AAECC (2018) 29:513–528
https://doi.org/10.1007/s00200-018-0354-2

ORIGINAL PAPER

Three-weight codes and near-bent functions from two-weight codes

J. Wolfmann[1]

Received: 30 September 2016 / Revised: 8 March 2017 / Accepted: 6 June 2017 /
Published online: 4 April 2018

Abstract We introduce a construction of binary 3-weight codes and near-bent functions from 2-weight projective codes.

Keywords 2-weight codes · 3-weight codes · Near-bent functions

1 Introduction

In a recent paper [19] it is mentioned that linear codes with few weights have applications in secrete sharing, authentication codes, association schemes and strongly regular graphs. These codes were the topic of several recent papers [5,11,18,19].

On the other hand, bent functions and near-bent functions are boolean functions interesting for coding theory, cryptology and well-correlated binary sequences and were the topic of a lot of works (for instance see [1,4,6,10,12,14–16]).

In this paper we introduce in the binary case a construction of 3-weight codes from every 2-weight code, with one exception (in [19] such a construction is restricted to codes from quadratic bent functions).

Furthermore we deduce a construction of near-bent functions always from 2-weight binary codes.

The paper is organized as follows:

In Sect. 2 we recall classical definitions on boolean functions and binary linear codes and we specify the vocabulary used in the paper. Further more, a new definition is introduced in Sect. 2.3. Section 3 is devoted to 1-weight and 2-weight binary codes. Useful results and examples are given with references and sometimes proofs are given

✉ J. Wolfmann
wolfmann@univ-tln.fr

1 IMATH (IAA), Université de Toulon, CS 60584, 83041 Toulon Cedex 9, France

for sake of convenience. Section 4 contains the main result with its proof and examples. In Sect. 5 we deduce near-bent functions from special 2-weight codes.

2 Preliminaries

$\mathbb{F}_2$ is the finite field of order 2 and an m-boolean function is a map from $\mathbb{F}_2^m$ to $\mathbb{F}_2$. As usual, in order to benefit from the properties of a finite field we identify the $\mathbb{F}_2$-vector space $\mathbb{F}_2^m$ with the finite field $\mathbb{F}_{2^m}$. We denote $\mathbb{F}_{2^k} \setminus \{0\}$ by $\mathbb{F}_{2^k}^*$.

The weight of a m-boolean function f is the number of x in $\mathbb{F}_{2^m}$ such that $f(x) = 1$.

The Fourier transform (or Walsh transform) $\hat{f}$ of an m-boolean function f is the map from $\mathbb{F}_{2^m}$ into $\mathbb{Z}$ defined by:

$$\hat{f}(v) = \sum_{x \in \mathbb{F}_{2^m}} (-1)^{f(x)+tr(vx)}$$

where tr is the trace of $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$. $\hat{f}(v)$ is called the Fourier coefficient of f at the point of v.

Notation: If $e \in \mathbb{F}_{2^m}$ then $t_e(x) = tr(ex)$ where tr is the trace of $\mathbb{F}_{2^m}$.
It is well-known and easy to prove that:

$$\hat{f}(0) = -2(2^{k-1} - n) \quad \text{and} \quad \text{if } v \neq 0,\ \hat{f}(v) = -2(n - 2w_v)$$

where n is the weight of f and w_v is the weight of $f * t_v$ where $*$ is the product of boolean functions.

2.1 Bent and near-bent functions

A m-boolean function F is bent if all its Fourier coefficients are in $\{-2^{m/2}, 2^{m/2}\}$.

F is near-bent if all its Fourier coefficients are in $\{-2^{(m+1)/2}, 0, 2^{(m+1)/2}\}$.

Since the Fourier coefficients are in $\mathbb{Z}$, bent functions exist only when m is even and near-bent functions exist only when m is odd.

If $m = 2t - 1$ then F is a near-bent function if all its Fourier coefficients are in $\{-2^t,\ 0,\ 2^t\}$.

The distribution of the Fourier coefficients of a $(2t - 1)$-near bent function f is well known (see [1, Proposition 4]).

$\hat{f}(v) = 2^t$ number of v: $2^{2t-3} + (-1)^{f(0)} 2^{t-2}$
$\hat{f}(v) = 0$ number of v: 2^{2t-2}
$\hat{f}(v) = -2^t$ number of v: $2^{2t-3} - (-1)^{f(0)} 2^{t-2}$.

2.2 Binary linear codes

We assume that the reader is familiar with the classical definitions and results of the theory of algebraic coding (see [7,9]).

Recall first classical definitions.

Definition 1 Let C be a binary linear code of dimension k and length n. Let B_1 and B_2 respectively the number of words with weight 1 and the number of words with weight 2 in the orthogonal of C.

(1) C is said to be a projective code if $B_1 = 0$ and $B_2 = 0$.
(2) If $B_2 = 0$:

- A sub-set $E = \{e_1, e_2, \ldots, e_n\}$ of $\mathbb{F}_{2^k}^*$ is said to be a support of C if

$$C = \{m_a = (tr(ae_1), tr(ae_2), \ldots tr(ae_n)) \mid a \in \mathbb{F}_{2^k}\}$$

  where tr is the trace of $\mathbb{F}_{2^k}$.
- If $m_a = (tr(ae_1), tr(ae_2), \ldots tr(ae_n))$ is a word of C then the support of m_a is supp(m_a)=$\{e_i \mid tr(ae_i) = 1\}$.
- A defining function of C is a k-boolean function indicator of a support of C.

