Few-weight linear codes over $\mathbb{F}_p$ from t-to-one mappings

René Rodríguez-Aldama*

Abstract

For any prime number p, we provide two classes of linear codes with few weights over a p-ary alphabet. These codes are based on a well-known generic construction (the defining-set method), stemming on a class of monomials and a class of trinomials over finite fields. The considered monomials are Dembowski-Ostrom monomials $x^{p^\alpha+1}$, for a suitable choice of the exponent α, so that, when $p > 2$ and $n \not\equiv 0 \pmod 4$, these monomials are planar. We study the properties of such monomials in detail for each integer $n > 1$ and any prime number p. In particular, we show that they are t-to-one, where the parameter t depends on the field $\mathbb{F}_{p^n}$ and it takes the values $1, 2$ or $p+1$. Moreover, we give a simple proof of the fact that the functions are δ-uniform with $\delta \in \{1, 4, p\}$. This result describes the differential behaviour of these monomials for any p and n. For the second class of functions, we consider an affine equivalent trinomial to $x^{p^\alpha+1}$, namely, $x^{p^\alpha+1} + \lambda x^{p^\alpha} + \lambda^{p^\alpha} x$ for $\lambda \in \mathbb{F}_{p^n}^*$. We prove that these trinomials satisfy certain regularity properties, which are useful for the specification of linear codes with three or four weights that are different than the monomial construction. These families of codes contain projective codes and optimal codes (with respect to the Griesmer bound). Remarkably, they contain infinite families of self-orthogonal and minimal p-ary linear codes for every prime number p. Our findings highlight the utility of studying affine equivalent functions, which is often overlooked in this context.

Keywords: Finite fields; p-ary functions; linear codes; minimal codes; optimal codes, self-orthogonal codes.

*The author is part of the Department of Mathematics at the University of Primorska and also part of the Andrej Marušič Institute, Koper, 6000, Slovenia. E-mail: rene7ca@gmail.com

1 Introduction

Since the late 1960s, codes with a few non-zero Hamming weights have been a subject of significant interest within the (discrete) mathematical community due to their connections with various mathematical structures, including strongly regular graphs, association schemes, designs, and projective sets [5, 6, 14, 17]. In recent decades, few-weight codes have garnered further attention driven by their practical applications, such as fault-tolerant circuits [39], secret sharing schemes [9], and authentication codes [23]. The construction of codes typically involves an interdisciplinary approach, drawing on tools and techniques from combinatorics, linear algebra, finite fields, finite geometry, and Boolean functions.

One of the earliest systematic studies of linear codes with two weights was given by Delsarte in [14]. One-weight codes, also referred as constant weight codes, are closely related to designs (see, for example, [4]), whereas two-weight (projective) codes are equivalent to certain projective sets and to certain strongly regular graphs [5, 14].

Two additional desirable properties of linear codes are self-orthogonality (characterized by the property that any two codewords are orthogonal) and minimality (linearly independent codewords do not cover each other) since self-orthogonal codes can be used to build quantum error-correcting codes [40] and minimal codes are used for two-party computations and secret sharing schemes [9].

In this article, we introduce two infinite families of p-ary linear codes, for any prime number p, using the image set of quadratic polynomials that are t-to-one functions. These codes may have 1, 2, 3, or 4 distinct non-zero weights. Our approach extends the existing literature on constructing linear codes from 2-to-one functions [32, 35, 36], thus continuing in the same line of research.

Our work is motivated by the rich properties of p-ary functions, whose behavior can often be studied exploiting finite field properties, such as exponential sums [13, 25]. We then use a well-known standard construction of linear codes from functions, called the defining set method, which has been widely employed to construct linear codes with good parameters and additional properties [17, 18, 20, 21, 24, 25, 31, 32, 34, 41]. In general, this construction relies on the selection of appropriate defining sets, yielding an intriguing ongoing research area.

Quadratic polynomials, closely related to quadratic forms, have been previously studied and utilized for constructing linear codes [9, 19, 20, 24, 25, 41, 43, 44]. We explore a specific class of Dembowski-Ostrom monomials [15, 13], namely, monomials of the form $x^{p^{k+1}+1}$, and derive its properties. Specifically, we use their image set to build an infinite family of codes with 1 or 2 weights and specify their exact weight distributions. While this construction was initially proposed in [17], the authors made an assumption on the rank of quadratic forms (Theorem 3 in [17]), which

turns out not to be true (see Remark 1 below). Hence, we provide a correct version of this result for the monomials in question. We then prove that this class of codes contains self-orthogonal, projective, minimal, and optimal codes.

Despite the common neglect of considering different affine equivalent functions in the context of p-ary functions for cryptography, we assert that considering them can be valuable. Based on this perspective, we introduce a second family of linear codes, employing the image set of a class of quadratic trinomials that are affine equivalent to $x^{p^{k+1}+1}$. To derive the exact weight distribution of codes stemming from these trinomials, one must compute the values of certain Weil sums from (interlaced) components of $x^{p^{k+1}+1}$—this is achieved by means of the Interwoven Lemma (Lemma 12). Notably, this family of codes contains codes that share some properties with their monomial counterpart including self-orthogonality, minimality and projectivity. While these two families share such properties, they are however structurally different as deduced from their weight distributions and the fact that these properties hold for different subclasses (see Remark 3).

The remainder of the article is organized as follows. In Section 2, we provide all the necessary background and preliminary concepts, including linear codes, characters, p-ary function and quadratic forms. The defining-set method and t-to-one functions are then introduced in Section 3.1, where we derive a general formula for determining weights in this setting. In Section 3.2, we present the first infinite family of linear codes from the image set of monomials $x^{p^{k+1}+1}$. Herein, we provide some (known) results on their Walsh and differential spectra. Then, we derive the exact weight distribution of the codes, thus showing they have either one or two non-zero weights. Furthermore, we prove that this family contains optimal, projective, minimal and self-orthogonal codes in Section 3.3 and Section 3.4. Afterwards, in Section 4, the second infinite family of linear codes from the image set of trinomials $x^{p^{k+1}+1} + \lambda x^{p^{k+1}} + \lambda^{p^{k+1}}$, where $\lambda \in \mathbb{F}_{p^n}^*$, is introduced. These codes have $2, 3$ or 4 non-zero weights. Similarly as for the first family, in Section 4.1, we prove that the second family contains projective, minimal and self-orthogonal codes. Finally, some numerical results are given in Section 5 and we set out our overall conclusions in Section 6.

2 Definitions

2.1 Linear codes

For a prime number p and a positive integer n, let $\mathbb{F}_{p^n}$ be the finite field with p^n elements and $\mathbb{F}_p^n$ denote an n-dimensional vector space over $\mathbb{F}_p$. The (Hamming) distance between two vectors $\mathbf{u} = (u_1, \ldots, u_n), \mathbf{v} = (v_1, \ldots, v_n) \in \mathbb{F}_p^n$ is the number

of indices where they differ. A p-ary $[n, k, d]$-code C is a k-dimensional subspace of $\mathbb{F}_p^n$ over $\mathbb{F}_p$ for which the minimum distance between two vectors is d. Vectors in C are called codewords. The dual code $C^\perp = \{\mathbf{x} \in \mathbb{F}_p^n | \mathbf{x} \cdot \mathbf{y} = 0 \text{ for all } \mathbf{y} \in C\}$ is an $[n, n-k]$-code, where " $\cdot$ " denotes the standard dot product. A code C is said to be self-orthogonal if $C \subset C^\perp$, whereas C is said to be a linear code with a complementary dual (LCD) if it intersects $C^\perp$ trivially, i.e., $C \cap C^\perp = \{0\}$. The weight $wt(\mathbf{v})$ of a vector $\mathbf{v}$ in $\mathbb{F}_p^n$ is its distance to zero, equivalently, the number of non-zero entries. The weight enumerator polynomial $W_C(z)$ of C is the polynomial $\sum_{i=0}^{n} A_i z^i$, where A_i is the number of codewords of weight i. A t-weight (or t-valued) code is a code C for which $|\{i \neq 0 | A_i \neq 0\}| = t$.

Given an $[n, k, d]$-code C, a $k \times n$ matrix G is called a generator matrix of C provided that its rows form a basis for C, i.e., $C = \{\mathbf{a}G : \mathbf{a} \in \mathbb{F}_q^k\}$. Similarly, an $(n-k) \times n$ matrix H is a parity-check matrix of C if its rows are a basis for $C^\perp$. If no two columns in H are dependent then the code C is said to be projective. Thus C is projective if and only if the minimum weight in the dual code $C^\perp$ is at least 3.

For a p-ary $[n, k, d]$-linear code C with weight enumerator $\sum_{i=1}^{n} A_i z^i$, whose dual has weight enumerator $\sum_{i=1}^{n} A_i^\perp z^i$, the first three Pless power moments [30, 38] are:

$$\sum_{i=1}^{n} A_i = p^k; \qquad \sum_{i=1}^{n} i A_i = p^{k-1}((p-1)n - A_1^\perp);$$

$$\sum_{i=1}^{n} i^2 A_i = p^{k-2}((p-1)n((p-1)n+1) - (2pn - p - 2n + 2)A_1^\perp + 2A_2^\perp).$$

2.2 Characters and p-ary functions

The absolute trace $\mathrm{Tr}_1^n(\cdot)$ on $\mathbb{F}_{p^n}$ is the linear function mapping from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$, given by

$$\mathrm{Tr}_1^n(x) = x + x^p + \cdots + x^{p^{n-1}}.$$

Let $\mathbb{i} = \sqrt{-1}$ and let $\xi_p = e^{\frac{2\pi \mathbb{i}}{p}}$ be the complex primitive p-th root of unity. The function χ_1 defined by $\chi_1(c) = \xi_p^{\mathrm{Tr}_1^n(c)}$ for all $c \in \mathbb{F}_{p^n}$ is a character of the additive group of $\mathbb{F}_{p^n}$, called the canonical additive character. Similarly, for each $j = 0, 1, \ldots, p^n - 2$, the function ψ_j with $\psi_j(\omega^k) = e^{\frac{2\pi \mathbb{i} jk}{p^n - 1}}$ for $k = 0, \ldots, q-2$, where ω is a fixed primitive element of $\mathbb{F}_{p^n}$, defines a multiplicative character of $\mathbb{F}_{p^n}^*$ and every other multiplicative character of $\mathbb{F}_{p^n}$ is obtained in this way.

A mapping $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ is called a p-ary function, where $n > 0$ and $m > 0$ are integers not necessarily equal. When $m = 1$ and $p = 2$, the function F corresponds to a Boolean function. If $m = n$, we also refer to F as a polynomial (function).

The component functions of $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ are the mappings $x \mapsto \mathrm{Tr}_1^n(aF(x))$ for $a \in \mathbb{F}_{p^n}^*$, where the superscript ' $*$ ' indicates the non-zero elements. Given

$f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ and $\lambda \in \mathbb{F}_{p^n}$, the Walsh-Hadamard transform of f at the point λ is defined as

$$W_f(\lambda) = \sum_{x \in \mathbb{F}_{p^n}} \xi_p^{f(x) - \mathrm{Tr}_1^n(\lambda x)}. \tag{1}$$

The multi-set of values $\{\{W_f(\lambda) : \lambda \in \mathbb{F}_{p^n}\}\}$ is called the Walsh spectrum of f and it will be denoted by $\mathcal{W}_f$. A p-ary function $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is said to be p-ary bent (or, simply, bent) if all its Walsh coefficients satisfy

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

In the binary case, a Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is bent if and only if $W_f(\lambda) = \pm 2^{\frac{n}{2}}$ for any $\lambda \in \mathbb{F}_{2^n}$. Note that bent Boolean functions exist only for even n. A function $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is called s-plateaued if and only if for every $\lambda \in \mathbb{F}_{p^n}$

$$|W_f(\lambda)|^2 = p^{n+s}. \tag{3}$$

When $p = 2$ and $s = 1$, f is called semi-bent (this implies that n is odd). A polynomial $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is called an almost bent or AB function if and only if the Walsh coefficients of its components belong to $\{0, \pm 2^{\frac{n+1}{2}}\}$, equivalently, if all of its components are semi-bent.

The derivative of a function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ at direction $a \in \mathbb{F}_{p^n}^*$ is defined as $D_a F(x) = F(x + a) - F(x)$. A mapping $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is called planar provided that all of its derivatives are permutations. Planar functions can exist only when p is odd. For any $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_{2^n}$, we define $\delta(a, b) = |\{x \in \mathbb{F}_{2^n} : D_a F(x) = b\}|$. The differential uniformity δ_F of $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is defined as

$$\delta_F = \max_{a \in \mathbb{F}_{2^m}^*, b \in \mathbb{F}_{2^m}} \delta(a, b). \tag{4}$$

We then say that F is δ_F-uniform. The subindex F will be dropped whenever it is clear from the context which function we refer to. A 2-uniform function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is called an almost perfect nonlinear, or, APN for short. It is well-known that every AB function is APN [8].

