Self-Orthogonal Minimal Codes From (Vectorial) p-ary Plateaued Functions

René Rodríguez-Aldama* Enes Pasalic* Fengrong Zhang† Yongzhuang Wei‡

Abstract

In this article, we derive the weight distribution of linear codes stemming from a subclass of (vectorial) p-ary plateaued functions (for a prime p), which includes all the explicitly known examples of weakly and non-weakly regular plateaued functions. This construction of linear codes is referred in the literature as the first generic construction. First, we partition the class of p-ary plateaued functions into three classes $\mathscr{C}_1, \mathscr{C}_2$, and $\mathscr{C}_3$, according to the behavior of their dual function f^*. Using these classes, we refine the results presented in a series of articles [9, 11, 15, 17, 20]. Namely, we derive the full weight distributions of codes stemming from all s-plateaued functions for $n+s$ odd (parametrized by the weight of the dual $wt(f^*)$), whereas for $n+s$ even, the weight distributions are derived from the class of s-plateaued functions in $\mathscr{C}_1$ parametrized using two parameters (including $wt(f^*)$ and a related parameter Z_0). Additionally, we provide more results on the different weight distributions of codes stemming from functions in subclasses of the three different classes. The exact derivation of such distributions is achieved by using some well-known equations over finite fields to count certain dual preimages. In order to improve the dimension of these codes, we then study the vectorial case, thus providing the weight distributions of a few codes associated to known vectorial plateaued functions and obtaining codes with parameters $[p^n-1, 2n, p^n-p^{n-1}-p^{(n+s-2)/2}(p-1)]$. For the first time, we provide the full weight distributions of codes from (a subclass of) vectorial p-ary plateaued functions. This class includes all known explicit examples in the literature. The obtained codes are minimal and self-orthogonal virtually in all cases.

1 Introduction

There are a vast number of methods for constructing linear codes—constructions based on p-ary functions are among the most renowned methods. In their pioneering work, Carlet, Charpin and Zinoviev [3] showed the first explicit connection between AB (and APN) functions and linear codes. Soon after, Carlet and Ding [4] constructed codes based on perfect nonlinear mappings. Since then, many authors have addressed the construction of linear codes using p-ary functions [2, 6, 19, 7, 10, 11, 12, 13, 18, 21, 22].

In this work, we address the construction of p-ary codes from (vectorial) plateaued functions. There has been much work on linear codes stemming from perfect nonlinear functions, however,

*Famnit & IAM, University of Primorska, Koper, Slovenia. rene7ca@gmail.com enes.pasalic6@gmail.com

†State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an, China. zhangfengrong@xidian.edu.cn

‡Guangxi Key Laboratory of Cryptography and Information Security, Guilin University of Electronic Technology, Guilin, China. walker_wyz@guet.edu.cn

less is known for the plateaued case. Elaborating on the results of [9, 11, 15, 17, 20], we present the full weight distribution of subclasses of weakly and **non-weakly regular** s-plateaued functions $f\colon \mathbb{F}_{p^n} \to \mathbb{F}_p$ yielding three-weight codes and five-weight codes, for $n+s$ odd and $n+s$ even, respectively. These results are obtained by using well-known solutions of equations over cyclotomic fields, which are field extension of the rational numbers by adding the complex p-th root of unity. These solutions are then used to compute the cardinalities of preimages of suitable dual functions that allow the exact derivation of their Walsh distributions and then the weight distributions of associated codes. The parameters of the obtained codes are $[p^n-1, n+1, (p-1)p^{n-1}-p^{\frac{n+s-1}{2}}]$ and $[p^n-1, n+1, p^n-p^{n-1}-p^{(n+s-2)/2}(p-1)]$, for $n+s$ odd and $n+s$ even respectively. In order to obtain linear codes with a larger dimension, we study the vectorial case. Little is known about infinite families of vectorial plateaued functions, however, some examples have been given in the literature. Based on such examples, we extract general properties of these functions to obtain the weight distribution of codes stemming from a class of vectorial plateaued functions yielding three weight codes with parameters $[p^n-1, 2n, p^n-p^{n-1}-p^{(n+s-2)/2}(p-1)]$. We then prove that these codes are minimal and self-orthogonal, which makes these codes quite interesting also from a practical point of view.

2 Preliminaries

Let $\mathbb{F}_{p^n}$ denote the finite field with p^n elements, where $n>0$ and p is prime. Let $\mathbb{F}_p^n$ be an n-dimensional vector space over $\mathbb{F}_p$. A function F from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ is called a vectorial p-ary function. When $p=2$, F is simply referred as a vectorial Boolean function. The adjective vectorial is dropped when we refer to functions mapping to the prime field $\mathbb{F}_p$ (thus $m=1$). Such functions will be usually denoted with lowercase letters. We treat a function $f\colon \mathbb{F}_{p^n} \to \mathbb{F}_p$ and its truth table as the same object whenever there is no ambiguity. The component functions $F_a : \mathbb{F}_{p^n} \to \mathbb{F}_p$ of a vectorial function $F\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ are the mappings $x \mapsto \mathrm{Tr}_1^m(aF(x))$ for $a \in \mathbb{F}_{p^m}^\star$, where $\mathbb{F}_{p^m}^\star = \mathbb{F}_{p^m} \setminus \{0\}$ and the function Tr_1^m denotes the usual 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 Walsh transform of $f\colon \mathbb{F}_{p^n} \to \mathbb{F}_p$ at a point $b \in \mathbb{F}_{p^n}$ is the sum of characters given by

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

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

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

The Walsh spectrum of f is the multi-set of values $\{* \; W_f(b) \; : \; b \in \mathbb{F}_{p^n} \; *\}$. For a vectorial functions F, its Walsh spectrum is given by $\{* \; W_{F_a}(b) \; : \; (a,b) \in \mathbb{F}_{p^m}^\star \times \mathbb{F}_{p^n} \; *\}$. The set of linear functions from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ will be denoted by $\mathcal{L}_{n,m}$, whereas the set of affine functions will be denoted by $\mathcal{A}_{n,m}$. A p-ary s-plateaued function $f\colon \mathbb{F}_{p^n} \to \mathbb{F}_p$ is characterized by the property $|W_f(b)|^2 = 0$ or p^{n+s} for every $b \in \mathbb{F}_{p^n}$. If $s=0$, then there are no zero spectral values and we call such a function a p-ary bent function. It can be shown [11] that the non-zero Walsh values of a p-ary s-plateaued function $f\colon \mathbb{F}_{p^n} \to \mathbb{F}_p$ can be expressed as $u_b p^{-(n+s)/2} W_f(b) = \xi_p^{f^*(b)}$ for a complex number u_b with $|u_b| = 1$ and a p-ary function f^*, where $f^*\colon \mathsf{supp}(W_f) \to \mathbb{F}_p$, where $\mathsf{supp}(W_f) = \{b \in \mathbb{F}_{p^n} : |W_f(b)|^2 = p^{n+s}\}$. If the value of u_b does not depend on b, then the function f is called p-ary weakly regular s-plateaued, and non-weakly regular s-plateaued otherwise. The function f^* is called the dual of f. Furthermore, it was shown [11] that a weakly regular s-plateaued function f satisfies $W_f(b) = \epsilon_f \sqrt{p^*}^{n+s} \xi_p^{f^*(b)}$, where $\epsilon_f = \pm 1$ is called the sign of the Walsh transform of f and $p^* = (-\frac{1}{p})p$, where the parentheses indicate the Legendre symbol. Similarly, one can easily show that a non-weakly regular s-plateaued function f satisfies $W_f(b) = \epsilon_f(b) \sqrt{p^*}^{n+s} \xi_p^{f^*(b)}$, where $\epsilon_f(b) = \pm 1$ will be called the sign of the Walsh transform of f at $b \in \mathbb{F}_{p^n}$.

2.1 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 $\mathcal{S}_n$ spanned by all linear functionals over $\mathbb{F}_{p^n}^\star$ is a $[p^n - 1, n, p^n - p^{n-1}]$ code, called the n-affine simplex code, i.e., $\mathcal{S}_n = \{(L(x))_{x \in \mathbb{F}_{p^n}^\star} : L \in \mathcal{L}_n\}$ (a pruning of the first order Reed-Muller code).

