamma_{p^k-1}\} \subseteq \mathbb{F}_{p^m}$. 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 $D_\gamma g \in U$, the function $D_\gamma g(x) + \mathrm{Tr}_1^m(vx)$ 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 $D_\gamma g(x) + cg(x+\gamma)$ is bent for every $D_\gamma g(x) \in U, c \in \mathbb{F}_p^*$ and $\gamma \in I$.*

*Then, the code $C$ spanned by ( evaluations of the elements in) $\mathcal{B} \cup \mathcal{B}' \cup \{g\}$ 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 the corresponding elements $C^*$ by puncturing the $x = 0$ coordinate. Note that every codeword in $C$ can be expressed as

$$\mathbf{c}_{v,\gamma,\delta} := (\mathrm{Tr}_1^m(vx) + g(x+\gamma) + (\delta - 1)g(x))_{x \in \mathbb{F}_{p^m}^*}$$

for some $v, \gamma \in \mathbb{F}_{p^m}, \delta \in \mathbb{F}_p$ (where we used $\delta - 1$ above for convenience of computation). 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 $v, \gamma, \delta$ and $v', \gamma', \delta'$. 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

$$\eta = (p-1)(p^{m-1} - p^{m/2-1}) \text{ and } \theta = (p-1)(p^{m-1} + p^{m/2-1}).$$

**Case $a$): $\gamma = 0, \delta = 1$ 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 $\eta$ 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 $b$): $\gamma' = 0, \delta' = 1$ 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 $\eta$ 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 $c$): $\delta \neq 0$ and either $\gamma' \neq 0$ or $\delta' \neq 1$.** 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 $\eta$

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 $d$): $\delta' \neq 0$ and either $\gamma \neq 0$ or $\delta \neq 1$.** 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 $\eta$ 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 $e$): $\delta = \delta' = 0$.** Let $\Psi : U + \mathcal{L}_m \to \mathcal{C}_\phi$ be a linear map as in Definition 3. Let $\Lambda_0, \Lambda_1$ be as in Condition $(iii)$ of Definition 3. Set

$$\mathfrak{v} := \mathrm{Tr}_1^m(vx) \in \mathcal{L}_m \text{ and } \mathfrak{v}' := \mathrm{Tr}_1^m(v'x) \in \mathcal{L}_m.$$

We will consider three additional subcases according to the possible memberships in $\Lambda_1$ or $\Lambda_0$.

**Subcase $e1$): either $\mathfrak{v} \in \Lambda_1$ and $\mathfrak{v}' \in \Lambda_0$, or $\mathfrak{v} \in \Lambda_0$ and $\mathfrak{v}' \in \Lambda_1$.** 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 $e2$): $\mathfrak{v} \in \Lambda_1$ and $\mathfrak{v}' \in \Lambda_1$.** 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 $e3$): $\mathfrak{v} \in \Lambda_0$ and $\mathfrak{v}' \in \Lambda_0$:** 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 $\Psi$ 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 $\phi$ 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 $p^{m-k}(p-1)wt(\Psi(\mathbf{c}_1)) - p^{m-k}wt(\Psi(\mathbf{c}_2)) = (p-1)wt(\mathbf{c}_1) - wt(\mathbf{c}_2)$. □

**Corollary 3.** *Let $m$ be an even integer greater than two. Let $g : \mathbb{F}_{p^{m/2}} \times \mathbb{F}_{p^{m/2}} \to \mathbb{F}_p$ be a bent function in the $\mathcal{MM}$ class defined as in (20) whose underlying permutation $\phi : \mathbb{F}_{p^{m/2}} \to \mathbb{F}_{p^{m/2}}$ is a non-covering permutation. Define*

$$U := \{D_{(\gamma,0)}g : \gamma \in \mathbb{F}_{p^{m/2}}\}. \tag{23}$$

*Let $\mathcal{B}$ be a basis for $U$ and $\mathcal{B}'$ be a basis for the linear functions over $\mathbb{F}_{p^m}$. Then, the code $C$ spanned by $\mathcal{B} \cup \mathcal{B}' \cup \{g\}$ punctured at zero (i.e., the evaluations over $\mathbb{F}_{p^m}^*$) is a minimal $[p^m - 1, m + \frac{m}{2} + 1]$-code.*