2.3 Quadratic forms

A function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is called a quadratic polynomial or Dembowski-Ostrom (DO) polynomial if

$$F(x) = \sum_{i,j=0}^{n-1} a_{i,j} x^{p^i + p^j}, a_{i,j} \in \mathbb{F}_{p^n}.$$

For $p > 2$ and $s \geq 1$, a homogeneous polynomial of degree two in the variables $(x_1, x_2, \ldots, x_n) \in \mathbb{F}_{p^s}^n$ of the form

$$Q(x_1, x_2, \ldots, x_n) = \sum_{1 \leq i,j, \leq s} a_{ij} x_i x_j,$$

where $a_{ij} \in \mathbb{F}_{p^s}$, is called a quadratic form over $\mathbb{F}_{p^s}$. Note that by choosing an $\mathbb{F}_p$-basis of $\mathbb{F}_{p^n}$, any quadratic function $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ induces a quadratic form over $\mathbb{F}_p$, hence we will also refer to it as a quadratic form hereinafter. The rank of the quadratic form Q over $\mathbb{F}_{p^s}$ is defined to be the codimension of the $\mathbb{F}_{p^s}$-vector space

$$V_Q = \{\mathbf{x} \in \mathbb{F}_{p^s}^n : Q(\mathbf{x} + \mathbf{z}) - Q(\mathbf{x}) - Q(\mathbf{z}) = 0, \ \forall z \in \mathbb{F}_{p^s}^n\}.$$

That is $|V_Q| = p^{n-r}$, where r denotes the rank of Q. For a quadratic form $Q(x)$ in n variables over $\mathbb{F}_{p^s}$, there exists a symmetric matrix A of order n over $\mathbb{F}_{p^s}$ such that $Q(x) = \mathbf{x}A\mathbf{x}^T$, where $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}_{p^s}^n$ and $\mathbf{x}^T$ denotes the transpose of $\mathbf{x}$. There is a nonsingular matrix M of order n such that MAM^T is diagonal, whenever A is a symmetric matrix of order n over $\mathbb{F}_{p^s}$. Setting $\mathbf{z} = \mathbf{x}M^{-1}$, we get $Q(x) = \mathbf{z}MAM^T\mathbf{z}^T = \sum_{i=1}^r d_i z_i^2$, where $\mathbf{z} = (z_1, \ldots, z_n) \in \mathbb{F}_{p^s}^n$, r is the rank of $Q(x)$ and $d_i \in \mathbb{F}_{p^s}^*$. Let $\Delta = d_1 \cdots d_r$ for $r \geqslant 1$ and $\Delta = 1$ for $r = 0$. Denoting by η the quadratic multiplicative character of $\mathbb{F}_{p^s}$ (thus $\eta = \psi_{\frac{p^s-1}{2}}$), one can prove that $\eta(\Delta)$ is an invariant of A under the conjugate action of $GL_n(\mathbb{F}_{p^s})$ (i.e., it does not depend on the choice of M).

3 Codes from t-to-one functions

3.1 The defining set-method

A generic construction of linear codes from functions works as follows [16, 42]. Fix a multi-set $D = \{\{d_1, d_2, \ldots, d_N\}\} \subset \mathbb{F}_{p^n}$, called the defining (multi-)set. Define

$$C_D = \{\mathbf{c}_a := (\mathrm{Tr}_1^n(d_1 a), \mathrm{Tr}_1^n(d_2 a), \ldots, \mathrm{Tr}_1^n(d_N a)) : a \in \mathbb{F}_{p^n}\}. \tag{5}$$

The length of C_D is N and its dimension is at most n. It can be noted that different orderings of D give equivalent linear codes C_D. The weight $wt(\mathbf{c}_a)$ of $\mathbf{c}_a$ is $N - Z_a$, where $Z_a = |\{i \in \{1, \ldots, N\} : \mathrm{Tr}_1^n(ad_i) = 0\}|$. Moreover, since

$$pZ_a = N + \sum_{y \in \mathbb{F}_p^*} \sum_{i=1}^{N} \xi_p^{\mathrm{Tr}_1^n(yad_i)}, \tag{6}$$

the weights of C_D are determined via the values $\sum_{y \in \mathbb{F}_p^*} \sum_{i=1}^{N} \xi_p^{\mathrm{Tr}_1^n(yad_i)}$.

Not surprisingly, suitable choices for D lead to linear codes with interesting specific properties. The most natural choice for D is the support $\mathrm{supp}(f)$ of a p-ary function, which has been widely used. For instance, some codes with good parameters were derived [16, 17] using supports of classes of vectorial mappings from $\mathbb{F}_p^m$ to $\mathbb{F}_p^m$. In particular, when Boolean functions are considered, so that $f : \mathbb{F}_2^m \to \mathbb{F}_2$, this method gives optimal codes when bent and semi-bent functions are employed [16]. Throughout, we will use the non-zero elements in the image set of a function F, denoted by $\mathrm{im}(F)$, as a defining set.

The preimage set of an element $\beta \in \mathbb{F}_{p^n}$ under a mapping $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is denoted by $F^{-1}\{\beta\}$. A function F is called t-to-one if there exists at most one $\beta_0 \in \mathbb{F}_{p^n}$ such that $|F^{-1}\{\beta_0\}| = 1$ and $|F^{-1}\{\beta\}| \in \{0, t\}$ for each $\beta \neq \beta_0$, i.e., every element in $\mathbb{F}_{p^n}$ has either t preimages or none, and there is at most one exception, which has exactly one preimage. Note that t-to-one functions exist only when t divides $p^n - 1$.

Theorem 1 *Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be a t-to-one function (so that t divides $p^n - 1$) without zero components. The code $C_{\mathrm{im}(F)^*}$, defined by (5), is an $[N, n, d]$-code, where $N = |\mathrm{im}(F)^*| = \frac{p^n-1}{t}$. Moreover, for $a \in \mathbb{F}_{p^n}$, the weight of the codeword $\mathbf{c}_a$ is given by*

$$wt(\mathbf{c}_a) = \frac{1}{pt}[(p-1)(p^n-1) - \sum_{\lambda \in \mathbb{F}_p^*} W_{\lambda f_a}(0) + \theta],$$

where $f_a(x) = \mathrm{Tr}_1^n(aF(x))$ and

$$\theta = \begin{cases} (p-1) & |F^{-1}\{0\}| = 1; \text{ or } \exists \beta_0 \neq 0, |F^{-1}\{\beta_0\}| = 1, \mathrm{Tr}_1^n(a\beta_0) = 0; \\ (t-1) + t(p-1) & |F^{-1}\{\beta_0\}| = 1 \text{ for some } \beta_0 \neq 0, \mathrm{Tr}_1^n(a\beta_0) \neq 0; \\ 0 & \text{otherwise.} \end{cases}$$

Proof. The result follows easily from (6) and a simple computation. ◇

3.2 Codes from $x^{p^{k+1}+1}$

In this section, we will derive the weight distributions of the codes $C_{\mathrm{im}(F)^*}$ derived from the monomial $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ given by $F(x) = x^{p^{k+1}+1}$, where $k = \lfloor \frac{n}{2} \rfloor$.

In general, it is easy to prove that the monomial $F(x) = x^s$ over $\mathbb{F}_{p^n}$ is t-to-one, where $t = \gcd(s, p^n - 1)$. Namely, $F^{-1}\{0\} = 0$ and, for every $\beta \in \mathbb{F}_{p^n}^*$, either $F^{-1}\{\beta\} = \emptyset$ or $\beta = \alpha^s$ for some $\alpha \in \mathbb{F}_{p^n}^*$. In the latter, since the (multiplicative) subgroup $\mathrm{im}(F)^*$ has order $\frac{p^n-1}{t}$, then

$$F^{-1}\{\beta\} = \{\alpha\gamma^i : 1 \leq i \leq t\},$$

for some $\gamma \in \mathbb{F}_{p^n}^*$ of order t.

The following lemma was independently proved in general for an odd prime p [13] and for the binary case [29].

Lemma 1 *[13, 29] Let $n > 1$ be an integer and p be a prime number. Let $k = \lfloor \frac{n}{2} \rfloor$ (hence $k \geq 1$). For $n \equiv 2 \pmod 4$, the greatest common divisor of n and $k+1$ is equal to two. Otherwise, it equals one. Moreover,*

$$\gcd(p^{k+1}+1, p^n-1) = \begin{cases} 1, & p = 2, n \not\equiv 0 \pmod 4; \\ 2, & p \neq 2, n \not\equiv 0 \pmod 4; \\ p+1, & n \equiv 0 \pmod 4. \end{cases}$$

In order to compute the differential uniformity of the monomials $F(x)$ in question, we must take a look at the behaviour of derivatives for different values of n and p, which is essentially the main content of the following lemma.

Lemma 2 *Let $n > 1$ be any integer and $k = \lfloor \frac{n}{2} \rfloor$. For $\alpha \in \mathbb{F}_{p^n}^*$, consider the affine polynomial $G_\alpha(x) = \alpha x^{p^{k+1}} + \alpha^{p^{k+1}} x + \alpha^{p^{k+1}+1}$ over $\mathbb{F}_{p^n}$, and set $G(x) = G_1(x)$. The set $G_\alpha^{-1}\{\beta\} = \{x \in \mathbb{F}_{p^n} : G_\alpha(x) = \beta\}$ for $\beta \in \mathbb{F}_{p^n}$ satisfies the following,*

$$|G_\alpha^{-1}\{\beta\}| = \begin{cases} 0 \text{ or } p, & \text{if } p = 2 \text{ and } n \not\equiv 2 \pmod 4 \text{ or } p > 2 \text{ and } n \equiv 0 \pmod 4; \\ 0 \text{ or } 4, & \text{if } p = 2 \text{ and } n \equiv 2 \pmod 4; \\ 1, & \text{if } p \neq 2 \text{ and } n \not\equiv 0 \pmod 4. \end{cases}$$

Proof. It is enough to prove the statement for the function $G(x) = x^{p^{k+1}} + x + 1$ since $|G_\alpha^{-1}\{\beta\}| = |G^{-1}\{\alpha^{-1}\beta - \alpha^{p^{k+1}}\}|$ (via the bijection $y \mapsto \alpha^{-1}y$). Moreover, it suffices to prove that

$$\dim_{\mathbb{F}_p}(\ker(G-1)) = \begin{cases} 1, & \text{if } p = 2 \text{ and } n \not\equiv 2 \pmod 4 \text{ or } p > 2 \text{ and } n \equiv 0 \pmod 4; \\ 2, & \text{if } p = 2 \text{ and } n \equiv 2 \pmod 4; \\ 0, & \text{if } p \neq 2 \text{ and } n \not\equiv 0 \pmod 4. \end{cases}$$

Let ω be a generator of $\mathbb{F}_{p^n}^*$. Assume that $p = 2$. A non-zero element ω^i belongs to $\ker(G-1)$ if and only if $\omega^{i(2^{k+1}-1)} = 1$. This is equivalent to finding all solutions modulo $2^n - 1$ of $i(2^{k+1}-1) = 2^n - 1$. Since this is a linear system of congruences, there must be $\gcd(2^{k+1}-1, 2^n-1)$ solutions. It can be seen that $\gcd(2^{k+1}-1, 2^n-1)$ equals $2^{\gcd(k+1,n)} - 1$, which is either $2^2 - 1 = 3$ or $2 - 1 = 1$ otherwise (by Lemma 1). Adding the solution $x = 0$, we get the result for the case $p = 2$.

Assume now that $p > 2$. A non-zero element ω^i belongs to $\ker(G-1)$ if and only if $\omega^{i(p^{k+1}-1)} = -1$. This is equivalent to finding all solutions (if any) modulo $p^n - 1$ of

$$i(p^{k+1} - 1) = \frac{p^n - 1}{2}. \tag{7}$$

In this case, there are no solution or exactly $\gcd(p^{k+1} - 1, p^n - 1) = p^{\gcd(k+1,n)} - 1$ according to whether $p^{\gcd(k+1,n)} - 1$ divides $\frac{p^n-1}{2}$ or not. There are no integer solutions for Equation (7) if and only if $\frac{n}{\gcd(k+1,n)}$ is odd [13]. By Lemma 1, this holds if and only if $n \not\equiv 0 \pmod 4$, so that zero is the only solution of $G(x) - 1$ in this case. Moreover, when $n \equiv 0 \pmod 4$, $\gcd(k+1, n) = 1$ and thus there are $p-1$ non-zero solutions. This establishes the result. ◇

The uniformity of binary power functions has been widely studied before for the so-called Gold functions [8]. For the case of fields with odd characteristics, the planar case has been addressed before (see, for instance, [12, 15]).

Theorem 2 *Let $n > 1$ be an integer and $k = \lfloor \frac{n}{2} \rfloor$. The monomial $F(x) = x^{p^{k+1}+1}$ over $\mathbb{F}_{p^n}$ satisfies the following:*

1. *If $n \equiv 0 \pmod 4$, then $F(x)$ is a $(p+1)$-to-one function. Moreover, $F(x)$ is p-uniform.*

2. *If $n \not\equiv 0 \pmod 4$ and $p = 2$, then $F(x)$ is one-to-one. Moreover, $F(x)$ is APN when n is odd, otherwise $F(x)$ is 4-uniform.*

3. *If $n \not\equiv 0 \pmod 4$ and $p \neq 2$, then $F(x)$ is two-to-one. Moreover, $F(x)$ is planar.*

Proof. From Lemma 1, we can see that $F(x)$ is t-to-one for $t = 1, 2$ or $p+1$, when n satisfies $n \not\equiv 0 \pmod 4$ and $p = 2$; $n \not\equiv 0 \pmod 4$ and $p \neq 2$; or, $n \equiv 0 \pmod 4$, respectively. The conclusion about uniformity can be obtained by Lemma 2 since the derivatives of $F(x)$ are of the form $D_\alpha F(x) = \alpha x^{p^{k+1}} + \alpha^{p^{k+1}} x + \alpha^{p^{k+1}+1}$. ◇

By Theorem 1, studying the Walsh transform of the functions $\mathrm{Tr}_1^n(aF(x))$ evaluated at zero is the first step towards computing the weights of the code $C_{\mathrm{im}(x^{p^{k+1}+1})}$.