If G is a generator matrix of C then $B_2 = 0$ means that the columns of G are two by two distinct and $B_1 = 0$ means that there is no zero vector in the set of columns of G.

Example: Let G be a generator matrix of a binary linear code C with $B_2 = 0$: If $\bar{c}_i$ is a column of G then let e_i be the element of $\mathbb{F}_{2^{2t}}$ such that $\bar{c}_i$ is the system of components of e_i with respect to a given basis of $\mathbb{F}_{2^{2t}}$. Then the set $\{e_i\}_{i=1\ldots N}$ is a support of C.

Example:

$$G = \begin{matrix} 1, & \alpha^{24}, & \alpha^{28}, & \alpha^{22}, & \alpha^{5}, & \alpha^{16}, & \alpha^{26} \\ 0, & 1, & 1, & 1, & 0, & 1, & 1 \\ 0, & 1, & 0, & 0, & 0, & 1, & 0 \\ 0, & 1, & 1, & 1, & 1, & 0, & 1 \\ 0, & 1, & 1, & 0, & 0, & 1, & 1 \\ 1, & 0, & 0, & 1, & 1, & 1, & 1 \end{matrix}$$

With $\mathbb{F}_{2^5} = \mathbb{F}_2(\alpha)$ and $\alpha^5 + \alpha^2 + 1 = 0$, the support of C obtained by the columns of G is:

$$\{1, \alpha^5, \alpha^{16}, \alpha^{22}, \alpha^{24}, \alpha^{26}, \alpha^{28}\}.$$

A defining function of C is:

$$tr(a^6x + a^{10}x^3 + a^{13}x^5 + a^8x^7 + a^{27}x^{11} + a^{11}x^{15} + x^{31})$$

where tr is the trace of $\mathbb{F}_{2^5}$.

Remark 2 – Of course, a binary linear code with $B_2 = 0$ has several supports and several defining functions depending of the choice of the generator matrix and the choice of the basis of $\mathbb{F}_{2^{2t}}$. However all the supports are equivalent under the action of the linear group of $\mathbb{F}_{2^k}$.

– A binary projective linear code is completely determined by one of its defining functions and every boolean function f such that $f(0) = 0$ defines a binary projective linear code.

Definition 3 If E is a support of a binary projective code C of dimension k then the complement code of C is the code whose support is $\mathbb{F}_{2^k}^* \setminus E$.

The proof of the next proposition is obvious.

Proposition 4 *The complement code of C is a projective code.*

The weights of a complement of C are the $2^{k-1} - w_i$ where the w_i are the weights of C.

2.3 Doubly restricted code

Now we introduce a new definition.

We restrict any binary projective code of dimension k to one of its $k-1$ subspace defined by a word m and we restrict the new code to the support of m.

Definition 5 Let C be a binary linear code of dimension k. Let m be a word of C.

- The restricted code of C with respect to m is the complementary space of $\{0, m\}$ in C denoted by C_m.
- The doubly restricted code of C with respect to m is the restricted code of C_m to the support of m. It is denoted by $\tilde{C}_m$.

2.3.1 Generator matrices

G, G_m, $\tilde{G}_m$ are respectively generator matrix of C, C_m, $\tilde{C}_m$. The rows of G form a basis of C with m as first row.

$$G = \begin{pmatrix} m^{(1)}, & m^{(2)}, & m^{(3)}, & \ldots\ldots & m^{(i)}, \ldots & , m^{(n)} \\ \bar{v}_1, & \bar{v}_2, & \bar{v}_3, & \ldots\ldots & \bar{v}_i\ , \ldots & \bar{v}_n \end{pmatrix}$$

where $m = (m^{(1)}, m^{(2)}, m^{(3)}, \ldots\ldots m^{(i)}, \ldots, m^{(n)})$ and $\bar{v}_i$ stands for a binary column vector of length $k-1$.

Deleting the first row of G we get a generator matrix of C_m.

$$G_m = (\bar{v}_1, \bar{v}_2, \bar{v}_3, \ldots\ldots\ldots \bar{v}_i, \ldots, \bar{v}_n)$$

In order to obtain a generator matrix of $\tilde{C}_m$ we restrict the columns of G_m to the support of m.

$$\tilde{G}_m = (\bar{v}_{i_1}, \bar{v}_{i_2} \ldots \bar{v}_{i_w})$$

where $m^{(i_1)}, m^{(i_2)}, \ldots m^{(i_w)}$ are the non-zero components of m.

Example:

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

$$G_m = \begin{pmatrix} 1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&1&0&0&0&1&0&1&1&1&0&1&1&0&0&0\\ 0&0&1&1&0&1&0&1&0&1&0&0&0&0&1&0&0&1&1&0&0\\ 0&0&0&0&1&1&0&0&0&0&1&1&0&0&0&1&1&0&1&1&0\\ 0&0&1&0&0&0&1&0&0&0&0&0&1&1&0&1&0&1&0&1&1 \end{pmatrix}$$

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

3 1-Weight and 2-weight codes

If $\mathcal{N} \in \mathbb{N}\setminus\{0\}$ then a code C is an $\mathcal{N}$-weight code if $\mathcal{N}$ is the cardinality of the set of non-zero weights of C.