*Proof.* The result follows immediately from Theorem 8 and the fact that $\phi$ and $g$ form an $\frac{m}{2}$-minimal pair witnessed by $U$, as pointed out in Remark 2. □

**Example 11.** *Let $m = 8$. 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 (to verify that none of the nonzero codewords is covered by each other), we verified that the code $C$ described in Corollary 3 derived from $g(x,y) = \mathrm{Tr}_1^4(x\phi(y))$ and the subspace of derivatives $U = \{D_{(\gamma,0)}g : \gamma \in \mathbb{F}_{3^4}\}$, is a minimal ternary $[3^m - 1 = 6560, m + \frac{m}{2} + 1 = 13, 3402]$-code, which is in accordance with Corollary 3. 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, *thus satisfying Ashikhmin and Barg's condition.*

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 3 is that wide minimal codes can be generated, as shown by the following example.

**Example 12.** *Let $m = 8$. 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 $\phi$ is a non-covering permutation. We have verified that the code $C$ described in Corollary 3 derived from $g(x, y) = \mathrm{Tr}_1^4(x\phi(y))$ 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 3. Moreover, its weight distribution is displayed in Table 9 so that $C$ is fourteen-valued and also* wide *since $\frac{3402}{5184} = \frac{21}{32} < \frac{2}{3}$.*

Table 9: Weight distribution of the ternary code in Example 12 showing weights 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 |

**Remark 8.** *One useful criterion for deciding the optimality of linear codes is the well-known Griesmer bound [16, 21]. It can be verified that the codes in Example 11 and Example 12 (having the same minimum distance) do not have optimal parameters. This is not surprising since wide minimal codes commonly do not reach optimality due to the fact that the Ashikhmin-Barg's bound is violated, which then implies that the ratio between the minimum and maximum weight becomes smaller implying a strong restriction on the minimum distance of such codes (see also Section 3.3)*

### 5.2 Combining $k$-minimal pairs with the direct sum method

Finally, we consider one more approach of designing minimal linear codes. In more detail, we will employ the direct sum $h(x, y) = f(x) + g(y)$, where $f : \mathbb{F}_{p^t} \to \mathbb{F}_p$, $g : \mathbb{F}_{p^m} \to \mathbb{F}_p$ and $n = t + m$, together with a suitable subspace of derivatives (of a bent function $g$ in $\mathcal{MM}$) for the purpose of increasing the dimension of the obtained codes. In addition, we will adjoin a single derivative $D_\lambda f$ of $f$ to build a code, denoted by $\mathcal{C}_h^{(\lambda)}$. To define $\mathcal{C}_h^{(\lambda)}$, consider the vectors

$$\big(h_{\alpha,\gamma}(x, y)\big)_{(x,y)\in\mathbb{F}_{p^t}\times\mathbb{F}_{p^m}\setminus\{(0,0)\}},$$

where $h_{\alpha,\gamma}(x, y) = h(x + \alpha, y + \gamma)$ and $\alpha \in \{0, \lambda\}$, $\gamma \in \mathbb{F}_{p^{m/2}} \times \{0\}$. Then, we define

$$\mathcal{C}_h^{(\lambda)} := \langle \big\{ (h_{\alpha,\gamma}(x, y))_{(x,y)\in\mathbb{F}_{p^t}\times\mathbb{F}_{p^m}\setminus\{(0,0)\}} : \alpha \in \{0, \lambda\}, \gamma \in \mathbb{F}_{p^{m/2}} \times \{0\} \big\} \cup \mathcal{S}_n \rangle. \tag{24}$$

That is, $\mathcal{C}_h^{(\lambda)}$ is the subspace spanned by (evaluations of) the functions $h_{\alpha,\gamma}$ and (evaluations of) the linear functions over $\mathbb{F}_{p^t} \times \mathbb{F}_{p^m}$.