Lemma 3 *[11, 12, 28, 29] Let p be a prime number and $n > 1$ be an arbitrary integer. Let $k = \lfloor \frac{n}{2} \rfloor$ and $\omega \in \mathbb{F}_{p^n}^*$ be a primitive element. Let $a = \omega^j \in \mathbb{F}_{p^n}^*$ for some $1 \leqslant j \leqslant p^n - 1$. The function $f(x) = \mathrm{Tr}_1^n(aF(x)) = \mathrm{Tr}_1^n(ax^{p^{k+1}+1})$ satisfies the following:*

1. *If $n \not\equiv 0 \pmod 4$ and $p = 2$, then $f(x)$ is balanced.*

2. If $n \not\equiv 0 \pmod 4$ *and* $p \neq 2$, *then*

$$W_f(0) = \begin{cases} \eta(a)(-1)^{n-1} p^{\frac{n}{2}}, & \text{if } p \equiv 1 (\text{mod } 4); \\ \eta(a)(-1)^{n-1} \mathbb{i}^n p^{\frac{n}{2}}, & \text{if } p \equiv 3 (\text{mod } 4). \end{cases}$$

3. If $n \equiv 0 \pmod 4$, *then*

$$W_f(0) = \begin{cases} -p^{\frac{n+2}{2}}, & \text{if } (p+1) | j; \\ p^{n/2}, & \text{otherwise.} \end{cases}$$

The Walsh spectra of the binary monomials $x^{2^\alpha+1}$ is known and it has been widely studied as particular cases of plateaued functions or quadratic forms (see [8, 29] and the references thereafter). To obtain the full Walsh spectrum of the considered function $F(x) = x^{p^\alpha+1}$, in general, we will study the behaviour of its components through the following lemmas.

Lemma 4 *[12] Let* p *be an odd prime,* $n > 1$, $\alpha \in \mathbb{N}$ *and* $d = \gcd(\alpha, n)$. *The kernel of the* $\mathbb{F}_p$*-linearized function* $F^*(x) = a^{p^\alpha} x^{p^{2\alpha}} + ax$ *for* $a \in \mathbb{F}_{p^n}^*$ *satisfies*

$$\dim(\ker(F^*)) = \begin{cases} 2d & \text{if } \frac{n}{d} \text{ is even, } n = 2k, \text{ and } a^{\frac{p^n-1}{p^d+1}} = (-1)^{\frac{k}{d}}; \\ 0 & \text{otherwise.} \end{cases}$$

Lemma 5 *[12, 29] Let* p *be a prime and* $n > 1$. *Let* $F : \mathbb{F}_{p^n} \to \mathbb{F}_p$ *be* $F(x) = x^{p^\alpha+1}$ *and* $f(x) = \mathrm{Tr}_1^n(aF(x))$ *for* $a \in \mathbb{F}_{p^n}^*$. *Let* $F^*(x) = a^{p^\alpha} x^{p^{2\alpha}} + ax$. *Suppose that* $W_{-f}(0) \neq 0$. *Then, for* $b \in \mathbb{F}_{p^n}$,

$$W_f(b) = \begin{cases} \overline{\xi_p^{f(x_0)} W_{-f}(0)}, & \text{if } F^*(x_0) = b^{p^\alpha}; \\ 0, & \text{otherwise,} \end{cases}$$

where the symbol $\bar{c}$ *means the complex conjugate of* $c \in \mathbb{C}$.

The following result exhibits the general description of the components of the quadratic monomial $x^{p^{k+1}+1}$. Note that Corollary 1 has been proved separately elsewhere, however, to the best of our knowledge, this is the first time that a complete unified treatment is given.

Corollary 1 *[12, 29] Let* $n > 1$ *be any integer and* $k = \lfloor \frac{n}{2} \rfloor$ *and* ω *be a primitive element in* $\mathbb{F}_{p^n}$. *The (quadratic) monomial* $F(x) = x^{p^{k+1}+1}$ *over* $\mathbb{F}_{p^n}$ *satisfies the following:*

1. *If* $n \equiv 0 \pmod 4$*, then* $\mathrm{Tr}_1^n(aF(x))$ *for* $a = \omega^j$ *is bent when* $p+1 \not| \ j$ *and it is* 2*-plateaued when* $p+1 \mid j$*.*

2. *If* $n \not\equiv 0 \pmod 4$ *and* $p = 2$*, then, for odd* n*,* F *is a plateaued function with* $W_F(b) \in \{0, \pm 2^{\frac{n+1}{2}}\}$ *for all* $b \in \mathbb{F}_{2^n}$ *(AB permutation) and, for even* n*,* $W_F(b) \in \{0, \pm 2^{\frac{n+2}{2}}\}$ *for all* $b \in \mathbb{F}_{2^n}$*.*

3. *If* $n \not\equiv 0 \pmod 4$ *and* $p \neq 2$*,* F *is planar, thus* $W_F(b) \in \{\iota p^{n/2}\}$ *for every* $b \in \mathbb{F}_{p^n}$*, where* $\iota \in \mathbb{C}$ *and* $|\iota| = 1$*.*

Proof. For $p = 2$, quadratic functions are plateaued, so when n is odd, the fact that F is APN implies that it is AB. The case when n is even and F is APN follows by [26], when F is 4-uniform by [37]. For $p > 2$ and n not divisible by 4, F is planar thus its components are bent. We then just need to prove 1) for $p > 2$. Let n be such that $n \equiv 0 \pmod 4$ and $p > 2$. Consider the function $F^*(x) = \mathrm{Tr}_1^n(a^{p^{k+1}} x^{p^{2(k+1)}} + ax)$. Since $d = \gcd(n, k+1) = 1$ and $n/d = n$ is even, the function $F^*(x)$ is either p^2-to-one or one-to-one by Lemma 4. Moreover, the former happens exactly when $a^{\frac{p^n-1}{p+1}} = 1$, or, equivalently, writing $a = \omega^j$, when $p+1$ divides j. This yields $p+1$ dividing $\frac{p^n-1}{2} + j$ (recall that $n \equiv 0 \pmod 4$) so that, in this case, $W_{-f}(0) = -p^{\frac{n+2}{2}}$. Hence $W_f(b)$ is zero or $-\overline{\xi_p^{f(x_0)}} p^{\frac{n+2}{2}}$ for some x_0 with $F^*(x_0) = b^{p^{k+1}}$ by Lemma 5. Another use of Lemma 4 shows that, when $p+1$ does not divides j, F^* is one-to-one. By Lemma 5, $W_f(b) = \overline{\xi_p^{f(x_0)}} p^{\frac{n}{2}}$ for the unique x_0 with $F^*(x_0) = b^{p^{k+1}}$. ◇

From a different perspective, the values of the Weil sums related to the Walsh transform of a quadratic form, evaluated at zero, can be computed by knowing the rank of the given quadratic form, as expressed in the following lemma.

Lemma 6 *[33, 34] Let* p *be an odd prime and* $n > 1$*. Let* $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ *be a quadratic form of rank* r *over* $\mathbb{F}_p$*. Then,*

$$W_f(0) = \begin{cases} \pm p^{n-\frac{r}{2}}, & \text{if } p \equiv 1 \pmod 4; \\ \pm \mathbb{i}^r p^{n-\frac{r}{2}}, & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Combining Lemma 3 with Lemma 6 yields the following.

Corollary 2 *For odd* p *and* $a \in \mathbb{F}_{p^n}^*$*, the rank of the quadratic form* $f(x) = \mathrm{Tr}_1^n(aF(x)) = \mathrm{Tr}_1^n(ax^{p^{k+1}+1})$ *is either* n *or* $n-2$*.*

Using Lemma 6 and the fact that $\lambda f(x)$ is a quadratic form for a given quadratic form $f(x)$ and $\lambda \in \mathbb{F}_p^*$, one can prove the following result.

Lemma 7 *[22] Let $n > 1$ and let f be a quadratic form of rank r over $\mathbb{F}_p$ and determinant Δ. If r is even, then*

$$\sum_{\lambda \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_{p^n}} \xi_p^{\lambda f(x)} = \eta(\Delta)(p-1)p^{n-\frac{r}{2}}.$$

If r is odd, then

$$\sum_{\lambda \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_{p^n}} \xi_p^{\lambda f(x)} = 0.$$

Now we are ready to provide a class of one-weight and two-weight codes using $\mathrm{im}(F)^*$ for $F(x) = x^{p^{k+1}+1}$. Note that this is a (complete) corrected version of Theorem 3 in [17] (see Remark 1 below).

Theorem 3 *Let $n > 1$ be an integer, $k = \lfloor \frac{n}{2} \rfloor$ and p be a prime number. The following holds for the code $C_{\mathrm{im}(F)^*}$ defined in (5), where $F(x) = x^{p^{k+1}+1}$.*

- *If $n \equiv 0 \pmod 4$, then $C_{\mathrm{im}(F)^*}$ is a two-weight code with parameters*

$$[\frac{p^n-1}{p+1}, n, \frac{(p-1)(p^{n-1}-p^{\frac{n}{2}-1})}{(p+1)}]$$

  and weight enumerator $1 + \frac{p(p^n-1)}{p+1} z^{\frac{(p-1)(p^{n-1}-p^{\frac{n}{2}-1})}{(p+1)}} + \frac{(p^n-1)}{p+1} z^{\frac{(p-1)(p^{n-1}+p^{\frac{n}{2}})}{(p+1)}}$.

- *If $n \equiv 2 \pmod 4$ and $p \neq 2$, then $C_{\mathrm{im}(F)^*}$ is a two-weight code with parameters*

$$[\frac{p^n-1}{2}, n, \frac{(p-1)}{2}(p^{n-1}-p^{\frac{n}{2}-1})]$$

  and

$$1 + \frac{p^n-1}{2} z^{\frac{(p-1)}{2}(p^{n-1}-p^{\frac{n}{2}-1})} + \frac{p^n-1}{2} z^{\frac{(p-1)}{2}(p^{n-1}+p^{\frac{n}{2}-1})}.$$

- *If $n \not\equiv 0 \pmod 4$ and $p = 2$, then $C_{\mathrm{im}(F)^*}$ is a one-weight code with parameters $[2^n-1, n, 2^{n-1}]$, i.e., the simplex code.*

- *If n odd and $p \neq 2$, then $C_{\mathrm{im}(F)^*}$ is a one-weight code with parameters*

$$[\frac{p^n-1}{2}, n, \frac{(p-1)}{2}p^{n-1}].$$

Proof. The monomial $F(x)$ is t-to-one, where $t = \gcd(p^{k+1}+1, p^n-1)$. By Lemma 1, we get that $t = 1; t = 2$; or $p+1$, when $n \not\equiv 0 \pmod 4$ and $p = 2$; $n \not\equiv 0 \pmod 4$ and $p > 2$; or $n \equiv 0 \pmod 4$, respectively. Therefore, $C_{\mathrm{im}(F)^*}$ is a $[\frac{p^n-1}{t}, n]$- code, where $t \in \{1, 2, p+1\}$. First, let us analize the case $n \not\equiv 0 \pmod 4$. By Lemma 3, Lemma 7 and Theorem 1, we get that the weight of a codeword $\mathbf{c}_a$ satisfies

$$wt(\mathbf{c}_a) = \begin{cases} 2^{n-1} & \text{if } n \not\equiv 0 \pmod 4 \text{ and } p = 2; \\ \frac{(p-1)}{2} p^{n-1} & \text{if } n \text{ odd and } p > 2; \\ \frac{(p-1)}{2}(p^{n-1} \pm p^{\frac{n}{2}-1}) & \text{if } n \equiv 2 \pmod 4 \text{ and } p > 2. \end{cases}$$

The weight distribution of the code for $n \equiv 2 \pmod 4$ and $p > 2$ now follows from the first two Pless power moments, which give the frequency $\frac{p^n-1}{2}$ for both weights. Assume that $n \equiv 0 \pmod 4$. In this case $t = p+1$. According to Lemmas 3 and 7, for $a \in \mathbb{F}_{p^n}^*$, the function $f_a(x) = \mathrm{Tr}_1^n(aF(x))$ satisfies

$$\sum_{\lambda \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_{p^n}} \xi_p^{\lambda f_a(x)} = -(p-1)p^{\frac{n+2}{2}}$$

or

$$\sum_{\lambda \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_{p^n}} \xi_p^{\lambda f_a(x)} = (p-1)p^{\frac{n}{2}},$$

depending on wether $p+1$ divides j or not. Therefore,

$$wt(\mathbf{c}_a) = \begin{cases} \frac{(p-1)(p^{n-1}-p^{\frac{n}{2}-1})}{(p+1)}, & \text{if } (p+1)|j; \\ \frac{(p-1)(p^{n-1}+p^{\frac{n+2}{2}-1})}{(p+1)} & \text{otherwise.} \end{cases}$$

Finally, the first two Pless power moments give the frequencies $\frac{p(p^n-1)}{p+1}$ and $\frac{p^n-1}{p+1}$, respectively. ◇

Remark 1 *As shown in Corollary 2, the rank of the quadratic form $aF(x) = ax^{p^{k+1}+1}$ could be n or $n-2$ depending on $a \in \mathbb{F}_{p^n}^*$ when $n \equiv 0 \pmod 4$. This yields the corresponding weight distribution given in Theorem 3, which is not symmetric unlike the other cases, i.e., $n \not\equiv 0 \pmod 4$. The authors of [17] were the first to obtain the linear code $C_{\mathrm{im}(F)^*}$ when considering quadratic monomials (see Theorem 3 and Example 1 in [17]), however, their result is inaccurate since $F(x)$ satisfies the assumptions of Theorem 3 in [17] but the conclusion is not correctly derived for the even case. The flaw in their proof lies in the mistaken assumption that $aF(x)$ has the same rank for every $a \in \mathbb{F}_{p^n}^*$. A similar observation is true for the complete weight enumerator derived in Theorem 4.2 (rank even) in [31].*

3.3 Main properties of $C_{\mathrm{im}(x^{p^{k+1}+1})^*}$

In this section, we derive some properties of the codes $C_{\mathrm{im}(x^{p^{k+1}+1})^*}$. Note that none of these properties were considered in [17]. In Table 6, we provide a computational verification of these properties for small values of p and n.