Let a_j be the number of codewords with Hamming weight j 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 $1 + a_1 z + \cdots + a_n z^n$. 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 $F\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ with $F(0) = 0$ is described as follows. For positive integers n and m, the linear code $\mathcal{C}_F \subset \mathbb{F}_p^{p^n - 1}$ is defined by

$$\mathcal{C}_F = \{\mathbf{c}_{a,u} : a \in \mathbb{F}_{p^m}, b \in \mathbb{F}_{p^n}\}, \tag{3}$$

where $\mathbf{c}_{a,u} := \left(\mathrm{Tr}_1^m(aF(x)) + \mathrm{Tr}_1^n(ux)\right)_{x \in \mathbb{F}_{p^n}^\star}$. The dimension of $\mathcal{C}_F$ is at most $n+m$ and its length is $p^n - 1$. If $F\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ has no linear components, the linear code $\mathcal{C}_F$ derived from the generic construction in (3) has dimension exactly $n+m$. Moreover, its weights can be expressed by the Walsh transform of absolute trace functions of the map $F\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ as shown in [9].

3 Cyclotomic relations relevant for plateaued functions

Let QR denote the set of quadratic residues modulo p and let NQR be the set of quadratic non-residues modulo p.

Lemma 1. *(Folklore) The following relations are true for the Legendre symbol and ξ_p:*

1. $\sum_{j \in \mathbb{F}_p^*} \left(\frac{j}{p}\right) = \sum_{j \in QR^*} 1 + \sum_{j \in NQR} (-1) = 0$;

2. $\sum_{j \in \mathbb{F}_p^*} \xi_p^j = -1$;

3. *For any $a \in \mathbb{Z}$, the integral equation*

$$\sum_{j \in \mathbb{F}_p^*} a_j \xi_p^j = \begin{cases} a\sqrt{p}, & p \equiv 1 \pmod 4; \\ \mathfrak{i} a\sqrt{p}, & p \equiv 3 \pmod 4; \end{cases}$$

has a unique solution $a_j = a\left(\frac{j}{p}\right) \in \mathbb{Z}$.

Note that $\mathfrak{i} \notin \mathbb{Z}(\xi)$ since it is not a root of unity for $p \not\equiv 0 \pmod 4$ [16]. Therefore, $\sum_{i=1}^{p-1} a_i \xi_p^i = p^{\frac{\theta}{2}}\nu$ for $a_i \in \mathbb{Z}$, $\theta \in \mathbb{N}$ and $\nu \in \{1, \mathfrak{i}\}$ implies that either θ is odd or $\nu \neq \mathfrak{i}$. Therefore, we have the following.

Lemma 2. *[8] Let $(a_1, \ldots, a_n) \in \mathbb{Z}^p$, $\theta \in \mathbb{N}$ and $\nu \in \{1, \mathfrak{i}\}$. Suppose that $\sum_{i=1}^{p-1} a_i \xi_p^i = p^{\frac{\theta}{2}}\nu$.*

1. *If $\theta \equiv 0 \pmod 2$, then $\nu = 1$;*
2. *If $\theta \equiv 1 \pmod 2$, then*

$$\nu = \begin{cases} 1, & p \equiv 1 \pmod 4; \\ \mathfrak{i}, & p \equiv 3 \pmod 4. \end{cases}$$

4 Dual value distributions of plateaued functions

Using a similar notation as in [11], given $f_1 \colon \mathbb{F}_{p^n} \to \mathbb{F}_p$ and any function $f_2 \colon \mathsf{supp}(W_{f_1}) \to \mathbb{F}_p$, we define the sets $N_{f_2}(j) = \{x \in \mathsf{supp}(W_{f_1}) : f_2(x) = j\}$ and the numbers $n_{f_2}(j) = \#N_{f_2}(j)$, for $j \in \mathbb{F}_p$. Following the terminology introduced in [14, 15], for a given set $S \subseteq \mathbb{F}_{p^n}$, we say that a function $f \colon S \to \mathbb{F}_p$ is *bent relative to* S if $|W_f(b)| = \#S^{1/2}$ for all $b \in \mathbb{F}_{p^n}$, where $W_f(b)$ is considered as the restriction to S of the Walsh transform of f, i.e., $W_f(b) = \sum_{x \in S} \xi_p^{f(x)+\mathrm{Tr}_1^n(bx)}$. 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 $S \subseteq \mathbb{F}_{p^m}$ and let $f \colon S \to \mathbb{F}_p$ 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, $\nu \in \{1, \mathfrak{i}\}$, $j \in \mathbb{F}_p$ for some $\mu \in \mathbb{N}$, $\mu > 0$. The number $t(f)$ will be called the *type of* f. For an s-plateaued function $f \colon \mathbb{F}_{p^n} \to \mathbb{F}_p$ with $0 \le s \le n$, let $\Gamma^+(f)$ and $\Gamma^-(f)$ be the sets that partition $S = \mathsf{supp}(W_f)$ and are given by

$$\Gamma^+(f) = \left\{b \in S : W_f(b) = \nu p^{\frac{n+s}{2}} \xi_p^{f^*(b)}\right\},\ \Gamma^-(f) = \left\{b \in S : W_f(b) = -\nu p^{\frac{n+s}{2}} \xi_p^{f^*(b)}\right\},$$

where $\nu \in \{1, \mathfrak{i}\}$. Note that in this case $t(f) = \epsilon_f(0)\left(\frac{-1}{p}\right)^{n+s}$, where $\epsilon_f(0)$ denotes the sign of W_f at 0. For an s-plateaued function $f \colon \mathbb{F}_{p^n} \to \mathbb{F}_p$, define the numbers $A_j := \#(N_{f^*}(j) \cap \Gamma^+(f))$ and $B_j := \#(N_{f^*}(j) \cap \Gamma^-(f))$ for $j \in \mathbb{F}_p$. We also define $Z_j := A_j - B_j$.

Lemma 3. *Let $f \colon \mathbb{F}_{p^n} \to \mathbb{F}_p$ be any s-plateaued function. Let $f(0) = j_0$. Then $A_{j_0} \neq B_{j_0}$ (i.e. $Z_{j_0} \neq 0$). The distribution values A_j, B_j associated to f satisfy exactly one of the following.*

i) $A_j \neq B_j$ for every j;

ii) The number $n-s$ is even and $A_j = B_j$ for each $j \neq j_0$. In this case, $A_{j_0} = p^{\frac{n-s}{2}} + B_{j_0}$ and, $\sum_{j\neq j_0} A_j = \sum_{j\neq j_0} B_j = \frac{p^{n-s}+p^{\frac{n-s}{2}}}{2} - A_{j_0} = \frac{p^{n-s}-p^{\frac{n-s}{2}}}{2} - B_{j_0}$;

iii) The number $n-s$ is odd and $A_{j+j_0} = B_{j+j_0}$ for $j \in \mathcal{I}$ and $A_{j+j_0} - B_{j+j_0} = 2\sigma \left(\frac{j}{p}\right) p^{\frac{n-s-1}{2}}$ for $j \notin \mathcal{I}$, where

$$\sigma = \begin{cases} 1, & p \equiv 1 \pmod 4; \\ -1, & p \equiv 3 \pmod 4; \end{cases}$$

and

$$\mathcal{I} = \begin{cases} QR^*, & \frac{Z_{j_0}}{|Z_{j_0}|} = -\sigma; \\ NQR, & \textit{otherwise}. \end{cases}$$

In this case, $Z_{j_0} = -\sigma \left(\frac{j}{p}\right) p^{\frac{n-s-1}{2}}$ for (any) $j \in \mathcal{I}$. Moreover, if $A_{j_0} \neq 0$, then $\sum_{i\neq j_0} A_i = \frac{p^{n-s}+\sigma\left(\frac{j}{p}\right)p^{\frac{n-s+1}{2}}}{2} - A_{j_0}$, and, if $B_{j_0} \neq 0$, then $\sum_{i\neq j_0} B_i = \frac{p^{n-s}-\sigma\left(\frac{j}{p}\right)p^{\frac{n-s+1}{2}}}{2} - B_{j_0}$, for (any) $j \notin \mathcal{I}$.

