Linear codes with few weights from weakly regular bent functions based on a generic construction

Sihem Mesnager*

Abstract

We contribute to the knowledge of linear codes with few weights from special polynomials and functions. Substantial efforts (especially due to C. Ding) have been directed towards their study in the past few years. Such codes have several applications in secret sharing, authentication codes, association schemes and strongly regular graphs. Based on a generic construction of linear codes from mappings and by employing weakly regular bent functions, we provide a new class of linear p-ary codes with three weights given with its weight distribution. The class of codes presented in this paper is different from those known in literature. Also, it contains some optimal codes meeting certain bound on linear codes.

Keywords Linear codes, weight distribution, p-ary functions, bent functions, weakly regular bent functions, vectorial functions, cyclotomic fields.

1 Introduction

Error correcting codes are widely studied by several researchers and employed by engineers. They have long been known to have applications in computer and communication systems, data storage devices (starting from the use of Reed Solomon codes in CDs) and consumer electronics. A lot of progress has been made on the constructions of linear codes with few weights. Such codes have applications in secret sharing [1],[6],[37],[9],[10],[19],[12], authentication codes [22], association schemes [2], and strongly regular graphs [3]. Interesting two-weight and three-weight codes have been obtained in several papers. A non-exhaustive list dealing with codes with few weights is [8], [13],[20],[36],[21],[23],[30],[38],[39],[18],[19],[33], [35],[34],[27] and [17].

Certain special types of functions over finite fields and vector spaces over finite fields are closely related to linear or nonlinear codes. Two generic constructions (say, of "type

*Department of Mathematics, University of Paris VIII, University of Paris XIII, CNRS, UMR 7539 LAGA and Telecom ParisTech, Paris, France. Email: smesnager@univ-paris8.fr

I" and of "type II") of linear codes involving special functions have been isolated and next investigated in literature. Linear codes obtained from the generic construction of type II are defined via their defining set while those obtained from the generic construction of type I are defined as the trace function of some functions involving polynomials which vanish at zero. Recently, based on the generic construction of type II, several approaches for constructing linear codes with special types of functions were proposed, and a lot of linear codes with excellent parameters were obtained. A very nice survey devoted to the construction of binary linear codes from Boolean functions based on the generic construction of type II is given by Ding in [17].

Bent functions are maximally nonlinear Boolean functions. They were introduced by Rothaus [32] in the 1960's and initially studied by Dillon as early as 1974 in this Thesis [15]. The notion of bent function has been extended in arbitrary characteristic by Kumar et al. [29]. For their own sake as interesting combinatorial objects, but also for their relations to coding theory (e.g. Reed-Muller codes, Kerdock codes, etc.), combinatorics (e.g. difference sets), design theory, sequence theory, and applications in cryptography (design of stream ciphers and of S-boxes for block ciphers), bent functions have attracted a lot of research for the past four decades as shown in a jubilee survey paper on bent functions [7] and a book [31] devoted especially to bent functions and containing a complete survey (including variations, generalizations and applications). It is well-known that Kerdock codes are constructed from bent functions. Very recently, it has been shown in a few papers [16, 40, 33] that bent functions lead to the construction of interesting linear codes with few weights based on the generic construction of type II.

In this paper, we focus on the construction of linear codes from bent functions in arbitrary characteristic based on the generic construction of type I. The paper is organized as follows. In Section 2, we fix our main notation and recall the necessary background. In Section 3, we present the two generic constructions of binary codes from functions which have been highlighted by Ding in [17] and focus on one of them. In Section 4, we study codes from mappings based on the first generic construction and present general results in a very general context. Finally, in Section 5, we derive a new class of linear codes with three weights from weakly regular bent and present its weight distribution. Such a class contains some optimal codes meeting certain bound on linear codes. The reader will notice that the general idea of the construction of our codes is a classical one since it has been already employed in [4, 5] in the binary case and in [6, 36] in odd characteristic. Nevertheless, our specific choice of the function employed for designing our code is new.

2 Notation and preliminaries

We present basic notation that will be employed in subsequent sections.

2.1 Some notation fixed throughout this paper

Throughout this paper we adopt the following notations unless otherwise stated.

- For any set E, $E^\star = E \setminus \{0\}$ and $\#E$ will denote the cardinality of E;
- p is a prime;
- h is a positive integer divisor of m. Set $m = hr$;
- $q = p^h$;
- $\mathbb{F}_n$ is the Galois field of order n;
- $\mathbb{Z}$ be the rational integer ring, $\mathbb{Q}$ the rational field and $\mathbb{C}$ the complex field;
- $(\frac{a}{p})$ be the Legendre symbol for $1 \leq a \leq p-1$;
- $p^* = (\frac{-1}{p})p = (-1)^{(p-1)/2}p$. Note that $p^m = (\frac{-1}{p})^m \sqrt{p^*}^{2m}$;
- $\xi_p = e^{\frac{2\pi\sqrt{-1}}{p}}$ be the primitive p-th root of unity.

2.2 Some background related to coding theory

Definition 1. A linear $[n, k, d]_q$ code $\mathcal{C}$ over $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q^n$ with minimum Hamming distance d.

The support of a vector $\bar{a} = (a_0, \cdots, a_{n-1}) \in \mathbb{F}_q^n$ denoted by $supp(\bar{a})$ is defined by $supp(\bar{a}) := \{0 \leq i \leq n-1 : a_i \neq 0\}$. The Hamming weight of a vector $\bar{a} \in \mathbb{F}_q^n$ denoted by $wt(\bar{a})$ is the cardinality of its support, that is, $wt(\bar{a}) := \#supp(\bar{a})$.

2.3 Cyclotomic field $\mathbb{Q}(\xi_p)$

In this subsection we recall some basic results on cyclotomic field. The ring of integers in $\mathbb{Q}(\xi_p)$ is $\mathcal{O}_K = \mathbb{Z}(\xi_p)$. An integral basis of $\mathcal{O}_{\mathbb{Q}(\xi_p)}$ is $\{\xi_p^i \mid 1 \leq i \leq p-1\}$. The field extension $\mathbb{Q}(\xi_p)/\mathbb{Q}$ is Galois of degree $p-1$ and the Galois group $Gal(\mathbb{Q}(\xi_p)/\mathbb{Q}) = \{\sigma_a \mid a \in \mathbb{Z}/p\mathbb{Z}^*\}$, where the automorphism σ_a of $\mathbb{Q}(\xi_p)$ is defined by $\sigma_a(\xi_p) = \xi_p^a$. The field $\mathbb{Q}(\xi_p)$ has a unique quadratic subfield $\mathbb{Q}(\sqrt{p^*})$ with $p^* = (\frac{-1}{p})p$ where $(\frac{a}{b})$ is the Legendre symbol for $1 \leq a \leq p-1$. For $1 \leq a \leq p-1$, $\sigma_a(\sqrt{p^*}) = (\frac{a}{p})\sqrt{p^*}$. Hence, the Galois group $Gal(\mathbb{Q}(\sqrt{p^*})/\mathbb{Q}$ is $\{1, \sigma_\gamma\}$, where γ is any quadratic nonresidue in $\mathbb{F}_p$.

2.4 Some background related to p-ary functions

The trace function $Tr_{q^r/q} : \mathbb{F}_{q^r} \to \mathbb{F}_q$ is defined as:

$$Tr_{q^r/q}(x) := \sum_{i=0}^{r-1} x^{q^i} = x + x^q + x^{q^2} + \cdots + x^{q^{r-1}}.$$

The trace function from $\mathbb{F}_{q^r}$ to its prime subfield is called the absolute trace function.

Recall that the trace function $Tr_{q^r/q}$ is $\mathbb{F}_q$-linear and satisfies the transitivity property in a chain of extension fields ($m = hr$): $Tr_{p^m/p}(x) = Tr_{p^h/p}(Tr_{p^m/p^h}(x))$ for all $x \in \mathbb{F}_{q^r}$.

