The construction and weight distributions of all projective binary linear codes

Cunsheng Ding

Department of Computer Science and Engineering, The Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong

Abstract

Boolean functions can be used to construct binary linear codes in many ways, and vice versa. The objective of this short article is to point out a connection between the weight distributions of all projective binary linear codes and the Walsh spectra of all Boolean functions. New research problems are also proposed.

Keywords: Boolean function, linear code, Walsh transform, weight distribution

1. Introduction

Let \( q \) be a prime and let \( r = q^m \) for some positive integer \( m \). An \([n, k, d]\) code \( C \over GF(q) \) is a \( k \)-dimensional subspace of \( GF(q)^n \) with minimum (Hamming) distance \( d \). A linear code \( C \) is called projective if its dual code has minimum distance at least 3. Let \( A_i \) denote the number of codewords with Hamming weight \( i \) in a code \( C \) of length \( n \). The weight enumerator of \( C \) is defined by

\[
1 + A_1 z + A_2 z^2 + \cdots + A_n z^n.
\]

The sequence \((1, A_1, A_2, \cdots, A_n)\) is called the weight distribution of the code \( C \). A code \( C \) is said to be a \( t \)-weight code if the number of nonzero \( A_i \) in the sequence \((A_1, A_2, \cdots, A_n)\) is equal to \( t \).

Boolean functions are functions from \( GF(2^m) \) or \( GF(2)^m \) to \( GF(2) \), where \( m \) is a positive integer. They are important building blocks for certain types of stream ciphers, and can also be employed to construct binary codes in many ways. Conversely, binary linear codes can be used to construct Boolean functions in different ways. The objective of this article is to point out a connection between the weight distributions of all projective binary linear codes and the Walsh spectra of all Boolean functions. New research problems are also proposed.

2. Mathematical foundations

2.1. Group characters in \( GF(q) \)

An additive character of \( GF(q) \) is a nonzero function \( \chi \) from \( GF(q) \) to the set of nonzero complex numbers such that \( \chi(x+y) = \chi(x)\chi(y) \) for any pair \((x, y) \in GF(q)^2\). For each \( b \in GF(q) \), the function

\[
\chi_b(c) = e^{2\pi i bc} \text{ for all } c \in GF(q)
\]  \hspace{1cm} (1)
defines an additive character of $GF(q)$, where and whereafter $e_p = e^{2\pi i / p}$ is a primitive complex $p$th root of unity and $Tr$ is the absolute trace function. When $b = 0$, $\chi_0(c) = 1$ for all $c \in GF(q)$, and is called the trivial additive character of $GF(q)$. The character $\chi_1$ in (11) is called the canonical additive character of $GF(q)$. It is known that every additive character of $GF(q)$ can be written as $\chi_d(x) = \chi_1(bx)$ [8, Theorem 5.7].

2.2. Boolean functions and their expressions

A function $f$ from $GF(2^m)$ or $GF(2)^m$ to $GF(2)$ is called a Boolean function. A function $f$ from $GF(2^m)$ to $GF(2)$ is called linear if $f(x + y) = f(x) + f(y)$ for all $(x, y) \in GF(2^m)^2$. A function $f$ from $GF(2^m)$ to $GF(2)$ is called affine if $f$ or $f - 1$ is linear.

The Walsh transform of $f : GF(2^m) \rightarrow GF(2)$ is defined by

$$\hat{f}(w) = \sum_{x \in GF(2^m)} (-1)^{f(x) + Tr(wx)}$$

(2)

where $w \in GF(2^m)$. The Walsh spectrum of $f$ is the following multiset

$$\{ \{ f(w) : w \in GF(2^m) \} \} .$$

Let $f$ be a Boolean function from $GF(2^m)$ to $GF(2)$. The support of $f$ is defined to be

$$D_f = \{ x \in GF(2^m) : f(x) = 1 \} \subseteq GF(2^m).$$

(3)

Clearly, $f \mapsto D_f$ is a one-to-one correspondence between the set of Boolean functions from $GF(2^m)$ to $GF(2)$ and the power set of $GF(2^m)$.

3. A fundamental construction of linear codes

Throughout this section, let $q$ be a prime power and let $r = q^m$, where $m$ is a positive integer. Let $Tr$ denote the trace function from $GF(r)$ to $GF(q)$ unless otherwise stated.

Let $D = \{ d_1, d_2, \ldots, d_n \} \subseteq GF(r)$. We define a code of length $n$ over $GF(q)$ by

$$C_D = \{ (Tr(xd_1), Tr(xd_2), \ldots, Tr(xd_n)) : x \in GF(r) \},$$

(4)

and call $D$ the defining set of this code $C_D$. Since the trace function is linear, the code $C_D$ is linear. By definition, the dimension of the code $C_D$ is at most $m$.