Proof. Consider the inverse Walsh transform (2) of $f(x)$ at $x = 0$,

$$p^n \xi_p^{j_0} = \sum_{b\in\mathbb{F}_{p^n}} W_f(b) = \sum_{j\in\mathbb{F}_p} (A_j - B_j)\xi_p^j \nu p^{\frac{n+s}{2}}.$$

Using Lemma 1, this equality can be arranged as

$$\sum_{j\neq j_0} (A_j - B_j - Z_{j_0})\xi_p^{j-j_0} = p^{\frac{n-s}{2}}\nu^{-1}. \tag{4}$$

Suppose that $n-s$ is even. Thus $\nu = 1$ by Lemma 2. We first show that $Z_{j_0} \neq 0$. Suppose not. Then (4) implies that $A_j - B_j = -p^{\frac{n-s}{2}}$ by Lemma 1. Since f is plateaued, $\sum_{j\in\mathbb{F}_p}(A_j + B_j) = p^{n-s}$. Then $2\sum_{j\in\mathbb{F}_p} A_j = p^{n-s} - p^{\frac{n-s}{2}}(p-1)$, which is a contradiction since $p^{n-s} - p^{\frac{n-s}{2}}(p-1)$ is an odd number. Therefore $Z_{j_0} \neq 0$. Let us suppose that *i*) is not true, i.e., suppose that there is an index $j' \neq j_0$ such that $A_{j'} = B_{j'}$. We will prove *ii*). From (4), we get $A_j - B_j = Z_{j_0} - p^{\frac{n-s}{2}}$ for each j. In particular, $0 = A_{j'} - B_{j'} = Z_{j_0} - p^{\frac{n-s}{2}}$, so that $Z_{j_0} = p^{\frac{n-s}{2}}$ and $A_j = B_j$ for every $j \neq j_0$. The second part of *ii*) comes from this and the fact that $\sum_{j\in\mathbb{F}_p}(A_j + B_j) = p^{n-s}$.

Suppose that $n-s$ is odd. To show that $Z_{j_0} \neq 0$, suppose the opposite. Equation (4) implies that $A_j - B_j = \sigma\left(\frac{j-j_0}{p}\right)p^{\frac{n-s-1}{2}}$, where $\sigma = 1$ if $p \equiv 1 \pmod 4$ and $\sigma = -1$ if $p \equiv 3 \pmod 4$, by Lemma 1. Since f is plateaued, $\sum_{j\in\mathbb{F}_p}(A_j + B_j) = p^{n-s}$. Then $2\sum_{j\in\mathbb{F}_p} A_j = p^{n-s}$, which is a contradiction since p^{n-s} is odd. Hence $Z_{j_0} \neq 0$. Again, suppose that *i*) is not true, i.e. suppose that there is an index $j' \neq j_0$ such that $A_{j'} = B_{j'}$. We will prove *iii*). From (4), we get $A_j - B_j = Z_{j_0} + \sigma\left(\frac{j-j_0}{p}\right)p^{\frac{n-s-1}{2}}$ for each j. In particular, $0 = A_{j'} - B_{j'} = Z_{j_0} + \sigma\left(\frac{j'-j_0}{p}\right)p^{\frac{n-s-1}{2}}$, so that $Z_{j_0} = -\sigma\left(\frac{j'-j_0}{p}\right)p^{\frac{n-s-1}{2}}$. This tells us that for every j such that $\left(\frac{j-j_0}{p}\right) = \left(\frac{j'-j_0}{p}\right)$, we have $A_j = B_j$. Defining $\mathcal{I}$ as in the statement, this is equivalent to $A_{j+j_0} = B_{j+j_0}$ for every $j \in \mathcal{I}$. Additionally, $A_j - B_j = 2\sigma\left(\frac{j-j_0}{p}\right)p^{\frac{n-s-1}{2}}$ for each $j - j_0 \notin \mathcal{I}$. The second part of *iii*) comes from the above and the fact that $\sum_{j\in\mathbb{F}_p}(A_j + B_j) = p^{n-s}$. □

Using the previous lemma, we can partition the set of s-plateaued functions into three classes. These classes will be denoted by $\mathscr{C}_1, \mathscr{C}_2$, and $\mathscr{C}_3$, respectively. Thus, $\mathscr{C}_1$ corresponds to the functions specified in $i)$ of Lemma 3, $\mathscr{C}_2$ corresponds to the functions specified in $ii)$ and $\mathscr{C}_3$ corresponds to the functions specified in $iii)$. We will now determine the exact values of A_j, B_j for certain plateaued functions.

Example 1. *Any weakly regular plateaued function whose dual is surjective belongs to $\mathscr{C}_1$ for which there are several infinite families of functions. To construct an infinite family inside $\mathscr{C}_2$, consider the function $f(x) = \mathrm{Tr}_1^3(x^7)$ over $\mathbb{F}_{3^3}$. This function is a non-weakly 1-plateaued function with zero dual, namely, $\{W_f(b) : b \in \mathbb{F}_{3^3}\} = \{0, 9, -9\}$ with distribution $\{*0^{18}, 9^6, -9^3*\}$. For any $l \in \mathbb{N}$, we consider the l-th iteration of the direct sum of f with itself, f^l, which is an l-plateaued function defined on $\mathbb{F}_{3^{3l}}$ with constant zero dual. For $\mathscr{C}_3$, consider the function $g(x) = \mathrm{Tr}_1^3(2x^4 + x^2)$ in $\mathbb{F}_{3^3}$. This function is a weakly regular 2-plateaued function with $\{W_f(b) : b \in \mathbb{F}_{3^3}\} = \{0, \mathrm{i}3^{5/2}, \mathrm{i}3^{5/2}\xi_3^2\}$ with distribution $\{*0^{24}, (\mathrm{i}3^{5/2})^1, (\mathrm{i}3^{5/2}\xi_3^2)^2*\}$ For any $l \in \mathbb{N}$, consider f^l as before. The direct sum of f^l with g gives a non-weakly regular $(l+2)$-plateaued function in $\mathbb{F}_{3^{3(l+1)}}$ with $\{W_f(b) : b \in \mathbb{F}_{3^{3(l+1)}}\} = \{0, \mathrm{i}3^{\frac{5+4l}{2}}, -\mathrm{i}3^{\frac{5+4l}{2}}, \mathrm{i}3^{\frac{5+4l}{2}}\xi_3^2, -\mathrm{i}3^{\frac{5+4l}{2}}\xi_3^2\}$, which belongs to $\mathscr{C}_3$.*

Although the previous example (Example 1) shows that the classes $\mathscr{C}_1, \mathscr{C}_2$ and $\mathscr{C}_3$ are non-empty, it also gives rise to some existence problems. Namely, the following questions arise naturally.

Question 1. Are the classes $\mathscr{C}_2$ and $\mathscr{C}_3$ non-empty for $p > 3$ and for every n?

Question 2. Are there infinite classes of functions in $\mathscr{C}_2$ whose dual is non-zero? Note also that every function in $\mathscr{C}_2$ is non-weakly regular.

Question 3. Are there infinite classes of functions in $\mathscr{C}_3$ whose dual is surjective (necessarily non-weakly regular plateaued)?

In the following (Lemmas 4-8) we determine the exact values of A_j, B_j for certain subfamilies of p-ary plateaued functions which carry enough information about the dual to derive these values.

Lemma 4. *Let $f \colon \mathbb{F}_{p^n} \to \mathbb{F}_p$ be an s-plateaued function in $\mathscr{C}_1$ with $f(0) = f^*(0) = 0$. Suppose that $W_f(0) = t(f)\nu p^{\frac{n+s}{2}}$ and $W_{f^*}(0) = t(f^*)\nu' p^{\frac{\theta}{2}}$ for some $\nu, \nu' \in \{1, \mathrm{i}\}$ and $\theta \in \mathbb{N}$, $\theta > 1$. For $j \in \mathbb{F}_p^\star$, the numbers A_j, B_j are either zero or depend on A_0 and B_0, respectively. Moreover, $A_0 + B_0 = p^{n-s-1}$ when θ is odd and $A_0 + B_0 = p^{n-s-1} + t(f^*)(p-1)p^{\frac{\theta}{2}-1}$ for θ even. The values of A_j, B_j are displayed in Table 1 for different parities of $n+s$ and θ.*