Given two positive integers s and r, the functions from $\mathbb{F}_q^s$ to to $\mathbb{F}_q^r$ will be called (s, r)-q-ary functions or (if the values s and r are omitted) vectorial q-ary functions. The component functions of F are the q-ary functions $l \circ F$, where l ranges over the set of all the nonzero linear forms over $\mathbb{F}_q^r$. Equivalently, they are the linear combinations of a non-null number of their coordinate functions, that is, the functions of the form $v \cdot F, \quad v \in \mathbb{F}_q^r \setminus \{0\}$, where "$\cdot$" denotes the usual inner product in $\mathbb{F}_q^r$ (or any other inner product). The vector spaces $\mathbb{F}_q^s$ and $\mathbb{F}_q^r$ can be identified with the Galois fields $\mathbb{F}_{q^s}$ and $\mathbb{F}_{q^r}$ of orders q^s and q^r respectively. Hence, (s, r)-q-ary functions can be viewed as functions from $\mathbb{F}_{q^s}$ to $\mathbb{F}_{q^r}$. In this case, the component functions are the functions $Tr_{q^r/q}(vF(x))$ where $Tr_{q^r/q}$ is the trace function from $\mathbb{F}_{q^r}$ to $\mathbb{F}_q$.

Let $f : \mathbb{F}_{p^m} \longrightarrow \mathbb{F}_p$ be a p-ary function. The Walsh transform of f is given by:

$$\widehat{\chi_f}(\lambda) = \sum_{x \in \mathbb{F}_{p^m}} \xi_p{}^{f(x) - Tr_{p^m/p}(\lambda x)}, \lambda \in \mathbb{F}_{p^m}$$

where $\xi_p = e^{\frac{2\pi\sqrt{-1}}{p}}$ is a complex primitive pth root of unity and the elements of $\mathbb{F}_p$ are considered as integers modulo p.

Function f can be recovered from $\widehat{\chi_f}$ by the inverse transform:

$$\xi_p^{f(x)} = \frac{1}{p^m} \sum_{b \in \mathbb{F}_{p^m}} \widehat{\chi_f}(b) \xi_p^{-Tr_{p^m/p}(bx)}. \tag{1}$$

2.5 Bent functions and (weakly) regular bent functions

A p-ary function $f : \mathbb{F}_{p^m} \longrightarrow \mathbb{F}_p$ is called *bent* if all its Walsh-Hadamard coefficients satisfy $|\widehat{\chi_f}(b)|^2 = p^m$. A bent function f is called *regular bent* if for every $b \in \mathbb{F}_{p^m}$, $p^{-\frac{m}{2}} \widehat{\chi_f}(b) = \xi_p^{f^\star(b)}$ for some p-ary function $f^\star : \mathbb{F}_{p^m} \to \mathbb{F}_p$ ([29], [definition 3]). The bent function f is called *weakly regular bent* if there exists a complex number u with $|u| = 1$ and a p-ary function $f^\star$ such that $up^{-\frac{n}{2}} \widehat{\chi_f}(b) = \xi_p^{f^\star(b)}$ for all $b \in \mathbb{F}_{p^m}$. Such function $f^*(x)$ is called the *dual* of $f(x)$. From [24, 25], a weakly regular bent function $f(x)$ satisfies that

$$\widehat{\chi_f}(b) = \epsilon \sqrt{p^*}^m \xi_p^{f^*(b)}, \tag{2}$$

Bent functions	m	p
$\sum_{i=0}^{\lfloor m/2 \rfloor} Tr_{p^m/p}(a_i x^{p^{i+1}})$	arbitrary	arbitrary
$\sum_{i=0}^{p^k-1} Tr_{p^m/p}(a_i x^{i(p^k-1)}) + Tr_{p^l/p}(\delta x^{\frac{p^m-1}{e}})$, $e \mid p^k+1$	$m=2k$	arbitrary
$Tr_{p^m/p}(ax^{\frac{3^m-1}{4}+3^k+1})$	$m=2k$	$p=3$
$Tr_{p^m/p}(x^{p^{3k}+p^{2k}-p^k+1}+x^2)$	$m=4k$	arbitrary
$Tr_{p^m/p}(ax^{\frac{3^i+1}{2}})$; i odd, $gcd(i,m)=1$	arbitrary	$p=3$

Table 1: Known weakly regular bent functions over $\mathbb{F}_{p^m}$, p odd

where $\epsilon = \pm 1$ is called the sign of the Walsh transform of $f(x)$ and p^* equals $(\frac{-1}{p})p$ where $(\frac{a}{b})$ is the Legendre symbol for $1 \leq a \leq p-1$. Note that from Equation (1), for the weakly regular bent function $f(x)$, we have $\sum_{b \in \mathbb{F}_{p^m}} \xi_p^{f^*(b)-Tr_{p^m/p}(bx)} = \epsilon p^m \xi_p^{f(x)}/\sqrt{p^*}^m$. Moreover, Walsh-Hadamard transform coefficients of a p-ary bent function f with odd p satisfy

$$p^{-\frac{m}{2}} \widehat{\chi_f}(b) = \begin{cases} \pm \xi_p^{f^\star(b)}, & \text{if } m \text{ is even or } m \text{ is odd and } p \equiv 1 \pmod 4, \\ \pm i \xi_p^{f^\star(b)}, & \text{if } m \text{ is odd and } p \equiv 3 \pmod 4, \end{cases} \tag{3}$$

where i is a complex primitive 4-th root of unity. Therefore, regular bent functions can only be found for even m and for odd m with $p \equiv 1 \pmod 4$. Moreover, for a weakly regular bent function, the constant u (defined above) can only be equal to ± 1 or $\pm i$.

We summarize in Table 1 all known weakly regular bent functions over $\mathbb{F}_{p^m}$ with odd characteristic p.

3 Two generic constructions of linear codes from functions

Boolean functions or more generally p-ary functions have important applications in cryptography and coding theory. In coding theory, they have been used to construct linear codes. Historically, the Reed-Muller codes and Kerdock codes have been -for a long time- the two famous classes of binary codes derived from Boolean functions. Next, a lot of progress has been made in this direction and further codes have been derived from more general and complex functions. Nevertheless, as highlighted by Ding in his very recent survey [17], despite the advances in the past two decades, one can isolate essentially only two generic constructions of linear codes from functions.

The first generic construction of linear codes from functions is obtained by considering a code $\mathcal{C}(f)$ over $\mathbb{F}_p$ involving a polynomial f from $\mathbb{F}_q$ to $\mathbb{F}_q$ (where $q = p^m$) defined by

$$\mathcal{C}(f) = \{\mathbf{c} = (Tr_{q/p}(af(x)+bx))_{x \in \mathbb{F}_q^*} \mid a \in \mathbb{F}_q, b \in \mathbb{F}_q\}.$$

The resulting code $\mathcal{C}(f)$ from f is a linear code of length $q-1$ and its dimension is upper bounded by $2m$ which is reached in many cases. As mentioned in the literature (see

for instance [17]), this generic construction has a long history and its importance is supported by Delsarte's Theorem [14]. In the binary case (that is, when $q = 2$), the first generic construction allows us to provide a kind of a coding-theory characterization of special cryptographic functions such as APN functions, almost bent functions and semi-bent functions (see for instance [5], [4] and [28]).

The second generic construction of linear codes from functions is obtained by fixing a set $D = \{d_1, d_2, \cdots, d_n\}$ in $\mathbb{F}_q$ (where $q = p^m$) and by defining a linear code involving D as follows:

$$\mathcal{C}_D = \{(Tr_{q/p}(xd_1), Tr_{q/p}(xd_2), \cdots, Tr_{q/p}(xd_n)) \mid x \in \mathbb{F}_q\}.$$

The set D is usually called the *defining set* of the code $\mathcal{C}_D$. The resulting code $\mathcal{C}_D$ is of length n and of dimension at most m. This construction is generic in the sense that many classes of known codes could be produced by selecting the defining set $D \subseteq \mathbb{F}_q$. The code quality (good or optimal parameters or the contrary) is closely related to the choice of the set D.

