Asymptotically optimal codebooks via the multiplicative characters

Xia Wu[1], Wei Lu[1*], Xiwang Cao[2]

Wednesday 2nd September, 2020

Abstract

In this paper, we describe three constructions of codebooks with multiplicative characters of finite fields. Our constructions generalize the first construction in A. X. Zhang and K. Q. Feng (IEEE Trans. Inf. Theory 58(4), 2507-2511, 2012) from one dimension to two dimensions. We determine the maximum cross-correlation amplitude of these codebooks by the orthogonal relation of multiplicative characters and the properties of Jacobi sum. We prove that all the codebooks we constructed are asymptotically optimal with respect to the Welch bound. The parameters of these codebooks are new.

Keywords: Codebook, asymptotically optimal, Welch bound, multiplicative character, Jacobi sum.
Mathematics Subject Classification: 94A05 11T24.

1 Introduction

An (N,K) codebook $\mathcal{C}=\{\mathbf{c}_0,\mathbf{c}_1,...,\mathbf{c}_{N-1}\}$ is a set of N unit-norm complex vectors $\mathbf{c}_i\in\mathbb{C}^K$ over an alphabet A, where $i=0,1,\ldots,N-1$. The size of A is called the alphabet size of $\mathcal{C}$. As a performance measure of a codebook in practical applications, the maximum cross-correlation magnitude of an (N,K) codebook $\mathcal{C}$ is defined by

$$I_{max}(\mathcal{C})=\max_{0\le i\ne j\le N-1}|\mathbf{c}_i\mathbf{c}_j^H|,$$

where $\mathbf{c}_j^H$ denotes the conjugate transpose of the complex vector $\mathbf{c}_j$. To evaluate an (N,K) codebook $\mathcal{C}$, it is important to find the minimum achievable $I_{max}(\mathcal{C})$ or its lower bound. The Welch bound [26] provides a well-known lower bound on $I_{max}(\mathcal{C})$,

$$I_{max}(\mathcal{C})\ge I_W=\sqrt{\frac{N-K}{(N-1)K}}.$$

The equality holds if and only if for all pairs of (i,j) with $i\ne j$

$$|\mathbf{c}_i\mathbf{c}_j^H|=\sqrt{\frac{N-K}{(N-1)K}}.$$

A codebook $\mathcal{C}$ achieving the Welch bound equality is called a maximum-Welch-bound-equality (MWBE) codebook [24] or an equiangular tight frame [14]. MWBE codebooks are employed in various applications including code-division multiple-access (CDMA) communication systems [21], communications [24], combinatorial designs [3, 4, 28], packing [2], compressed sensing [1], coding theory [5] and quantum computing [22]. To our knowledge, only the following MWBE codebooks are presented as follows:

- (N,N) orthogonal MWBE codebooks for any $N>1$ [24, 28];

This work was supported by the National Natural Science Foundation of China (Grant No. 11971102, 11801070, 11771007, 61572027) and the Basic Research Foundation (Natural Science).
[1]School of Mathematics, Southeast University, Nanjing 210096, China. (Email: wuxia80@seu.edu.cn)
[1]School of Mathematics, Southeast University, Nanjing 210096, China. (Email:luwei1010@seu.edu.cn)
[2]Department of Math, Nanjing University of Aeronautics and Astronautics, Nanjing 211100, China. (Email: xwcao@nuaa.edu.cn)
*Corresponding author. (Email: luwei1010@seu.edu.cn)

- $(N, N-1)$ MWBE codebooks for $N > 1$ based on discrete Fourier transformation matrices [24, 28] or m-sequences [24];
- (N, K) MWBE codebooks from conference matrices [2, 25], where $N = 2K = 2^{d+1}$ for a positive integer d or $N = 2K = p^d + 1$ for an odd prime p and a positive integer d;
- (N, K) MWBE codebooks based on (N, K, λ) difference sets in cyclic groups [28] and abelian groups [3, 4];
- (N, K) MWBE codebooks from $(2, k, \nu)$-Steiner systems [6];
- (N, K) MWBE codebooks depended on graph theory and finite geometries [7–9, 23].

The construction of an MWBE codebook is known to be very hard in general, and the known classes of MWBE codebooks only exist for very restrictive N and K. Many researches have been done instead to construct asymptotically optimal codebooks, i.e., codebook $\mathcal{C}$ whose $I_{max}(\mathcal{C})$ asymptotically achieves the Welch bound. In [24], Sarwate gave some asymptotically optimal codebooks from codes and signal sets. As an extension of the optimal codebooks based on difference sets, various types of asymptotically optimal codebooks based on almost difference sets, relative difference sets and cyclotomic classes were proposed, see [3, 10, 30–32]. Asymptotically optimal codebooks constructed from binary row selection sequences were presented in [11, 29]. In [12, 13, 16–19], some asymptotically optimal codebooks were constructed via Jacobi sums and hyper Eisenstein sum.