Proof. Suppose that $n + s$ is even. Suppose that θ is even, too. By Lemma 1,

$$A_j - B_j = A_0 - B_0 - p^{\frac{n-s}{2}} \tag{5}$$

for each $j \in \mathbb{F}_p^\star$. On the other hand, $W_{f^*}(0) = t(f^*)\nu' p^{\frac{\theta}{2}}$. By Lemma 2, $\nu' = 1$. Since $t(f^*)p^{\frac{\theta}{2}} = W_{f^*}(0) = \sum_{j=1}^{p-1}(A_j + B_j - A_0 - B_0)\xi_p^j$, we have

$$A_j + B_j = A_0 + B_0 - t(f^*)p^{\frac{\theta}{2}} \tag{6}$$

for each j. From (5) and (6), one can obtain the values of A_j, B_j in terms of A_0, B_0 respectively. Lastly,

$$p^{n-s} = \sum_{j=0}^{p-1}(A_j + B_j) = (p-1)(A_0 + B_0 - t(f^*)p^{\frac{\theta}{2}}) + A_0 + B_0.$$

Thus, $A_0+B_0 = p^{n-s-1}+t(f^*)(p-1)p^{\frac{\theta}{2}-1}$. Assume now that θ is odd. Since $t(f^*)\nu' p^{\frac{\theta}{2}} = W_{f^*}(0) = \sum_{j=1}^{p-1}(A_j + B_j - A_0 - B_0)\xi_p^j$, we have

$$A_j + B_j = A_0 + B_0 + \left(\frac{j}{p}\right) t(f^*)p^{\frac{\theta}{2}} \tag{7}$$

for each j. From (5) and (7), one can obtain the values of A_j, B_j in terms of A_0, B_0 respectively. Lastly,

$$p^{n-s} = \sum_{j=0}^{p-1}(A_j + B_j) = p(A_0 + B_0)$$

Thus, $A_0 + B_0 = p^{n-s-1}$.

For the case when $n + s$ is odd, use the fact that (by Lemma 1)

$$A_j - B_j = A_0 - B_0 + \left(\frac{j}{p}\right) p^{\frac{n-s}{2}} \tag{8}$$

for each j. Combining this with (6) and (7), we obtain the desired result. □

Remark 1. *Lemma 4 extends the results of [9, 11, 15, 17, 20]. Namely, in [9], the value distribution of the dual of a weakly regular bent function f was studied. Then the extension to weakly regular plateaued functions was given in [11]. In [15], the case of f being a non-weakly regular bent function whose dual is bent with respect to* $\mathsf{supp}(f)$. *Later, in [17], the authors presented the case of non-weakly regular s-plateaued functions f whose dual is bent with respect to* $\mathsf{supp}(f)$, *which was further analyzed in [20]. Therefore Lemma 4 is the most general result of this kind.*

Remark 2. *Lemma 4 covers the value distributions of all known instances of weakly and non-weakly bent functions.*

Lemma 5. *Let $f\colon \mathbb{F}_{p^n} \to \mathbb{F}_p$ be an unbalanced s-plateaued function in $\mathscr{C}_2$ such that $f(0) = f^*(0) = 0$. Suppose that $W_{f^*}(0) = t(f^*)p^{\frac{\theta}{2}}$ for some $\theta \in \mathbb{N}$, $\theta > 1$, θ even. Then, $A_0 = \frac{p^{n-s-1}+p^{\frac{n-s}{2}}+t(f^*)(p-1)p^{\frac{\theta}{2}-1}}{2}$, $B_0 = \frac{p^{n-s-1}-p^{\frac{n-s}{2}}+t(f^*)(p-1)p^{\frac{\theta}{2}-1}}{2}$. Moreover, for $j \in \mathbb{F}_p^\star$, $A_j = B_j = A_0 - \frac{p^{\frac{n-s}{2}}+t(f^*)p^{\frac{\theta}{2}}}{2}$.*

Proof. Since $t(f^*)p^{\frac{\theta}{2}} = W_{f^*}(0) = \sum_{j=1}^{p-1}(2A_j - 2A_0 + p^{\frac{n-s}{2}})\xi_p^j$, we have

$$A_j = A_0 - \frac{p^{\frac{n-s}{2}} + t(f^*)p^{\frac{\theta}{2}}}{2} \tag{9}$$

for each j. From Lemma 3, $\frac{p^{n-s}+p^{\frac{n-s}{2}}}{2} = \sum_{j=0}^{p-1} A_j = (p-1)(A_0 - \frac{p^{\frac{n-s}{2}}+t(f^*)p^{\frac{\theta}{2}}}{2}) + A_0$. Thus, $A_0 = \frac{p^{n-s-1}+p^{\frac{n-s}{2}}+t(f^*)(p-1)p^{\frac{\theta}{2}-1}}{2}$. So that $B_0 = \frac{p^{n-s-1}-p^{\frac{n-s}{2}}+t(f^*)(p-1)p^{\frac{\theta}{2}-1}}{2}$. The values of A_j are then obtained via (9). □

The following is pretty straightforward, we thus omit its proof.

Proposition 1. *Let $f \in \mathscr{C}_2$ be a plateaued function with $f(0) = f^*(0) = 0$ such that $W_{f^*}(0) = t(f^*)p^{\frac{\theta}{2}}\nu$, $\theta \in \mathbb{N}$ and $\nu \in \{1, \mathfrak{i}\}$. Then f^* is the constant zero function if and only if $\nu = 1$, $\theta = 2(n-s)$ and $t(f^*) = 1$.*

Lemma 6. *Let $f\colon \mathbb{F}_{p^n} \to \mathbb{F}_p$ be an unbalanced s-plateaued function in $\mathscr{C}_2$ such that $f(0) = f^*(0) = 0$. Suppose that $W_{f^*}(0) = t(f^*)\nu' p^{\frac{\theta}{2}}$ for some $\nu' \in \{1, \mathfrak{i}\}$ and $\theta \in \mathbb{N}$, $\theta > 1$, θ odd. Then, we have $A_0 = \frac{p^{n-s-1}+p^{\frac{n-s}{2}}}{2}$, $B_0 = \frac{p^{n-s-1}-p^{\frac{n-s}{2}}}{2}$. Moreover, for $j \in \mathbb{F}_p^\star$, the value of $A_j (= B_j)$ is equal to $A_j = B_j = A_0 - \frac{p^{\frac{n-s}{2}}+\left(\frac{j}{p}\right)t(f^*)p^{\frac{\theta-1}{2}}}{2}$.*

Proof. Since $W_{f^*}(0) = t(f^*)\nu' p^{\frac{\theta-1}{2}}\sqrt{p}$, we have

$$2A_j = 2A_0 - p^{\frac{n-s}{2}} + \left(\frac{j}{p}\right) t(f^*)p^{\frac{\theta-1}{2}}$$

for each j. Summing these terms up, we get

$$p^{n-s} = \sum_{j=0}^{p-1} 2A_j - p^{\frac{n-s}{2}} = 2pA_0 - p^{\frac{n-s}{2}+1}.$$

Thus $2A_0 = p^{n-s-1} + p^{\frac{n-s}{2}}$ and the result follows. □

Lemma 7. *Let $f\colon \mathbb{F}_{p^n} \to \mathbb{F}_p$ be an unbalanced s-plateaued function in $\mathscr{C}_3$ such that $f(0) = f^*(0) = 0$. Let the set $\mathcal{I}$ be defined as in Lemma 3. Suppose that $W_{f^*}(0) = t(f^*)p^{\frac{\theta}{2}}$ for some $\theta \in \mathbb{N}$, $\theta > 1$, θ even. Then, $A_0 = \frac{p^{n-s-1}+t(f^*)(p-1)p^{\frac{\theta}{2}-1}-\sigma\left(\frac{i}{p}\right)p^{\frac{n-s-1}{2}}}{2}$ and $B_0 = \frac{p^{n-s-1}+t(f^*)(p-1)p^{\frac{\theta}{2}-1}+\sigma\left(\frac{i}{p}\right)p^{\frac{n-s-1}{2}}}{2}$ for any $i \in \mathcal{I}$. Moreover, for $j \in \mathcal{I}$, $A_j = B_j = \frac{p^{n-s-1}-t(f^*)p^{\frac{\theta}{2}-1}}{2}$ and, for $j \notin \mathcal{I}$, we have*

$$A_j = \frac{p^{n-s-1} - t(f^*)p^{\frac{\theta}{2}-1}}{2} - \sigma\left(\frac{j}{p}\right)p^{\frac{n-s-1}{2}}$$

and $B_j = \frac{p^{n-s-1}-t(f^*)p^{\frac{\theta}{2}-1}}{2} + \sigma\left(\frac{j}{p}\right)p^{\frac{n-s-1}{2}}$, where $\sigma = 1$ if $p \equiv 1 \pmod 4$ and $\sigma = -1$ if $p \equiv 3 \pmod 4$.

