

TWO CLASSES OF NEAR-OPTIMAL CODEBOOKS WITH RESPECT TO THE WELCH BOUND

GAOJUN LUO

Department of Math
Nanjing University of Aeronautics and Astronautics
Nanjing 210016, China

XIWANG CAO∗

Department of Math
Nanjing University of Aeronautics and Astronautics
Nanjing 210016, China

and

State Key Laboratory of Information Security
Institute of Information Engineering
Chinese Academy of Sciences, Beijing 100093, China

(Communicated by Zhengchun Zhou)

Abstract. An \((N, K)\) codebook \(C\) is a collection of \(N\) unit norm vectors in a \(K\)-dimensional vectors space. In applications of codebooks such as CDMA, those vectors in a codebook should have a small maximum magnitude of inner products between any pair of distinct code vectors. In this paper, we propose two constructions of codebooks based on \(p\)-ary linear codes and on a hybrid character sum of a special kind of functions, respectively. With these constructions, two classes of codebooks asymptotically meeting the Welch bound are presented.

1. Introduction

An \((N, K)\) codebook (also called signal set) \(C = \{c_i\}_{i=0}^{N-1}\) is a set of \(N\) unit-norm complex vectors \(c_i \in \mathbb{C}^K\) over an alphabet \(A\), where \(i = 0, 1, \ldots, N - 1\). The size of \(A\) is called the alphabet size of \(C\). As a performance measure of a codebook in practical applications, the maximum magnitude of inner products between a pair of distinct code vectors in \(C\) is defined by

\[ I_{\text{max}}(C) = \max_{0 \leq i \neq j \leq N-1} |c_i c_j^H|, \]

where \(c^H\) denotes the conjugate transpose of the complex vector \(c\). For \(I_{\text{max}}(C)\), Welch [27] gave the following well-known lower bound:

\[ I_{\text{max}}(C) \geq I_{\text{welch}} = \sqrt{\frac{N - K}{(N - 1)K}}. \]

2010 Mathematics Subject Classification: Primary: 11T71; Secondary: 11T23.

Key words and phrases: Codebook, Welch bound, linear code, permutation polynomial.

The second author is supported by the National Natural Science Foundation of China (Grant No. 11771007 and 61572027).

* Corresponding author: Xiwang Cao.
Moreover, the equality holds if and only if for all pairs of \((i, j)\) with \(i \neq j\), it holds that
\[
|c_i c_j^H| = \sqrt{\frac{N - K}{(N - 1)K}}.
\]

A codebook \(C\) achieving the Welch bound with equality is called a maximum-Welch-bound-equality (MWBE) codebook [23]. MWBE codebooks have been widely used in many areas, e.g., communications [23], combinatorial designs [8, 9, 29], code-division multiple-access (CDMA) communication systems [21], packing [5], compressed sensing [2], signal processing [28], coding theory [6] and quantum computing [22]. However, it is very hard to construct an MWBE codebook in general [23]. The known classes of MWBE codebooks are presented as follows:

- \((N, N)\) orthogonal MWBE codebooks for any \(N > 1\) [23], [29].
- \((N, N - 1)\) MWBE codebooks for \(N > 1\) based on discrete Fourier transformation matrices [23], [29] or \(m\)-sequences [23].
- \((N, K)\) MWBE codebooks from conference matrices [5], [24], where \(N = 2K = 2^{d+1}\) for a positive integer \(d\) or \(N = 2K = p^d + 1\) for a prime \(p\) and a positive integer \(d\).
- \((N, K)\) MWBE codebooks based on \((N, K, \lambda)\) difference sets in cyclic groups [29] and abelian groups [8], [9].
- \((N, K)\) MWBE codebooks from \((2, k, \nu)\)-Steiner systems [13].

Since the above MWBE codebooks only exist for very restrictive \(N\) and \(K\), many researchers have tried to construct near-optimal codebooks \(C\), i.e., \(I_{\max}(C)\) asymptotically meets the Welch bound. As an extension of the MWBE codebooks based on difference sets, various types of near-optimal codebooks based on almost difference sets and cyclotomic classes are proposed, see [8, 9, 17, 32, 33, 34, 36] etc. Near-optimal codebooks constructed from binary row selection sequences are presented in [4, 16, 31]. In [25], the authors provided a class of asymptotically optimal codebooks by Gauss sums over finite fields.