The well-known Griesmer bound [27] states that for a p-ary code C with parameters $[n, k, d]$, where $k \geq 1$, it holds that $\sum_{i=0}^{k-1} \left\lceil \frac{d}{p^i} \right\rceil \leq n$. Some of the codes stemming from $x^{p^{k+1}+1}$ are in fact optimal, as shown by the following proposition.

Proposition 1 *Let p be a prime number, $n > 1$ be any integer and $k = \lfloor \frac{n}{2} \rfloor$. Let $C_{\mathrm{im}(F)^*}$ be the code from Theorem 3, where $F(x) = x^{p^{k+1}+1}$. Then, $C_{\mathrm{im}(F)^*}$ is optimal with respect to the Griesmer bound when $p = 2$ and $n \not\equiv 0 \pmod 4$ or $n = 4, 8$; $p = 3, n = 4$; or $p > 2$ and n odd.*

Proof. Suppose that $p > 2$ and n be odd. A p-ary code C with dimension n and minimum distance $d := \frac{(p-1)p^{n-1}}{2} + 1$ has length N at least

$$\sum_{i=0}^{n-1} \left\lceil \frac{d}{p^i} \right\rceil = \sum_{i=0}^{n-1} \left\lceil \frac{(p-1)p^{n-1-i}}{2} + \frac{1}{p^i} \right\rceil = \frac{(p-1)}{2} \left(\frac{p^n - 1}{p-1} \right) + n = \frac{p^n - 1}{2} + n,$$

by the Griesmer bound. Therefore, the code $C_{\mathrm{im}(F)^*}$ is optimal since its length equals $\frac{p^n-1}{2}$. For $n \not\equiv 0 \pmod 4$ and $p = 2$, $C_{\mathrm{im}(F)^*}$ is the simplex code, hence optimal. Finally, using tables for the best known linear codes, one can verify that the codes are optimal for $p = 2, n = 8$ (parameters [85,8,40]); $p = 2, n = 4$ (parameters [5,4,2]); $p = 3, n = 4$ (parameters [20,4,12]). Note also that for $p = 5, n = 4$, the code has parameters $[104, 3, 80]$, whose distance differs in at most two from the best code's minimum distance, which is known to be either 81 or 82. ◇

Using the first three Pless moments together with the derived weight distributions of the codes $C_{\mathrm{im}(F)^*}$, we can obtain the values of the dual enumerators $A_1^\perp$ and $A_2^\perp$ for the weights 1 and 2 in the dual code $C_{\mathrm{im}(F)^*}^\perp$. This yields that the codes are projective only when $p = 2$ or n is odd. We state this observation as the following proposition while omitting the routinary computation.

Proposition 2 *Let p be a prime number, $n > 1$ be any integer and $k = \lfloor \frac{n}{2} \rfloor$. Let $C_{\mathrm{im}(F)^*}$ be the code from Theorem 3, where $F(x) = x^{p^{k+1}+1}$. Then, $C_{\mathrm{im}(F)^*}$ is projective if and only if $p = 2$ or n is odd.*

A code C is called minimal if the supports of every two linearly independent codewords do not include each other. A simple sufficient condition was provided by

Ashikhmin and Barg [1] and it states that a p-ary code C is minimal if $\frac{w_{\min}}{w_{\max}} > \frac{p-1}{p}$, where $w_{\min}$ and $w_{\max}$ are the minimum and the maximum weight of C, respectively. Using this condition, we can prove that our codes are almost always minimal.

Proposition 3 *Let p be a prime number, $n > 1$ be any integer and $k = \lfloor \frac{n}{2} \rfloor$. Let $C_{\mathrm{im}(F)^*}$ be the code from Theorem 3, where $F(x) = x^{p^{k+1}+1}$. Then, $C_{\mathrm{im}(F)^*}$ is minimal except for $n = 4$ or $p > 2, n = 2$.*

Proof. The only non-trivial cases are when $n \equiv 0 \pmod 4$ or when $p > 2$, $n \equiv 2 \pmod 4$. Suppose that $n \equiv 0 \pmod 4$. The minimum weight $w_{\min}$ is $\frac{(p-1)(p^{n-1}-p^{n/2-1})}{p+1}$ and the maximum weight $w_{\max}$ equals $\frac{(p-1)(p^{n-1}+p^{n/2})}{p+1}$. The inequality $\frac{w_{\min}}{w_{\max}} > \frac{p-1}{p}$ holds if and only if $p^n - p^{n/2} > p^n + p^{n/2+1} - p^{n-1} - p^{n/2}$. This happens if and only if $p^{n/2-2} > 1$, which is true if and only if $n > 4$. Suppose now that $p > 2$ and $n \equiv 2 \pmod 4$. In this case, the minimum weight $w_{\min}$ is $\frac{(p-1)(p^{n-1}-p^{n/2-1})}{2}$, whereas the maximum weights $w_{\max}$ is equal to $\frac{(p-1)(p^{n-1}+p^{n/2-1})}{2}$. We have $\frac{w_{\min}}{w_{\max}} > \frac{p-1}{p}$ if and only if $p^n - p^{n/2} > p^n + p^{n/2} - p^{n-1} - p^{n/2-1}$. This happens if and only if $p^{n/2} > 2p - 1$, which is true if and only if $n > 2$. ◇

3.4 Self-orthogonality of $C_{\mathrm{im}(F)^*}$

It turns out that the codes $C_{\mathrm{im}(F)^*}$ associated with the monomial $F(x) = x^{p^{k+1}+1}$ are (almost always) self-orthogonal. To prove this, we will need some results regarding quadratic residues and exponential sums.

For a prime number $p > 2$, define the sets QR_p and QNR_p to be the set of quadratic residues mod p and the set of quadratic non-residues mod p. Let $\nu \in \mathbb{C}$ be defined as

$$\nu = \begin{cases} 1, & p \equiv 1 \pmod 4; \\ \mathbb{i}, & p \equiv 3 \pmod 4. \end{cases} \tag{8}$$

Lemma 8 *Let QR_p, QNR_p and ν as above. The following hold:*

1) $\sum_{i=1}^{p-1} \xi_p^i = -1$;

2) $\sum_{i \in QR_p^*} \xi_p^i = \frac{-1+\nu\sqrt{p}}{2}$;

3) $\sum_{i \in QNR_p} \xi_p^i = \frac{-1-\nu\sqrt{p}}{2}$;

Proof. Item 1) follows from the fact that $1 + x + x^2 + \cdots + x^{p-1}$ is the minimal polynomial of ξ_p over $\mathbb{Q}$. For 2) and 3), combine 1) with the well-known result that $\sum_{i \in QR_p^*} \xi_p^i - \sum_{i \in QNR_p} \xi_p^i = \nu\sqrt{p}$ (see, for instance [33]). ◇

Lemma 9 *Let SQ denote the set of squares in $\mathbb{F}_{p^n}$ and NSQ be the set of non-squares. Let ν be defined as above. The following hold:*

1) $\sum_{x\in SQ^*} \xi_p^{\mathrm{Tr}_1^n(x)} + \sum_{x\in NSQ} \xi_p^{\mathrm{Tr}_1^n(x)} = -1$;

2) $\sum_{x\in SQ^*} \xi_p^{\mathrm{Tr}_1^n(x)} - \sum_{x\in NSQ} \xi_p^{\mathrm{Tr}_1^n(x)} = (-1)^{n-1}\nu^n p^{n/2}$.

Moreover, the values of the individual sums are determined as $2\sum_{x\in SQ^*} \xi_p^{\mathrm{Tr}_1^n(x)} = -1 + (-1)^{n-1}\nu^n p^{n/2}$ *and* $2\sum_{x\in NSQ} \xi_p^{\mathrm{Tr}_1^n(x)} = -1 - (-1)^{n-1}\nu^n p^{n/2}$.

Proof. Since SQ and NSQ form a partition of $\mathbb{F}_{p^n}$, the sum of characters

$$\sum_{x\in\mathbb{F}_{p^n}} \xi_p^{\mathrm{Tr}_1^n(x)} = \sum_{x\in SQ} \xi_p^{\mathrm{Tr}_1^n(x)} + \sum_{x\in NSQ} \xi_p^{\mathrm{Tr}_1^n(x)} = 1 + \sum_{x\in SQ^*} \xi_p^{\mathrm{Tr}_1^n(x)} + \sum_{x\in NSQ} \xi_p^{\mathrm{Tr}_1^n(x)}$$

must be 0. For 2), note that the sum in the statement equals the Gaussian sum $\sum_{x\in\mathbb{F}_{p^n}^*} \eta(x)\chi_1(x)$, hence it is equal to $(-1)^{n-1}\nu^n p^{n/2}$. The rest of the theorem is now established by combining 1) and 2). ◇

For a prime number $p > 2$, define the sets $\Gamma_i, \widetilde{\Gamma}_i$, for $i \in QR_p$ as

$$\Gamma_i = \{x \in SQ^* : \mathrm{Tr}_1^n(x) = i\},\ \widetilde{\Gamma}_i = \{x \in NSQ : \mathrm{Tr}_1^n(x) = i\},$$

and, for $i \in QNR_p$, define the sets $\Delta_i, \widetilde{\Delta}_i$ as

$$\Delta_i = \{x \in SQ : \mathrm{Tr}_1^n(x) = i\},\ \widetilde{\Delta}_i = \{x \in NSQ : \mathrm{Tr}_1^n(x) = i\}.$$

Let $\kappa_i = |\Gamma_i|$, $\widetilde{\kappa}_i = |\widetilde{\Gamma}_i|$, $\mu_i = |\Delta_i|$ and $\widetilde{\mu}_i = |\widetilde{\Delta}_i|$. It is easy to see that $\kappa_i + \widetilde{\kappa}_i = \mu_i + \widetilde{\mu}_i = p^{n-1}$ for each $i \neq 0$; $\kappa_0 + \widetilde{\kappa}_0 = p^{n-1} - 1$ and $\kappa_i, \widetilde{\kappa}_i, \mu_i, \widetilde{\mu}_i$ are all non-zero. Moreover,

$$\kappa_0 + \sum_{i\in QR_p} \kappa_i + \sum_{i\in QNR_p} \mu_i = \widetilde{\kappa}_0 + \sum_{i\in QR_p} \widetilde{\kappa}_i + \sum_{i\in QNR_p} \widetilde{\mu}_i = \frac{p^n - 1}{2}$$

since Γ_i, Δ_i (resp. $\widetilde{\Gamma}_i, \widetilde{\Delta}_i$) form a partition of SQ^* (resp. NSQ).