Proof. Since $t(f^*)p^{\frac{\theta}{2}} = W_{f^*}(0) = \sum_{j=1}^{p-1}(A_j + B_j - A_0 - B_0)\xi_p^j$, we have

$$A_j + B_j = A_0 + B_0 - t(f^*)p^{\frac{\theta}{2}} \tag{10}$$

for each j. Summing up, we get

$$p^{n-s} - A_0 - B_0 = \sum_{j=1}^{p-1} A_j + B_j = (p-1)(A_0 + B_0 - t(f^*)p^{\frac{\theta}{2}}).$$

Thus, $A_0+B_0=p^{n-s-1}+t(f^*)p^{\frac{\theta}{2}-1}(p-1)$. By Lemma 3, we know that $A_0-B_0=-\sigma\left(\frac{i}{p}\right)p^{\frac{n-s-1}{2}}$ for any $i\in\mathcal{I}$. Combining these two equations, we have

$$A_0=\frac{p^{n-s-1}+t(f^*)(p-1)p^{\frac{\theta}{2}-1}-\sigma\left(\frac{i}{p}\right)p^{\frac{n-s-1}{2}}}{2}$$

and

$$B_0=\frac{p^{n-s-1}+t(f^*)(p-1)p^{\frac{\theta}{2}-1}+\sigma\left(\frac{i}{p}\right)p^{\frac{n-s-1}{2}}}{2}.$$

The result follows at once from Lemma 3. □

Lemma 8. *Let $f\colon\mathbb{F}_{p^n}\to\mathbb{F}_p$ be an unbalanced s-plateaued function in $\mathscr{C}_3$ such that $f^*(0)=0$. Let the set $\mathcal{I}$ be defined as in Lemma 3. Suppose that $W_{f^*}(0)=t(f^*)\nu' p^{\frac{\theta}{2}}$ for some $\nu'\in\{1,\mathrm{i}\}$ and $\theta\in\mathbb{N}$, $\theta>1$, θ odd. Then $A_0=\frac{p^{n-s-1}-\left(\frac{i}{p}\right)p^{\frac{n-s-1}{2}}}{2}$ and $B_0=\frac{p^{n-s-1}+\left(\frac{i}{p}\right)p^{\frac{n-s-1}{2}}}{2}$ for any $i\in\mathcal{I}$. Moreover, for $j\in\mathcal{I}$, we have $A_j=B_j=\frac{p^{n-s-1}+\left(\frac{j}{p}\right)t(f^*)p^{\frac{\theta-1}{2}}}{2}$ and, for $j\notin\mathcal{I}$, we have $A_j=\frac{p^{n-s-1}+\left(\frac{j}{p}\right)t(f^*)p^{\frac{\theta-1}{2}}}{2}-\sigma\left(\frac{j}{p}\right)p^{\frac{n-s-1}{2}}$ and $B_j=\frac{p^{n-s-1}+\left(\frac{j}{p}\right)t(f^*)p^{\frac{\theta-1}{2}}}{2}+\sigma\left(\frac{j}{p}\right)p^{\frac{n-s-1}{2}}$, where $\sigma=1$ if $p\equiv 1\pmod 4$ and $\sigma=-1$ if $p\equiv 3\pmod 4$.*

Proof. Since $t(f^*)\nu' p^{\frac{\theta-1}{2}}\sqrt{p}=W_{f^*}(0)=\sum_{j=1}^{p-1}(A_j+B_j-A_0-B_0)\xi_p^j$, we have

$$A_j+B_j=A_0+B_0+\left(\frac{j}{p}\right)t(f^*)p^{\frac{\theta-1}{2}}\tag{11}$$

for each j. Summing up, we get $A_0+B_0=p^{n-s-1}$. By Lemma 3, we know that $A_0-B_0=-\sigma\left(\frac{i}{p}\right)p^{\frac{n-s-1}{2}}$ for any $i\in\mathcal{I}$. Combining these two equations, we have $A_0=\frac{p^{n-s-1}-\sigma\left(\frac{i}{p}\right)p^{\frac{n-s-1}{2}}}{2}$ and $B_0=\frac{p^{n-s-1}+\sigma\left(\frac{i}{p}\right)p^{\frac{n-s-1}{2}}}{2}$. Combining these values with Lemma 3, we obtain the desired conclusion. □

Remark 3. *Lemmas 4, 5 and 8 cover all known examples of plateaued functions (up to now).*

5 Codes from plateaued functions

In this section, we will use plateaued functions $f\colon\mathbb{F}_{p^n}\to\mathbb{F}_p$ to construct linear codes using (3). This approach extends the results in [9, 11, 15, 17, 20]. In order to explicitly compute the weights of the derived codes $\mathcal{C}_f$, where f is an s-plateaued function, we must count the number of elements in the preimage of a given function. We will do so by considering the possible dual value distributions studied in Section 4. In the following sections, we derive the full weight distributions of codes stemming from plateaued functions such that $f(0)=0$, where the distributions are parametrized by $wt(f^*)$ when $n+s$ is odd and by $wt(f^*)$ and Z_0 when $n+s$ is even, in the latter it is also required that $f^*(0)=0$.

5.1 The weight distribution of $\mathcal{C}_f$ for $n + s$ odd

Throughout this section, $n + s$ will be odd. Define the following three subclasses of plateaued functions:

$$\widehat{\mathcal{P}_2} = \{f \in \mathscr{C}_3 \mid f \text{ is weakly regular}\},$$

$$\widetilde{\mathcal{P}_2} = \{f \in \mathscr{C}_1 \mid \forall i \in QR^* A_i = 0, B_i \neq 0 \text{ and } \forall i \in NQR\ A_i \neq 0, B_i = 0\},$$

and

$$\overline{\mathcal{P}_2} = \{f \in \mathscr{C}_1 \mid \forall i \in NQR\ A_i = 0, B_i = 0 \text{ and } \forall i \in NQR\ A_i = 0, B_i \neq 0\}.$$

Define $\mathcal{P}_2 = \widehat{\mathcal{P}_2} \cup \widetilde{\mathcal{P}_2} \cup \overline{\mathcal{P}_2}$. These classes yield codes with two weights, thus they can be regarded as exceptions since every other plateaued function gives rise to a 3-valued code, as shown in the following theorem, which is quite general and it does not necessarily follow from Lemma 4.

Theorem 1. *Let $n > 0$ and $0 \leq s < n$ be integers such that $n + s$ is odd. Let f be any s-plateaued function defined over $\mathbb{F}_{p^n}$ with $f(0) = 0$ such that $f \notin \mathcal{P}_2$. The code $\mathcal{C}_f$ in (3) ($m = 1$) is a three-valued code with parameters $[p^n - 1, n + 1, (p - 1)p^{n-1} - p^{\frac{n+s-1}{2}}]$, whose weight distribution is displayed in Table 3.*

Proof. The weights are easily derived from the results in [9], which are $w_1 := p^n - p^{n-1} - p^{(n+s-1)/2}$, $w_2 := p^n - p^{n-1}$ and $w_3 := p^n - p^{n-1} + p^{(n+s-1)/2}$. Note that there are exactly three weights since $f \notin \mathcal{P}_2$. Denote by X, Y and Z the number of codewords attaining the weight $p^n - p^{n-1} - p^{(n+s-1)/2}, p^n - p^{n-1}$ and $p^n - p^{n-1} + p^{(n+s-1)/2}$, respectively. Using the first two Pless Power moments, we get the system of equations

$$X + Y + Z = p^{n+1} - 1 \tag{12}$$

$$w_1 X + w_2 Y + w_3 Z = p^n(p - 1)(p^n - 1). \tag{13}$$

Since the number of balanced codewords can be counted as

$$Y = p^n - 1 + (p - 1)(p^n - p^{n-s}) + (p - 1)(p^{n-s} - wt(f^*)) = p^{n+1} - (p - 1)wt(f^*) - 1,$$

we can solve the above system in terms of $wt(f^*)$. Namely,

$$X = \frac{(p-1)}{2}(wt(f^*) - (p - 1)p^{(n-s-1)/2}) \tag{14}$$

$$Z = \frac{(p-1)}{2}(wt(f^*) + (p - 1)p^{(n-s-1)/2}) \tag{15}$$

□

When $f \in \mathcal{P}_2$, one can show that the code $\mathcal{C}_f$ is two-valued, thus the frequencies corresponding to the same weight must be added up. From Theorem 1, we can easily derive the weight distribution of $\mathcal{C}_f$ for s-plateaued functions with $f(0) = 0$ such that $wt(f^*) = p^n - p^{n-s-1}$. The corresponding values are displayed in Table 3.