For the rest of this section, we will identify $\mathbb{F}_{p^t} \times \mathbb{F}_{p^m}$ and $\mathbb{F}_{p^n}$. Similarly, the elements in $\mathbb{F}_{p^{m/2}} \times \{0\}$ will be identified with elements in $\mathbb{F}_{p^{m/2}}$ without further mentioning. Additionally, we will use lower case Latin letters to refer to scalars, and lower case Greek letters for the elements in the extension field.

**Lemma 4.** *Let $t, m, n$ be positive integers such that $t \geq 2$, $m > 2$ is even and $n = t+m$. Let $f : \mathbb{F}_{p^t} \to \mathbb{F}_p$ be a non-affine function, $\lambda \in \mathbb{F}_{p^t}^*$ be such that $f$ and $D_\lambda f$ are linearly independent and $g(y_1, y_2) = \mathrm{Tr}_1^{\frac{m}{2}}(y_1\phi(y_2))$ be a bent function over $\mathbb{F}_{p^{m/2}} \times \mathbb{F}_{p^{m/2}}$, where $\phi$ is a permutation (not necessarily non-covering) on $\mathbb{F}_{p^{m/2}}$ without affine components. Consider the direct sum $h(x, y) = f(x) + g(y)$, where $y = (y_1, y_2)$. Then the linear code $\mathcal{C}_h^{(\lambda)}$, defined in (24), has parameters $[p^n - 1, n + \frac{m}{2} + 2]$.*

*Proof.* Set $\gamma_0 := 0$. Let $\mathscr{B} = \{\gamma_1, \ldots, \gamma_{\frac{m}{2}}\}$ be a basis of $\mathbb{F}_{p^{m/2}} \times \{0\}$ and define $\mathcal{B} = \mathscr{B} \cup \{\gamma_0\}$. We claim that the set $\{h_{0,\gamma} : \gamma \in \mathcal{B}\} \cup \{h_{\lambda,0}\}$ is linearly independent. Suppose that

$$\varsigma(x, y) := \sum_{i=0}^{\frac{m}{2}} a_i h_{0,\gamma_i}(x, y) + a_{\frac{m}{2}+1} h_{\lambda,0}(x, y) = 0,$$

for some scalars $a_0, \ldots, a_{\frac{m}{2}}, a_{\frac{m}{2}+1} \in \mathbb{F}_p$. Since $\varsigma$ is the direct sum of the functions

$$(\sum_{i=0}^{\frac{m}{2}} a_i) f(x) + a_{\frac{m}{2}+1} f(x + \lambda) \text{ and } \sum_{i=1}^{\frac{m}{2}} a_i g(y + \gamma_i) + (a_0 + a_{\frac{m}{2}+1}) g(y),$$

then $\varsigma$ equals zero if and only if $\sum_{i=0}^{\frac{m}{2}} a_i g(y + \gamma_i) + (a_0 + a_{\frac{m}{2}+1}) g(y) = 0$, $\sum_{i=0}^{\frac{m}{2}} a_i = 0$ and $a_{\frac{m}{2}+1} = 0$. The latter can be inferred from the linear independence of $f$ and $D_\lambda f$. By definition, the sum $\sum_{i=0}^{\frac{m}{2}} a_i g(y+\gamma_i)$ can be rewritten as $\mathrm{Tr}_1^{\frac{m}{2}}(\phi(y_2)(y_1(\sum_{i=0}^{\frac{m}{2}} a_i) + \sum_{i=0}^{\frac{m}{2}} a_i\gamma_i))$. Since $\sum_{i=0}^{\frac{m}{2}} a_i = 0$, it holds that $\sum_{i=0}^{\frac{m}{2}} a_i g(y+\gamma_i) = 0$ if and only if $\sum_{i=0}^{\frac{m}{2}} a_i\gamma_i = 0$. This last condition implies that $a_i = 0$ for each $1 \leqslant i \leqslant \frac{m}{2}$ by linear independence of $\mathscr{B}$. Thus, $a_0 = 0$ as well. Finally, note that the code $\mathcal{C}_h^{(\lambda)}$ is equal to the direct sum of the subspace of linear functions over $\mathbb{F}_{p^n}$ and the span $\langle\{h_{0,\gamma_i} : 0 \leq i \leq \frac{m}{2}\} \cup \{h_{\lambda,0}\}\rangle$, hence its dimension is $n + \frac{m}{2} + 2$. □