4 On the first generic construction of linear codes from mappings over finite fields

For any $\alpha, \beta \in \mathbb{F}_{p^m}$, defined as:

$$\begin{array}{rccl} f_{\alpha,\beta} & : & \mathbb{F}_{q^r} & \longrightarrow & \mathbb{F}_q \\ & & x & \longmapsto & f_{\alpha,\beta}(x) := Tr_{q^r/q}(\alpha\Psi(x) - \beta x) \end{array}$$

where Ψ is a mapping from $\mathbb{F}_{q^r}$ to $\mathbb{F}_{q^r}$ such that $\Psi(0) = 0$.

We now define a linear code $\mathcal{C}_\Psi$ over $\mathbb{F}_q$ as :

$$\mathcal{C}_\Psi := \{\bar{c}_{\alpha,\beta} = (f_{\alpha,\beta}(\zeta_1), f_{\alpha,\beta}(\zeta_2), \cdots, f_{\alpha,\beta}(\zeta_{q^r-1})), \alpha, \beta \in \mathbb{F}_{q^r}\}$$

where $\zeta_1, \cdots, \zeta_{q^r-1}$ denote the nonzero elements of $\mathbb{F}_{q^r}$.

Proposition 1. *The linear code $\mathcal{C}_\Psi$ is of length $q^r - 1$. If the mapping Ψ has no linear component then $\mathcal{C}_\Psi$ is of dimension $k = \frac{2m}{h} = 2r$. Otherwise, k is less than $2r$.*

Proof. It is clear that $\mathcal{C}_\Psi$ is of length $q^r - 1$. Now, let compute the cardinality of $\mathcal{C}_\Psi$. Let $\bar{c}_{\alpha,\beta}$ be a codeword of $\mathcal{C}_\Psi$. We have

$$\begin{aligned} \bar{c}_{\alpha,\beta} = 0 &\iff Tr_{q^r/q}(\alpha\Psi(\zeta_i) - \beta\zeta_i) = 0, \forall i \in \{1, \cdots, q^r - 1\} \\ &\iff Tr_{q^r/q}(\alpha\Psi(x) - \beta x) = 0, \forall x \in \mathbb{F}_{q^r}^\star \\ &\Rightarrow Tr_{q^r/p}(\alpha\Psi(x) - \beta x) = 0, \forall x \in \mathbb{F}_{q^r}^\star \\ &\Rightarrow Tr_{q^r/p}(\alpha\Psi(x) - \beta x) = 0, \forall x \in \mathbb{F}_{q^r} \\ &\Rightarrow Tr_{q^r/p}(\alpha\Psi(x)) = Tr_{q^r/p}(\beta x), \forall x \in \mathbb{F}_{q^r} \end{aligned}$$

Hence, $\bar{c}_{\alpha,\beta} = 0$ implies that the mapping from $\mathbb{F}_{q^r}$ to $\mathbb{F}_q$ component of Ψ associated with $\alpha \neq 0$ is linear (or null) and coincides with $x \mapsto Tr_{q^r/p}(\beta x)$. Therefore, it suffices that no component function of Ψ not be identically equal to 0 or linear to ensure that the only null codeword appears only one time at $\alpha = \beta = 0$. Furthermore, it implies that all the codewords $\bar{c}_{\alpha,\beta}$ are pairwise distinct. In this case, the size of the code is q^{2r} and the dimension of the code is thus equals $2r$. □

The following statement shows that the weight distribution of the code $\mathcal{C}_\Psi$ of length $q^r - 1$ can be expressed by means of the Walsh transform of some absolute trace functions over $\mathbb{F}_{p^m}$ involving the map Ψ.

Proposition 2. *We keep the notation above. Let $a \in \mathbb{F}_{p^m}$. Let us denote by ψ a mapping from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p$ defined as:*

$$\psi_a(x) = Tr_{p^m/p}(a\Psi(x)).$$

For $\bar{c}_{\alpha,\beta} \in \mathcal{C}_\Psi$, we have:

$$wt(\bar{c}_{\alpha,\beta}) = p^m - \frac{1}{q} \sum_{\omega \in \mathbb{F}_q} \widehat{\chi_{\psi_{\omega\alpha}}}(\omega\beta).$$

Proof. Note that $\Psi(0) = 0$ implies that $f_{\alpha,\beta}(0) = 0$. Now, let $\bar{c}_{\alpha,\beta}$ be a codeword of $\mathcal{C}_\Psi$ then,

$$\begin{aligned} wt(\bar{c}_{\alpha,\beta}) &= \#\{x \in \mathbb{F}_{q^r}^\star \mid f_{\alpha,\beta}(x) \neq 0\} \\ &= \#\{x \in \mathbb{F}_{q^r} \mid f_{\alpha,\beta}(x) \neq 0\} \\ &= p^m - \#\{x \in \mathbb{F}_{q^r} \mid f_{\alpha,\beta}(x) = 0\} \\ &= p^m - \sum_{x \in \mathbb{F}_{q^r}} \frac{1}{q} \sum_{\omega \in \mathbb{F}_q} \xi_p{}^{Tr_{q/p}(\omega f_{\alpha,\beta}(x))}. \end{aligned}$$

The latter equality comes from the fact that the sum of characters equals q if $f_{\alpha,\beta}(x) = 0$ and 0 otherwise. Moreover (using the transitivity property of the trace function $Tr_{q^r/p}$ and the fact that $Tr_{q^r/q}$ is $\mathbb{F}_q$-linear)

$$
\begin{aligned}
wt(\bar{c}_{\alpha,\beta}) &= p^m - \frac{1}{q}\sum_{\omega\in\mathbb{F}_q}\sum_{x\in\mathbb{F}_{q^r}} \xi_p{}^{Tr_{q/p}(\omega f_{\alpha,\beta}(x))} \\
&= p^m - \frac{1}{q}\sum_{\omega\in\mathbb{F}_q}\sum_{x\in\mathbb{F}_{q^r}} \xi_p{}^{Tr_{q/p}(\omega Tr_{q^r/q}(\alpha\Psi(x)-\beta x))} \\
&= p^m - \frac{1}{q}\sum_{\omega\in\mathbb{F}_q}\sum_{x\in\mathbb{F}_{q^r}} \xi_p{}^{Tr_{q/p}(Tr_{q^r/q}(\omega\alpha\Psi(x)-\omega\beta x))} \\
&= p^m - \frac{1}{q}\sum_{\omega\in\mathbb{F}_q}\sum_{x\in\mathbb{F}_{q^r}} \xi_p{}^{Tr_{q^r/p}(\omega\alpha\Psi(x)-\omega\beta x)} \\
&= p^m - \frac{1}{q}\sum_{\omega\in\mathbb{F}_q}\sum_{x\in\mathbb{F}_{q^r}} \xi_p{}^{Tr_{q^r/p}(\omega\alpha\Psi(x))-Tr_{q^r/p}(\omega\beta x)} \\
&= p^m - \frac{1}{q}\sum_{\omega\in\mathbb{F}_q}\sum_{x\in\mathbb{F}_{q^r}} \xi_p{}^{\psi_{\omega\alpha}(x)-Tr_{q^r/p}(\omega\beta x)} \\
&= p^m - \frac{1}{q}\sum_{\omega\in\mathbb{F}_q} \widehat{\chi_{\psi_{\omega\alpha}}}(\omega\beta).
\end{aligned}
$$

□

In the following, we denote by $S_\psi(\alpha,\beta)$ the sum $\frac{1}{q}\sum_{\omega\in\mathbb{F}_q}\widehat{\chi_{\psi_{\omega\alpha}}}(\omega\beta)$. We compute the sum of all the values of $S_\psi(\alpha,\beta)$ when α (resp. β) ranges the field $\mathbb{F}_{q^r}$.