5.2 The weight distribution of $\mathcal{C}_f$ for $n+s$ even

Theorem 2. *Let $n > 0$ and $0 \le s \le n$ be integers such that $n+s$ is even. Let $f \in \mathscr{C}_1$ be an s-plateaued function defined over $\mathbb{F}_{p^n}$ with $f(0) = f^*(0) = 0$. The code $\mathcal{C}_f$ in (3) ($m = 1$) is a five-valued code with parameters $[p^n - 1, n+1, p^n - p^{n-1} - p^{(n+s-2)/2}(p-1)]$, whose weight distribution is displayed in Table 4.*

Proof. The weights are easily obtained from the results of [9]. We have the weights $w_1 = p^n - p^{n-1} - t(f^*)p^{(n+s-2)/2}(p-1)$, $w_2 = p^n - p^{n-1} - t(f^*)p^{(n+s-2)/2}$, $w_3 = p^n - p^{n-1}$, $w_4 = p^n - p^{n-1} + t(f^*)p^{(n+s-2)/2}$ and $w_5 = p^n - p^{n-1} + t(f^*)p^{(n+s-2)/2}(p-1)$. The number of codewords with weight w_1 is

$$(p-1)A_0 = \frac{(p-1)}{2}(p^{n-s} - wt(f^*) - t(f^*)Z_0).$$

Similarly, the number of codewords with weight w_5 is

$$(p-1)B_0 = \frac{(p-1)}{2}(p^{n-s} - wt(f^*) + t(f^*)Z_0).$$

The number of codewords of weight w_2 and w_4 are

$$(p-1)\sum_{j=1}^{p-1} A_j = \frac{(p-1)}{2}(wt(f^*) + t(f^*)(p-1)(Z_0 - t(f^*)p^{\frac{n-s}{2}}))$$

and

$$(p-1)\sum_{j=1}^{p-1} B_j = \frac{(p-1)}{2}(wt(f^*) - t(f^*)(p-1)(Z_0 - t(f^*)p^{\frac{n-s}{2}})),$$

respectively. Finally, there are $p^n - 1 + (p-1)(p^n - p^{n-s})$ balanced codewords. □

Corollary 1. *Let $n > 0$ and $0 \le s \le n$ be integers such that $n+s$ is even. Let $f \in \mathscr{C}_1$ be any s-plateaued function defined over $\mathbb{F}_{p^n}$ with $f(0) = f^*(0) = 0$. Suppose that $W_{f^*}(0) = t(f^*)\nu' p^{\frac{n-s}{2}}$ for some $\nu' \in \{1, \mathfrak{i}\}$. Let $Z_0 := A_0 - B_0$. The code $\mathcal{C}_f$ in (3) ($m = 1$) is a five-valued code with parameters $[p^n - 1, n+1, p^n - p^{n-1} - p^{(n+s-2)/2}(p-1)]$, whose weight distributions is displayed in Table 5.*

Proof. One can easily obtain the value of $wt(f^*)$ and plug it into Theorem 2. □

When $f \in \mathcal{C}_2$ and f^* is the constant zero function the code $\mathcal{C}_f$ is a three-weighted code [17]. We then analyze the remaining cases.

Theorem 3. *Let $n > 0$ and $0 \le s \le n$ be integers such that $n+s$ is even. Let $f \in \mathscr{C}_2$ be an s-plateaued function defined over $\mathbb{F}_{p^n}$ with $f(0) = f^*(0) = 0$. Suppose that $W_{f^*}(0) = t(f^*)\nu' p^{\frac{\theta}{2}}$ for some $\nu' \in \{1, \mathfrak{i}\}$ and $\theta \in \mathbb{N}, \theta > 0$ even. Suppose that f^* is not constant zero. The code $\mathcal{C}_f$ in (3) ($m = 1$) is a five-valued code with parameters $[p^n - 1, n+1, p^n - p^{n-1} - p^{(n+s-2)/2}(p-1)]$, whose weight distribution is displayed in Table 6.*

Proof. Again, the weights are seen to be $w_1 = p^n - p^{n-1} - t(f^*)p^{(n+s-2)/2}(p-1)$, $w_2 = p^n - p^{n-1} - t(f^*)p^{(n+s-2)/2}$, $w_3 = p^n - p^{n-1}$, $w_4 = p^n - p^{n-1} + t(f^*)p^{(n+s-2)/2}$ and $w_5 = p^n - p^{n-1} + t(f^*)p^{(n+s-2)/2}(p-1)$. Following a similar reasoning as in Theorem 2 and using Lemma 5, the number of codewords with weights w_1 and w_5 are, respectively,

$$(p-1)A_0 = (p-1)\left(\frac{p^{n-s-1} + p^{\frac{n-s}{2}} + t(f^*)(p-1)p^{\frac{\theta}{2}-1}}{2}\right),$$

and

$$(p-1)B_0 = (p-1)\left(\frac{p^{n-s-1} - p^{\frac{n-s}{2}} + t(f^*)(p-1)p^{\frac{\theta}{2}-1}}{2}\right).$$

The number of codewords with weights w_3 and w_4 equals

$$(p-1)\sum_{j=1}^{p-1} A_j = \frac{(p-1)}{2}(p^{n-s-1} - t(f^*)p^{\frac{\theta}{2}-1}).$$

Finally, there are $p^n - 1 + (p-1)(p^n - p^{n-s})$ balanced codewords. □

Theorem 4. *Let $n > 0$ and $0 \le s \le n$ be integers such that $n+s$ is even. Let $f \in \mathscr{C}_2$ be an s-plateaued function defined over $\mathbb{F}_{p^n}$ with $f(0) = f^*(0) = 0$. Suppose that $W_{f^*}(0) = t(f^*)\nu' p^{\frac{\theta}{2}}$ for some $\nu' \in \{1, \mathfrak{i}\}$ and $\theta \in \mathbb{N}$, $\theta > 0$ odd. Suppose that f^* is not constant zero. The code $\mathcal{C}_f$ in (3) ($m = 1$) is a five-valued code with parameters $[p^n - 1, n+1, p^n - p^{n-1} - p^{(n+s-2)/2}(p-1)]$, whose weight distribution is displayed in Table 7.*

Proof. As before, the weights are $w_1 = p^n - p^{n-1} - t(f^*)p^{(n+s-2)/2}(p-1)$, $w_2 = p^n - p^{n-1} - t(f^*)p^{(n+s-2)/2}$, $w_3 = p^n - p^{n-1}$, $w_4 = p^n - p^{n-1} + t(f^*)p^{(n+s-2)/2}$ and $w_5 = p^n - p^{n-1} + t(f^*)p^{(n+s-2)/2}(p-1)$. Using Lemma 6, we compute the frequencies of codewords. The number of codewords with weight w_1 is

$$(p-1)A_0 = \frac{(p-1)}{2}(p^{n-s-1} + p^{\frac{n-s}{2}}).$$

The number of codewords with weight w_5 is

$$(p-1)B_0 = \frac{(p-1)}{2}(p^{n-s-1} - p^{\frac{n-s}{2}}).$$

The number of codewords of weight w_2 and w_4 is

$$(p-1)\sum_{j=1}^{p-1} A_j = \frac{(p-1)^2}{2}p^{n-s-1}.$$

Finally, there are $p^n - 1 + (p-1)(p^n - p^{n-s})$ balanced codewords. □

5.3 The weight distribution of $\mathcal{C}_F$

In this section, we extend the results in the previous sections to the case of vectorial plateaued functions. Little is known about infinite families of vectorial non-bent plateaued functions [5]. Namely, the only known examples are some power functions.