First recall the first three Pless identities which are the main tool to prove results in this section.

3.1 Pless identities

The Pless identities are well-known. We recall the first three identities in the binary case (see [8, Section II, page 50]).

Proposition 6 *Let C be a binary linear code of length n, dimension k and with N weights w_i, $i = 1, 2, \ldots, N$.*
A_{w_i} is the number of words of C with weight w_i and B_i is the number of words of C with weight i in the orthogonal of C respectively.
Then:

(1) $\sum_{i=1}^{N} A_{w_i} = 2^k - 1.$
(2) $\sum_{i=1}^{N} w_i A_{w_i} = (n - B_1)2^{k-1}.$
(3) $\sum_{i=1}^{N} w_i^2 A_{w_i} = \{n(n+1) - 2nB_1 + 2B_2\}2^{k-2}.$

The following Proposition 7 and Corollary 8 are well known. Proposition 10 was already published in [13]. The proofs are given here for reader's convenience.

3.2 Binary 1-weight codes

Proposition 7 *If C is a binary linear 1-weight code of length n dimension k with w as unique non-zero weight then there exists* $\lambda \in \mathbb{N}$ *such that:*

$$n - B_1 = \lambda(2^k - 1) \quad and \quad w = \lambda 2^{k-1}.$$

Proof In this case the second Pless identity is:

$$(2^k - 1)w = (n - B_1)2^{k-1}.$$

Since 2^{k-1} and $2^k - 1$ are coprime then 2^{k-1} divides w.
We obtain $w = \lambda 2^{k-1}$ and consequently $n - B_1 = \lambda(2^k - 1)$. □

Corollary 8 *If C is a binary projective 1-weight code of length n dimension k with w as unique non-zero weight then:*

$$n = 2^k - 1 \quad and \quad w = 2^{k-1}.$$

Proof The proof is obvious. □

The following definition is classical.

Definition 9 (*Simplex code*) The previous result shows that a defining set of such a code is $\mathbb{F}_{2^k} \setminus \{0\}$. It is called a binary Simplex code of length $2^k - 1$

3.3 Binary 2-weight codes

For further use we need the following propositions.

Proposition 10 *Let C be a binary 2-weight code of length n, dimension k and weight* w_1 *and* w_2.

(a) Define $F(n, w_1, w_2, k) = n^2 - [2(w_1 + w_2) - 1]n + \frac{(2^k-1)w_1 w_2}{2^{k-2}}$.
(4) If C is a projective code then $F(n, w_1, w_2, k) = 0$.
(b) Let A_{w_1} *and* A_{w_2} *be respectively the numbers of words of weights* w_1 *and* w_2. *Then:*
(5) $A_{w_1} = \frac{(2^k-1)w_2-(n-B_1)2^{k-1}}{w_2-w_1}$
(6) $A_{w_2} = \frac{(n-B_1)2^{k-1}-(2^k-1)w_1}{w_2-w_1}$
where B_1 *is the number of words of weight* 1 *in the orthogonal of* C.

Proof • Proof of (a):
Since C is projective then $B_1 = B_2 = 0$ and the first Pless identities are:

(1′) $A_{w_1} + A_{w_2} = 2^k - 1.$

(2′) $w_1 A_{w_1} + w_2 A_{w_2} = n2^{k-1}.$

(3′) $w_1^2 A_{w_1} + w_2^2 A_{w_2} = n(n+1)2^{k-2}$.

Let consider the following polynomial over $\mathbb{Z}$:

$$(x - w_1)(x - w_2) = a_0 + a_1 x + x^2.$$

We know that $a_0 = w_1 w_2$ and $a_1 = -(w_1 + w_2)$.

The combination $a_0(1') + a_1(2') + (3)$ gives:

$$A_{w_1}(a_0 + a_1 w_1 + w_1^2) + A_{w_2}(a_0 + a_1 w_2 + w_2^2) = a_0(2^k - 1) + a_1 n 2^{k-1} + n(n+1)2^{k-2}.$$

From the definition of a_0 and a_1: $a_0 + a_1 w_1 + w_1^2 = a_0 + a_1 w_2 + w_2^2 = 0$.

And this leads to the expected result.

- Proof of (b):

The result is obtained by solving the linear system of identities (1′) and (2′). □

The following lemma was proved by Delsarte.

Lemma 11 (Delsarte) *If w_1 and w_2 are the weights of a binary projective 2-weight code then there exist $a \in \mathbb{N}^*$ and $r \in \mathbb{N}$ such that*

$$w_1 = a2^r \text{ and } w_2 = (a+1)2^r.$$

Proof See [3, Section 3, Corollary 2, page 53]. □

3.4 Semi-primitive code

Definition 12 Let C be an irreductible cyclic code of length n over $\mathbb{F}_q$ with $(n, q) = 1$. Let $\mathbb{F}_{q^k}$ be the splitting field of $x^n - 1$ over $\mathbb{F}_q$ and let d such that $nd = q^k - 1$ and $d \geq 2$.

C is called a semi-primitive code if $k = 2t$ and if there exists a divisor r of t such that $q^r \equiv -1 \mod d$.

Proposition 13 *Let C be a semi-primitive code and let k, r, t, d be defined as above. The weight distribution of C is:*

- *$n(d-1)$ words of weight $w_1 = (q-1)q^{t-1}\left[\frac{q^t - \epsilon}{d}\right]$.*
- *n words of weight $w_2 = (q-1)q^{t-1}\left[\frac{q^t + \epsilon(d-1)}{d}\right]$.*

where $\epsilon = (-1)^{\frac{t}{r}}$.