According to [24], the Welch bound on \(I_{\max}(C)\) of a codebook \(C\) is not tight when \(N > K(K+1)/2\) for real codebooks and \(N > K^2\) for all codebooks. Levenshtein [18] has given a tight lower bound for \(I_{\max}(C)\) as follows. For any real-valued codebook \(C\) with \(N > K(K+1)/2\),
\[
I_{\max}(C) \geq \sqrt{\frac{3N - K^2 - 2K}{(N - K)(K + 2)}}.
\]

For any real-valued codebook \(C\) with \(N > K^2\),
\[
I_{\max}(C) \geq \sqrt{\frac{2N - K^2 - K}{(N - K)(K + 1)}}.
\]

In [30, 35], the authors constructed several classes of codebooks meeting the Levenshtein bound from Kerdock codes, bent functions and semi-bent functions.

Let \(p\) be an odd prime and \(\mathbb{F}_{p^m}\) be the finite field with \(p^m\) elements. An \([n, k, d]\) linear code \(C\) over \(\mathbb{F}_p\) is a \(k\)-dimensional subspace of \(\mathbb{F}_p^n\) with minimum (Hamming) distance \(d\). Let \(A_i\) denote the number of codewords with Hamming weight \(i\) in a linear code \(C\). 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 \(C\).
Let $\text{Tr}_1^m$ denote the trace function from $\mathbb{F}_{p^m}$ onto $\mathbb{F}_p$ and define $n$ linear functions as follows:

$$f_i : \mathbb{F}_{p^m} \rightarrow \mathbb{F}_p, \ i = 1, \ldots, n.$$ 

From the equation (2.2) in [1], we can represent an $(n, k)$ linear code $C$ by

$$C = \{(f_1(x), \ldots, f_n(x)), x \in \mathbb{F}_{p^m}\}.$$ 

Moreover, since every linear function $L(x)$ from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p$ can be written as

$$L(x) = \text{Tr}_1^m(ax),$$

for some $a \in \mathbb{F}_{p^m}$, see [19, Theorem 2.24], there exist elements $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q^*$ such that

$$C = \{(\text{Tr}_1^m(x\alpha_1), \text{Tr}_1^m(x\alpha_2), \ldots, \text{Tr}_1^m(x\alpha_n)) : x \in \mathbb{F}_{p^m}\}.$$ 

Let $D = \{\alpha_1, \ldots, \alpha_n\}$ be a subset of $\mathbb{F}_q^*$ and name it the defining set of the code $C$. In what follows, we denote the code $C$ whose defining set is $D$ by $C_D$ for clarity. It is clear that all linear codes can be obtained in this way. This generic construction of linear codes was first introduced by Ding in [7, 10]. In the past two years, constructing linear codes from this approach and studying the weight distributions of these linear codes have attracted extensively attention, see e.g. [12, 26, 37, 11, 20].

In [30], Xiang et al. presented a construction of codebooks from binary codes as follows. Given any $[n, k]$ binary code $C$, define a $(2^\pi, n)$ codebook $B(C)$ by

$$B(C) = \left\{\frac{1}{\sqrt{n}}(-1)^c : c \in C\right\},$$

where $(-1)^c$ denotes the vector $((-1)^{c_1}, (-1)^{c_2}, \ldots, (-1)^{c_n})$ for any codeword $c = (c_1, c_2, \ldots, c_n)$ in $C$. Moreover, the authors gave a simple expression of the maximum magnitude $I_{\text{max}}(B(C))$. The above construction of codebooks can be extended to $p$-ary codes by replacing $-1$ with $\xi_p$, where $\xi_p = e^{\frac{2\pi i}{p-1}}$ is the primitive $p$-th root of unity. As indicated in [30], the extended construction does not have a simple expression of the maximum magnitude $I_{\text{max}}(B(C))$.

In this paper, we describe two approaches to construct codebooks whose maximum magnitudes $I_{\text{max}}(B(C))$ asymptotically meet the Welch bound. The first approach is derived from $p$-ary linear codes defined by (1). For any $p$-ary linear codes $C_D$, following Xiang’s extended construction of codebooks, we define a codebook $B(C_D)$ by

$$B(C_D) = \left\{\frac{1}{\sqrt{n}}(\xi_p)^c : c \in C_D\right\}.$$ 

By choosing suitable defining sets from (1), we can give a simple expression of the maximum magnitude $I_{\text{max}}(B(C_D))$. With this construction, we obtain a class of near-optimal codebooks. To say it explicitly, for every weakly regular bent functions, we define a special subset of $\mathbb{F}_q$ as the defining set of a linear code, then define a codebook as in (2). One can show that such a codebook asymptotically meets the Welch bound. Details on it are discussed in later sections. For the second approach, we use a hybrid character sum of a special kind of functions to construct codebooks and the maximum magnitude of the codebooks can be obtained by estimating some character sums. With this construction, a class of codebooks asymptotically meeting the Welch bound is presented as well.