Lemma 10 *Let $p > 2$ be any prime number and $n > 1$ be an arbitrary integer.*

1. *If n is odd, then $\kappa_i = \frac{\nu^{n-1}p^{\frac{n-1}{2}}+1}{2} + \kappa_0$ and $\widetilde{\kappa}_i = \frac{1-\nu^{n-1}p^{\frac{n-1}{2}}}{2} + \widetilde{\kappa}_0$ for $i \in QR_p^*$ and $\mu_i = \frac{1-\nu^{n-1}p^{\frac{n-1}{2}}}{2} + \kappa_0$ and $\widetilde{\mu}_i = \frac{\nu^{n-1}p^{\frac{n-1}{2}}+1}{2} + \widetilde{\kappa}_0$ for $i \in QNR_p$.*

2. *If n is even, then $\kappa_i = \mu_i = \frac{\nu^n p^{\frac{n}{2}}+1}{2} + \kappa_0$ and $\widetilde{\kappa}_i = \widetilde{\mu}_i = \frac{1-\nu^n p^{\frac{n}{2}}}{2} + \widetilde{\kappa}_0$ for every $1 \leq i \leq p-1$.*

Proof. Consider the sums $2\sum_{x\in SQ^*} \xi_p^{\mathrm{Tr}_1^n(x)}$ and $2\sum_{x\in NSQ} \xi_p^{\mathrm{Tr}_1^n(x)}$, which equal $-1+(-1)^{n-1}\nu^n p^{n/2}$ and $-1-(-1)^{n-1}\nu^n p^{n/2}$, respectively, by Lemma 9. These sums can be rewritten as

$$2\sum_{x\in SQ^*} \xi_p^{\mathrm{Tr}_1^n(x)} = \sum_{i\in QR_p} 2\kappa_i \xi_p^i + \sum_{i\in QNR_p} 2\mu_i \xi_p^i = \sum_{i\in QR_p^*} 2(\kappa_i-\kappa_0)\xi_p^i + \sum_{i\in QNR_p} 2(\mu_i-\kappa_0)\xi_p^i$$

and

$$2\sum_{x\in NSQ} \xi_p^{\mathrm{Tr}_1^n(x)} = \sum_{i\in QR_p} 2\widetilde{\kappa}_i \xi_p^i + \sum_{i\in QNR_p} 2\widetilde{\mu}_i \xi_p^i = \sum_{i\in QR_p^*} 2(\widetilde{\kappa}_i-\widetilde{\kappa}_0)\xi_p^i + \sum_{i\in QNR_p} 2(\widetilde{\mu}_i-\widetilde{\kappa}_0)\xi_p^i.$$

Since the elements $\xi_p, \xi_p^2, \ldots, \xi_p^{p-1}$ form an integral basis for the cyclotomic field $\mathbb{Q}(\xi_p)$ (extension of the field $\mathbb{Q}$ by adjoining the root ξ_p), the coefficients $\mu_i, \widetilde{\mu}_i, \kappa_i, \widetilde{\kappa}_i$ are uniquely determined by κ_0, $\widetilde{\kappa}_0$. One can then easily verify that the values given in the statement indeed form a solution for these equations. ◇

Proposition 4 *Let p be a prime number, $n > 1$ be any integer and $k = \lfloor \frac{n}{2} \rfloor$. Let $C_{\mathrm{im}(F)^*}$ be the code from Theorem 3, where $F(x) = x^{p^{k+1}+1}$. Then, $C_{\mathrm{im}(F)^*}$ is self-orthogonal except for $p = 2, n = 2$ or $p = 3, n = 2$.*

Proof. It can be proved that a sufficient condition for a binary code to be self-orthogonal is that its weights are divisible by 4 (see, for instance, [30]). Hence, the binary case follows from the weight distributions obtained in Theorem 3. Suppose that $p > 2$ and set $D = \mathrm{im}(F)^*$. To prove that the code is self-orthogonal, we must show that for any $x \in \mathbb{F}_{p^n}^*$, the sum $\sum_{y\in D} \mathrm{Tr}_1^n(xy)^2$ (over the integers) is divisible by p. We split the proof into two cases according to the values of n.
Case $n \not\equiv 0 \pmod 4$**:** First note that, in this case, the set D is exactly the set SQ^* of squares in $\mathbb{F}_{p^n}^*$[1], indeed, if $\beta \in D$, then $\beta = \alpha^{p^{k+1}+1} = (\alpha^{p^{k+1}-1})^2$ for some $\alpha \in \mathbb{F}_{p^n}^*$, hence $\beta \in SQ^*$. Since $|D| = \frac{p^n-1}{2}$, it must be $D = SQ^*$. Since $xSQ^* = SQ^*$ or $xSQ^* = NSQ$ (depending on whether $x \in SQ^*$ or not), it suffices to prove that $p|\sum_{y\in SQ^*} \mathrm{Tr}_1^n(y)^2$ and $p|\sum_{y\in NSQ} \mathrm{Tr}_1^n(y)^2$. Using the definitions of κ_i, μ_i, we can write

$$\sum_{y\in SQ^*} \mathrm{Tr}_1^n(y)^2 = \sum_{i\in QNR_p} (\kappa_{i^2} + \mu_i) i^2.$$

[1] In fact, $\mathrm{im}(F)^*$ forms a difference set when n is odd and it forms an almost difference set when n is even [17].

Similarly, $\sum_{y\in NSQ} \mathrm{Tr}_1^n(y)^2 = \sum_{i\in QNR_p}(\widetilde{\kappa}_{i^2}+\widetilde{\mu}_i)i^2$. By the weight distribution of C_D derived in Theorem 3, we can infer that $2\kappa_0 = p^{n-1}-1$ (thus $\widetilde{\kappa}_0 = \kappa_0$) for odd n whereas, for $n \equiv 2 \pmod 4$, $2\kappa_0$ is equal to either $p^{n-1}+p^{n/2}-p^{n/2-1}-1$ or $p^{n-1}-p^{n/2}+p^{n/2-1}-1$ and $\widetilde{\kappa}_0 = p^{n-1}-1-\kappa_0$. Combining these values with Lemma 10 yields that $p|(\kappa_{i^2}+\mu_i)$ and $p|(\widetilde{\kappa}_{i^2}+\widetilde{\mu}_i)$ for each $i \in QNR_p$ (except when $p=3$, $n=2$). This establishes the result in this case.

Case $n \equiv 0 \pmod 4$**:** Define $\kappa_i^D = |\{y \in D : \mathrm{Tr}_1^n(y) = i\}|$. The sum $(p+1)\sum_{i=0}^{p-1}\kappa_i^D\xi_p^i = (p+1)\sum_{y\in D}\xi_p^{\mathrm{Tr}_1^n(y)}$ equals $W_f(0)-1$, where $f(x) = \mathrm{Tr}_1^n(x^{p^{k+1}+1})$. Hence,

$$\sum_{i=0}^{p-1}\kappa_i^D\xi_p^i = \sum_{i=1}^{p-1}(\kappa_i^D-\kappa_0^D)\xi_p^i = \frac{-p^{n/2+1}-1}{p+1}, \tag{9}$$

by Lemma 3. Since $\xi_p,\ldots,\xi_p^{p-1}$ form an integral basis of $\mathbb{Q}(\xi_p)$, the coefficients in (9) are unique. The value of κ_0^D is known by the weight distribution given in Theorem 3, namely, $\kappa_0^D = \frac{p^{n-1}-p^{n/2+1}+p^{n/2}-1}{p+1}$. The solution of (9) is then given by $\kappa_i^D = \frac{p^{n/2+1}+1}{p+1}+\kappa_0^D = \frac{p^{n-1}+p^{n/2}}{p+1}$ for each $1 \le i \le p-1$. From here, we conclude that $\sum_{y\in D}\mathrm{Tr}_1^n(y) = \sum_{i=1}^{p-1}\kappa_i^D i$ is divisible by p since $p|\kappa_i^D$ for $1 \le i \le p-1$. This also implies that $\sum_{y\in D}\mathrm{Tr}_1^n(y)^2$ equals 0 modulo p. A similar argument yields the result for $\sum_{y\in D}\mathrm{Tr}_1^n(xy)^2$ for any $x \notin D$. ◇

Open Problem 1. For $n \not\equiv 0 \pmod 4$ and $p > 2$, the proof of Proposition 4 relies heavily on the fact that the image of the planar function $x^{p^{k+1}+1}$ is the full set of squares. Can we get similar results for arbitrary planar functions? Namely, what are the properties of $C_{\mathrm{im}(F)^*}$ when F is planar?

4 A family of codes from t-to-one trinomials

In this section, 3-weight and 4-weight linear codes from a special class of trinomials will be presented. These constructions are brought about by a simple (affine) modification to the monomials studied in the previous section.

Adding a linearized polynomial to a polynomial gives affine equivalent functions. Thus the following two results are mostly established by using Theorem 2, Corollary 1 and the fact that $\lambda x^{p^{k+1}}+\lambda^{p^{k+1}}x$ is a linearized polynomial for each $\lambda \in \mathbb{F}_{p^n}$.

Proposition 5 *Let p be a prime number, $n > 1$ be an integer and $k = \lfloor \frac{n}{2} \rfloor$. The polynomial $F(x) = x^{p^{k+1}+1}+\lambda x^{p^{k+1}}+\lambda^{p^{k+1}}x$ over $\mathbb{F}_{p^n}$, where $\lambda \in \mathbb{F}_{p^n}^*$, satisfies the following:*

1. *If $n \equiv 0 \pmod 4$, then $F(x)$ is a $(p+1)$-to-one p-uniform function.*

2. *If* $n \not\equiv 0 \pmod 4$ *and* $p = 2$*, then* $F(x)$ *is one-to-one. Moreover,* $F(x)$ *is AB when* n *is odd, otherwise* $F(x)$ *is* 4*-uniform.*

3. *If* $n \not\equiv 0 \pmod 4$ *and* $p \neq 2$*, then* $F(x)$ *is two-to-one. Moreover,* $F(x)$ *is planar.*

Proof. The element $\alpha \in \mathbb{F}_{p^n}$ is a solution of $x^{p^{k+1}+1} + \lambda x^{p^{k+1}} + \lambda^{p^{k+1}} x = \beta$ if and only $\alpha + \lambda$ is a solution of $x^{p^{k+1}+1} = \beta + \lambda^{p^{k+1}+1}$. The rest follows at once from Theorem 2. ◇

Proposition 6 *Let* p *be a prime number,* $n > 1$ *be any integer and* $k = \lfloor \frac{n}{2} \rfloor$*. Let* ω *be a primitive element in* $\mathbb{F}_{p^n}$*. The polynomial* $F(x) = x^{p^{k+1}+1} + \lambda x^{p^{k+1}} + \lambda^{p^{k+1}} x$ *over* $\mathbb{F}_{p^n}$*, where* $\lambda \in \mathbb{F}_{p^n}$*, satisfies the following:*

1. *If* $n \equiv 0 \pmod 4$*, then* $\mathrm{Tr}_1^n(aF(x))$ *for* $a = \omega^j \in \mathbb{F}_{p^n}^*$ *is bent when* $p + 1 \not| \ j$*, and it is* 2*-plateaued when* $p + 1 \mid j$*.*

2. *If* $n \not\equiv 0 \pmod 4$ *and* $p = 2$*, then* F *is a plateaued function such that, for each* $b \in \mathbb{F}_{p^n}^*$*,* $W_F(b) \in \{0, \pm 2^{\frac{n+1}{2}}\}$ *for odd* n *and* $W_F(b) \in \{0, \pm 2^{\frac{n+2}{2}}\}$ *for even* n*.*

3. *If* $n \not\equiv 0 \pmod 4$ *and* $p \neq 2$*,* $W_F(b) \in \{\iota p^{n/2}\}$ *for each* $b \in \mathbb{F}_{p^n}$*, where* $\iota \in \mathbb{C}$ *and* $|\iota| = 1$*.*

Proof. It is an immediate consequence of Corollary 1. ◇

Lemma 11 *Let* p *be prime and* $n > 1$ *be an integer. Let* ω *be a primitive element in* $\mathbb{F}_{p^n}$*. Let* $k = \lfloor \frac{n}{2} \rfloor$ *and* $a = \omega^j \in \mathbb{F}_{p^n}^*$*. Define* $b_a \in \mathbb{F}_{p^n}$ *to be such that* $\mathrm{Tr}_1^n(b_a x) = \mathrm{Tr}_1^n(a(\lambda x^{p^{k+1}} + \lambda^{p^{k+1}} x))$*, where* $\lambda \in \mathbb{F}_{p^n}^*$*. Consider the function*

$$f(x) = \mathrm{Tr}_1^n(aF(x)) = \mathrm{Tr}_1^n(a(x^{p^{k+1}+1} + \lambda x^{p^{k+1}} + \lambda^{p^{k+1}} x)) = g(x) + \mathrm{Tr}_1^n(b_a x).$$

Define $F^*(x) = a^{p^{k+1}} x^{p^{2(k+1)}} + ax$*. Then,*

1. *If* $n \equiv 0 \pmod 4$*, then*

$$W_f(0) = \begin{cases} -\overline{\xi_p^{g(x_a)}} p^{\frac{n+2}{2}}, & \text{if } (p+1) | j; \\ \overline{\xi_p^{g(x_a)}} p^{n/2}, & \text{otherwise,} \end{cases}$$

   where x_a *is such that* $F^*(x_a) = b_a^{p^{k+1}}$*.*

2. *If* $n \not\equiv 0 \pmod 4$ *and* $p = 2$*, then* $f(x)$ *is balanced.*

3. If $n \not\equiv 0 \pmod 4$ and $p \neq 2$, then

$$W_f(0) = \begin{cases} \overline{\xi_p^{g(x_a)}}\eta(-a)(-1)^{n-1}p^{\frac{n}{2}}, & \text{if } p \equiv 1 \pmod 4; \\ \overline{\xi_p^{g(x_a)}}\eta(-a)(-1)^{n-1}\mathbb{i}^{3n}p^{\frac{n}{2}}; & \text{if } p \equiv 3 \pmod 4, \end{cases}$$

where x_a is unique such that $F^*(x_a) = b_a^{p^{k+1}}$.