For a function $f : \mathbb{F}_{p^t} \to \mathbb{F}_p$ with a derivative $D_\lambda f$, $\lambda \in \mathbb{F}_{p^t}^*$, we also define the code $\mathcal{C}_f \oplus \mathcal{C}_{D_\lambda f}$ by

$$\mathcal{C}_f \oplus \mathcal{C}_{D_\lambda f} := \{(a_1 f(x) + a_2 D_\lambda f(x) + l_v(x))_{x \in \mathbb{F}_{p^t}^*} : a_1, a_2 \in \mathbb{F}_p, v \in \mathbb{F}_{p^t}\}. \tag{25}$$

This code has length $p^t - 1$ and dimension at most $t+2$. As we will see in Theorem 9, some properties of the code $\mathcal{C}_h^{(\lambda)}$ introduced in Equation (24) can be related to those of $\mathcal{C}_f \oplus \mathcal{C}_{D_\lambda f}$.

**Example 13.** *Consider the field $\mathbb{F}_{3^4}$. Define the function $f(x) = \mathrm{Tr}_1^4(x^8 + x^4 + x^2)$ and consider its derivative $D_\lambda f$ at direction $\lambda = \omega^{61}$, where $\omega$ is a generator of $\mathbb{F}_{3^4}^*$. Using* Magma, *we have verified that the code $\mathcal{C}_f$ is a narrow $[80, 5, 47]$-code with weight enumerator polynomial*

$$1 + 16z^{47} + 40z^{50} + 52z^{53} + 80z^{54} + 20z^{56} + 32z^{59} + 2z^{62}.$$

*Whereas, the code $\mathcal{C}_{D_\lambda f}$ is a wide minimal $[80, 5, 42]$-code with weight enumerator polynomial*

$$1 + 4z^{42} + 16z^{48} + 26z^{51} + 146z^{54} + 24z^{57} + 18z^{60} + 8z^{66}.$$

*Furthermore, the code $\mathcal{C}_f \oplus \mathcal{C}_{D_\lambda f}$, defined by (25), is a wide minimal $[80, 6, 42]$-code whose enumerator polynomial is*

$$1+4z^{42}+2z^{44}+46z^{47}+16z^{48}+88z^{50}+26z^{51}+126z^{53}+146z^{54}+116z^{56}+24z^{57}+92z^{59}+18z^{60}+16z^{62}+8z^{66}.$$

**Remark 9.** *In comparison to [3, 41], the wide minimal codes in Example 13 have better error-correcting parameters. In particular, the constructions in [41] for $p = 3, m = 4$ yield the following: Theorem 1 gives wide minimal codes with parameters $[80, 4, 36]$ or $[80, 3, 36]$ (see Tables II and III); Theorem 2 yields a wide minimal code with parameters $[80, 3, 27]$ (Table V); and Theorem 3 yields wide minimal codes with parameters $[80, 5, 16]$ or $[80, 5, 32]$ (Table VII). Similarly, the construction in Proposition III.3 in [3] for $p = 3, m = 4$ yields a wide minimal code with parameters either $[80, 5, 8]$ or $[80, 5, 32]$. This shows that the wide minimal code $C_{D_\lambda f}$ in Example 13 stemming from a single derivative has better parameters.*

Now we are in a position to prove the main result of this section.