This paper is organized as follows. In Section 2, we provide some basic notations and preliminaries which are needed in our discussion. In Section 3, we propose...
our constructions of codebooks and present two classes of near-optimal codebooks. Finally, Section 4 is devoted to conclusions.

2. Preliminaries

In this section, we present some notations and preliminaries that will be employed in our discussions.

2.1. Some notations fixed throughout this paper. We adopt the following notations unless otherwise stated throughout this paper.

- For any set \( D, D^* = D \setminus \{0\} \) and \( \# D \) denote the cardinality of \( D \);
- \( p \) is an odd prime and \( q = p^m \), where \( m \) is a positive integer;
- \( \mathbb{F}_q \) is a finite field with \( q \) elements and \( \mathbb{F}_q^* \) denotes the nonzero elements in \( \mathbb{F}_q \);
- \( \left( \frac{a}{p} \right) \) denotes the Legendre symbol for \( 1 \leq a \leq p - 1 \);
- \( p^* = \left( \frac{-1}{p} \right)p = (-1)^{\frac{p-1}{2}}p \);
- \( \xi_p = e^{\frac{2\pi i}{p}} \) is the primitive \( p \)-th root of unity;
- \( \Omega_n = \{e_1 = (1, 0, \ldots, 0), e_2 = (0, 1, \ldots, 0), \ldots, e_n = (0, 0, \ldots, 1)\} \) is the standard basis of the \( n \)-dimensional Hilbert space.

2.2. Characters over finite fields. In this subsection we introduce characters over finite fields.

An additive character of \( \mathbb{F}_q \) is a nonzero function \( \chi \) from \( \mathbb{F}_q \) to the set of nonzero complex numbers of absolute value 1 with \( \chi(g + h) = \chi(g)\chi(h) \) for all \( g, h \in \mathbb{F}_q \). For each \( b \in \mathbb{F}_q \), the function

\[
\chi_b(c) = \xi_p^{\text{Tr}_q^m(bc)} \text{ for all } c \in \mathbb{F}_q,
\]

(3)

defines an additive character of \( \mathbb{F}_q \). The character \( \chi_0(c) = 1 \) for all \( c \in \mathbb{F}_q \) is called the trivial additive character of \( \mathbb{F}_q \). As \( b = 1 \) the character \( \chi_1 \) in (3) is the canonical additive character of \( \mathbb{F}_q \).

Characters of the multiplicative group of \( \mathbb{F}_q \) are called multiplicative character of \( \mathbb{F}_q \). All the multiplicative characters of \( \mathbb{F}_q \) are given by

\[
\psi_j(g^k) = \xi_{q-1}^{jk}, k = 0, 1, \ldots, q - 2,
\]

where \( 0 \leq j \leq q - 2 \) and \( g \) is a generator of \( \mathbb{F}_q^* \). For \( j = \frac{q-1}{2} \), we have the quadratic character \( \eta = \psi_{(q-1)/2} \). All the multiplicative characters form a group, called the multiplicative character group and denoted by \( \hat{\mathbb{F}}_q^* \), which is isomorphic to the multiplicative group of the finite field \( \mathbb{F}_q^* \).

2.3. Walsh transformation and weakly regular bent functions. Let \( f(x) \) be a function from \( \mathbb{F}_q \) to \( \mathbb{F}_p \). The Walsh (Hadamard) transform of \( f(x) \) is defined by

\[
W_f(a) = \sum_{x \in \mathbb{F}_q} \xi_p^{f(x) - \text{Tr}_q^m(ax)}, a \in \mathbb{F}_q.
\]

An \( p \)-ary function from \( \mathbb{F}_q \) to \( \mathbb{F}_p \) is called a bent function if \( W_f(a) = \pm p^{m/2} \) for all \( a \in \mathbb{F}_q \). A bent function \( f \) satisfies (cf. [14])

\[
\pm p^{-m/2}W_f(a) = \begin{cases} 
\pm \xi_p^{f(a)}, & n \text{ even or } n \text{ odd and } p \equiv 1 \mod 4, \\
\pm \sqrt{-1}\xi_p^{f(a)}, & n \text{ odd and } p \equiv 3 \mod 4,
\end{cases}
\]
where $f^*$ is the dual of $f$. Accordingly, $f$ is regular if $W_f(a) = p^{m/2}ξ_p^f(a)$ for all $a ∈ F_q$. If for some complex numbers $u$ with unit magnitude we have $W_f(a) = up^{m/2}ξ_p^f(a)$ for all $a ∈ F_q$, then we call $f$ weakly regular. From [14, 15], we know that a weakly regular bent function $f(x)$ satisfies

$$W_f(b) = ε\sqrt{p^m}ξ_p^f(b),$$

where $ε = ±1$ is called the sign of the Walsh transform of $f(x)$. All known weakly regular bent functions over $F_p$ with odd characteristic $p$ are summarized in Table 1.