Proof See [2,9]. □

3.5 A special case

The first proposition below was proved in [17] and the second one seems to be new.

Proposition 14 *If the support E of a binary projective code C of dimension k is the complement of a subspace S and if the dimension of S is s then:*

(a) The length of C is $n = 2^k - 2^s$
(b) The weight distribution C is:

$2^{k-s} - 1$ *words of weight* 2^{k-1}
$2^k - 2^{k-s}$ *words of weight* $2^{k-1} - 2^{s-1}$.

Proof Let n be the length of C and let m_a be a word of C.

$m_a = (tr(ae_1), tr(ae_2), \dots tr(ae_n))$ with $a \in \mathbb{F}_{2^k}$.
$\bar{m}_a = (tr(a\bar{e}_1), tr(a\bar{e}_2) \dots tr(a\bar{e}_{2^s-1}))$ where $\{\bar{e}_1, \bar{e}_2, \dots \bar{e}_{2^s-1}\} = S$.

The concatenation of m_a and $\bar{m}_a$ is a word of the Simplex code of length $2^k - 1$ whence its weight is 2^{k-1}.

(1) If the hyperplane H_a of $\mathbb{F}_{2^k}$ with equation $tr(ax) = 0$ contains S then the weight of $\bar{m}_a$ is 0 and then the weight of m_a is $2^k - 1$. There exist $2^{k-s} - 1$ such hyperplanes.
(2) If S is not in H_a then $H_a \cap S$ contains 2^{s-1} elements of S and the weight of m_a is $2^{k-1} - 2^{s-1}$ and we have $2^k - 2^{k-s}$ words of this type.

□

Proposition 15 *If a projective code C of dimension k is a 2-weight code and if one of the weights is 2^{k-1} then a support of C is a complement of a subspace.*

Proof Let n be the length of C and let $\bar{C}$ be the complement of C. The length of $\bar{C}$ is $\bar{n} = 2^k - 1 - n$.

If the weights of C are $w_1 = 2^{k-1}$ and w_2 then $w_2 < 2^{k-1}$ and the weights of $\bar{C}$ are $2^{k-1} - w_1 = 0$ and $2^{k-1} - w_2$. Hence $\bar{C}$ is a 1-weight code with weight $2^{k-1} - w_2$. Then $\bar{C}$ is a 1-weight projective code and according to Corollary 8 there exists r such that $\bar{n} = 2^r - 1$ and $\mathbb{F}_{2^r} \setminus \{0\}$ is a defining set of $\bar{C}$. In other words C is the complement set of a subspace. □

4 3-Weight codes from binary 2-weight codes

The next theorem is the main result of this work.

Notation:

- If E is a set then $\mid E \mid$ denotes the cardinality of E.
- For $i = 1, 2$ E_i is the set of words of weight w_i in C and $\mathcal{A}_i$ is the cardinality of E_i.
- E_i^m is the set of words of weight w_i in C_m and $\mathcal{A}_i^m$ is the cardinality of E_i^m.
- B_1^m is the number of words of weight 1 in the orthogonal of C_m.

Remark 16 B_1^m is also the number of zero-vectors among the columns of a generator matrix of C_m. This number is independent of the choice of such a generator matrix.

We now use the generator matrix introduced in Sect. 2.3.1. Note that $\bar{0}$ is a column of G_m if and only if $\binom{1}{\bar{0}}$ or $\binom{0}{\bar{0}}$ is a column of G.

Because C is a projective code then $\binom{0}{\bar{0}}$ is not a column of G and $\binom{1}{\bar{0}}$ can be a column of G at most once. Conclusion:

$\mathcal{R}_1$: $B_1^m = 0$ or $B_1^m = 1$.

On the other hand, $\bar{v}_{i_l}$ is a column of $\tilde{G}_m$ if and only if $\binom{1}{\bar{v}_{i_l}}$ is a column of G. Since C is projective then:

$\mathcal{R}_2$: The $\bar{v}_{i_l}$ $l = 1, 2, \ldots w$ are distinct and $\bar{v}_{i_l} = \bar{0}$ at most once.

Theorem 17 *Let C be a binary projective 2-weight code of dimension k with weights w_1 and w_2. Let m be a word of C with weight w. Let E be a support of C.*

If E is not the complement of a subspace then:

The doubly restricted code $\tilde{C}_m$ of C is a projective three-weight code of length w and dimension $k-1$ and the weights of $\tilde{C}_m$ are:

$$\frac{1}{2}\left[w-(w_1-w_2)\right], \quad \frac{1}{2}w, \quad \frac{1}{2}\left[w+(w_1-w_2)\right].$$

Proof From the definition the weights of $\tilde{C}_m$ are the cardinalities of the intersections of $supp(m)$ with the supports of the words of C_m. In other words they are:

$w(m_1 * m)$ where $m_1 \in E_1^m$ and $w(m_2 * m)$ where $m_2 \in E_2^m$.

Since $w(m_1+m) = w(m_1) + w(m) - 2w(m_1 * m)$ and $w(m_2+m) = w(m_2) + w(m) - 2w(m_2 * m)$, we have:

$w(m_1 * m) = \frac{1}{2}[w(m_1) + w(m) - w(m_1+m)]$ and similarly:
$w(m_2 * m) = \frac{1}{2}[w(m_2) + w(m) - w(m_2+m)]$.