**Theorem 9.** *Let $t, m, n$ be positive integers such that $t \geq 2$, $m > 2$ is even and $n = t + m$. Let $f : \mathbb{F}_{p^t} \to \mathbb{F}_p$ be a non-affine function with $f(0) = 0$ and $\lambda \in \mathbb{F}_{p^t}^*$ be such that $D_\lambda f(0) = 0$ and $\{f, D_\lambda f\}$ is linearly independent. Let $g : \mathbb{F}_{p^{m/2}} \times \mathbb{F}_{p^{m/2}} \to \mathbb{F}_p$ be a bent function in $\mathcal{MM}$ of the form $g(y_1, y_2) = \mathrm{Tr}_1^{\frac{m}{2}}(y_1\phi(y_2))$, where $\phi$ is a non-covering permutation on $\mathbb{F}_{p^{m/2}}$. Suppose that the following two conditions hold:*

1. *For each $\gamma \in \mathbb{F}_{p^{m/2}}$ and $a, b \in \mathbb{F}_p$ such that the triplet $(\gamma, a, b)$ is not zero, the function $ag(y_1, y_2) + g(by_1 + \gamma, y_2)$ is $\mathcal{L}_m$-surjective.*
2. *The code $\mathcal{C}_f \oplus \mathcal{C}_{D_\lambda f}$ defined in (25) is a $(t + 2)$-dimensional minimal code.*

*Then, the code $\mathcal{C}_h^{(\lambda)}$, defined in (24), is a minimal linear code with parameters $[p^n - 1, n + \frac{m}{2} + 2]$. Moreover, if $\mathcal{C}_{D_\lambda f}$ is wide, then so is $\mathcal{C}_h^{(\lambda)}$.*

*Proof.* The parameters of $\mathcal{C}_h^{(\lambda)}$ can be deduced from Lemma 4. Let $\mathscr{B} = \{\gamma_1, \ldots, \gamma_{\frac{m}{2}}\}$ be a basis of $\mathbb{F}_{p^{m/2}}$. Note that each codeword in $\mathcal{C}_h^{(\lambda)}$ can be expressed as (an evaluation of)

$$a(f(x) + g(y_1, y_2)) + bf(x) + g(by_1 + \gamma, y_2) + c(f(x + \lambda) + g(y_1, y_2)) + L(x, y_1, y_2) \tag{26}$$

for some $a, c \in \mathbb{F}_p$, $L \in \mathcal{L}_n$, $\gamma = \sum_{i=1}^{\frac{m}{2}} b_i\gamma_i \in \mathbb{F}_{p^{m/2}}$, where $b_i \in \mathbb{F}_p$, and $b = \sum_{i=1}^{\frac{m}{2}} b_i$. First, we will show that if the underlying functions that depend on $y$ are non-zero and linearly dependent then the corresponding codewords are linearly dependent, provided they cover each other. Let $\mathbf{c}, \mathbf{c}' \in \mathcal{C}_h^{(\lambda)}$ be two non-zero codewords such that $\mathbf{c}' \preceq \mathbf{c}$, where the defining parameters of $\mathbf{c}$ and $\mathbf{c}'$ are $a, b, c, \gamma, L$ and $a', b', c', \gamma', L'$. Assume that

$$(a' + c')g(y_1, y_2) + g(b'y_1 + \gamma', y_2) + L'^y(y_1, y_2)$$

is equal to

$$e((a + c)g(y_1, y_2) + g(by_1 + \gamma, y_2) + L^y(y_1, y_2))$$

for some $e \in \mathbb{F}_p$, where $L^y$ denotes the restriction of $L$ to the $(y_1, y_2)$ coordinates. Notice that the above expressions indeed correspond to the restriction of the underlying functions of $\mathbf{c}$ and $\mathbf{c}'$ (derived from (26)) to the coordinate $y = (y_1, y_2)$.