Different orderings of the elements of $D$ give different linear codes $C_D$, which are however permutation equivalent. Hence, we do not distinguish these codes obtained by different orderings of the elements in $D$. It should be noticed that the defining set $D$ could be a multiset, i.e., some elements in $D$ may be the same.

Define for each $x \in GF(r)$,

$$c_x = (Tr(xd_1), Tr(xd_2), \ldots, Tr(xd_n)).$$

The Hamming weight $wt(c_x)$ of $c_x$ is $n - N(x)$, where

$$N(x) = | \{ 1 \leq i \leq n : Tr(xd_i) = 0 \} |$$

for each $x \in GF(r)$. 

2
It is easily seen that for any $\mathcal{D} = \{d_1, d_2, \ldots, d_n\} \subseteq \text{GF}(r)$ we have

$$qN_x(0) = \sum_{i=1}^{n} \sum_{y \in \text{GF}(q)} \tilde{\chi}_1(y \text{Tr}(xd_i)) = n + \sum_{y \in \text{GF}(q)^*} \chi_1(yxD),$$

where $\chi_1$ and $\tilde{\chi}_1$ are the canonical additive characters of $\text{GF}(r)$ and $\text{GF}(q)$, respectively, $a\mathcal{D}$ denotes the set $\{ad : d \in \mathcal{D}\}$, and $\chi_1(S) := \sum_{x \in S} \chi_1(x)$ for any subset $S$ of $\text{GF}(r)$. Hence,

$$\text{wt}(c_x) = n - N_x(0) = \frac{(q-1)n - \sum_{y \in \text{GF}(q)^*} \chi_1(yxD)}{q}. \quad (5)$$

Thus, the computation of the weight distribution of the code $\mathcal{C}_\mathcal{D}$ reduces to the determination of the value distribution of the character sum

$$\sum_{y \in \text{GF}(q)^*} \sum_{i=1}^{n} \chi_1(yxD).$$

This construction technique was employed many years ago for obtaining linear codes with a few weights (see, for example, [10], [7], [6] and [2]), and is called the defining-set construction of linear codes. Recently, this trace construction of linear codes has attracted a lot of attention, and a huge amount of linear codes with good parameters have been obtained. The following theorem shows that the trace construction is fundamental.

**Theorem 1.** Every $[n,k]$ code over $\text{GF}(q)$ can be expressed as $\mathcal{C}_\mathcal{D}$ for some defining set $\mathcal{D} \subseteq \text{GF}(q^k)$.

**Proof.** Let $(g_{1j}, g_{2j}, \ldots, g_{kj})^T$ denote the $j$th column of a generator matrix of the code for $1 \leq j \leq n$. Define

$$f_j(x) = (x_1, x_2, \ldots, x_k)(g_{1j}, g_{2j}, \ldots, g_{kj})^T,$$

where $x = (x_1, x_2, \ldots, x_k) \in \text{GF}(q)^k$. By definition, the code is the set

$$\{(f_1(x), f_2(x), \ldots, f_n(x)) : x \in \text{GF}(q^k)\}.$$

Let $\{\alpha_1, \alpha_2, \ldots, \alpha_k\}$ be a basis of $\text{GF}(q^k)$ over $\text{GF}(q)$, and let $\{\beta_1, \beta_2, \ldots, \beta_k\}$ denote its dual basis. For each $j$ with $1 \leq j \leq n$, define

$$d_j = \sum_{i=1}^{k} g_{ij} \beta_i \quad (6)$$

and $\mathcal{D} = \{d_1, d_2, \ldots, d_n\} \subseteq \text{GF}(q^k)$. For $x = (x_1, x_2, \ldots, x_k) \in \text{GF}(q)^k$, define

$$x' = \sum_{i=1}^{k} x_i \alpha_i \in \text{GF}(q^k).$$

Clearly, we have

$$\text{Tr}_{q^k/q}(d_jx') = \sum_{i=1}^{k} s_{ij}g_{ij} = f_j(x).$$

3
Consequently,
\[
\{(f_1(x), \ldots, f_n(x)) : x \in \text{GF}(q^k)\} = \{\text{Tr}_{q^k/q}(d_1 x'), \ldots, \text{Tr}_{q^k/q}(d_n x') : x' \in \text{GF}(q^k)\} = C_D.
\]
This completes the proof.