Consequently

(a) If there exists $m_1 \in E_1^m$ such that $m_1 + m \in E_1$ then
$w(m_1 * m) = \frac{1}{2}w(m)$.
(b) If there exists $m_1 \in E_1^m$ such that $m_1 + m \in E_2$ then
$w(m_1 * m) = \frac{1}{2}[w(m) + (w_1 - w_2)]$.
(c) If there exists $m_2 \in E_2^m$ such that $m_2 + m \in E_1$ then
$w(m_2 * m) = \frac{1}{2}[w(m) - (w_1 - w_2)]$.
(d) If there exists $m_2 \in E_2^m$ such that $m_2 + m \in E_2$ then
$w(m_2 * m) = \frac{1}{2}w(m)$.

Conclusion: the weights of $\tilde{C}_m$ belong to the set:

$$\left\{\frac{1}{2}[w-(w_1-w_2)], \frac{1}{2}w, \frac{1}{2}[w+(w_1-w_2)\right\}.$$

We are now facing the problem to search if the cases (a), (b), (c), (d) effectively exist.

First remark, from the definition of C_m, that:

$(*)\quad C = C_m + (m + C_m)$ and,

since m is not in C_m:

$(**)\quad C_m \cap (m + C_m) = \emptyset$.

For $i, j \in \{1, 2\}$, define $E_{(i,j)}$ as the set of words with weight w_j in $(m + E_i^m)$.

Our task is to prove that, with one exception, properties (a), (b), (c), (d) are satisfied or, equivalently that $E_{(1,1)},\ E_{(2,1)},\ E_{(1,2)},\ E_{(2,2)}$ are not empty.

Our strategy now is to examine what happen when such sets are not empty.

Step 1

Case 1 : $E_{(1,1)} = \emptyset,\ E_{(2,1)} = \emptyset$

In this case there is no word of weight w_1 in $m + C_m$. Therefore the words of weight w_1 in C are the elements of E_i^m and w if $w = w_1$. Thus:

$\mathcal{A}_1 = \mathcal{A}_1^m + \epsilon$ with $\epsilon = 1$ if $w = w_1$ and $\epsilon = 0$ if $w = w_2$.

We find from (5) and (6) of Proposition 10:

$(\Diamond)\quad (2^{k-1} - \epsilon)w_2 + \epsilon w_1 - \left(n - B_1^m\right) 2^{k-2} = 0.$

- If $\epsilon = 0$ and $B_1^m = 0$:
  $(\Diamond)$ gives $2w_2 = n$ and with (4) of Proposition 10 we obtain $(2^k - 1)w_1 = (2w_1 - 1)2^{k-1}$. Since $2w_1 - 1 \neq 0$ and because $2^k - 1$ and 2^{k-1} are coprime then 2^{k-1} divides w_1 and thus $w_1 = \mu 2^{k-1}$. The case $\mu \geq 2$ is not possible since $w_1 \leq 2^{k-1}$ and therefore $w_1 = 2^{k-1}$. According to Proposition 15, E is the complement of a subspace.
- If $\epsilon = 0$ and $B_1^m = 1$:
  With $(\Diamond)$ we have $2w_2 = n + 1$. Using (4) we have: $w_1(2^k - 1 - n) = 0$. If $2^k - 1 - n = 0$ then C is the simplex code (see Definition 9), which is not a 2 weight code. Hence $w_1 = 0$ which is not possible.
- If $\epsilon = 1$ and $B_1^m = 0$:
  $(\Diamond)$ gives $2^{k-2}(2w_2 - n) = w_2 - w_1$.
  Following Delsarte (Lemma 11) we know that the two weights are $a2^r$ and $(a+1)2^r$. The previous result gives $2^{k-2} \mid 2w_2 - n) \mid = 2^r$ that is $2^{k-2-r} \mid 2w_2 - n) \mid = 1$. Then $2^{k-2-r} = 1$ and $\mid 2w_2 - n) \mid = 1$. It comes $r = k - 2$. Because $a \geq 1$ then one of the weights is $(a+1)2^{k-2}$ which is greater or equal than 2^{k-1}. Therefore, this weight is 2^{k-1} and then C is the complement of a subspace.
- If $\epsilon = 1$ and $B_1^m = 1$:

With the same method we find $2^{k-2}(2w_2 - n - 1) = w_2 - w_1$ and this leads to the same conclusion: a support of C is the complement of a subspace.

Finally, if E is not the complement of a subspace then $E_{(1,1)} = \emptyset$ and $E_{(2,1)} = \emptyset$ is not possible. Conclusion:

($\mathcal{C}_1$) If E is not the complement of a subspace then

$$E_{(1,1)} \neq \emptyset \text{ or } E_{(2,1)} \neq \emptyset.$$

Case 2 :$E_{(1,1)} = \emptyset,\ E_{(2,1)} \neq \emptyset$

In this case:

$$\mathcal{A}_1 = \mathcal{A}_1^m + \mid E_{(2,1)} \mid + \epsilon \quad \text{with } \epsilon = 1 \text{ if } w = w_1 \text{ and } \epsilon = 0 \text{ if } w = w_2.$$

Since all the weights of $m + E_1^m$ are w_2 and $\mid m + E_1^m \mid = \mid E_1^m \mid$, then:

$$\mathcal{A}_2 = \mathcal{A}_1^m + \mid E_{(2,2)} \mid + \mu \quad \text{with } \mu = 1 \text{ if } w = w_2 \text{ and } \mu = 0 \text{ if } w = w_1.$$

We deduce: $\mathcal{A}_1 + \mathcal{A}_2 = 2\mathcal{A}_1^m + \mid E_{(2,1)} \mid + \mid E_{(2,2)} \mid + 1$.