**Table 1.** Known weakly regular bent functions over $F_p$ with odd characteristic $p$

| Bent functions | $m$ | $p$ |
|----------------|-----|-----|
| $\sum_{i=0}^{(m/2)} Tr_1^m(ax_i^{p^i} + 1)$ | arbitrary | arbitrary |
| $\sum_{i=0}^{p^k-1} Tr_1^m(ax_i^{p^{i+p^k}(p^k-1)}) + Tr_1^m(ax_i^{p^{i+p^k}(p^k-1)}) c|p^k + 1$ | $m = 2k$ | arbitrary |
| $Tr_1^m(ax_i^{p^{i+p^k}(p^k-1)+3^k+1})$ | $m = 2k$ | $p = 3$ |
| $Tr_1^m(ax_i^{p^{i+p^k}(p^k-1)+3^k+1})$ | $m = 4k$ | arbitrary |
| $Tr_1^m(ax_i^{p^{i+p^k}(p^k-1)}), i \text{ odd}, \gcd(i, m) = 1$ | arbitrary | $p = 3$ |

Let $RF$ be the set of $p$-ary weakly regular bent functions with the following two properties:

- $f(0) = 0$;
- $f(ax) = a^h f(x)$ for any $a ∈ F_p^*$ and $x ∈ F_q$, where $h$ is a positive even integer with $\gcd(h - 1, p - 1) = 1$.

It is a routine to check that the set $RF$ contains all known weakly regular bent functions.

3. **Constructions of near-optimal codebooks**

In this section, we will introduce the proposed constructions of codebooks and show its near-optimality.

3.1. **Codebooks from $p$-ary linear codes.** Recall that every linear code can be obtained by (1) in the Section 1. For any $[n, k]$ $p$-ary linear codes $C_D$ defined in (1), we define an $(p^k, n)$ codebook $B(C_D)$ by

$$B(C_D) = \left\{ \frac{1}{\sqrt{n}}(ξ_p)^c : c ∈ C_D \right\},$$

where $(ξ_p)^c$ denotes the vector $((ξ_p)^{c_1}, (ξ_p)^{c_2}, \ldots, (ξ_p)^{c_n})$ for any codeword $c = (c_1, c_2, \ldots, c_n) ∈ C_D$. As indicated in [30], the above construction does not have a simple expression of the maximum magnitude $I_{\max}(B(C_D))$. In the following theorem, we give the parameters of codebook $B(C_D)$ and a simple expression of the maximum magnitude $I_{\max}(B(C_D))$ by choosing suitable defining sets from (1).

**Theorem 3.1.** Let $D ⊆ F_q^*$ be a defining set of a linear code satisfying $yD = D$ for every $y ∈ F_q^*$. For any $[n, k]$ $p$-ary linear codes $C_D$ defined in (1), the set $B(C_D)$ is an $(p^k, n)$ codebook with the maximum magnitude

$$I_{\max}(B(C_D)) = \frac{\max\left\{ \frac{p}{p-1}d_{\max} - n, n - \frac{p}{p-1}d_{\min} \right\}}{n}.$$
where $d_{\text{min}}$ and $d_{\text{max}}$ denote the minimum and maximum Hamming distance of the code $C_D$, respectively.

**Proof.** Let $n = \#D$ and $N_a = \#\{x \in D : \text{Tr}_1^m(ax) = 0\}$ for any $a \in \mathbb{F}_q^*$. Using the orthogonal relation of exponential sums, one can express $N_a$ as follows:

$$pN_a = \sum_{x \in D} \sum_{y \in \mathbb{F}_p} \xi_p^{xy} \text{Tr}_1^m(ax) = n + \sum_{x \in D} \sum_{y \in \mathbb{F}_p} \xi_p^{xy} \text{Tr}_1^m(ax) = n + (p-1) \sum_{x \in D} \chi_a(x) = n + (p-1) \chi_a(D).$$

We assume that $D = \{d_1, d_2, \ldots, d_n\}$. Let $wt(c_a)$ denote the Hamming weight of the codeword $c_a$ in $C_D$, where $c_a = (\text{Tr}_1^m(ad_1), \text{Tr}_1^m(ad_2), \ldots, \text{Tr}_1^m(ad_n))$. It is obvious that $wt(c_a) = n - N_a$. For any pair of distinct vectors $\mu_b = \frac{1}{\sqrt{n}} (\xi_p)^{\text{Tr}_1^m(b \cdot x) \in B(C_D)}$, $b = c$, $b \neq c$, we have

$$\mu_b \mu_c^H = \frac{1}{n} \sum_{i=1}^{n} \xi_p^{\text{Tr}_1^m(d_i(b-c))} = \frac{1}{n} \sum_{x \in D} \xi_p^{\text{Tr}_1^m((b-c)(x))} = \frac{1}{n} \chi((b-c)(D)).$$