Theorem 1 is a direct consequence of the classical result that every linear function from \(\text{GF}(q^m)\) to \(\text{GF}(q)\) can be expressed as \(\text{Tr}(ax)\) for some \(a \in \text{GF}(q^m)\) \[9\]. The proof of Theorem 1 clearly shows that the defining-set construction is equivalent to the generator matrix construction of all linear codes. Hence, it is impossible to find out the first one who introduced the defining-set construction. This construction technique was employed many years ago for obtaining linear codes with a few weights (see, for example, \[10\], \[7\], \[6\] and \[2\]). The weight formula in (5) tells us that an advantage of the defining-set approach over the generator-matrix approach is that the former can make full use of results about character sums for determining the parameters and weight distributions of linear codes. This advantage has been demonstrated in a lot of recent references on the defining-set construction of linear codes.

A slightly different version of Theorem 1 was proved in \[11\]. Theorem 1 and its proof above are refined ones in \[8\].

4. The construction and weight distributions of all projective binary linear codes

Let \(f\) be a function from \(\text{GF}(2^m)\) to \(\text{GF}(2)\), and let \(D_f\) be the support of \(f\) defined in \[3\]. Let \(n_f = |D_f|\). The following theorem was proved in \[3\].

**Theorem 2.** Let \(f\) be a function from \(\text{GF}(2^m)\) to \(\text{GF}(2)\), and let \(D_f\) be the support of \(f\). If \(2n_f + \hat{f}(w) \neq 0\) for all \(w \in \text{GF}(2^m)^*\), then \(C_{D_f}\) is a binary linear code with length \(n_f\) and dimension \(m\), and its weight distribution is given by the following multiset:

\[
\left\{ \left\{ \frac{2n_f + \hat{f}(w)}{4} : w \in \text{GF}(2^m)^* \right\} \cup \left\{ 0 \right\} \right\}.
\]

(7)

Theorem 2 establishes a connection between the set of Boolean functions \(f\) such that \(2n_f + \hat{f}(w) \neq 0\) for all \(w \in \text{GF}(2^m)^*\) and a class of binary linear codes. The determination of the weight distribution of the binary linear code \(C_{D_f}\) is equivalent to that of the Walsh spectral of the Boolean function \(f\) satisfying \(2n_f + \hat{f}(w) \neq 0\) for all \(w \in \text{GF}(2^m)^*\). When the Boolean function \(f\) is selected properly, the code \(C_{D_f}\) has only a few weights and may have good parameters. A lot of binary linear codes \(C_{D_f}\) with a few weights were reported in \[4\].

Theorem 2 was generalized into the following in \[4\].

**Theorem 3.** Let \(f\) be a function from \(\text{GF}(2^m)\) to \(\text{GF}(2)\), and let \(D_f\) be the support of \(f\). Let \(e_w\) denote the multiplicity of the element \(\frac{2n_f + \hat{f}(w)}{4}\) and \(e\) the multiplicity of 0 in the multiset of (7). Then \(C_{D_f}\) is a binary linear code with length \(n_f\) and dimension \(m - \log_2 e\), and the weight distribution of the code is given by

\[
\frac{2n_f + \hat{f}(w)}{4} \text{ with frequency } \frac{e_w}{e}
\]

for all \(\frac{2n_f + \hat{f}(w)}{4}\) in the multiset of (7).
Theorem 3 says that every Boolean function can be used to construct a binary linear code with the defining-set construction whose weight distribution is determined by the Walsh spectrum of the Boolean function. Conversely, we have the following.

**Theorem 4.** Let $C$ be any projective binary linear code. Then there is a Boolean function $f$ such that $C = C_D$. Furthermore, Let $f$ be a function from $\mathbb{GF}(2^m)$ to $\mathbb{GF}(2)$, and let $D_f$ be the support of $f$. Let $e_w$ denote the multiplicity of the element $2^{n_f} + \hat{f}(w)$ and $e$ the multiplicity of 0 in the multiset of $\mathbb{GF}(2)$. Then $C_D$ is a binary linear code with length $n_f$ and dimension $m - \log_2 e$, and the weight distribution of the code is given by

$$\frac{2n_f + \hat{f}(w)}{4} \text{ with frequency } \frac{e_w}{e}$$

for all $2^{n_f} + \hat{f}(w)$ in the multiset of $\mathbb{GF}(2)$.