Example 2. *For an integer k with $n/\gcd(n,k)$ odd, consider the functions $F\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ given by $F(x) = x^{(p^{2k}+1)/2}$ and $F'\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ given by $F'(x) = x^{p^{2k}-p^k+1}$. Then, $F(x)$ is an s-plateaued function whose components have zero dual, and $F'(x)$ is an s-plateaued function whose components have zero dual.*

Example 3. *Working in $\mathbb{F}_{3^5}$, consider the 1-plateaued function $F\colon \mathbb{F}_{3^5} \to \mathbb{F}_{3^5}$ defined by $F(x) = x^{\frac{3^2+1}{2}} = x^5$. Using MAGMA, we have verified that the code $\mathcal{C}_F$ is a minimal self-orthogonal code with parameters $[242, 10, 144]$, $d^{\perp} = 2$ and weight enumerator polynomial $1+10890z^{144}+39446z^{162}+8712z^{180}$.*

The weight distribution for these two (vectorial) examples are easily derived in general.

Theorem 5. *Let $n > 0$ and $0 \leq s \leq n$ be integers such that $n + s$ is even. Let $F\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be a vectorial plateaued function whose components have zero duals such that $F(0) = 0$. The code $\mathcal{C}_f$ in (3) ($m = 1$) is a three-valued code with parameters $[p^n - 1, 2n, p^n - p^{n-1} - p^{(n+s-2)/2}(p-1)]$, whose weight distribution is displayed in Table 8.*

6 Properties of the obtained codes

It is easily seen that the obtained codes are minimal by Ashikhmin-Barg's condition [1]. Furthermore, codes stemming from plateaued functions are also self-orthogonal.

Theorem 6. *Let $f : \mathbb{F}_{p^m} \to \mathbb{F}_p$ be a plateaued function such that $f(0) = 0$. The code $\mathcal{C}_f$ is included in its dual $\mathcal{C}_f^{\perp}$, i.e., $\mathcal{C}_f$ is self-orthogonal.*

Proof. It suffices to prove that

$$\sum_{x\in\mathbb{F}_{p^m}} f(x)^2 + (\mathrm{Tr}_1^m((v_1+v_2)x))f(x) + \mathrm{Tr}_1^m(v_1x)\mathrm{Tr}_1^m(v_2x)$$

is divisible by p. Since $(\mathrm{Tr}_1^m((v_1+v_2)x))$ is balanced, the sum $\sum_{x\in\mathbb{F}_{p^m}}(\mathrm{Tr}_1^m((v_1+v_2)x))$ is divisible by p. Moreover, so is $\mathrm{Tr}_1^m(v_1x)\mathrm{Tr}_1^m(v_2x)$ by a similar reason. The value of $\sum_{x\in\mathbb{F}_{p^m}} f(x)$ is determined through the sums $\sum_{j=1}^{\frac{p-1}{2}} j^2(|f^{-1}(j)|+|f^{-1}(-j)|)$. It is a well-known result that $f^{-1}(j)$ is congruent to 0 modulo p for each j [23]. □

Remark 4. *A similar approach can be used to proving that codes stemming from vectorial plateaued functions with zero dual are also self-orthogonal (codes in Theorem 5).*

A code that is simultaneously minimal and self-orthogonal is *the best* we can expect, namely, there are no minimal self-dual codes besides two exceptions, as shown in the following.

Proposition 2. *There are no self-dual minimal linear codes for $q > 3$. The only self-dual minimal ternary code is the tetracode $[4, 2, 3]_3$, whereas the only self-dual minimal binary code is the repetition code $[2, 1, 2]_2$.*

Proof. Let C be a linear code with parameters $[n, k, d]_q$ with n even. If C is minimal then $k+q-2 \le d_{min} \le d_{max} \le n-k+1$, where d_{min} and d_{max} denote the minimum and the maximum distance in C, respectively. Thus if C is self-dual and minimal, we have

$$\frac{n}{2} + q - 2 \le d_{min} \le d_{max} \le \frac{n}{2} + 1. \tag{16}$$

Hence, for $q > 3$, the result follows. Let $q = 3$, i.e., C is a Type III code. In this case, the only possibility is that $d_{min} = d_{max} = \frac{n}{2} + 1$, so that C is also a one-weight code with parameters $[n, n/2, n/2 + 1]$. It's known that n is divisible by 4. Since C is self-dual, it is self-orthogonal, so $n/2 + 1 \equiv 0 \pmod 3$, which implies $n \equiv 1 \pmod 3$. Then $n = 4(3r + 1)$ for some $r \ge 0$. For a Type III code, $d_{min} \le 3\lfloor \frac{n}{12} \rfloor + 3$. Hence, $d_{min} \le 3\lfloor r + \frac{1}{3} \rfloor + 3 = 3r + 3$. On the other hand, $d_{min} = 6r + 3$, which yields $r = 0$. Thus C must be the tetracode $[4, 2, 3]_3$. Let $q = 2$. By (16), we get: $d_{min} = d_{max} = \frac{n}{2}$, $d_{min} = d_{max} = \frac{n}{2} + 1$ or $d_{min} = \frac{n}{2}$ and $d_{max} = \frac{n}{2} + 1$. Since a self-dual binary code is even, it must be that $d_{min} = d_{max}$. First suppose that C is of Type II, i.e. all codewords are divisible by four. In this case, $n \equiv 0 \pmod 8$, say, $n = 8r$ for some $r \ge 1$. It's well-known that for self-dual binary codes it holds $d_{min} \le 2\lfloor \frac{n}{8} \rfloor + 2$. This yields $d_{min} \le 2r + 2$. Since $d_{min} = 4r$, the only possibility is that C has parameters $[8, 4, 4]_2$, that is, the extended Hamming code, which contains the all one vector $\mathbf{1}$. Now suppose that C is of Type I (there are some codewords which are not divisible by four). For Type I codes, it holds $d_{min} \le 2\lfloor \frac{n+6}{10} \rfloor$ for $n \notin E := \{2, 12, 22, 32\}$. Assume that $n \notin E$. Suppose that $n \equiv 0 \pmod 4$, say, $n = 4r$ for some $r \ge 1$. It follows that $d_{min} = \frac{n}{2}$. This yields $2r = d_{min} \le 2\lfloor \frac{2r+3}{5} \rfloor$. So $r \le \lfloor \frac{2r+3}{5} \rfloor$, which is true only for $r = 1$, in other words, the code C has parameters $[4, 2, 2]_2$, which can be seen to contain $\mathbf{1}$. Suppose that $n \equiv 2 \pmod 4$, say, $n = 4r + 2$ for some $r \ge 1$. It follows that $d_{min} = \frac{n}{2} + 1$. This yields $2r + 2 = d_{min} \le 2\lfloor \frac{2r+3}{5} \rfloor$. So $r + 1 \le \lfloor \frac{2r+3}{5} \rfloor$, which cannot happen. Using again the bound $d_{min} \le 2\lfloor \frac{n}{8} \rfloor + 2$, we can rule out all the values of $n \in E$ except for $n = 2$. This finishes the proof. □

7 Conclusions

To be added.

References

[1] Ashikhmin, A., and Barg, A. Minimal vectors in linear codes. *IEEE Trans. Inf. Theory 44*, 5 (1998), 2010–2017.

[2] Bartoli, D., and Bonini, M. Minimal linear codes in odd characteristic. *IEEE Trans. Inf. Theory 65*, 7 (2019), 4152–4155.

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

[4] Carlet, C., Ding, C., and Yuan, J. Linear codes from highly nonlinear functions and their secret sharing schemes. *IEEE Trans. Inf. Theory 51*, 6 (2005), 1089–2102.

[5] Çeşmelioğlu, A., and Olmez, O. Graphs of vectorial plateaued functions as difference sets. *Finite Fields and Their Applications 71* (2021), 101795.

[6] Ding, K., and Ding, C. A class of two-weight and three-weight codes and their applications in secret sharing. *IEEE Trans. Inf. Theory 61*, 11 (2015), 5835–5842.

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

[8] Kumar, P. V., Scholtz, R. A., and Welch, L. R. Generalized bent functions and their properties. *Journal Comb. Theory (Series A) 40* (1985), 90–107.

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

[10] Mesnager, S. Linear codes from functions. In *Concise Encycl. Coding Theory*, W. C. Huffman, J. Kim, and P. Solé, Eds. Chapman and Hall/CRC, London, New York, 2021, pp. 463–526.

[11] Mesnager, S., Özbudak, F., and Sinak, A. Linear codes from weakly regular plateaued functions and their secret sharing schemes. *Des. Codes Cryptogr. 87* (2019), 463–480.