On the other hand $m + E_2^m = E_{(2,1)} \cup E_{(2,2)}$ and $E_{(2,1)} \cap E_{(2,2)} = \emptyset$ whence $\mid E_{(2,1)} \mid + \mid E_{(2,2)} \mid = \mid m + E_2^m \mid = \mid E_2^m \mid = \mathcal{A}_2^m$.

Finally:

$$\mathcal{A}_1 + \mathcal{A}_2 = \mathcal{A}_1^m + \mathcal{A}_1^m + \mathcal{A}_2^m + 1.$$

We know that $\mathcal{A}_1 + \mathcal{A}_2 = 2^k - 1$ and $\mathcal{A}_1^m + \mathcal{A}_2^m = 2^{k-1} - 1$. This gives: $\mathcal{A}_1^m = 2^{k-1} - 1$ and we conclude that C_m is a 1-weight code of dimension $k - 1$.

According to Proposition 7: $n - B_1^m = \lambda(2^{k-1} - 1)$ and $w_1 = \lambda 2^{k-2}$ with $\lambda \in \mathbb{N} \setminus \{0\}$.

The length of C_m is also the length of C and w_1 is a weight of C. Then $\lambda \geq 2$ is impossible since the length of a projective code of dimension k is at most $2^k - 1$ and a weight of such a code is at most 2^{k-1}.

The unique solution is $\lambda = 1$ and $n - B_1^m = 2^{k-1} - 1,\ w_1 = 2^{k-2}$.

(I) From (4) we have: $F(n, w_1, w_2, k) = 0$.

(i) If $B_1^m = 1$ then $n = 2^{k-1}$. With $w_1 = 2^{k-2}$ condition (I) gives $w_2 = 2^{k-1}$. Once again this proves that E is the complement of a subspace.

(ii) If $B_1^m = 0$ then $n = 2^{k-1} - 1,\ w_1 = 2^{k-2}$ and (I) gives $w_2 = 0$ which is not possible.

Then if E is not the complement of a subspace then $E_{(1,1)} = \emptyset$ and $E_{(2,1)} \neq \emptyset$ is not possible. Conclusion:

($\mathcal{C}_2$) If E is not the complement of a subspace then

$$E_{(1,1)} \neq \emptyset \quad \text{or} \quad E_{(2,1)} = \emptyset.$$

Case 3 :$E_{(1,1)} \neq \emptyset,\ E_{(2,1)} = \emptyset$

Using the same method we find $\mathcal{A}_2^m = 2^{k-1} - 1$ and thus:

($\mathcal{C}_3$) If E is not the complement of a subspace then

$$E_{(1,1)} = \emptyset \quad \text{or} \quad E_{(2,1)} \neq \emptyset.$$

Partial conclusion: Since $E_{(1,1)} \neq \emptyset$ or $E_{(2,1)} \neq \emptyset$ and because neither ($E_{(1,1)} = \emptyset$ and $E_{(1,1)} \neq \emptyset$) nor ($E_{(1,1)} \neq \emptyset$ and $E_{(2,1)} = \emptyset$) are true, then:

($\mathcal{C}_4$) If E is not the complement of a subspace then

$$E_{(1,1)} \neq \emptyset \quad \text{and} \quad E_{(2,1)} \neq \emptyset.$$

Step 2

Replacing $E_{(1,1)}$ and $E_{(2,1)}$ respectively by $E_{(1,2)}$ and $E_{(2,2)}$ and using the method of Step 1 we have a similar result:

($\mathcal{C}_5$) If E is not the complement of a subspace then

$$E_{(1,1)} \neq \emptyset \quad \text{and} \quad E_{(2,1)} \neq \emptyset.$$

General conclusion

($\mathcal{C}$) If E is not the complement of a subspace then $E_{(1,1)}$, $E_{(2,1)}$, $E_{(1,2)}$, $E_{(2,2)}$ are not empty.

This is the proof that (a), (b), (c), (d) are satisfied and thus the theorem is proved. □

Remark 18 The previous result is independent of the choice of E because, in one hand all support of C and in other hand all subspaces of a given dimension, are equivalent under the action of the linear group of $\mathbb{F}_{2^k}$.

4.1 Examples

Recall that the weights of $\tilde{C}_m$ are:

$$\tilde{w}_1 = \frac{1}{2}[w - (w_1 - w_2)], \quad \tilde{w}_2 = \frac{1}{2}w, \quad \tilde{w}_3 = \frac{1}{2}[w + (w_1 - w_2)].$$

4.1.1 Semi-primitive code

The weights of C are $w_1 = 2^{t-1}\left(\frac{2^t-\epsilon}{d}\right)$ and $w_2 = 2^{t-1}\left(\frac{2^t+\epsilon(d-1)}{d}\right)$.