**Proof.** By Theorem 1, there is a set $D \subset \mathbb{GF}(2^m)$ for some positive integer $m$ such that $C = C_D$. Since $C$ is projective, $D$ does not contain repeated elements. We now define a Boolean function $f$ from $\mathbb{GF}(2^m)$ to $\mathbb{GF}(2)$ as

$$f(x) = \begin{cases} 
1 & \text{if } x \in D, \\
0 & \text{otherwise.} 
\end{cases} \quad (8)$$

By definition, the support $D_f$ of $f$ is $D$. It then follows that

$$C = C_D = C_{D_f}.$$ 

The desired conclusion on the weight distribution of $C$ then follows from Theorem 3. \qed

Note that Theorem 4 is a direct consequence of Theorems 1 and 3. It gives a general approach to the computation of the weight distribution of projective binary linear codes $C_D$. The procedure is the following.

- Let $C_D$ be a projective binary linear code constructed with the defining-set approach, where $D \subset \mathbb{GF}(2^m)$ for some positive $m$ and $D$ does not contain repeated elements. The first step is to construct the characteristic Boolean function $f$ of $D$, which was defined in (8).

- The second step is to compute the Walsh spectrum of the Boolean function $f$.

Hence, determining the weight distribution of any projective binary linear code is equivalent to determining the Walsh spectrum of the corresponding Boolean function.

The proofs of Theorems 1 and 4 clearly show that every projective binary linear code $C$ with dimension $k$ gives a Boolean function $f_C$ from $\mathbb{GF}(2^k)$ to $\mathbb{GF}(2)$ whose Walsh spectrum is completely determined by the weight distribution of $C$. The Boolean function $f_C(x)$ is constructed as follows:

- Select a generator matrix of $C$ and a basis of $\mathbb{GF}(2^k)$ over $\mathbb{GF}(2)$ (see the proof of Theorem 1).

- Construct the set $D = \{d_1, d_2, \ldots, d_n\}$, where $d_j$ was defined in (6).

- Construct $f_C$ as the characteristic function of $D$, i.e., $f_C(x) = 1$ if and only if $x \in D$. 

5
This \( f_C(x) \) depends on the choice of the generator matrix and a basis of \( \text{GF}(2^k) \) over \( \text{GF}(2) \). Hence, such a code \( C \) gives many Boolean functions with the same Walsh spectrum. Below we propose some research problems in this direction.

**Research Problem 1.** Let \( C \) denote the binary Golay code with parameters \([23, 12, 7]\) or its extended code. Study the Boolean functions \( f_C(x) \) from \( \text{GF}(2^{12}) \) to \( \text{GF}(2) \).

**Research Problem 2.** Let \( C \) denote the binary MacDonald code with parameters \([2^k - 2, k, 2^{k-1} - 1]\) (i.e., a punctured code of the binary Simplex code with parameters \([2^k - 1, k, 2^{k-1}]\)). Then \( C \) has only two nonzero weights \( 2^{k-1} \) and \( 2^{k-1} - 1 \). Study the Boolean functions \( f_C(x) \).

**Research Problem 3.** Let \( \mathcal{R}_2(\ell, m) \) denote the binary Reed-Muller code of order \( 1 \leq \ell < m \). Study the Boolean functions \( f_{\mathcal{R}_2(\ell, m)}(x) \).

**Research Problem 4.** Let \( m \geq 3 \) and let \( C \) denote the binary Hamming code with parameters \([2^m - 1, 2^m - 1 - m, 3]\). Study the Boolean functions \( f_C(x) \).

**Research Problem 5.** Let \( C \) denote a binary irreducible cyclic code. Study the Boolean functions \( f_C(x) \).

**Research Problem 6.** Let \( C \) denote a binary BCH code. Study the Boolean functions \( f_C(x) \).

**Research Problem 7.** For binary quadratic residue codes \( C \), study the Boolean functions \( f_C(x) \).

**Research Problem 8.** Let \( m \geq 4 \) be even and let \( C \) denote the binary linear code with parameters \([2^m, m + 2, 2^{m-1} - 2^{(m-2)/2}]\) in Theorem 14.4 in [5, p. 336], study the Boolean functions \( f_C(x) \) from \( \text{GF}(2^{m+2}) \) to \( \text{GF}(2) \).

**Research Problem 9.** Let \( m \geq 4 \) be even and let \( C \) denote the binary linear code with parameters \([2^m - 1 - 2^{(m-2)/2}, m + 1, 2^{m-2} - 2^{(m-2)/2}]\) in Theorem 14.9 in [5, p. 341], study the Boolean functions \( f_C(x) \) from \( \text{GF}(2^{m+1}) \) to \( \text{GF}(2) \).