Proposition 3. *Keeping the same notation as above, set* $S_\psi(\alpha,\beta) := \frac{1}{q}\sum_{\omega\in\mathbb{F}_{q^r}}\widehat{\chi_{\psi_{\omega\alpha}}}(\omega\beta)$. *we have*

1. $\sum_{\alpha\in\mathbb{F}_{q^r}} S_\psi(\alpha,\beta) = q^{r-1}\Big(q^r+q+\#\{x\in\mathbb{F}_{q^r} \mid \psi(x)=Tr_{q^r/q}(\beta x)=0\} - \#\{x\in\mathbb{F}_{q^r} \mid \psi(x)=0\}\Big)$.
2. $\sum_{\beta\in\mathbb{F}_{q^r}} S_\psi(\alpha,\beta) = q^{2r-1}+q^r-q^{r-1}$.

Proof. Let compute the sum $\sum_{\alpha\in\mathbb{F}_{q^r}} S_\psi(\alpha,\beta)$.

$$
\begin{aligned}
\sum_{\alpha\in\mathbb{F}_{q^r}} S_\psi(\alpha,\beta) &= \frac{1}{q}\sum_{\omega\in\mathbb{F}_q}\sum_{x\in\mathbb{F}_{q^r}}\sum_{\alpha\in\mathbb{F}_{q^r}} \xi_p{}^{Tr_{q^r/p}(\omega\alpha\psi(x)-\omega\beta x)} \\
&= \frac{q^r}{q}\sum_{\omega\in\mathbb{F}_q}\sum_{x\in\mathbb{F}_{q^r}|\omega\psi(x)=0} \xi_p{}^{-Tr_{q^r/p}(\omega\beta x)}
\end{aligned}
$$

In the second equality we have used the fact that $\sum_{\alpha\in\mathbb{F}_{q^r}} \xi_p^{Tr_{q^r/p}(\omega\alpha\psi(x))}$ equals $p^m = q^r$ if $\omega\psi(x) = 0$ and equals 0 otherwise. Now, let separate the case when $\omega = 0$ and $\omega \neq 0$.

$$\begin{aligned}
\sum_{\alpha\in\mathbb{F}_{q^r}} S_\psi(\alpha,\beta) &= \frac{q^r}{q}\Big(\sum_{x\in\mathbb{F}_{q^r}} 1 + \sum_{\omega\in\mathbb{F}_q^\star}\sum_{x\in\mathbb{F}_{q^r}|\psi(x)=0} \xi_p^{-Tr_{q^r/p}(\omega\beta x)}\Big)\\
&= \frac{q^r}{q}\Big(q^r + \sum_{\omega\in\mathbb{F}_q}\sum_{x\in\mathbb{F}_{q^r}|\psi(x)=0} \xi_p^{-Tr_{q^r/p}(\omega\beta x)} - \#\{x\in\mathbb{F}_{q^r} \mid \psi(x)=0\}\Big)\\
&= \frac{q^r}{q}\Big(q^r + \sum_{x\in\mathbb{F}_{q^r}|\psi(x)=0}\sum_{\omega\in\mathbb{F}_q} \xi_p^{-Tr_{q/p}(Tr_{q^r/q}(\beta x)\omega)} - \#\{x\in\mathbb{F}_{q^r} \mid \psi(x)=0\}\Big)\\
&= \frac{q^r}{q}\Big(q^r + q\#\{x\in\mathbb{F}_{q^r} \mid \psi(x) = Tr_{q^r/q}(\beta x)=0\} - \#\{x\in\mathbb{F}_{q^r} \mid \psi(x)=0\}\Big).
\end{aligned}$$

Now, let us compute the sum $\sum_{\beta\in\mathbb{F}_{q^r}} S_\psi(\alpha,\beta)$.

$$\begin{aligned}
\sum_{(\beta\in\mathbb{F}_{q^r}} S_\psi(\alpha,\beta) &= \frac{1}{q}\sum_{\omega\in\mathbb{F}_q}\sum_{x\in\mathbb{F}_{q^r}}\sum_{\beta\in\mathbb{F}_{q^r}} \xi_p^{Tr_{q^r/p}(\omega\alpha\psi(x)-\omega\beta x)}\\
&= \frac{q^r}{q}\sum_{\omega\in\mathbb{F}_q}\sum_{x\in\mathbb{F}_{q^r}|\omega x=0} \xi_p^{Tr_{q^r/p}(\omega\alpha\psi(x))}\\
&= q^{r-1}\Big(\sum_{x\in\mathbb{F}_{q^r}} 1 + \sum_{\omega\in\mathbb{F}_q^\star} 1\Big).\\
&= q^{r-1}\Big(q^r + q - 1\Big).
\end{aligned}$$

□

5 A new family of linear codes with few weights from weakly regular bent functions based on the first genetic construction

In this section we study a particular subclass of the previous family of linear codes considered in the previous section. We shall fix $h = 1$ and assume $\alpha \in \mathbb{F}_p$. Let then $g_{\alpha,\beta}$ be the p-ary function from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p$ given by $g_{\alpha,\beta}(x) = \alpha Tr_{p^m/p}(\Psi(x)) - Tr_{p^m/p}(\beta x)$. Note that $g_{\alpha,\beta}(x) = \alpha\psi_1(x) - Tr_{p^m/p}(\beta x)$ where ψ_a is defined as in Section 4 by $\psi_a(x) = Tr_{p^m/p}(a\Psi(x))$.
Now let us define a subcode $\mathcal{C}$ of $\mathcal{C}_\Psi$ as follows:

$$\mathcal{C} := \{\tilde{c}_{\alpha,\beta} = (g_{\alpha,\beta}(\zeta_1), g_{\alpha,\beta}(\zeta_2), \cdots, g_{\alpha,\beta}(\zeta_{p^m-1})), \alpha\in\mathbb{F}_p, \beta\in\mathbb{F}_{p^m}\}. \tag{4}$$

where $\zeta_1, \cdots, \zeta_{p^m-1}$ denote the nonzero elements of $\mathbb{F}_{p^m}$.
According to Proposition 2 (where $Tr_{q/p}$ is the identity function),

$$\begin{aligned}
wt(\tilde{c}_{\alpha,\beta}) &= p^m - \frac{1}{p}\sum_{\omega\in\mathbb{F}_p} \widehat{\chi_{\psi_{\omega\alpha}}}(\omega\beta) \\
&= p^m - p^{m-1} - \frac{1}{p}\sum_{\omega\in\mathbb{F}_p^\star} \widehat{\chi_{\psi_{\omega\alpha}}}(\omega\beta) \\
&= p^m - p^{m-1} - \frac{1}{p}\sum_{\omega\in\mathbb{F}_p^\star}\sum_{x\in\mathbb{F}_{p^m}} \xi_p^{\psi_{\omega\alpha}(x)-Tr_{p^m/p}(\omega\beta x)} \\
&= p^m - p^{m-1} - \frac{1}{p}\sum_{\omega\in\mathbb{F}_p^\star}\sum_{x\in\mathbb{F}_{p^m}} \xi_p^{Tr_{p^m/p}(\omega\alpha\Psi(x)-\omega\beta x)} \\
&= p^m - p^{m-1} - \frac{1}{p}\sum_{\omega\in\mathbb{F}_p^\star}\sum_{x\in\mathbb{F}_{p^m}} \xi_p^{\omega Tr_{p^m/p}(\alpha\Psi(x)-\beta x)} \\
&= p^m - p^{m-1} - \frac{1}{p}\sum_{\omega\in\mathbb{F}_p^\star} \sigma_\omega(\widehat{\chi_{\psi_\alpha}}(\beta)).
\end{aligned}$$