Then we get

$$I_{\text{max}}(B(C_D)) = \max_{\mu_b \mu_c^H} |\mu_b \mu_c^H| = \frac{1}{n} \max_{a \in \mathbb{F}_q^*} |\chi_a(D)|.$$

Since $wt(c_a) = n - N_a = \frac{p-1}{p}(n - \chi_a(D))$, we have

$$\chi_a(D) = n - \frac{p}{p-1}wt(c_a), \text{for any } a \in \mathbb{F}_q^*.$$

It follows from (6) and (7) that

$$I_{\text{max}}(B(C_D)) = \frac{1}{n} \max_{a \in \mathbb{F}_q^*} \left| n - \frac{p}{p-1}wt(c_a) \right|.$$ 

The desired conclusion on $I_{\text{max}}(B(C_D))$ then follows. \qed

Many known linear codes (see, e.g., [12, 26, 37, 11]) constructed by (1) can be used to obtain codebooks with the maximum magnitude by Theorem 3.1. In [26], Tang takes the defining set by $D_f = \{x \in \mathbb{F}_p^m : f(x) = 0\}$ and obtains a class of three-weight linear codes, where $f(x)$ is a $p$-ary weakly regular bent function.
Lemma 3.2. [26] Let \( m \) be odd, \( f(x) \in \mathcal{RF} \) and \( D_f = \{ x \in \mathbb{F}_p^* : f(x) = 0 \} \). Then \( C_{D_f} \) is an \([p^{m-1} - 1, m]\) linear code with the following weight enumerator:

\[
1 + (p^{m-1} - 1)z^{(p-1)p^{m-2}} + \left(\frac{p-1}{2}\right)\left(p^{m-1} + p^{(m-1)/2}\right)z^{(p-1)(p^{m-2} - p^{(m-3)/2})} + \left(\frac{p-1}{2}\right)p^{m-1} - p^{(m-1)/2}\right)z^{(p-1)(p^{m-2} - p^{(m-3)/2})}.
\]

It is easy to see that \( yD_f = D_f \) for every \( y \in \mathbb{F}_p^* \). By Lemma 3.2 and Theorem 3.1, we have the following result.

Theorem 3.3. Let \( m > 1 \) and \( C_{D_f} \) be an \([p^{m-1} - 1, m]\) linear code defined in Lemma 3.2. Then the set \( B(C_{D_f}) \) is an \((p^m, p^{m-1} - 1)\) codebook with the maximum magnitude

\[
I_{\text{max}}(B(C_{D_f})) = \frac{p^{m-1} - 1}{p^{m-1} - 1}.
\]

Remark 1. (1) In the above theorem, the corresponding Welch bound is

\[
I_{\text{welch}} = \sqrt{\frac{p^m - p^{m-1} + 1}{(p^{m-1} - 1)(p^m - 1)}}.
\]

It is obvious that

\[
I_{\text{welch}} > \sqrt{\frac{p^m - p^{m-1}}{p^{m-1} - 1}} = \frac{p - 1}{p^m},
\]

and

\[
I_{\text{max}}(B(C_{D_f})) < \frac{p^{m-1}}{p^{m-1}} = \frac{1}{p^{m-1}}.
\]

Clearly, we have

\[
1 \leq \frac{I_{\text{max}}(B(C_{D_f}))}{I_{\text{welch}}} < \sqrt{\frac{p^m}{(p - 1)p^{m-1}}} = \sqrt{\frac{p}{p - 1}}.
\]

It is straightforward to show that \( I_{\text{max}}(B(C_{D_f})) \) of the proposed codebook asymptotically achieves the Welch bound equality for sufficiently large \( p \).

(2) If we set

\[
\mathcal{B} = B(C_{D_f}) \cup \Omega_{p^{m-1}-1},
\]

then \( \mathcal{B} \) is an \((p^m + p^{m-1} - 1, p^{m-1} - 1)\) codebook and

\[
I_{\text{max}}(\mathcal{B}) = \max\left\{\frac{p^{m-1} - 1}{p^{m-1} - 1}, \frac{1}{\sqrt{p^{m-1} - 1}}\right\} = \frac{1}{\sqrt{p^{m-1} - 1}},
\]

\[
I_{\text{welch}} = \sqrt{\frac{p^{m-1} + p^{m-2} - 2}{p^m}}.
\]

Thus, we have

\[
1 \leq \frac{I_{\text{max}}(B(C_{D_f}))}{I_{\text{welch}}} < \sqrt{\frac{p + 1}{p}}.
\]

Therefore, the maximum magnitude of new codebook \( \mathcal{B} \) asymptotically achieves the Welch bound equality for sufficiently large \( p \).