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

[13] Mesnager, S., and Sinak, A. Several classes of minimal linear codes with few weights from weakly regular plateaued functions. *IEEE Trans. Inf. Theory 66*, 4 (2020), 2296–2310.

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

[15] Pelen, R. M. Studies on non-weakly regular bent functions and related structures. *PhD Dissertation,* (2020).

[16] Potapov, V. N. On q-ary bent and plateaued functions. *Des. Codes Cryptogr. 88* (2020), 2037–2049.

[17] Rodríguez, R., Pasalic, E., Zhang, F., and Wei, Y. Minimal p-ary codes via the direct sum of functions, non-covering permutations and subspaces of derivatives. *IEEE Trans. Inf. Theory* (2023).

[18] Sinak, A. Minimal linear codes from weakly regular plateaued balanced functions. *Discrete Math. 344*, 3 (2021).

[19] Tang, D., Carlet, C., and Zhou, Z. Binary linear codes from vectorial boolean functions and their weight distribution. *Discrete Math. 340*, 12 (2017), 3055–3072.

[20] Wei, Y., Wang, J., and Fu, F. Linear codes with few weights from non-weakly regular plateaued functions. *IEEE Trans. Inf. Theory* (2023). Accesed Dec 2023.

[21] Xu, G., and Qu, L. Three classes of minimal linear codes over the finite fields of odd characteristic. *IEEE Trans. Inf. Theory 65*, 11 (2019), 7067–7078.

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

[23] Zheng, Y., and Zhang, X. M. On plateaued functions. *IEEE Trans. Inf. Theory 47*, 3 (2001), 1215–1223.

8 Tables

Table 1: Values of A_j, B_j and $A_0 + B_0$ in Lemma 4 for different parities of $n+s$ and θ, where the pairs stand for $(n+s \pmod 2, \theta \pmod 2)$.

	A_j	B_j	$A_0 + B_0$
$(0,0)$	0, or, $A_0 - p^{\frac{n-s}{2}-1}\frac{(1+t(f^*))}{2}$	0, or, $B_0 - p^{\frac{n-s}{2}-1}\frac{(1-t(f^*))}{2}$	$p^{n-s-1} + t(f^*)(p-1)p^{\frac{\theta}{2}-1}$
$(0,1)$	0, or, $A_0 + \frac{\left(\frac{j}{p}\right)t(f^*)p^{\frac{\theta}{2}} - p^{\frac{n-s}{2}-1}}{2}$	0, or, $B_0 + \frac{\left(\frac{j}{p}\right)t(f^*)p^{\frac{\theta}{2}} + p^{\frac{n-s}{2}-1}}{2}$	p^{n-s-1}
$(1,0)$	0, or, $A_0 + \frac{\left(\frac{j}{p}\right)p^{\frac{n-s}{2}} - t(f^*)p^{\frac{\theta}{2}}}{2}$	0, or, $B_0 + \frac{-\left(\frac{j}{p}\right)p^{\frac{n-s}{2}} - t(f^*)p^{\frac{\theta}{2}}}{2}$	$p^{n-s-1} + t(f^*)(p-1)p^{\frac{\theta}{2}-1}$
$(1,1)$	0, or, $A_0 + \frac{\left(\frac{j}{p}\right)(t(f^*)p^{\frac{\theta}{2}} + p^{\frac{n-s}{2}})}{2}$	0, or, $B_0 + \frac{\left(\frac{j}{p}\right)(t(f^*)p^{\frac{\theta}{2}} - p^{\frac{n-s}{2}})}{2}$	p^{n-s-1}

Table 2: Weight distribution of the code $\mathcal{C}_f$, derived in Theorem 1, for an s-plateaued function $f\colon \mathbb{F}_{p^n} \to \mathbb{F}_p$ with $f(0) = 0$ and $A_j \neq B_j$ for each j, when $n+s$ is odd.

Weight w	Number of codewords
$p^n - p^{n-1} - p^{(n+s-1)/2}$	$\frac{(p-1)}{2}(wt(f^*) + (p-1)p^{\frac{n-s-1}{2}})$
$p^n - p^{n-1}$	$p^{n+1} - (p-1)wt(f^*) - 1$
$p^n - p^{n-1} + p^{(n+s-1)/2}$	$\frac{(p-1)}{2}(wt(f^*) - (p-1)p^{\frac{n-s-1}{2}})$

Table 3: Weight distribution of the code $\mathcal{C}_f$, derived in Theorem 1, for an s-plateaued function $f\colon \mathbb{F}_{p^n} \to \mathbb{F}_p$ with $f(0) = 0$, $A_j \neq B_j$ for each j, and $wt(f^*) = p^{n-s} - p^{n-s-1}$, when $n+s$ is odd.

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

Table 4: Weight distribution of the code $\mathcal{C}_f$, derived in Theorem 2, for an s-plateaued function $f\colon \mathbb{F}_{p^n} \to \mathbb{F}_p$ such that $f(0) = f^*(0) = 0$, when $n+s$ is even, $A_j \neq B_j$ for each j and $Z_0 = A_0 - B_0$.

Weight w	Number of codewords
$p^n - p^{n-1} - p^{(n+s-2)/2}(p-1)$	$\frac{(p-1)}{2}(p^{n-s} - wt(f^*) + Z_0)$
$p^n - p^{n-1} - p^{(n+s-2)/2}$	$\frac{(p-1)}{2}(wt(f^*) - (p-1)Z_0 + (p-1)p^{\frac{n-s}{2}})$
$p^n - p^{n-1}$	$p^{n+1} - (p-1)p^{n-s} - 1$
$p^n - p^{n-1} + p^{(n+s-2)/2}$	$\frac{(p-1)}{2}(wt(f^*) + (p-1)Z_0 - (p-1)p^{\frac{n-s}{2}})$
$p^n - p^{n-1} + p^{(n+s-2)/2}(p-1)$	$\frac{(p-1)}{2}(p^{n-s} - wt(f^*) - Z_0)$

Table 5: Weight distribution of the code $\mathcal{C}_f$, derived in Corollary 1, for an s-plateaued function $f\colon \mathbb{F}_{p^n} \to \mathbb{F}_p$ such that $f(0) = f^*(0) = 0$ and $W_{f^*}(0) = t(f^*)\nu' p^{\frac{n-s}{2}}$, when $n+s$ is even.

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

Table 6: Weight distribution of the code $\mathcal{C}_f$, derived in Theorem 3, for an s-plateaued function $f\colon \mathbb{F}_{p^n} \to \mathbb{F}_p$ such that $f(0) = f^*(0) = 0$ and $W_{f^*}(0) = t(f^*)\nu p^{\frac{\theta}{2}}$, when $n+s$ and θ are even.

Weight w	Number of codewords
$p^n - p^{n-1} - p^{(n+s-2)/2}(p-1)$	$\frac{(p-1)}{2}(p^{n-s-1} + p^{\frac{n-s}{2}} + t(f^*)(p-1)p^{\frac{\theta}{2}-1})$
$p^n - p^{n-1} - p^{(n+s-2)/2}$	$\frac{(p-1)^2}{2}(p^{n-s-1} - t(f^*)p^{\frac{\theta}{2}-1})$
$p^n - p^{n-1}$	$p^{n+1} - (p-1)p^{n-s} - 1$
$p^n - p^{n-1} + p^{(n+s-2)/2}$	$\frac{(p-1)^2}{2}(p^{n-s-1} - t(f^*)p^{\frac{\theta}{2}-1})$
$p^n - p^{n-1} + p^{(n+s-2)/2}(p-1)$	$\frac{(p-1)}{2}(p^{n-s-1} - p^{\frac{n-s}{2}} + t(f^*)(p-1)p^{\frac{\theta}{2}-1})$

Table 7: Weight distribution of the code $\mathcal{C}_f$, derived in Theorem 4, for an s-plateaued function $f\colon \mathbb{F}_{p^n} \to \mathbb{F}_p$ such that $f(0) = f^*(0) = 0$ and $W_{f^*}(0) = t(f^*)\nu p^{\frac{\theta}{2}}$, when $n+s$ is even and θ is odd.

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

Table 8: Weight distribution of $\mathcal{C}_F$ in Theorem 5, where $F\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is an s-plateaued function, whose components have zero dual and $F(0) = 0$ ($n + k$ is even).

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