But $\widehat{\chi_{\psi_\alpha}}(\beta) = \sigma_\alpha(\widehat{\chi_{\psi_1}}(\bar{\alpha}\beta))$ where $\bar{\alpha}$ satisfies $\bar{\alpha}\alpha = 1$ in $\mathbb{F}_p$. Indeed,

$$\begin{aligned}
\sigma_\alpha(\widehat{\chi_{\psi_1}}(\bar{\alpha}\beta)) &= \sigma_\alpha\Big(\sum_{x\in\mathbb{F}_{p^m}} \xi_p^{\psi_1(x)-Tr_{p^m/p}(\bar{\alpha}\beta x)}\Big) \\
&= \sum_{x\in\mathbb{F}_{p^m}} \xi_p^{\alpha\psi_1(x)-Tr_{p^m/p}(\beta x)} \\
&= \widehat{\chi_{\alpha\psi_1}}(\beta) = \widehat{\chi_{\psi_\alpha}}(\beta).
\end{aligned}$$

Consequently,

$$wt(\tilde{c}_{\alpha,\beta}) = p^m - p^{m-1} - \frac{1}{p}\sum_{\omega\in\mathbb{F}_p^\star} \sigma_\omega(\sigma_\alpha(\widehat{\chi_{\psi_1}}(\bar{\alpha}\beta))).$$

Note that if $\alpha = 0$ then $wt(\tilde{c}_{\alpha,\beta}) = p^m - p^{m-1} - \frac{1}{p}\sum_{\omega\in\mathbb{F}_p^\star} \sigma_\omega(\widehat{\chi_{\mathbf{0}}}(\beta))$ (where $\mathbf{0}$ denotes the zero function). Since $\widehat{\chi_{\mathbf{0}}}(\beta) = \sum_{x\in\mathbb{F}_p^m} \xi_p^{-\beta x} = p^m\delta_{0,\beta}$ (where $\delta_{r,s}$ denotes the Dirac symbol defined by $\delta_{r,s} = 1$ if $s = r$ and 0 otherwise). Therefore,

$$\begin{aligned}
wt(\tilde{c}_{\alpha,\beta}) &= p^m - p^{m-1} - \frac{1}{p}\sum_{\omega\in\mathbb{F}_p^\star} \sigma_\omega(p^m\delta_{0,\beta}) \\
&= p^m - p^{m-1} - p^{m-1}(p-1)\delta_{0,\beta}.
\end{aligned}$$

Hence, we obtain $wt(\tilde{c}_{0,0}) = 0$ and for $\beta \neq 0$, $wt(\tilde{c}_{0,\beta}) = p^m - p^{m-1}$, which concludes the Hamming weight of any codeword $\tilde{c}_{0,\beta}$ in any characteristic.

Let us consider firstly the binary case, that is, the case where $p = 2$. Assume $\psi_1 := Tr_{2^m/2}(\Phi)$ is bent. Then $\widehat{\chi_{\psi_1}}(\beta) = (-1)^{\psi_1^*(\beta)} 2^{\frac{m}{2}}$. Hence, according to above, $wt(\tilde{c}_{1,\beta}) = 2^m - 2^{m-1} - \frac{1}{2}(-1)^{\psi_1^*(\beta)} 2^{\frac{m}{2}} = 2^{m-1} - (-1)^{\psi_1^*(\beta)} 2^{\frac{m}{2}-1}$.

From now on, we assume p odd and $\psi_1 := Tr_{p^m/p}(\Phi)$ is weakly regular bent. Then, by definition, we have:

$$\widehat{\chi_{\psi_1}}(\bar{\alpha}\beta) = \epsilon \sqrt{p^*}^m \xi_p^{\psi_1^*(\bar{\alpha}\beta)}.$$

Using the fact $\sigma_\alpha(\sqrt{p^*}^m) = \sigma_\alpha(\sqrt{p}^\star)^m = (\frac{\alpha}{p})^m \sqrt{p^*}^m$ and if m is even, $(\frac{\alpha}{p})^m = 1$ and $\sqrt{p^*}^m = \sqrt{p}^m$, one get

$$\begin{aligned}\sigma_\alpha(\widehat{\chi_{\psi_1}}(\bar{\alpha}\beta)) &= \epsilon \sigma_\alpha(\sqrt{p^*}^m) \xi_p^{\alpha\psi_1^*(\bar{\alpha}\beta)} \\ &= \epsilon (\frac{\alpha}{p})^m \sqrt{p^*}^m \xi_p^{\alpha\psi_1^*(\bar{\alpha}\beta)}.\end{aligned}$$

Therefore,

$$\begin{aligned}wt(\tilde{c}_{\alpha,\beta}) &= p^m - p^{m-1} - \frac{1}{p} \sum_{\omega \in \mathbb{F}_p^*} \sigma_\omega\Big(\epsilon (\frac{\alpha}{p})^m \sqrt{p^*}^m \xi_p^{\alpha\psi_1^*(\bar{\alpha}\beta)}\Big) \\ &= p^m - p^{m-1} - \frac{1}{p} \epsilon (\frac{\alpha}{p})^m \sum_{\omega \in \mathbb{F}_p^*} \sigma_\omega(\sqrt{p^*}^m) \xi_p^{\omega\alpha\psi_1^*(\bar{\alpha}\beta)} \\ &= p^m - p^{m-1} - \frac{1}{p} \epsilon (\frac{\alpha}{p})^m \sum_{\omega \in \mathbb{F}_p^*} (\frac{\omega}{p})^m \sqrt{p^*}^m \xi_p^{\omega\alpha\psi_1^*(\bar{\alpha}\beta)} \\ &= \begin{cases} p^m - p^{m-1} - \frac{1}{p}\epsilon(\frac{\alpha}{p}) \sqrt{p^*}^m \sum_{\omega \in \mathbb{F}_p^*} (\frac{\omega}{p}) \xi_p^{\omega\alpha\psi_1^*(\bar{\alpha}\beta)} & \text{if } m \text{ odd} \\ p^m - p^{m-1} - p^{\frac{m}{2}-1} \epsilon \sum_{\omega \in \mathbb{F}_p^*} \xi_p^{\omega\alpha\psi_1^*(\bar{\alpha}\beta)} & \text{if } m \text{ even.} \end{cases}\end{aligned}$$

Let us distinguish both cases.

1. Case m **odd**.

   - If $\psi_1^*(\bar{\alpha}\beta) = 0$ then (using the fact that $\sum_{\omega \in \mathbb{F}_p^*} (\frac{\omega}{p}) = 0$)

$$\begin{aligned}wt(\tilde{c}_{\alpha,\beta}) &= p^m - p^{m-1} - \frac{1}{p} \epsilon (\frac{\alpha}{p}) \sqrt{p^*}^m \sum_{\omega \in \mathbb{F}_p^*} (\frac{\omega}{p}) \\ &= p^m - p^{m-1}.\end{aligned}$$

- If $\psi_1^*(\bar{\alpha}\beta) \neq 0$ then (using in particular the evaluation of the Gauss sum: $\sum_{\omega\in\mathbb{F}_p^*}(\frac{\omega}{p})\xi_p^{\omega} = \sqrt{p^*}$)

$$\begin{aligned}
wt(\tilde{c}_{\alpha,\beta}) &= p^m - p^{m-1} - \frac{1}{p}\epsilon(\frac{\alpha}{p})\sqrt{p^*}^m \sum_{\omega\in\mathbb{F}_p^*}(\frac{\omega}{p})(\xi_p^{\omega})^{\alpha\psi_1^*(\bar{\alpha}\beta)} \\
&= p^m - p^{m-1} - \frac{1}{p}\epsilon(\frac{\alpha}{p})\sqrt{p^*}^m \sigma_{\alpha\psi_1^*(\bar{\alpha}\beta)}\Big(\sum_{\omega\in\mathbb{F}_p^*}(\frac{\omega}{p})\xi_p^{\omega}\Big) \\
&= p^m - p^{m-1} - \frac{1}{p}\epsilon(\frac{\alpha}{p})\sqrt{p^*}^m \sigma_{\alpha\psi_1^*(\bar{\alpha}\beta)}(\sqrt{p^*}) \\
&= p^m - p^{m-1} - \frac{1}{p}\epsilon(\frac{\alpha}{p})\sqrt{p^*}^m \Big(\frac{\alpha\psi_1^*(\bar{\alpha}\beta)}{p}\Big)\sqrt{p^*} \\
&= p^m - p^{m-1} - \frac{1}{p}\epsilon p^{*\frac{m+1}{2}}\Big(\frac{\psi_1^*(\bar{\alpha}\beta)}{p}\Big) \\
&= p^m - p^{m-1} - \frac{1}{p}\epsilon((\frac{-1}{p})p)^{\frac{m+1}{2}}\Big(\frac{\psi_1^*(\bar{\alpha}\beta)}{p}\Big) \\
&= p^m - p^{m-1} - \epsilon(\frac{-1}{p})^{\frac{m+1}{2}} p^{\frac{m-1}{2}}\Big(\frac{\psi_1^*(\bar{\alpha}\beta)}{p}\Big).
\end{aligned}$$