Proof. Since $F(x)$ is a permutation for $p = 2$ and $n \not\equiv 0 \pmod 4$, all its components are balanced. For $n \not\equiv 0 \pmod 4$ and $p > 2$, by Lemma 4, $F^*(x) = 0$ has exactly one solution since $\frac{n}{\gcd(k+1,n)}$ is odd. From Lemma 3 and Lemma 5 applied to $g(x) = \mathrm{Tr}_1^n(ax^{p^{k+1}+1})$, we get the Walsh value $W_g(b_a) = W_f(0)$. By adapting the results of [11], one can prove that, for $n \equiv 0 \pmod 4$, $F^*(x) = 0$ has either p^2 or 1 solutions depending on whether $\omega^{j\frac{p^n-1}{p+1}} = 1$ or not. This is equivalent to whether $p+1$ divides j or not. Thus, again from Lemma 3 and Lemma 5, we get the result. ◇

Remark 2 *The first thing to beware when glancing at Lemma 11 must be showing that $g(x_a)$ does not depend on the choice of the solution x_a (when there is more than one solution), i.e., $g(x_a) = g(x'_a)$ for any two solutions x_a, x'_a of $F^*(x) = b_a^{p^{k+1}}$. To show this, first note that x'_a belongs to the coset $x_a + \ker(F^*)$. Let $x'_a = x_a + \tilde{x}$ for some $\tilde{x} \in \ker(F^*)$ then $a^{p^{k+1}}\tilde{x}^{p^{2(k+1)}} = -a\tilde{x}$. Suppose that $p > 2$. Working out the definitions and using $\mathrm{Tr}_1^n(x) = \mathrm{Tr}_1^n(x^p)$ for each x, we get*

$$\mathrm{Tr}_1^n(a\tilde{x}^{p^{k+1}+1}) = \mathrm{Tr}_1^n(a^{p^{k+1}}\tilde{x}^{p^{2(k+1)}}\tilde{x}^{p^{k+1}}) = -\mathrm{Tr}_1^n(a\tilde{x}^{p^{k+1}+1}).$$

This yields $\mathrm{Tr}_1^n(a\tilde{x}^{p^{k+1}+1}) = 0$, so that $g(x_a) = g(x'_a)$ when $p > 2$. Now, suppose that $p = 2$. Let $\tilde{x}$ be a non-zero element in $\ker(F^*)$. The equation $a^{2^{k+1}}\tilde{x}^{2^{2(k+1)}} = a\tilde{x}$ implies that $\tilde{x}^3 = a^{1-2^{k+1}}$. Raising both sides to the power of $2^{k+1}+1$, we get $(\tilde{x}^{2^{k+1}+1})^3 = a^{-2^{2k+2}+1} = a^{-3}$. Hence, $\tilde{x}^{2^{k+1}+1} = a^{-1}$ and $\mathrm{Tr}_1^n(a\tilde{x}^{p^{k+1}+1}) = \mathrm{Tr}_1^n(1) = 0$ We conclude that $g(x_a) = g(x'_a)$.

The last (and crucial) step to obtain the weight distributions of the codes $C_{\mathrm{im}(F)^*}$ is to put everything together by interlacing the appropriate values of the component functions to compute the aimed sums in (6). This is the purpose of the following key lemma.

Lemma 12 (Interwoven Lemma) *Let p be a prime and $n > 1$ be an integer. Let $k = \lfloor \frac{n}{2} \rfloor$, $\omega \in \mathbb{F}_{p^n}^*$ be a generator and $a = \omega^j \in \mathbb{F}_{p^n}^*$. The function*

$$f(x) = \mathrm{Tr}_1^n(aF(x)) = \mathrm{Tr}_1^n(a(x^{p^{k+1}+1} + \lambda x^{p^{k+1}} + \lambda^{p^{k+1}}x)) := g(x) + \mathrm{Tr}_1^n(b_a x),$$

where $\lambda \in \mathbb{F}_{p^n}^*$, has the following properties, for a solution x_a of $a^{p^{k+1}}x^{p^{2(k+1)}} + ax = b_a^{p^{k+1}}$:

1. *For $p > 2$, n odd,*

$$\sum_{y\in\mathbb{F}_p^*}\sum_{x\in\mathbb{F}_{p^n}}\xi_p^{yf(x)} = \begin{cases} 0, & g(x_a)=0; \\ -\eta(g(x_a))\eta(a)p^{\frac{n+1}{2}}, & g(x_a)\neq 0, p\equiv n\equiv 3 \pmod 4; \\ \eta(g(x_a))\eta(a)p^{\frac{n+1}{2}}, & g(x_a)\neq 0, p\equiv 1 \text{ or } n\equiv 1 \pmod 4. \end{cases}$$

2. *For $p > 2$, $n \equiv 2 \pmod 4$,*

$$\sum_{y\in\mathbb{F}_p^*}\sum_{x\in\mathbb{F}_{p^n}}\xi_p^{yf(x)} = \begin{cases} -\eta(-a)p^{\frac{n}{2}}, & g(x_a)\neq 0; \\ \eta(-a)p^{\frac{n}{2}}(p-1), & g(x_a)=0. \end{cases}$$

3. *For $n \equiv 0 \pmod 4$,*

$$\sum_{y\in\mathbb{F}_p^*}\sum_{x\in\mathbb{F}_{p^n}}\xi_p^{yf(x)} = \begin{cases} p^{\frac{n+2}{2}}, & g(x_a)\neq 0 \text{ and } p+1|j; \\ -p^{\frac{n+2}{2}}(p-1), & g(x_a)=0 \text{ and } p+1|j; \\ p^{\frac{n}{2}}(p-1), & g(x_a)=0 \text{ and } p+1\not|j; \\ -p^{\frac{n}{2}}, & g(x_a)\neq 0 \text{ and } p+1\not|j. \end{cases}$$

Proof. Let $n \not\equiv 0 \pmod 4$ and $p > 2$. For this proof, denote by η_0 the Legendre symbol modulo p. We can write

$$\sum_{y\in\mathbb{F}_p^*} W_{yf}(0) = \sum_{y\in\mathbb{F}_p^*}\overline{\xi_p^{yg(x_{ya})}}\eta(-ya)(-1)^{n-1}p^{\frac{n}{2}}\sqrt{\eta_0(-1)}^{3n}, \tag{10}$$

where we used Lemma 11 and set x_{ya} to be the only solution to $(ya)^{p^{k+1}}x^{p^{2(k+1)}} + (ya)x = b_{ya}^{p^{k+1}}$. Note that, moreover, $b_{ya}^{p^{k+1}} = yb_a^{p^{k+1}}$ so that $x_a = x_{ya}$ by uniqueness. Then the right hand side of Equation 10 can be turned into

$$(-1)^{n-1}p^{\frac{n}{2}}\eta(-a)\sqrt{\eta_0(-1)}^{3n}\sum_{y\in\mathbb{F}_p^*}\overline{\xi_p^{yg(x_a)}}\eta(y). \tag{11}$$

Suppose that $g(x_a) \neq 0$. The Gaussian sum $\sum_{y\in\mathbb{F}_p^*} \overline{\xi_p^{yg(x_a)}}\eta(y)$ is equal to -1 when n is even and it is equal to $\eta(g(x_a))\eta(-1)\sqrt{\eta_0(-1)}p^{1/2}$ when n is odd, by the Davenport-Hassen Theorem[33]. Now suppose that $g(x_a) = 0$. The Gaussian sum $\sum_{y\in\mathbb{F}_p^*}\eta(y)$ is equal to $p-1$ when n is even and it is equal to 0 when n is odd. Combining these observations with Equation 11, we get the result for $p > 2$ and $n \not\equiv 0 \pmod 4$. Assume that $n \equiv 0 \pmod 4$. Let $F^*(x) = a^{p^{k+1}}x^{p^{2(k+1)}} + ax$ and x_{ya} be a solution of $yF(x) = yb_a^{p^{k+1}} = b_{ya}^{p^{k+1}}$. Since $g(x_a) = g(x_{ya})$ for each $y \in \mathbb{F}_p^*$, the sum $\sum_{y\in\mathbb{F}_p^*} W_{yf}(0)$ equals $-p^{\frac{n+2}{2}}\sum_{y\in\mathbb{F}_p^*}\overline{\xi_p^{yg(x_a)}}$, when $p+1|j$ and $p^{\frac{n}{2}}\sum_{y\in\mathbb{F}_p^*}\overline{\xi_p^{yg(x_a)}}$ when $p+1 \not| j$. The fact that $\sum_{y\in\mathbb{F}_p^*}\overline{\xi_p^{yg(x_a)}} = -1$ when $g(x_a) \neq 0$, and, otherwise, $\sum_{y\in\mathbb{F}_p^*}\overline{\xi_p^{yg(x_a)}} = p-1$ yields the result. ◇

The remaining case, $p = 2$, $n \not\equiv 0 \pmod 4$ is much simpler and can be handled similarly. It will however not be relevant for our purposes (since the obtained code is the simplex code). Thus we omit its proof.

As per Remark 2, notice that the value of $g(x_a)$ is independent of the choice of x_a. Moreover, it turns out that, for the chosen $F(x)$, $g(x_a) \neq 0$ is equivalent to $\mathrm{Tr}_1^n(a\lambda^{p^{k+1}+1}) \neq 0$. Indeed, we can take $x_a = \lambda$ for the considered function. To prove this, recall that $x^{p^{k+1}}$ is a linearized permutation polynomial, so that every non-zero element a is a (p^{k+1})-power element, i.e., $a = (a')^{p^{k+1}}$ for some $a' \in \mathbb{F}_{p^n}^*$. Thus we get

$$\mathrm{Tr}_1^n(a\lambda x^{p^{k+1}}) = \mathrm{Tr}_1^n((a'\lambda' x)^{p^{k+1}}) = \mathrm{Tr}_1^n(a'\lambda' x).$$

This implies that $b_a = a'\lambda' + a\lambda^{p^{k+1}}$. From here, $b_a^{p^{k+1}} = \lambda^{p^{2(k+1)}}a^{p^{k+1}} + a\lambda$, whence λ is a solution of $a^{p^{k+1}}x^{p^{2(k+1)}} + ax = b_a^{p^{k+1}}$. The reason why we presented Lemma 12 in such a generality is essentially to call upon a generalization of our results to the use of different functions which do not satisfy this condition.

Now we are in position to prove the main result of the paper.

Theorem 4 *Let p be a prime number and let $n > 1$ be an integer such that $n \equiv 0 \pmod 4$ or $p > 2$, but $p^n \neq 16$. Let $k = \lfloor \frac{n}{2} \rfloor$ and $\lambda \in \mathbb{F}_{p^n}^*$. The following holds for the code $C_{\mathrm{im}(F)^*}$, where $F(x) = x^{p^{k+1}+1} + \lambda x^{p^{k+1}} + \lambda^{p^{k+1}}$.*

- *If n is odd and $p \neq 2$, then $C_{\mathrm{im}(F)^*}$ is a three-valued code with parameters*

$$[\frac{p^n-1}{2}, n, \frac{p^n - p^{n-1} - p^{\frac{n-1}{2}} + 1}{2}],$$

whose weight distribution is displayed in Table 1.

- *If $n \equiv 2 \pmod 4$, $n \neq 2$, and $p \neq 2$, then $C_{\mathrm{im}(F)^*}$ is a four-valued code with parameters*
$$[\frac{p^n-1}{2}, n, \frac{p^n - p^{n-1} - p^{\frac{n}{2}} + p^{\frac{n}{2}-1}}{2}],$$
whose weight distribution is displayed in Table 2.

- *If $n \equiv 0 \pmod 4$ and $n \neq 4$, then $C_{\mathrm{im}(F)^*}$ is a four-valued code with parameters*
$$[\frac{p^n-1}{p+1}, n, \frac{p^n - p^{n-1} - p^{\frac{n}{2}} + p}{p+1}],$$
whose weight distribution displayed in Table 3.

- *If $n = 4$ and $p > 2$, then $C_{\mathrm{im}(F)^*}$ is a three-valued code with parameters*
$$[\frac{p^n-1}{p+1}, n, \frac{p^n - p^{n-1} - p^{\frac{n}{2}} + p}{p+1}],$$
whose weight distribution is displayed in Table 4.

- *If $n = 2$ and $p > 2$, then $C_{\mathrm{im}(F)^*}$ is a three-valued code with parameters*
$$[\frac{p^n-1}{2}, n, \frac{p^n - p^{n-1} - p^{\frac{n}{2}} + p^{\frac{n}{2}-1}}{2}],$$
whose weight distribution is displayed in Table 5.

Proof. We will only provide all the details for the first three cases since the proofs for the other cases can be easily deduced from these.