As shown in Table 1, there are five families of weakly regular bent functions. So we can generate a lot of codebooks which asymptotically achieve the Welch bound equality for sufficiently large \( p \). In the next subsection, we will propose another construction of codebooks.
3.2. Codebooks from special functions. In this subsection, we use some special functions over finite fields to propose a construction of codebooks.

**Theorem 3.4.** For $b \in \mathbb{F}_q^*$, and a nontrivial multiplicative character $\psi \in \mathbb{F}_q^*$, define the following vector:

$$
\mu_{\psi, b} = \frac{1}{\sqrt{q-1}} \left( \psi(x) \chi_1(bf(x)) \right)_{x \in \mathbb{F}_q^*} \in \mathbb{C}^{q-1},
$$

where $f(x)$ is a mapping from $\mathbb{F}_q$ to $\mathbb{F}_q$ with $f(0) = 0$ and $f(xz) - f(x)$ is a permutation of $\mathbb{F}_q$ for every $z \neq 1 \in \mathbb{F}_q^*$. Let

$$
\mathcal{B}_f = \{ \mu_{\psi, b}, \psi \in \mathbb{F}_q^* and b \in \mathbb{F}_q^* \}
$$

be a set of $(q-1)^2$ vectors. Then $\mathcal{B}_f$ is an $((q-1)^2, q-1)$ codebook and the maximum magnitude is given by

$$
I_{\text{max}}(\mathcal{B}_f) = \sqrt{q}.
$$

For proving the theorem, we need a result on character sums from [3].

**Lemma 3.5.** Let $f(x)$ be a mapping from $\mathbb{F}_q$ to $\mathbb{F}_q$ with $f(0) = 0$ and $f(xz) - f(x)$ is a permutation of $\mathbb{F}_q$ for every $z \neq 1 \in \mathbb{F}_q^*$. Then for every multiplicative character $\psi$ of $\mathbb{F}_q^*$ and additive character $\chi$ of $\mathbb{F}_q$ and $b \in \mathbb{F}_q^*$, we have

$$
\left| \sum_{x \in \mathbb{F}_q^*} \psi(x) \chi(bf(x)) \right| = \begin{cases} 
0, & \text{if } \chi \text{ is trivial and } \psi \text{ is nontrivial,} \\
1, & \text{if } \chi \text{ is nontrivial and } \psi \text{ is trivial,} \\
\sqrt{q}, & \text{if } \chi \text{ is nontrivial and } \psi \text{ is nontrivial.}
\end{cases}
$$

Now, we give the proof of Theorem 3.4.

**Proof.** For any pair of distinct vectors $\mu_{\psi_1, a}$ and $\mu_{\psi_2, b}$ in $\mathcal{B}_f$, we have

$$
\mu_{\psi_1, a}^H \mu_{\psi_2, b} = \frac{1}{q-1} \sum_{x \in \mathbb{F}_q^*} \psi_1 \psi_2^{-1}(x) \chi_1(af(x) - bf(x))
= \frac{1}{q-1} \sum_{x \in \mathbb{F}_q^*} \psi(x) \chi_1(\alpha f(x)),
$$

where $\psi = \psi_1 \psi_2^{-1}$ and $\alpha = a - b$. According to Lemma 3.5, we get that

$$
I_{\text{max}}(\mathcal{B}_f) = \max_{\psi_1, \psi_2 \in \mathbb{F}_q^*, a, b \in \mathbb{F}_q^*} |\mu_{\psi_1, a}^H \mu_{\psi_2, b}| = \frac{\sqrt{q}}{q-1}.
$$

**Remark 2.** (1) The Welch bound of an $((q-1)^2, q-1)$ codebook is $I_{\text{welch}} = \sqrt{\frac{q-2}{q^2-2q}}$. It is simple to check that

$$
\frac{I_{\text{max}}(\mathcal{B}_f)}{I_{\text{welch}}} < \sqrt{\frac{q}{q-1}}.
$$

Hence, $I_{\text{max}}(\mathcal{B}(C_D))$ of the proposed codebook asymptotically achieves the Welch bound equality for sufficiently large $q$.