2. Case m **even**.

- If $\psi_1^*(\bar{\alpha}\beta) = 0$ then we have

$$\begin{aligned}
wt(\tilde{c}_{\alpha,\beta}) &= p^m - p^{m-1} - p^{\frac{m}{2}-1}\epsilon \sum_{\omega\in\mathbb{F}_p^*}\xi_p^{\omega\alpha\psi_1^*(\bar{\alpha}\beta)} \\
&= p^m - p^{m-1} - p^{\frac{m}{2}-1}\epsilon(p-1).
\end{aligned}$$

- If $\psi_1^*(\bar{\alpha}\beta) \neq 0$ then (since $\alpha\omega \in \mathbb{F}_p^*$) we have $\sum_{\omega\in\mathbb{F}_p}\xi_p^{\alpha\omega\psi_1^*(\bar{\alpha}\beta)} = 0$. Thus

$$\begin{aligned}
wt(\tilde{c}_{\alpha,\beta}) &= p^m - p^{m-1} - p^{\frac{m}{2}-1}\epsilon \sum_{\omega\in\mathbb{F}_p^*}\xi_p^{\omega\alpha\psi_1^*(\bar{\alpha}\beta)} \\
&= p^m - p^{m-1} + p^{\frac{m}{2}-1}\epsilon.
\end{aligned}$$

Collecting the previous results, we give in Theorem 1 the Hamming weights of the codewords of $\mathcal{C}$.

Theorem 1. *Let $\mathcal{C}$ be the linear code defined by (4) whose codewords are denoted by $\tilde{c}_{\alpha,\beta}$. Assume that the function $\psi_1 := Tr_{p^m/p}(\Psi)$ is bent or weakly regular bent if $p = 2$ or p*

odd, respectively. We denote by $\psi_1^\star$ its dual function. Then the weight distribution of $\mathcal{C}$ is given as follows. In any characteristic, $wt(\tilde{c}_{0,0}) = 0$ and for $\beta \neq 0$, $wt(\tilde{c}_{0,\beta}) = p^m - p^{m-1}$. Moreover,

1. *if $p = 2$ then the Hamming weight of $\tilde{c}_{1,\beta}$ ($\beta \in \mathbb{F}_{2^m}^\star$) is given by $wt(\tilde{c}_{1,\beta}) = 2^{m-1} - (-1)^{\psi_1^*(\beta)} 2^{\frac{m}{2}-1}$.*

2. *if p is odd then*

   - *if m is odd then the Hamming weight of $\tilde{c}_{\alpha,\beta}$ is given by*

$$\begin{cases} p^m - p^{m-1} \text{ if } \alpha \in \mathbb{F}_p^\star \text{ and } \psi_1^*(\bar{\alpha}\beta) = 0; \\ p^m - p^{m-1} - \epsilon(\frac{-1}{p})^{\frac{m+1}{2}} p^{\frac{m-1}{2}} \left(\frac{\psi_1^*(\bar{\alpha}\beta)}{p}\right) \text{ if } \alpha \in \mathbb{F}_p^\star \text{ and } \psi_1^*(\bar{\alpha}\beta) \in \mathbb{F}_{p^m}^\star. \end{cases}$$

   - *if m is even then the Hamming weight of $\tilde{c}_{\alpha,\beta}$ is given by*

$$\begin{cases} p^m - p^{m-1} - p^{\frac{m}{2}-1}\epsilon(p-1) \text{ if } \alpha \in \mathbb{F}_p^\star \text{ and } \psi_1^*(\bar{\alpha}\beta) = 0; \\ p^m - p^{m-1} + p^{\frac{m}{2}-1}\epsilon \text{ if } \alpha \in \mathbb{F}_p^\star \text{ and } \psi_1^*(\bar{\alpha}\beta) \in \mathbb{F}_{p^m}^\star. \end{cases}$$

We are now going to compute the weight distribution of $\mathcal{C}$ in the case where p is an odd prime. To this end, let us write the Walsh transform of ψ_1 as

$$\widehat{\chi_{\psi_1}}(\omega) = \epsilon u p^{\frac{m}{2}} \xi_p^{\psi_1^*(\omega)},$$

where $\epsilon \in \{-1, 1\}$ denotes the sign of the Walsh transform $\widehat{\chi_{\psi_1}}$ and $u \in \{1, i\} \in \mathbb{C}$.

The weight distribution of the code $\mathcal{C}$ is closely related to the bentness of the involved function. Let g be a weakly regular bent function over $\mathbb{F}_{p^m}$:

$$\widehat{\chi_g}(\omega) = \epsilon u p^{\frac{m}{2}} \xi_p^{g^*(\omega)}, \omega \in \mathbb{F}_{p^m},\ \epsilon = \pm 1,\ u \in \{1, i\}.$$

Then g^* is a weakly regular bent function and

$$\widehat{\chi_g}(\omega) = \epsilon u^{-1} p^{\frac{m}{2}} \xi_p^{g(-\omega)}, \omega \in \mathbb{F}_{p^m}.$$

Set

$$N_j := \#\{x \in \mathbb{F}_{p^m} \mid g(x) = j\}.$$

The following useful result shows that we are able to compute the cardinalities of the sets N_j. The values of the numbers N_j are known (see for instance [26], Theorem 2.2) for the even case). However, for the sake of completeness, we state their values in Proposition 4 translated in our framework together with a proof.

Proposition 4. *Using the above notation and assuming $g^*(0) = 0$. Then if m is even,*

$$N_0 = p^{m-1} - \epsilon p^{\frac{m}{2}-1} + \epsilon p^{\frac{m}{2}};$$
$$N_j = p^{m-1} - \epsilon p^{\frac{m}{2}-1}, 1 \leq j \leq p-1;$$

if m is odd,

$$N_0 = p^{m-1};$$
$$N_j = p^{m-1} + \epsilon p^{\frac{m-1}{2}}(\frac{j}{p}), 1 \leq j \leq p.$$

Proof. One has

$$\widehat{\chi_g}(0) = \sum_{x \in \mathbb{F}_{p^m}} \xi_p^{g(x)} = \epsilon u p^{\frac{m}{2}} \xi_p^{g^*(0)} = \sum_{j=0}^{p-1} N_j \xi_p^j$$

that is,

$$\sum_{j=0}^{p-1} N_j \xi_p^j - \epsilon u p^{\frac{m}{2}} = 0. \tag{5}$$

- If m is even, $u = 1$. Now since $\sum_{j=0}^{p-1} x^j$ is irreducible over the rational number field and since it is the minimal polynomial of ξ_p over the rational number field, we have

  $$N_j = a, 1 \leq j \leq p-1 \text{ and } N_0 - \epsilon p^{\frac{m}{2}} = N_1$$

  for some a, that is, all the N_jth are equal except for N_0 that differs from $-\epsilon p^{\frac{m}{2}}$. Now, $\sum_{j=0}^{p-1} N_j = p^m$. Hence $a + \epsilon p^{\frac{m}{2}} + (p-1)a = p^m$ from which one deduces $a = p^{m-1} -_e psilonp^{\frac{m}{2}-1}$.