Case $p > 2$ and n odd. By Theorem 1, Theorem 5, Lemma 7 and Lemma 11, we get that the weight of a codeword $\mathbf{c}$ is equal to
$$wt(\mathbf{c}) = \frac{p^n - p^{n-1} \pm p^{\frac{n-1}{2}} + 1}{2}$$
or
$$wt(\mathbf{c}) = \frac{p^n - p^{n-1}}{2}.$$
The minimum distance follows at once from these equations. Denoting by $w_1 = \frac{p^n - p^{n-1} - p^{\frac{n-1}{2}} + 1}{2}$, $w_2 = \frac{p^n - p^{n-1}}{2}$ and $w_3 = \frac{p^n - p^{n-1} + p^{\frac{n-1}{2}} + 1}{2}$. Since $A_{w_2} = p^{n-1} - 1$ and $d^\perp \geq 2$, the first two Pless power moments become:
$$\begin{aligned} A_{w_1} + A_{w_3} &= p^n - p^{n-1}; \\ w_1 A_{w_1} + w_3 A_{w_3} &= \frac{(p^n - p^{n-1})^2}{2}. \end{aligned} \tag{12}$$

Solving this system of equations gives,

$$A_{w_1} = \frac{p^{\frac{n-1}{2}} + p^{\frac{n+1}{2}} + p^{n-1} + p^n}{4}$$

and

$$A_{w_3} = \frac{-p^{\frac{n-1}{2}} - p^{\frac{n+1}{2}} + p^{n-1} + p^n}{4}.$$

Case $n \equiv 2 \pmod 4$ and $p > 2$. By Theorem 1, Theorem 5, Lemma 7 and Lemma 11, we get that the weight of codewords is equal to $w_1 = \frac{p^n - p^{n-1} - p^{\frac{n}{2}-1}(p-1)}{2}$, $w_2 = \frac{p^n - p^{n-1} - p^{\frac{n}{2}-1} + 1}{2}$, $w_3 = \frac{p^n - p^{n-1} + p^{\frac{n}{2}-1} + 1}{2}$, and $w_4 = \frac{p^n - p^{n-1} + p^{\frac{n}{2}-1}(p-1)}{2}$. The minimum weight follows from these. Now, it is easy to see that $A_{w_1} + A_{w_3} = A_{w_2} + A_{w_4}$ and $A_{w_1} + A_{w_4} = p^{n-1} - 1$. Together with the first two Pless power moments, we get the system:

$$\begin{aligned} A_{w_1} + A_{w_3} &= A_{w_2} + A_{w_4}; \\ A_{w_1} + A_{w_4} &= p^{n-1} - 1; \\ A_{w_1} + A_{w_2} + A_{w_3} + A_{w_3} &= p^n - 1; \\ w_1 A_{w_1} + w_2 A_{w_2} + w_3 A_{w_4} + w_4 A_{w_4} &= \frac{(p^n - p^{n-1})(p^n - 1)}{2}, \end{aligned} \tag{13}$$

whose solution is $A_{w_1} = \frac{(p^{n/2}-1)(p+p^{n/2})}{2p}$, $A_{w_2} = \frac{(p-1)p^{n/2-1}(p^{n/2}+1)}{2}$, $A_{w_3} = \frac{(p-1)p^{n/2-1}(p^{n/2}-1)}{2}$ and $A_{w_4} = \frac{(p^{n/2}-p)(p^{n/2}+1)}{2p}$.

Case $n \equiv 0 \pmod 4$. By Theorem 1, Theorem 5, Lemma 7 and Lemma 11, we get that the weight of codewords is equal to $w_1 = \frac{p^n - p^{n-1} - p^{\frac{n}{2}} + p}{p+1}, w_2 = \frac{p^n - p^{n-1} - p^{\frac{n}{2}} + p^{\frac{n}{2}-1}}{p+1}, w_3 = \frac{p^n - p^{n-1} + p^{\frac{n}{2}-1} + p}{p+1}$, and $w_4 = \frac{p^n - p^{n-1} + p^{\frac{n}{2}+1} - p^{\frac{n}{2}}}{p+1}$. The minimum distance follows at once from these equations. For each $a \in \mathbb{F}_{p^n}^*$, choose one x_a such that it is a solution of $a^{p^{k+1}} x^{p^{2(k+1)}} + ax$. Note that $x_a = 1$ is always a solution for $a^{p^{k+1}} x^{p^{2(k+1)}} + ax = b_a^{p^{k+1}}$. Hence $g(x_a) = \mathrm{Tr}_1^n(a)$. Since the trace is a linear function, we have $A_{w_1} + A_{w_3} = p^n - p^{n-1}$ (and $A_{w_2} + A_{w_4} = p^{n-1} - 1$). Moreover, as the number of elements a such that $p+1|j$ is $\frac{p^n-1}{p+1}$, then $A_{w_1} + A_{w_4} = \frac{p^n-1}{p+1}$. Combining these with the first two Pless power moments, we get the system:

$$\begin{aligned} A_{w_1} + A_{w_3} &= p^n - p^{n-1}; \\ A_{w_1} + A_{w_4} &= \frac{p^n - 1}{p+1}; \\ A_{w_1} + A_{w_2} + A_{w_3} + A_{w_3} &= p^n - 1; \\ w_1 A_{w_1} + w_2 A_{w_2} + w_3 A_{w_4} + w_4 A_{w_4} &= \frac{(p^n - p^{n-1})(p^n - 1)}{p+1}. \end{aligned} \tag{14}$$

The solution of this system is $A_{w_1} = \frac{(p-1)p^{n/2-1}(p+p^{n/2})}{p+1}$, $A_{w_2} = \frac{(p^{n/2}-1)(p+p^{n/2})}{p+1}$, $A_{w_3} = \frac{(p-1)p^{n/2}(p^{n/2}-1)}{p+1}$ and $A_{w_4} = \frac{p^{n-1}-p^{n/2+1}+p^{n/2}-1}{p+1}$. This establishes the weight distributions of the code $C_{\mathrm{im}(F)^*}$. $\diamond$

The weight distribution of the code $C_{\mathrm{im}(F)^*}$ in Theorem 4, where $F(x) = x^{p^{k+1}+1} + \lambda x^{p^{k+1}} + \lambda^{p^{k+1}} x,\ \lambda \in \mathbb{F}_{p^n}^*$, are displayed in Tables 1-5 for different values of p and n.

Table 1: Weight distribution of $C_{\mathrm{im}(F)^*}$, $F(x) = x^{p^{k+1}+1} + \lambda x^{p^{k+1}} + \lambda^{p^{k+1}} x$, for $p > 2$, n odd and $\lambda \in \mathbb{F}_{p^n}^*$.

Weight w	Number of codewords
$\frac{p^n - p^{n-1} - p^{\frac{n-1}{2}} + 1}{2}$	$\frac{p^{\frac{n-1}{2}} + p^{\frac{n+1}{2}} + p^{n-1} + p^n}{4}$
$\frac{p^n - p^{n-1}}{2}$	$p^{n-1} - 1$
$\frac{p^n - p^{n-1} + p^{\frac{n-1}{2}} + 1}{2}$	$\frac{p^n + p^{n-1} - p^{\frac{n-1}{2}} - p^{\frac{n+1}{2}}}{4}$.

Table 2: Weight distribution of $C_{\mathrm{im}(F)^*}$, $F(x) = x^{p^{k+1}+1} + \lambda x^{p^{k+1}} + \lambda^{p^{k+1}} x$, for $p > 2$, $n \equiv 2 \pmod 4$ and $\lambda \in \mathbb{F}_{p^n}^*$.

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

Table 3: Weight distribution of $C_{\mathrm{im}(F)^*}$, $F(x) = x^{p^{k+1}+1} + \lambda x^{p^{k+1}} + \lambda^{p^{k+1}} x$, for $n \equiv 0 \pmod 4$, $n \neq 4$.

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

Table 4: Weight distribution of $C_{\mathrm{im}(F)^*}$, $F(x) = x^{p^{k+1}+1} + \lambda x^{p^{k+1}} + \lambda^{p^{k+1}} x$, for $n = 4$, $p > 2$ and $\lambda \in \mathbb{F}_{p^n}^*$.

Weight w	Number of codewords
$\frac{p^4-p^3-p^2+p}{p+1}$	$2p^3 - p^2 - p$
$\frac{p^4-p^3+2p}{p+1}$	$(p-1)^2 p^2$
$\frac{p^4-p^2}{p+1}$	$p-1$

Table 5: Weight distribution of $C_{\mathrm{im}(F)^*}$, $F(x) = x^{p^{k+1}+1} + \lambda x^{p^{k+1}} + \lambda^{p^{k+1}} x$, for $p > 2$, $n = 2$ and $\lambda \in \mathbb{F}_{p^n}^*$.

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

4.1 Main properties of codes stemming from trinomials

Some properties of the codes $C_{\mathrm{im}(F)^*}$, where $F(x) = x^{p^{k+1}+1} + \lambda^{p^{k+1}+1} x + \lambda$ for $\lambda \in \mathbb{F}_{p^n}^*$, can be derived using similar arguments as in Section 3.3. In this case, except when $n = 4$ and $p = 3$, the codes are not optimal with respect to the Griesmer bound, we observed however that the minimum distance of our codes is in general large (see Table 7).

Proposition 7 *Let p be a prime number, $n > 1$ be any integer such that $n \equiv 0 \pmod 4$ or $p > 2$, but $p^n \neq 16$. Let $k = \lfloor \frac{n}{2} \rfloor$ and $C_{\mathrm{im}(F)^*}$ be the code from Theorem 3, where $F(x) = x^{p^{k+1}+1} + \lambda^{p^{k+1}+1} x + \lambda$, $\lambda \in \mathbb{F}_{p^n}^*$. Then, $C_{\mathrm{im}(F)^*}$ is minimal except for $n = 2, 4$.*

Proof. A similar argument as for Proposition 3 yields the result. ◇

Again, using the first three Pless power moments and the weight distributions derived in Theorem 4, we can prove that the codes are projective in certain cases.

Proposition 8 *Let p be a prime number and let $n > 1$ be any integer such that $n \equiv 0 \pmod 4$ or $p > 2$, but $p^n \neq 16$. Let $k = \lfloor \frac{n}{2} \rfloor$ and let $C_{\mathrm{im}(F)^*}$ be the code from Theorem 4, where $F(x) = x^{p^{k+1}+1} + \lambda^{p^{k+1}+1} x + \lambda$. Then, $C_{\mathrm{im}(F)^*}$ is projective if and only if $p = 2$ and $n \equiv 0 \pmod 4$.*

Now, we turn to prove one of the most remarkable properties of the family of codes $C_{\mathrm{im}(F)^*}$ associated with t-to-one trinomials. Namely, we will prove that it contains an infinite family of self-orthogonal codes.

Proposition 9 *Let p be a prime number and let $n > 1$ be any integer such that $n \equiv 0 \pmod 4$ or $p > 2$, but $p^n \neq 16$. Let $k = \lfloor \frac{n}{2} \rfloor$. Consider the code $C_{\mathrm{im}(F)^*}$ from Theorem 4, where $F(x) = x^{p^{k+1}+1} + \lambda^{p^{k+1}+1}x + \lambda$. Then, $C_{\mathrm{im}(F)^*}$ is self-orthogonal when $n \equiv 0 \pmod 4$.*

Proof. Set $D = \mathrm{im}(F)^*$, $E = \mathrm{im}(x^{p^{k+1}+1})$ and $c = \lambda^{p^{k+1}+1}$. It is not hard to see that $D = (E - c)^*$. For every $x, y \in \mathbb{F}_{p^n}^*$, the sum $\sum_{d \in D} \mathrm{Tr}_1^n(xd)\mathrm{Tr}_1^n(yd)$ (over the integers) equals

$$\sum_{e \in E} \mathrm{Tr}_1^n(xe)\mathrm{Tr}_1^n(ye) - c(\sum_{e \in E} \mathrm{Tr}_1^n(xe) + \sum_{e \in E} \mathrm{Tr}_1^n(ye)) + (\mathrm{Tr}_1^n(xc)\mathrm{Tr}_1^n(yc))(|E| + 1).$$

Suppose that $n \equiv 0 \pmod 4$. Since C_{E^*} is self-orthogonal by Proposition 4, we get that $p \mid \sum_{e \in E} \mathrm{Tr}_1^n(xe)\mathrm{Tr}_1^n(ye)$. By the proof of Proposition 4, we can deduce that $\sum_{e \in E} \mathrm{Tr}_1^n(xe)$ and $\sum_{e \in E} \mathrm{Tr}_1^n(ye)$ are also divisible by p. Moreover, $|E| + 1 = \frac{p^n - 1}{p+1} + 1 = \frac{p(p^{n-1}+1)}{p+1}$, so that $p \mid |E| + 1$ since $\frac{(p^{n-1}+1)}{p+1}$ is an integer ($n - 1$ is odd). Therefore, p divides $\sum_{d \in D} \mathrm{Tr}_1^n(xd)\mathrm{Tr}_1^n(yd)$, which gives the result. $\diamond$

Remark 3 *Consider the classes of codes $\mathcal{C} = \{C_{\mathrm{im}(x^{p^{k+1}+1})} : p \text{ is prime}, n > 1\}$, where $k = \lfloor \frac{n}{2} \rfloor$, and*

$$\mathcal{C}' = \left\{ C_{\mathrm{im}(F)} : p \text{ is prime}, n \equiv 0 \pmod 4 \text{ or } p > 2, p^n \neq 16 \right\},$$

where $F(x) = x^{p^{k+1}+1} + \lambda^{p^{k+1}+1}x + \lambda$, $\lambda \in \mathbb{F}_{p^n}^*$, and $k = \lfloor \frac{n}{2} \rfloor$. While $\mathcal{C}$ and $\mathcal{C}'$ share a number of properties, they are however structurally different as shown by their weight distributions (cf. Theorem 3 and Theorem 4), and, for instance, the fact that almost all elements in $\mathcal{C}$ are self-orthogonal (except for $p^n = 4, 9$), whereas, for $\mathcal{C}'$, they are self-orthogonal only when $n \equiv 0 \pmod 4$.

We finish this section by posing a natural question that arises from this work.

Open Problem 2. Given a t-to-one polynomial $F(x)$ over $\mathbb{F}_{p^n}$, which affine functions L over $\mathbb{F}_{p^n}$ yield that $F + L$ is a t'-to-one function for some $t' \in \mathbb{N}$? In this case, which properties of $C_{\mathrm{im}(F)^*}$ are preserved? What are the best choices for L in terms of parameters and properties of the obtained codes?