(2) Let

$$
\mathcal{B} = \mathcal{B}_f \cup \Omega_{q-1},
$$

Advances in Mathematics of Communications Volume X, No. X (200X), X–XX
then $B$ is an $(q^2 - q, q - 1)$ codebook and

$$I_{\text{max}}(B) = \max \{ \frac{\sqrt{q}}{q - 1}, \frac{1}{\sqrt{q - 1}} \} = \frac{\sqrt{q}}{q - 1},$$

$$I_{\text{welch}} = \sqrt{\frac{q - 1}{q^2 - q - 1}}.$$  

Thus, we have

$$1 \leq \frac{I_{\text{max}}(B(C_D))}{I_{\text{welch}}} < \frac{q}{q - 1},$$

which implies that the maximum magnitude of new codebook $B$ asymptotically achieves the Welch bound equality for sufficiently large $q$.

**Remark 3.** By [3], we denote the set of functions which satisfy $f(0) = 0$ and $f(xz) - f(x)$ is a permutation of $\mathbb{F}_q$ for every $z \neq 1 \in \mathbb{F}_q^*$ by $\mathcal{PF}$. Then we have the following properties on $\mathcal{PF}$:

(i) $f(x) = ax^d \in \mathcal{PF}$, where $a \in \mathbb{F}_q^*$ and $\gcd(d, q - 1) = 1$;

(ii) If $L(x) = \sum_{i=0}^{m-1} a_i x^{p^i} \in \mathbb{F}_q[x]$ and $L(x)$ is a permutation polynomial over $\mathbb{F}_q$, then $L(x) \in \mathcal{PF}$;

(iii) If $g(x) = \sum_{i=0}^{m-1} a_i x^{p^i} \in \mathbb{F}_q[x]$ and $L(x)$ is a permutation polynomial over $\mathbb{F}_q$, then $L(g(x)) \in \mathcal{PF}$.

By Theorem 3.4 and Remark 3, one can obtain infinitely many codebooks whose maximum magnitude asymptotically meet the Welch bound.

### 4. Concluding remarks

In this paper, firstly, we proposed a construction of codebooks utilizing $p$-ary linear codes satisfying certain conditions. Namely, for every weakly regular bent functions, we define a special subset of $\mathbb{F}_q$ as the defining set of a linear code, then the codebooks generated by the construction can asymptotically achieve the Welch bound equality with sufficiently large alphabet size. We hope that this approach can be applied to generate more near-optimal codebooks. Secondly, We proposed another construction of codebooks based on the hybrid character sum of a special kind of functions. Furthermore, one can get infinitely many codebooks which asymptotically achieve the Welch bound equality for sufficiently large alphabet size by the second construction. We believe that our constructions especially the second method which uses characters of some special functions may have some applications in other areas such as compressed sensing, signal processing and so on.

### Acknowledgments

We are grateful to the two anonymous referees and the editor for useful comments and suggestions that improved the presentation and quality of this paper.

### References

[1] A. Calderbank and W. Kantor, The geometry of two-weight codes, *Bull. London Math. Soc.*, 18 (1986), 97–122.

[2] E. J. Candes and M. B. Wakin, An introduction to compressive sampling, *IEEE Signal Process*, 25 (2008), 21–30.
[3] X. W. Cao, J. F. Mi and S. D. Xu, Two constructions of approximately symmetric information complete positive operator-valued measures, *J. Math. Phys.*, 58 (2017), 062201, 12pp.

[4] X. W. Cao, W. Chou and X. Zhang, More constructions of near optimal codebooks associated with binary sequences, *Adv. Math. Commun.*, 11 (2017), 187–202.

[5] J. H. Conway, R. H. Hardin and N. J. A. Sloane, Packing lines, planes, etc.: Packings in Grassmannian spaces, *Exp. Math.*, 5 (1996), 139–159.

[6] P. Delsarte, J. M. Goethals and J. J. Seidel, Spherical codes and designs, *Geometry and Combinatorics*, (1991), 68–93.

[7] C. S. Ding, J. Q. Luo and H. Niederreiter, Two-weight codes punctured from irreducible cyclic codes, *Ser. Coding Theory Cryptol.*, 4 (2008), 119–124.

[8] C. S. Ding, Complex codebooks from combinatorial designs, *IEEE Trans. Inform. Theory*, 52 (2006), 4229–4235.

[9] C. S. Ding and T. Feng, A generic construction of complex codebooks meeting the Welch bound, *IEEE Trans. Inform. Theory*, 53 (2007), 4245–4250.

[10] C. S. Ding and H. Niederreiter, Cyclotomic linear codes of order 3, *IEEE Trans. Inform. Theory*, 53 (2007), 2274–2277.

[11] C. S. Ding, A construction of binary linear codes from Boolean functions, *Discret. Math.*, 339 (2016), 2288–2303.