- If m is odd, $u = i$. Recall now the well-known identity

  $$\sum_{j=1}^{p} (\frac{j}{p}) \xi_p^j = \begin{cases} p^{\frac{1}{2}}; & \text{if } p \equiv 1 \pmod 4; \\ ip^{\frac{1}{2}}, & \text{if } p \equiv 3 \pmod 4, \end{cases} \tag{6}$$

  that is, $\sum_{j=1}^{p} (\frac{j}{p}) \xi_p^j = up^{\frac{1}{2}}$. Equation (5) can therefore be rewritten as

  $$\sum_{j=0}^{p-1} N_j \xi_p^j - \epsilon p^{\frac{m-1}{2}} \sum_{j=1}^{p} (\frac{j}{p}) \xi_p^j = 0.$$

  By similar arguments as those used in the even case, we conclude that

  $$N_0 = N_j - \epsilon p^{\frac{m-1}{2}}(\frac{j}{p}), 1 \leq j \leq p.$$

  Now, $\sum_{j=0}^{p-1} N_j = p^m = pN_0 + \epsilon p^{\frac{m-1}{2}} \sum_{j=1}^{p} (\frac{j}{p}) = pN_0$. Thus $N_0 = p^{m-1}$.

Hamming weight	Multiplicity
0	1
$p^m - p^{m-1}$	$p^m - 1$
$p^m - p^{m-1} - \epsilon p^{\frac{m}{2}-1}(p-1)$	$p^m - p^{m-1} + \epsilon p^{\frac{m}{2}-1}(p-1)^2$
$p^m - p^{m-1} + \epsilon p^{\frac{m}{2}-1}$	$(p^m - p^{m-1})(p-1) - \epsilon p^{\frac{m}{2}-1}(p-1)^2$

Table 2: The weight distribution of $\mathcal{C}$ when m is even

Hamming weight	Multiplicity
0	1
2^{m-1}	$2^m - 1$
$2^{m-1} - 2^{\frac{m}{2}-1}$	$2^{m-1} + 2^{\frac{m}{2}-1}$
$2^{m-1} + 2^{\frac{m}{2}-1}$	$2^{m-1} - 2^{\frac{m}{2}-1}$

Table 3: The weight distribution of $\mathcal{C}$ when m is even

□

Now, using Proposition 4, we give in the following theorem the weight distribution of the code $\mathcal{C}$ when m is even in any characteristic.

Theorem 2. *Let $p = 2$ or p an odd prime. If m is even, then the weight distribution of $\mathcal{C}$ is given by Table 2 and Table 3.*

Proof. The weights comme from Theorem 1. One can easily get from Theorem 1 that there are $p^m - 1$ codewords of Hamming weight $p^m - p^{m-1}$. Set $K := \#\{(\alpha, \beta) \in \mathbb{F}_p^* \times \mathbb{F}_{p^m} \mid \psi_1^*(\bar{\alpha}\beta) = 0\}$ and $N_0 := \{\gamma \in \mathbb{F}_{p^m} \mid \psi_1^*(\gamma) = 0\}$. Clearly, $K = (p-1)N_0$ and $(p-1)(p^m - N_0) = \#\{(\alpha, \beta) \in \mathbb{F}_p^* \times \mathbb{F}_{p^m} \mid \psi_1^*(\bar{\alpha}\beta) \neq 0\}$. Now, according to Proposition 4, $N_0 = p^m - \epsilon p^{\frac{m}{2}-1} + \epsilon p^{\frac{m}{2}}$. Thus,

$$\begin{aligned} K &= (p-1)(p^{m-1} + \epsilon p^{\frac{m}{2}-1}(p-1)) \\ &= p^m - p^{m-1} + \epsilon p^{\frac{m}{2}-1}(p-1)^2, \end{aligned}$$

and

$$\begin{aligned} (p-1)(p^m - N_0) &= (p-1)(p^m - p^{m-1} - \epsilon p^{\frac{m}{2}-1}(p-1)) \\ &= (p^m - p^{m-1})(p-1) - \epsilon p^{\frac{m}{2}-1}(p-1)^2. \end{aligned}$$

Now, according to Theorem 1, the number of codewords of Hamming weight $p^m - p^{m-1} - \epsilon p^{\frac{m}{2}-1}(p-1)$ is equal to $p^m - p^{m-1} + \epsilon p^{\frac{m}{2}-1}(p-1)^2$ and the number of codewords of Hamming weight $p^m - p^{m-1} + \epsilon p^{\frac{m}{2}-1}$ is equal to $(p^m - p^{m-1})(p-1) - \epsilon p^{\frac{m}{2}-1}(p-1)^2$. □

Hamming weight	Multiplicity
0	1
$p^m - p^{m-1}$	$2p^m - p^{m-1} - 1$
$p^m - p^{m-1} - \epsilon(\frac{-1}{p})^{\frac{m+1}{2}} p^{\frac{m-1}{2}}$	$(p^{m-1} + \epsilon p^{\frac{m-1}{2}})\frac{(p-1)^2}{2}$
$p^m - p^{m-1} + \epsilon(\frac{-1}{p})^{\frac{m+1}{2}} p^{\frac{m-1}{2}}$	$(p^{m-1} - \epsilon p^{\frac{m-1}{2}})\frac{(p-1)^2}{2}$

Table 4: The weight distribution of $\mathcal{C}$ when m is odd

Theorem 3. *Let p be an odd prime. If m is odd, then the weight distribution of $\mathcal{C}$ is given by Table 4.*

Proof. Let us take again similar notations as those used in the proof of Theorem 2. Set $K := \#\{(\alpha, \beta) \in \mathbb{F}_p^* \times \mathbb{F}_{p^m} \mid \psi_1^*(\bar{\alpha}\beta) = 0\}$ and $N_j := \{\gamma \in \mathbb{F}_{p^m} \mid \psi_1^*(\gamma) = j\}$. According to Theorem 1, the number of codewords of weight $p^m - p^{m-1}$ is equal to $p^m - 1 + K = p^m - 1 + (p-1)N_0$ while the number of codewords of Hamming weight $p^m - p^{m-1} - \epsilon(\frac{-1}{p})p^{\frac{m-1}{2}}$ and of Hamming weight $p^m - p^{m-1} + \epsilon(\frac{-1}{p})p^{\frac{m-1}{2}}$ are equal respectively to $\sum_{j\in\{1,\cdots,p-1\},(\frac{j}{p})=1} N_j$ and $\sum_{j\in\{1,\cdots,p-1\},(\frac{j}{p})=-1} N_j$. According to Proposition 4,

$$p^m - 1 + (p-1)N_0 = p^m - 1 + (p-1)(p^{m-1}) = 2p^m - p^{m-1} - 1;$$

$$\begin{aligned}\sum_{j\in\{1,\cdots,p-1\},(\frac{j}{p})=1} N_j &= \sum_{j\in\{1,\cdots,p-1\},(\frac{j}{p})=1} (p-1)(p^{m-1} + \epsilon p^{\frac{m-1}{2}}) \\ &= (p^{m-1} + \epsilon p^{\frac{m-1}{2}})(\frac{p-1}{2})(p-1);\end{aligned}$$

and

$$\begin{aligned}\sum_{j\in\{1,\cdots,p-1\},(\frac{j}{p})=-1} N_j &= \sum_{j\in\{1,\cdots,p-1\},(\frac{j}{p})=-1} (p-1)(p^{m-1} - \epsilon p^{\frac{m-1}{2}}) \\ &= (p^{m-1} - \epsilon p^{\frac{m-1}{2}})(\frac{p-1}{2})(p-1).\end{aligned}$$

□

6 Concluding remarks

The paper is a contribution to the knowledge of codes from weakly bent functions with few weights. The general idea of the construction is a classical one but our specific choice of the function employed is new. Our codes are different from those studied in literature [18, 19, 33] due to the differences in the lengths and dimensions. Moreover, we notice that

our codes have dimension $m+1$, they have the same weight distribution as a subcode of some of the codes in [4] when $p=2$ and the same weight distribution as a subcode of some of the codes in [6, 36] when p is odd.