The equality above implies then that $\mathrm{Tr}_1^{\frac{m}{2}}(\phi(y_2)((a' - ea + c' - ec + b' - eb)y_1 + \gamma' - e\gamma))$ is a linear function. This is possible only if

$$\gamma' - e\gamma = 0 \text{ and } a' - ea + c' - ec + b' - eb = 0, \tag{27}$$

so that $\gamma' = e\gamma$. This implies $b' = eb$ since $\gamma = \sum_{i=1}^{m/2} b_i\gamma_i$, $\gamma' = \sum_{i=1}^{m/2} b_i'\gamma_i'$, and the $\gamma_i$'s are linearly independent. From (27), we also have $a' + c' = e(a + c)$ and $(L')^y = eL^y$. This shows a linear dependency of $\mathbf{c}$ and $\mathbf{c}'$ with respect to the $y$ variable.

Now we prove that there is a linear dependency of $\mathbf{c}$ and $\mathbf{c}'$ with respect to the $x$ variable. Since $(a + c, b, \gamma)$ is non-zero, condition (i) implies that $(a + c)g(y_1, y_2) + g(by_1 + \gamma, y_2)$ is $\mathcal{L}_m$-surjective. As $-(af(x) + bf(x) + cf(x + \lambda) + L^x(x)) \in \mathbb{F}_p$ for each $x \in \mathbb{F}_{p^t}$, there exists $y^{(x)} = (y_1^{(x)}, y_2^{(x)})$ such that

$$(a + c)g(y_1^{(x)}, y_2^{(x)}) + g(by_1^{(x)} + \gamma, y_2^{(x)}) + L^y(y_1^{(x)}, y_2^{(x)})$$

is equal to $-(af(x)+bf(x)+cf(x+\lambda)+L^x(x))$ by $\mathcal{L}_m$-surjectivity. Since $\mathbf{c}' \preceq \mathbf{c}$ by assumption, for every $x \in \mathbb{F}_{p^t}$, $a'f(x)+ebf(x)+c'f(x+\gamma)+L'^x(x)$ is equal to

$$-e((a+c)g(y_1^{(x)},y_2^{(x)})+g(by_1^{(x)}+\gamma)+L^y(y_1^{(x)},y_2^{(x)})).$$

In other words, for every $x \in \mathbb{F}_{p^t}$, $(a'-ea)f(x)+(c'-ec)f(x+\lambda)+(L'-eL^x)(x)=0$. Since $C_f \oplus C_{D_\lambda f}$ is $(t+2)$-dimensional, we infer that $a'=ea$, $c'=ec$ and $L'^x=eL^x$. This shows linear dependency with respect to the $x$ variable. Therefore, $\mathbf{c},\mathbf{c}'$ are linearly dependent whenever $\mathbf{c}' \preceq \mathbf{c}$ and the restrictions to the $y$-coordinate are non-zero and linearly dependent.

By the above discussion and Lemma 3, the only case that remains to rule out is when $\mathbf{c},\mathbf{c}' \in \mathcal{C}_h^{(\lambda)}$ are linearly independent, $\mathbf{c}' \preceq \mathbf{c}$ and the function corresponding to the coordinate $y$ of either $\mathbf{c}$ or $\mathbf{c}'$ is zero. Both of these functions cannot be simultaneously zero by minimality of $\mathcal{C}_f \oplus \mathcal{C}_{D_\lambda f}$. Without loss of generality, assume that the underlying function of $\mathbf{c}'$ that depends on $y$ is zero. In this case, using condition (i), take an element $(x,y) \in \mathbb{F}_{p^t} \times \mathbb{F}_{p^m}$ such that (the underlying function of) $\mathbf{c}$ evaluated at this point is zero but $\mathbf{c}'$ evaluated at $x$ is non-zero. This contradicts $\mathbf{c}' \preceq \mathbf{c}$. Analogously, we can rule out the case when the underlying function of $\mathbf{c}$ that depends on $y$ is zero. Hence, if $\mathbf{c},\mathbf{c}'$ are linearly independent, then they cannot cover each other. This proves that $\mathcal{C}_h^{(\lambda)}$ is minimal. To prove the last part of the statement, note that each element in $\mathcal{C}_{D_\lambda f}$ can be identified (up to weight-scaling) with a codeword in $\mathcal{C}_h^{(\lambda)}$ (take $b=0$, $\gamma=0$, $c=-a$ and $L^y=0$ in Equation (26)). $\square$