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

[13] M. Fickus, D. G. Mixon and J. C. Tremain, Steiner equiangular tight frames, *Linear Algebra Appl.*, 436 (2012), 1014–1027.

[14] T. Helleseth and A. Kholosha, Monomial and quadratic bent functions over the finite fields of odd characteristic, *IEEE Trans. Inform. Theory*, 52 (2006), 2018–2032.

[15] T. Helleseth and A. Kholosha, New binomial bent functions over the finite fields of odd characteristic, *IEEE Trans. Inform. Theory*, 56 (2010), 4646–4652.

[16] S. Hong, H. Park, T. Helleseth and Y. S. Kim, Near optimal partial Hadamard codebook construction using binary sequences obtained from quadratic residue mapping, *IEEE Trans. Inform. Theory*, 60 (2014), 3698–3705.

[17] H. Hu and J. Wu, New constructions of codebooks nearly meeting the Welch bound with equality, *IEEE Trans. Inform. Theory*, 60 (2014), 1348–1355.

[18] V. I. Levenshtein, Bounds for packing of metric spaces and some of their applications, *Probl. Cybern.*, 40 (1983), 43–110.

[19] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge university press, 1997.

[20] G. J. Luo, X. W. Cao, D. Xu and J. Mi, Binary linear codes with two or three weights from niho exponents, *Cryptogr. Commun.*, 10 (2018), 301–318.

[21] J. L. Massey and T. Mittelholzer, Welch's bound and sequence sets for code-division multiple-access systems, *Sequences II, Springer New York*, (1993), 63–78.

[22] J. M. Renes, R. Blume-Kohout, A. Scot and C. Caves, Symmetric informationally complete quantum measurements, *J. Math. Phys.*, 45 (2004), 2171–2180.

[23] D. V. Sarwate, Meeting the Welch bound with equality, *Sequences and their Applications*, Springer London, (1999), 79–102.

[24] T. Strohmer and R. W. Heath, Grassmannian frames with applications to coding and communication, *Appl. Comput. Harmon. Anal.*, 14 (2003), 257–275.

[25] P. Tan, Z. C. Zhou and D. Zhang, A construction of codebooks nearly achieving the Levenshtein bound, *IEEE Signal Processing Letters*, 23 (2016), 1306–1309.

[26] C. M. Tang, N. Li, Y. Qi and Z. C. Zhou, Linear codes with two or three weights from weakly regular bent functions, *IEEE Trans. Inform. Theory*, 62 (2016), 1166–1176.

[27] L. R. Welch, Lower bounds on the maximum cross correlation of signals, *IEEE Trans. Inform. Theory*, 20 (1974), 397–399.

[28] W. Wootters and B. Fields, Optimal state-determination by mutually unbiased measurements, *Ann. Phys.*, 191 (1989), 363–381.

[29] P. Xia, S. Zhou and G. B. Giannakis, Achieving the Welch bound with difference sets, *IEEE Trans. Inform. Theory*, 51 (2005), 1900–1907.

[30] C. Xiang, C. S. Ding and S. Mesnager, Optimal codebooks from binary codes meeting the levenshtein bound, *IEEE Trans. Inform. Theory*, 61 (2015), 6526–6535.

[31] N. Y. Yu, A construction of codebooks associated with binary sequences, *IEEE Trans. Inform. Theory*, 58 (2012), 5522–5533.
Two classes of near-optimal codebooks

[32] N. Y. Yu, K. Feng and A. X. Zhang, A new class of near-optimal partial Fourier codebooks from an almost difference set, *Des. Codes Cryptogr.*, 71 (2014), 493–501.

[33] A. X. Zhang and K. Feng, Two classes of codebooks nearly meeting the Welch bound, *IEEE Trans. Inform. Theory*, 58 (2012), 2507–2511.

[34] A. X. Zhang and K. Feng, Construction of cyclotomic codebooks nearly meeting the Welch bound, *Des. Codes Cryptogr.*, 63 (2012), 209–224.

[35] Z. C. Zhou, C. S. Ding and N. Li, New families of codebooks achieving the Levenshtein bound, *IEEE Trans. Inf. Theory*, 60 (2014), 7382–7387.

[36] Z. C. Zhou and X. H. Tang, New nearly optimal codebooks from relative difference sets, *Adv. Math. Commun.*, 5 (2011), 521–527.

[37] Z. C. Zhou, N. Li, C. L. Fan and T. Helleseth, Linear codes with two or three weights from quadratic Bent functions, *Des. Codes Cryptogr.*, 81 (2016), 283–295.

Received March 2017; revised June 2017.

E-mail address: gjluo1990@163.com

E-mail address: xwcao@nuaa.edu.cn