References

[1] R. Anderson, C. Ding, T. Helleseth, and T. Klve. How to build robust shared control systems. *Designs, Codes Cryptography*, vol. 15, no. 2, pages 111-124, 1998.

[2] A. R. Calderbank and J. M. Goethals. Three-weight codes and association schemes. *Philips J. Res.*, vol. 39, pages 143-152, 1984.

[3] A. R. Calderbank and W. M. Kantor. The geometry of two-weight codes. *Bull. London Math. Soc.*, vol. 18, pages 97-122, 1986.

[4] A. Canteaut, P. Charpin and H. Dobbertin, Weight divisibility of cyclic codes, highly nonlinear functions on $GF(2^m)$, and crosscorrelation of maximum-length sequences, *SIAM J. Discrete Math.*, vol. 13, pages 105–137, 2000

[5] C. Carlet, P. Charpin and V. Zinoviev, Codes, bent functions and permutations suitable for DES-like cryptosystems, *Designs, Codes and Cryptography*, vol. 15, pages 125–156, 1998.

[6] C. Carlet, C. Ding, and J. Yuan. Linear codes from perfect nonlinear mappings and their secret sharing schemes. *IEEE Trans. Inform. Theory*, vol. 51, no.6, pages 2089-2102, 2005.

[7] C. Carlet and S. Mesnager. Four decades of research on bent functions. Journal Designs, Codes and Cryptography. To appear.

[8] S.-T. Choi, J.-Y. Kim, J.-S. No, and H. Chung. Weight distribution of some cyclic codes. *IEEE Int. Symp. Inf. Theory*, pages. 2901-2903, 2012.

[9] G. Cohen, S. Mesnager and A. Patey On Minimal and quasi-minimal linear codes. *Proceedings of Fourteenth International Conference on Cryptography and Coding*, Oxford, United Kingdom, IMACC 2013, LNCS 8308, pages 85-98. Springer, Heidelberg, 2013.

[10] G. Cohen and S. Mesnager. On Minimal and Almost-Minimal Linear Codes. *Proceedings of the 21st International Symposium on Mathematical Theory of Networks and Systems* (MTNS 2014), Session "Coding theory", pages 928-931, Groningen, Netherlands, 2014.

[11] G. Cohen and S. Mesnager. Variations on Minimal Linear Codes. *Proceedings of the 4th International Castle Meeting on coding theory and Application*Series: CIM Series in Mathematical Sciences, Vol. 3, Springer-Verlag, pages 125-131, 2015.

[12] G. Cohen, S. Mesnager and H. Randriambololona. Yet another variation on minimal linear codes. *Journal Advances in Mathematics of Communications* (AMC). To appear.

[13] B. Courteau and J.Wolfmann. On triple-sum-sets and two or three weights codes. *Discrete Math.*, vol. 50, pages 179-191, 1984.

[14] P. Delsarte. On triple-sum-sets and two or three weights codes. *IEEE Trans. Inf. Theory*, 21(5) pages 575-576, 1975.

[15] J. Dillon. *Elementary Hadamard difference sets.* PhD thesis, University of Maryland, 1974.

[16] C. Ding. Linear codes from some 2-Designs *IEEE Transactions on Information Theory* 61(6), pages 3265-3275, 2015.

[17] C. Ding. A Construction of binary linear codes from Boolean functions *arXiv:1511.00321v1*, 2015.

[18] K. Ding and C. Ding. Binary linear codes with three weights. *IEEE Communications Letters* 18(11), pages 1879-1882, 2014.

[19] K. Ding and C. Ding. A Class of two-weight and three-weight codes and their applications in secret sharing. *IEEE Transactions on Information Theory* 61(11), pages 5835-5842, 2015.

[20] C. Ding, C. Li, N. Li, and Z. Zhou. Three-weight cyclic codes and their weight distributions. Preprint.

[21] C. Ding, J. Luo, and H. Niederreiter. Two weight codes punctured from irreducible cyclic codes. *Proc. 1st Int. Workshop Coding Theory Cryp- tography, Y. Li, S. Ling, H. Niederreiter, H. Wang, C. Xing, and S. Zhang, Eds., Singapore*, pages 119-124, 2008.

[22] C. Ding and X. Wang. A coding theory construction of new systematic authentication codes. *Theoretical Comput. Sci.*, vol. 330, no. 1, pages 81-99, 2005.

[23] K. Feng and J. Luo. Value distribution of exponential sums from perfect nonlinear functions and their applications. *IEEE Trans. Inf. Theory*, vol. 53, no. 9, pages 3035-3041, 2007.

[24] T. Helleseth and A. Kholosha. Monomial and quadratic bent functions over the finite fields of odd characteristic. *IEEE Transactions on Information Theory*, 52(5), pages 2018- 2032, 2006.

[25] T. Helleseth and A. Kholosha. New binomial bent functions over the finite fields of odd characteristic. *IEEE Transactions on Information Theory* 56(9), pages 4646-4652, 2010.

[26] T. Helleseth and A. Kholosha. Bent functions and their connections to combinatorics. *Surveys in Combinatorics 2013*, Cambridge University Press, pages 91-126, 2013.

[27] Z. Heng and Q. Yue Several class of cyclic codes with either optimal three weights or a few weights. *arxiv.org/pdf/1510.05355*, 2015.

[28] H. D. L. Hollmann and Q. Xiang A proof of the Welch and Niho conjectures on cross-correlations of binary m-sequences. *Finite Fields Appl.*, Cambridge University Press, pages 253-286, 2001.

[29] P.V. Kumar, R.A. Scholtz and L.R. Welch. Generalized bent functions and their properties. *Journal of Combinatorial Theory, Series A* 40, pages 90-107, 1985.

[30] C. Li, Q. Yue, and F. Li. Hamming weights of the duals of cyclic codes with two zeros. *IEEE Trans. Inf. Theory,* vol. 60, no. 7, pages 3895-3902, 2014.

[31] S. Mesnager. Bent functions: fundamentals and results. Springer, New-York, 2016. To appear.

[32] O. S. Rothaus. On "bent" functions. *Journal of Combinatorial Theory, Series A*, 20, pages 300-305, 1976.

[33] C. Tang, N. Li, Y. Qi, Z. Zhou and T. Helleseth Linear codes with two or three weights from weakly regular bent functions. *ArXiv: 1507.06148v3*, 2015.

[34] G. Xu and X. Cao Linear codes with two or three weights from some functions with low Walsh spectrum in odd characteristic. *arXiv:1510.01031*, 2015.

[35] Y. Xia, T. Helleseth, and C. Li Some new classes of cyclic codes with three or six weights. *Adv. in Math. of Comm.*, 9(1), pages 23-36, 2015.

[36] J. Yuan, C. Carlet and C. Ding, The weight distribution of a class of linear codes from perfect nonlinear functions, *IEEE Trans. Information Theory*, Vol. 52, No. 2, pages 712–717, Feb. 2006.

[37] J. Yuan and C. Ding. Secret sharing schemes from three classes of linear codes. *IEEE Trans. Inf. Theory*, vol. 52, no. 1, pages 206-212, 2006.

[38] X. Zeng, L. Hu, W. Jiang, Q. Yue, and X. Cao. The weight distribution of a class of p-ary cyclic codes. *Finite Fields Appl.,* vol. 16, no. 1, pages 56-73, 2010.

[39] Z. Zhou and C. Ding. A class of three-weight codes. *Finite Fields Appl.,* vol. 25, pages 79-93, 2014.

[40] Z. Zhou, N. Li, C. Fan, and T. Helleseth Linear Codes with two or three weights from quadratic bent functions. *ArXiv: 1506.06830v1*, 2015.