In view of Example 13, there exist functions $f(x)$ that satisfy the conditions of Theorem 9. Therefore, employing any such function together with a non-covering permutation will yield wide minimal codes in arbitrary characteristics. Note that, in general, explicitly specifying infinite classes of wide minimal codes over non-binary alphabets is a hard problem. In our case, the choice for the permutation $\phi(x)$ will heavily influence the resulting code $\mathcal{C}_h^{(\lambda)}$, so that one can, in principle, obtain infinite classes of non-equivalent (wide) minimal codes. However, we then have to specify infinite classes of $p$-ary non-covering permutations, which seems to be a non-trivial task.

# 6 Conclusions

In this article, we have presented three generic methods of constructing minimal linear codes over non-binary alphabets. These results are generalizations of the constructions presented in [46]. The first class of minimal linear codes involves the use of the direct sum of functions. It is important to remark that this method does not require strong conditions thus it is a very general method. More remarkably, we provide the first explicit construction of linear codes from non-weakly regular plateaued functions, partially solving an open problem proposed in [18]. We have also studied structural properties of non-covering permutations, introduced in [46]. In particular, we have observed that every power APN permutation and every 4-uniform permutation are non-covering, thus raising the question whether this is true in general for arbitrary APN or 4-uniform permutations. Moreover, we provided a sound definition of non-covering permutations in fields with odd characteristic. Employing these generalizations, we have given a second generic method for constructing classes of minimal codes using suitable subspaces of derivatives of a bent function. Furthermore, extending these approaches, we provided a construction of minimal codes which gives rise to non-equivalent minimal codes depending upon the election of the underlying non-covering permutation. We leave as a research challenge to provide different approaches to specifying the weight distributions of more classes of minimal codes that arise from the constructions presented in this work.

# References


[1] Alfarano, G. N., Borello, M., Neri, A.: A geometric characterization of minimal codes and their asymptotic performance. Adv. Math. Commun. 16 (1), 115–133 (2022).

[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] Bonini, M., Borello, M.: Minimal linear codes arising from blocking sets. J. Algebr. Comb. 53, 327–341 (2021)

[5] Carlet, C., Charpin, P., Zinoviev, V.: Codes, bent functions and permutations suitable for DES-like cryptosystems. Des. Codes Cryptogr. 15, 125–156 (1998)

[6] 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)

[7] Chang, S., Hyun, J.: Linear codes from simplicial complexes. Des. Codes Cryptogr. 86, 2167–2181 (2018)

[8] Charpin, P., Peng, J.: New links between nonlinearity and differential uniformity. Finite Fields Appl. 56, 188–208 (2019)

[9] 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)

[10] Ding, C: Linear codes from some 2-designs. IEEE Trans. Inf. Theory 61 (6), 3265–3275 (2015)

[11] Ding, C.: A construction of binary linear codes from Boolean functions. Discrete Math. 339 (9), 2288–2303 (2016)

[12] Ding, C., Heng, Z., Zhou, Z.: Minimal binary linear codes. IEEE Trans. Inf. Theory 64 (10), 6536–6545 (2018)

[13] 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)

[14] 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)

[15] 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)

[16] Griesmer, J. H.: A bound for error-correcting codes. IBM J. Res. Dev. 4 (5), 532–542 (1960)

[17] Heng, Z., Ding, C., Zhou, Z.: Minimal linear codes over finite fields. Finite Fields Appl. 54, 176–196 (2018)