The weights of $\tilde{C}_m$ are:

$$\tilde{w}_1 = \frac{1}{2}[w - (w_1 - w_2)], \quad \tilde{w}_2 = \frac{1}{2}w, \quad \tilde{w}_3 = \frac{1}{2}[w + (w_1 - w_2)].$$

With $w = w_1$ we find:

$$\tilde{w}_1 = 2^{t-2}\left(\frac{2^t + \epsilon(d-1)}{d}\right), \quad \tilde{w}_2 = 2^{t-2}\left(\frac{2^t - \epsilon}{d}\right),$$
$$\tilde{w}_3 = 2^{t-2}\left(\frac{2^t - \epsilon(d+1)}{d}\right).$$

With $w = w_2$ we find:

$$\tilde{w}_1 = 2^{t-2}\left(\frac{2^t + \epsilon(2d-1)}{d}\right), \quad \tilde{w}_2 = 2^{t-2}\left(\frac{2^t + \epsilon(d-1)}{d}\right),$$
$$\tilde{w}_3 = 2^{t-2}\left(\frac{2^t - \epsilon}{d}\right).$$

4.1.2 Bent function code

If the support of a code C is the support of a bent function then it is well known (see [12]) that the dimension of C is $2t$ and the two weights of C are $w_1 = 2^{2t-2}$ and $w_2 = 2^{2t-2} - \epsilon 2^{t-1}$ where $\epsilon \in \{-1, +1\}$.

If $w = w_1$:

$$\tilde{w}_1 = 2^{2t-3} - \epsilon 2^{t-2},\ \tilde{w}_2 = 2^{2t-3},\ \tilde{w}_3 = 2^{2t-3} + \epsilon 2^{t-2}.$$

If $w = w_2$:

$$\tilde{w}_1 = 2^{2t-3} - \epsilon 2^{t-1},\ \tilde{w}_2 = 2^{2t-3} - \epsilon 2^{t-2},\ \tilde{w}_3 = 2^{2t-3}.$$

5 Near-bent functions from 2-weight code

Theorem 19 *Let C be a binary projective linear 2-weight code of dimension $2t$ with weights w_1 and w_2 such that a support of C is not the complement of a subspace.*

(a) If there exists a word m in C with weight $w = 2^{2t-2} - \eta 2^{t-1}$ with $\eta \in \{-1,\ 0,\ +1\}$ and

(b) If $\mid w_2 - w_1 \mid = 2^{t-1}$

then every defining function of the doubly restricted code $\tilde{C}_m$ is a near-bent function.

Proof Note that the dimension of is $2t - 1$ and the length of $\tilde{C}_m$ is w which also is the weight of f. Then:

- If $w = 2^{2t-2} - \eta 2^{t-1}$ then $\hat{f}(0) = 2(2^{2t-2} - (2^{2t-2} - \eta 2^{t-1})) = \eta 2^t$.
- If $w = 2^{2t-2}$ then $\hat{f}(0) = 2(2^{2t-2} - 2^{2t-2}) = 0$.
- If $v \neq 0$ then $\hat{f}(v) = -2(n - 2w_v)$.

If f is a defining function of $\tilde{C}_m$ then $n = w$ and for every v the w_v are the weights of $\tilde{C}_m$: $\frac{1}{2}[w - (w_1 - w_2)]$, $\frac{1}{2}w$, $\frac{1}{2}[w + (w_1 - w_2)]$.

With $\mid w_2 - w_1 \mid = 2^{t-1}$:

$$\hat{f}(v) = -2[w - [w - (w_1 - w_2)] = 2^t$$

or

$$\hat{f}(v) = -2[w - [w]] = 0$$

or

$$\hat{f}(v) = -2[w - [w - (w_1 + w_2)] = +2^t.$$

□

5.1 Weight distribution

The defining function involved in the previous theorem is a three-valued boolean function. The distribution of a three-valued m-boolean function is given in [1, Proposition 4].

Assume that the hypotheses of Theorem 19 are satisfied for a code C. Using the link, which appears in the proof of the theorem, between the weights of $\tilde{C}_m$ and the Fourier coefficients of f, and using [1, Proposition 4], we are able to determine the weight distribution of $\tilde{C}_m$.

Theorem 20 *If C is a binary projective 2-weight code satisfying the hypothesis of Theorem 19 then the weight distribution of $\tilde{C}_m$ is as follows. (iff stands for if an only if).*

Weight	Number of words
$\frac{1}{2}[w-(w_1-w_2)]$	$2^{2t-3}+2^{t-2}-\theta$ with $\theta=1$ iff $\eta=1$
$\frac{1}{2}w$	$2^{2t-2}-\gamma$ with $\gamma=1$ iff $\eta=0$
$\frac{1}{2}[w+(w_1-w_2)]$	$2^{2t-3}-2^{t-2}-\omega$ with $\omega=1$ iff $\eta=-1$

Proof We just have to connect the weights of $\tilde{C}_m$ with the Fourier coefficients of f as in the proof of Theorem 19, then use the coefficient distribution introduced in 2.1 and remark that $\hat{f}(0)=-2^t$ if $\eta=1$, $\hat{f}(0)=0$ if $\eta=0$ and $\hat{f}(0)=2^t$ if $\eta=-1$. □

5.2 Examples

5.2.1 Special semi-primitive code

Let us consider the binary cyclic code C of dimension 6 and length 21 with generator $g(x)=1+x^2+x^5+x^8+x^9+x^{12}+x^{14}+x^{15}$.