There are a lot of binary linear codes \( C \) with only two nonzero weights documented in [1]. The corresponding Boolean functions \( f_C \) should be very interesting. It would be very interesting to study the Boolean functions \( f_C(x) \) for binary three-weight codes \( C \). There are many three-weight binary codes in the literature. Little work in this direction is done. The reader is cordially invited to join the venture in this direction.

5. A special case of the defining-set construction of linear codes

Let notation be the same as in Section 3. In this section, we consider a special case of the defining-set construction in 4.

Assume that \( m = 2h \). Let \( \{u_1, u_2\} \) be a basis of \( \text{GF}(q^m) \) over \( \text{GF}(q^h) \), and let \( \{v_1, v_2\} \) be its dual basis. Then

\[
d_i = d_{i,1} v_1 + d_{i,2} v_2
\]

where \( d_{i,j} \in \text{GF}(q^h) \). Similarly each \( x \in \text{GF}(q^m) \) can be expressed as

\[
x = x_1 u_1 + x_2 u_2,
\]

where \( x_i \in \text{GF}(q^h) \). It then follows that

\[
\text{Tr}_{q^m/q}(xd_i) = \text{Tr}_{q^h/q}(\text{Tr}_{q^m/q}(xd_i)) = \text{Tr}_{q^h/q}(d_{i,1} x_1 + d_{i,2} x_2).
\]
Consequently, the code in (4) can be expressed as

\[ C_D = \{ (\text{Tr}_{q^h/q}(d_1x_1 + d_2x_2)) : (x_1, x_2) \in GF(q^h) \times GF(q^h) \} \]

\[ = \{ (\text{Tr}_{q^h/q}(e_1x_1 + e_2x_2)) : (x_1, x_2) \in GF(q^h) \times GF(q^h) \}, \] (9)

where \( E = \{ (d_{1,1}, d_{1,2}), (d_{2,1}, d_{2,2}), \ldots, (d_{n,1}, d_{n,2}) \} \). Thus, the construction of (3) is a special case of the general defining-set construction, and was studied in some recent papers.

Let \( q = 2 \) and consider the code \( C_E \) in (9). Let \( f \) be the characteristic Boolean function of \( E \). Then \( f \) is a function from \( GF(2^h) \times GF(2^h) \) to \( GF(2) \). Then the weight distribution of the binary code \( C_E \) in (9) is given in a similar way as in Theorem 4.

6. Concluding remarks

The Boolean function construction of projective binary linear codes \( C_{D_f} \) gives a coding-theoretical characterisation of bent and other special Boolean functions with Theorems 3 and 4. For example, \( f \) is bent if and only if the code \( C_{D_f} \) has the weight distribution in Table II in [3]. In addition, other connections between projective binary codes and Boolean functions could also be developed.

References

[1] R. Calderbank, W. M. Kantor, The geometry of two-weight codes, Bull. London Math. Soc. 18 (1986) 97–122.
[2] C. Ding, A class of three-weight and four-weight codes, in Proceedings of International Conference on Coding and Cryptography, Lecture Notes in Computer Science 5557 (Springer Verlag, Heidelberg), 2009, pp. 34–42.
[3] C. Ding, Linear codes from some 2-designs, IEEE Trans. Inf. Theory 60(6) (2015) 3265–3275.
[4] C. Ding, A construction of binary linear codes from Boolean functions, Discrete Mathematics 339(9) (2016) 2288–2303.
[5] C. Ding, Designs from Linear Codes, World Scientific, Singapore, 2018.
[6] C. Ding, J. Luo, H. Niederreiter, Two weight codes punctured from irreducible cyclic codes, in Proc. of the First International Workshop on Coding Theory and Cryptography, Eds., Li, Y., Ling, S., Niederreiter, H., Wang, H., Xing, C., Zhang, S. (Singapore, World Scientific), 2008, pp. 119–124.
[7] C., Ding, H. Niederreiter, Cyclotomic linear codes of order 3, IEEE Trans. Inform. Theory 53(6) (2007) 2274–2277.
[8] Z. Heng, W. Wang, Y. Wang, Projective binary linear codes from special Boolean functions, Applicable Algebra in Engineering, Communication and Computing, https://doi.org/10.1007/s00200-019-00412-z.
[9] R. Lidl, H. Niederreiter, Finite Fields, Cambridge University Press, Cambridge, 1997.
[10] J. Wolfmann, Codes projectifs à deux ou trois poids associés aux hyperquadriques d’une géométrie finie, Discrete Math. 13(2) (1975) 185–211.
[11] C. Xiang, It is indeed a fundamental construction of all linear codes, arXiv:1610.06355.