[18] Li, N., Mesnager, S.: Recent results and problems on constructions of linear codes from cryptographic functions. Cryptogr. Commun. 12 (5), 965–986 (2020)

[19] Lidl, R., Niederreiter, H.: Finite fields (second edition). Encycl. Math. App. (20), Cambridge University Press, Cambridge (1997)

[20] Lu, W., Wu, X., Cao, X.: The parameters of minimal linear codes. Finite Fields Appl. 71, 101799 (2021). https://doi.org/10.1016/j.ffa.2020.101799

[21] MacWilliams, F., Sloane, N.: The theory of error-correcting codes. North Holland, Amsterdam (1977)

[22] Mesnager, S.: Linear codes with few weights from weakly regular bent functions based on a generic construction. Cryptogr. Commun. 9, 71–84 (2017)

[23] 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)

[24] 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)

[25] Mesnager, S., Qi, Y., Ru, H., Tang, C.: Minimal linear codes from characteristic functions. IEEE Trans. Inf. Theory 66 (9), 5404–5413 (2020)

[26] 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)

[27] Mesnager, S., Sinak, A.: Infinite classes of six-weight linear codes derived from weakly regular plateaued functions. Int. Conf. Inf. Secur. Cryptol. (ISCTURKEY), 93–100 (2020)

[28] 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)

[29] Özbudak, F., Pelen, R. M.: Two or three weight linear codes from non-weakly regular bent functions. IEEE Trans. Inf. Theory 68 (5), 3014–3027 (2022)

[30] 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)

[31] Pelen, R. M.: Studies on non-weakly regular bent functions and related structures. PhD Dissertation (2020). `https://etd.lib.metu.edu.tr/upload/12625556/index.pdf`

[32] Qi, Y., Yang, T., Dai, B.: Minimal linear codes from vectors with given weights. IEEE Commun. Lett. 24 (12), 2674–2677 (2020)

[33] 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)

[34] Sinak, A.: Minimal linear codes from weakly regular plateaued balanced functions. Discrete Math. 344 (3), 112215 (2021). `https://doi.org/10.1016/j.disc.2020.112215`

[35] Tang, C., Li, N., Qi, Y., Zhou, Z., Helleseth, T.: Linear codes with two or three weights from weakly regular bent functions. IEEE Trans. on Inf. Theory 62 (3), 1166–1176 (2016)

[36] 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)

[37] 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)

[38] Xu, G., Qu, L., Cao, X.: Minimal linear codes from Maiorana-McFarland functions. Finite Fields Appl. 65, 101688 (2020). `https://doi.org/10.1016/j.ffa.2020.101688`

[39] 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)

[40] Wu, Y., Li, N., Zeng, X.: Linear codes from perfect nonlinear functions over finite fields. IEEE Trans. Commun. 68 (1), 3–11 (2020)

[41] 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)

[42] Xu, G., Qu, L., Cao, X.: Minimal linear codes from Maiorana-McFarland functions. Finite Fields Appl. 65, 101688 (2020). `https://doi.org/10.1016/j.ffa.2020.101688`

[43] Xu, G., Qu, L., Luo, G.: Minimal linear codes from weakly regular bent functions. Cryptogr. Commun. 14, 415–431 (2022)

[44] Yuan, J., Ding, C.: Secret sharing schemes from three classes of linear codes. IEEE Trans. Inf. Theory 52 (1), 206–212 (2006)

[45] 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)

[46] 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).

[47] Zhang, W., Yan, H., Wei, H.: Four families of minimal binary linear codes with $w_{min}/w_{max} \leq 1/2$. Appl. Algebra Eng. Commun. Comput. 30, 75–184 (2019)

[48] Zhou, Z., Li, N., Fan, C., Helleseth, T.: Linear codes with two or three weights from quadratic bent functions. Des. Codes Cryptogr. 81, 283–295 (2016)