5 Numerical results

For small values of p and n, one can provide some computational verification and examples of the codes obtained in this work. A MAGMA [3] script was used to derive these examples.

Table 6: Computational results for the family of codes in Theorem 3, where P, M, O and S stand for projective, minimal, optimal and self-orthogonal.

(p,n)	# Weights	P	M	O	S	Enumerator poly. $\sum A_w z^w$
$(2,4)$	2	Yes	No	Yes	No	$1+10z^2+5z^4$
$(2,8)$	2	Yes	Yes	Yes	Yes	$1+170z^{40}+85z^{48}$
$(3,2)$	2	No	No	No	No	$1+4z^2+4z^4$
$(3,3)$	1	Yes	Yes	Yes	Yes	$1+26z^9$
$(3,4)$	2	No	No	Yes	Yes	$1+60z^{12}+20z^{18}$
$(3,5)$	1	Yes	Yes	Yes	Yes	$1+242z^{81}$
$(3,6)$	2	No	Yes	No	Yes	$1+364z^{234}+364z^{252}$
$(5,2)$	2	No	No	No	Yes	$1+12z^8+12z^{12}$
$(5,3)$	1	No	Yes	Yes	Yes	$1+124z^{60}$
$(5,4)$	2	No	No	No	Yes	$1+520z^{80}+104z^{100}$

Table 7: Computational results for the family of codes in Theorem 4, where W, P, M, O and S stand for weights, projective, minimal, optimal and self-orthogonal.

(p,n)	$\#W$	P	M	O	S	Enumerator poly. $\sum A_w z^w$
$(2,8)$	4	Yes	Yes	No	Yes	$1+48z^{38}+90z^{40}+80z^{46}+37z^{48}$
$(3,2)$	2	No	No	No	No	$1+2z^2+4z^3+2z^4$
$(3,3)$	3	No	Yes	No	No	$1+12z^8+8z^9+6z^{11}$
$(3,4)$	3	No	No	Yes	Yes	$1+42z^{12}+36z^{15}+2z^{18}$
$(3,5)$	3	No	Yes	No	No	$1+90z^{77}+80z^{81}+72z^{86}$
$(3,6)$	4	No	Yes	No	No	$1+130z^{240}+252z^{239}+234z^{248}+112z^{252}$
$(5,2)$	3	No	No	No	No	$1+4z^8+12z^{10}+8z^{11}$
$(5,3)$	3	No	Yes	No	No	$1+60z^{48}+24z^{50}+40z^{53}$
$(5,4)$	3	No	No	No	Yes	$1+220z^{80}+400z^{85}+4z^{100}$

6 Conclusion

In this article, we have provided two families of p-ary linear codes with few weights employing quadratic polynomials over $\mathbb{F}_{p^n}$ that are also t-to-one mappings. Using

the image set of a Dembowski-Ostrom monomial $x^{p^{k+1}+1}$ as a defining-set, we built an infinite family of linear codes for which we have provided its exact weight distribution and important properties. Notably, this family contains optimal, minimal, projective and self-orthogonal codes. The first attempt to obtain the weight distributions of codes using these monomials was given in [17], however, the authors made an erroneous assumption on the rank of the component functions, which led to an incomplete conclusion. Hence, we have presented a complete correct version of such results. Then, using the image set of an affine equivalent (to $x^{p^{k+1}+1}$) trinomial, we have introduced and specified the weight distributions of the second family of linear codes with $2, 3$ or 4 weights. While this family preserves some properties exhibited by the monomial construction, they are structurally different (see Remark 3). Remarkably, it also contains infinite subclasses of self-orthogonal and minimal codes for each prime number p. The crucial point to derive the distributions for the second family is to properly analyze the interlacing of component functions of $x^{p^{k+1}+1}$. This was achieved by using the Interwoven Lemma (Lemma 12), which might be seen as a somewhat general tool based on Gaussian sums. Since most cryptographic properties are preserved under affine equivalence, one usually ignores affine equivalent functions. The results in this work emphasize the value of considering affine equivalent functions in the coding-theoretical context since similar (but not equivalent) objects with interesting properties can be obtained.

Acknowledgments, funding and competing interests

The author would like to thank Dr. Enes Pasalic for pointing out this line of research and for fruitful discussions that helped improve this work. The author is partly supported by the Slovenian Research Agency (research projects J1-4084, J1-2451 and N1-0159). There are no competing interests with other researchers or scientific institutions.

References

[1] Ashikhmin, A., Barg, A.: Minimal vectors in linear codes. IEEE Trans. Inf. Theory 44 (5), 2010–2017 (1998). https://doi.org/10.1109/18.705584

[2] Assmus, E. F., Mattson, H. F.: Coding and combinatorics. SIAM Review 16 (3), 349–388 (1974). https://doi.org/10.1137/1016056

[3] Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. I. The user language. J. Symbolic Comput. 24, (3–4), 235–265 (1997). https://doi.org/10.1006/jsco.1996.0125

[4] Brouwer, A.E., Shearer, J.B., Sloane, N.J.A., Smith, W.D.: A new table of constant weight codes. IEEE Trans. Inf. Theory 36 (6), 1334–1380 (1990). https://doi.org/10.1109/18.59932

[5] Calderbank, A.R., Kantor, W.M.: The geometry of two-weight codes. Bull. London Math. Soc. 18, 97–122 (1986). https://doi.org/10.1112/blms/18.2.97

[6] Calderbank, A.R., Goethals, J.M.: Three-weight codes and association schemes. Phillips Journal Research 39 (3-4), 143–152 (1984)

[7] Carlet, C.: Boolean and vectorial plateaued functions and APN functions. IEEE Trans. Inf. Theory 61 (11), 6272–6289 (2015). https://doi.org/10.1109/TIT.2015.2481384

[8] Carlet, C.: Boolean functions for cryptography and coding theory. Cambridge University Press, Cambridge (2021). https://doi.org/10.1017/9781108606806

[9] 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). https://doi.org/10.1109/TIT.2005.847722

[10] Carlet, C., Charpin, P., Zinoviev, V.: Codes, bent functions and permutations suitable for DES-like cryptosystems. Des. Codes Cryptogr. 15, 125–156 (1998). https://doi.org/10.1023/A:1008344232130

[11] Carlitz, L.: Evaluation of some exponential sums over a finite field. Math. Nachr. 96 (1), 319–339 (1980). https://doi.org/10.1002/mana.19800960125

[12] Coulter, R. S.: Explicit evaluations of some Weil sums. Acta Arith. 83 (3), 241–251 (1998). https://doi.org/10.4064/aa-83-3-241-251

[13] Coulter, R. S., Matthews, R. W.: Planar Functions and Planes of Lenz-Barlotti Class II. Des. Codes Cryptogr. 10, 167–184 (1997). https://doi.org/10.1023/A:1008292303803

[14] Delsarte, P.: Weights of linear codes and strongly regular normed spaces. Discrete Math. 3, Issues 1-3, 47–64 (1972). https://doi.org/10.1016/0012-365X(72)90024-6

[15] Dembowski, P., Ostrom, T.: Planes of order n with collineation groups of order n^2. Math. Z. 103, 239–258 (1968)

[16] Ding, C. A class of three-weight and four-weight codes. In: Proc. Int. Conf. Coding Crypt., Lecture Notes Comput. Sci. 5557 (Springer Verlag, Heidelberg), pp. 34–42 (2009). https://doi.org/10.1007/978-3-642-01877-0_4

[17] Ding, C: Linear codes from some 2-designs. IEEE Trans. Inf. Theory 61 (6), 3265–3275 (2015). https://doi.org/10.1109/TIT.2015.2420118

[18] Ding, C.: A construction of binary linear codes from Boolean functions. Discrete Math. 339 (9), 2288—2303 (2016). https://doi.org/10.1016/j.disc.2016.03.029

[19] 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). https://doi.org/10.1109/TIT.2015.2473861

[20] Ding, C., Li, N., Li, C., Zhou, Z.: Three-weight cyclic codes and their weight distributions. Discrete Math. 339 (2), 415–427 (2016). https://doi.org/10.1016/j.disc.2015.09.001

[21] Ding, C., Niederreiter, H.: Cyclotomic linear codes of order 3. IEEE Trans. Inf. Theory 53 (6), 2274–2277 (2007). https:/doi.org/10.1109/TIT.2007.896886

[22] Ding, C., Zhou, Z.: A class of three weight-cyclic codes. Finite Fields Appl. 25, 79–93 (2014). https://doi.org/10.1016/j.ffa.2013.08.005

[23] Ding, C., Wang, X.: A coding theory construction of new systematic authentication codes. Theor. Comput. Sci. 330 (1), 81–89, (2005). https://doi.org/10.1016/j.tcs.2004.09.011

[24] Du, X., Wan, Y.: Linear codes from quadratic forms. AAECC 28, 535–547 (2017). https://doi.org/10.1007/s00200-017-0319-x

[25] Feng, K., Luo, J.: Value distributions of exponential sums from perfect nonlinear functions and their applications. IEEE Trans. Inf. Theory 53 (9), 3035–3041 (2007). https://doi.org/10.1109/TIT.2007.903153

[26] Gold, R.: Maximal recursive sequences with 3-valued recursive crosscorrelation functions. IEEE Trans. Inform. Theory 14 (1), 154–156 (1968). https://doi.org/10.1109/TIT.1968.1054106

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

[28] Helleseth, T., Kholosha, A.: On the dual of monomial quadratic p-ary bent functions. In: Golomb, S.W., Gong, G., Helleseth, T., Song, HY. (eds) Sequences, Subsequences, and Consequences. Lecture Notes in Computer Science, vol 4893. Springer, Berlin, Heidelberg (2007). https://doi.org/10.1007/978-3-540-77404-4_5

[29] Hou, X.: Explicit evaluation of certain exponential sums of binary quadratic functions. Finite Fields Appl. 13, 843–868 (2007). https://doi.org/10.1016/j.ffa.2006.09.009

[30] Huffman, W. C., Pless, V.: Fundamentals of error-correcting codes. Cambridge: Cambridge University Press (2003). https://doi.org/10.1017/CBO9780511807077

[31] Li, C., Bae, S., Ahn, J., Yang, S., Yap, Z.: Complete weight enumerators of some linear codes and their applications. Des. Codes Cryptogr. 81, 153–168 (2016). https://doi.org/10.1007/s10623-015-0136-9

[32] Li, K., Li, C., Helleseth, T., Qu, L.: Binary linear codes with few weights from two-to-one functions. IEEE Trans. Inf. Theory 67 (7), 4263–4275 (2021). https://doi.org/10.1109/TIT.2021.3068743

[33] Lidl, R., Niederreiter, H.: Finite Fields (2nd ed.). Encycl. Math. Appl., Cambridge University Press, Cambridge (1996). https://doi.org/10.1017/CBO9780511525926

[34] Luo, J., Feng, K.: On the weight distributions of two classes of cyclic codes. IEEE Trans. Inf. Theory 54 (12), 5332—5344 (2008). https://doi.org/10.1109/TIT.2008.2006424

[35] Mesnager, S., Qian, L., Cao, X.: Further projective binary linear codes derived from two-to-one functions and their duals. Des. Codes Cryptogr. 91, 719–746 (2023). https://doi.org/10.1007/s10623-022-01122-3

[36] Mesnager, S., Qian, L., Cao, X., Yuan, M.: Several families of binary minimal linear codes from two-to-one functions. IEEE Trans. Inf. Theory 69 (5), 3285—3301 (2023). https://doi.org/10.1109/TIT.2023.3236955

[37] Nyberg, K.: Differentially uniform mappings for cryptography. In: Helleseth, T. (eds) Advances in Cryptology — EUROCRYPT '93. EUROCRYPT 1993. Lecture Notes in Computer Science, vol 765. Springer, Berlin, Heidelberg (1994).https://doi.org/10.1007/3-540-48285-7_6

[38] Pless, V.: Power moment identities on weight distributions in error correcting codes. Inf. Control 6 (2), 147–152 (1963). https://doi.org/10.1016/S0019-9958(63)90189-X

[39] Pradhan, D.K., Stiffler, J.J.: Error-correcting codes and self-checking circuits in fault-tolerant computers. IEEE Comput., 27–37 (1980). https://doi.org/10.1109/MC.1980.1653527

[40] Steane, A.M.: Enlargement of Calderbank-Shor-Steane quantum codes. IEEE Trans. Inf. Theory 45 (7), 2492–2495 (1999). https:/doi.org/10.1109/18.796388

[41] 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). https:/doi.org/10.1109/TIT.2016.2518678

[42] Wolfmann, J: Codes projectifs à deux ou trois poids associés aux hyperquadriques d'une géométrie finie. Discrete Math. 13 (2), 185–211 (1975)

[43] Xie, X., Ouyang, Y., Mao, M.: Vectorial bent functions and linear codes from quadratic forms. Cryptogr. Commun. 15, 1011–1029 (2023). https://doi.org/10.1007/s12095-023-00664-0

[44] Yang, S., Yao, Z., Zhao, C.: The weight distributions of two classes of p-ary cyclic codes with few weights. Finite Fields Appl. 44, 76–91 (2017). https://doi.org/10.1016/j.ffa.2016.11.004