This is a semi-primitive code with $t=3$, $d=3$, $r=1$, $\epsilon=-1$ the weights are $w_1=2^2(\frac{2^3+1}{3})=12$ and $w_2=2^2(\frac{2^3-2}{3})=8$.

Remark that $12=2^{2t-2}-2^{t-1}$ whence part (a) of Theorem 19 holds. Then:

If m is a word of weight 12 in C and if f is a defining function of the doubly restricted code $\tilde{C}_m$ of C then f is a near-bent function. This is the example of Sect. 2.3.1.

With $\mathbb{F}_{2^5}=\mathbb{F}_2(\alpha)$ and $\alpha^5+\alpha^2+1=0$, the support of $\tilde{C}_m$ obtained by the columns of $\tilde{G}_m$ is:

$$E=\{0,1,\alpha,\alpha^2,\alpha^6,\alpha^7,\alpha^8,\alpha^{18},\alpha^{20},\alpha^{21},\alpha^{25},\alpha^{30}\}$$

A defining function of C, indicator of E is:

$$tr(1+a^4x+a^{11}x^3+a^{22}x^5+a^{24}x^7+a^{28}x^{11}+a^{17}x^{15})$$

where tr is the trace of $\mathbb{F}_{2^5}$.

It seems that this is the unique semi-primitive code satisfying the conditions of Theorem 19.

5.2.2 Bent function code

Theorem 21 *Let C be a binary linear code such that a support of C is the support of a bent function. Let m be a word of C.*

If f is a defining function of the doubly restricted code $\tilde{C}_m$ then f is a near-bent function.

Proof It is well known (see [12]) that the dimension of C is $2t$ and the two weights of C are $w_1 = 2^{2t-2}$ and $w_2 = 2^{2t-2} - \epsilon 2^{t-1}$ where $\epsilon \in \{-1, +1\}$. And we have $w_1 - w_2 = \epsilon 2^{t-1}$. The conclusion comes directly from Theorem 19. □

6 Conclusion

We have constructed binary 3-weight codes and near-bent functions from 3-weight codes. An open question now is to find new examples of near-bent functions obtained with Theorem 19.

References

1. Canteaut, A., Charpin, P.: Decomposing bent functions. IEEE Trans. Inf. Theory. **49**(8), 2004–2019 (2003)
2. Baumert, D., McEliece, R.J.: Weights of irreducible cyclic codes. Inf. Control **20**, 158–175 (1972)
3. Delsarte, P.: Weights of linear codes and strongly regular normed spaces. Discrete Math. **3**, 47–64 (1972)
4. Dillon, J.F.: Elementary Hadamard difference sets. Ph.D. thesis, University of Maryland (1974)
5. Ding, C., Li, C., Li, N., Zhou, Z.C.: Three-weight cyclic codes and their weight distributions. Discrete Math. **339**, 415–427 (2016)
6. Leander, G., McGuire, G.: Construction of bent functions from near-bent functions. J. Comb. Theory Ser. A **116**(4), 960–970 (2009)
7. Mac Williams, F.J., Sloane, N.J.A.: The Theory of Error Correcting Codes. North-Holland, Amsterdam (1977)
8. Pless, V.: Power moment identities on weight distribution in error correcting codes. Inf. Control **6**, 147–152 (1963)
9. Pless, V., Huffman, W.C. (eds.): Handbook of Coding Theory. Elsevier, Amsterdam (1998)
10. Rothaus, O.S.: On bent functions. J. Comb. Theory Ser. A **20**, 300–305 (1976)
11. Tang, C., Li, N., Qi, Y.F., Zhou, Z.C., Helleseth, T.: Linear codes with two or three weights from weakly regular bent functions. IEEE Trans. Inf. Theory **62**(3), 1166–1176 (2016)
12. Wolfmann, J.: Bent functions and coding theory. In: Pott, A., Kumar, P.V., Helleseth, T., Jungnickel, D. (eds.) Difference Sets, Sequences and Their Correlation Properties, NATO Sciences Series, Series C, vol. 542, pp. 393–418. Kluwer, Dordrecht (1999)
13. Wolfmann, J.: Are 2-weight projective cyclic codes irreducible? IEEE Trans. Inf. Theory **51**(2), 733–737 (2005)
14. Wolfmann, J.: Cyclic code aspects of bent functions. In: Finite Fields: Theory and Applications, AMS Series "Contemporary Mathematics". vol. 518, pp. 363–384 (2010)
15. Wolfmann, J.: Special bent and near-bent functions. Adv. Math. Commun. **8**(1), 21–33 (2014)
16. Wolfmann, J.: From near-bent to bent: a special case. In: Topics in Finite Fields, AMS Series "Contemporary Mathematics" vol. 632, pp. 359–371 (2015)

17. Wolfmann, J.: Codes Projectifs à deux poids, Caps complets et Ensembles de Différences. J. Comb. Theory Ser. A **23**, 208–222 (1977)
18. Zhang, D., Fan, C., Peng, D., Tang, X.: Complete weight enumerators of some linear codes from quadratic forms. Cryptogr. Commun. **9**(1), 151–163 (2017)
19. Zhou, Z., Li, N., Fan, C., Helleseth, T.: Linear code with two or three weights from quadratic bent functions. Des. Codes Cryptogr. **81**(2), 283–295 (2016)