In this paper, we describe three constructions of codebooks with multiplicative characters of finite fields. Our construction generalize the first construction in [30] from one dimension to two dimensions. We determine the maximum cross-correlation amplitude of these codebooks by the orthogonal relation of multiplicative characters and the properties of Jacobi sum. We prove that all the codebooks we constructed are asymptotically optimal with respect to the Welch bound. The parameters of these codebooks are new. As a comparison, in Table 1, we list the parameters of some known classes of asymptotically optimal codebooks and those of the new ones.

This paper is organized as follows. In section 2, we recall some notations and basic results which will be needed in our discussion. In section 3, we present three constructions of asymptotically optimal codebooks. In section 4, we conclude this paper.

2 Preliminaries

In this section, we introduce some basic results on characters and character sums over finite fields, which will play important roles in the constructions of codebooks.

In this paper, we set q be a power of an odd prime p, and $\mathbb{F}_q$ be a finite field with q elements. For a set E, $\#E$ denotes the cardinality of E.

2.1 Multiplicative characters over finite fields

Let $\mathbb{F}_q$ be a finite field. In this subsection, we recall the definitions of the multiplicative characters of $\mathbb{F}_q$.

As in [20], the multiplicative characters of $\mathbb{F}_q$ is defined as follows. For $j = 0, 1, ..., q-2$, the functions φ^j defined by

$$\varphi^j(\alpha^i) = \zeta_{q-1}^{ij},$$

are all the multiplicative characters of $\mathbb{F}_q$, where $\zeta_{q-1} = e^{\frac{2\pi\sqrt{-1}}{q-1}}$, α is a primitive element of $\mathbb{F}_q^*$, and $0 \leq i \leq q-2$. If $j = 0$, we have $\varphi^0(x) = 1$ for any $x \in \mathbb{F}_q^*$, φ^0 is called the trivial multiplicative character of $\mathbb{F}_q$. Let $\widehat{\mathbb{F}_q^*}$ be the set of all the multiplicative characters of $\mathbb{F}_q$.

Let φ be a multiplicative character of $\mathbb{F}_q$. The orthogonal relation of multiplicative characters (see [20]) is given by

$$\sum_{x \in \mathbb{F}_q^*} \varphi(x) = \begin{cases} q-1, & \text{if } \varphi = \varphi^0, \\ 0, & \text{otherwise.} \end{cases}$$

Table 1: The parameters of codebooks asymptotically meeting the Welch bound

Parameters (N, K)	I_{max}	References
$(p^n, K = \frac{p-1}{2p}(p^n + p^{n/2}) + 1)$ with odd p	$\frac{(p+1)p^{n/2}}{2pK}$	[11]
$(q^2, \frac{(q-1)^2}{2})$, $q = p^s$ with odd p	$\frac{q+1}{(q-1)^2}$	[30]
$q(q+4)$, $\frac{q+1}{2}$, q is a prime power	$\frac{1}{q+1}$	[15]
$(q, \frac{(q+3)(q+1)}{2})$, q is a prime power	$\frac{\sqrt{q}+1}{q-1}$	[15]
$(p^n - 1, \frac{p^n-1}{2})$ with odd p	$\frac{\sqrt{p^n}+1}{p^n-1}$	[29]
$(q^l + q^{l-1} - 1, q^{l-1})$ for any $l > 2$	$\frac{1}{\sqrt{q^{l-1}}}$	[32]
$((q-1)^k + q^{k-1}, q^{k-1})$, for any $k > 2$ and $q \geq 4$	$\frac{\sqrt{q^{k+1}}}{(q-1)^k+(-1)^{k+1}}$	[12]
$((q-1)^k + K, K)$, for any $k > 2$, where $K = \frac{(q-1)^k+(-1)^{k+1}}{q}$	$\frac{\sqrt{q^{k-1}}}{K}$	[12]
$((q^s - 1)^n + K, K)$, for any $s > 1$ and $n > 1$, where $K = \frac{(q^s-1)^n+(-1)^{n+1}}{q}$)	$\frac{\sqrt{q^{sn+1}}}{(q^s-1)^n+(-1)^{n+1}}$	[17]
$((q^s - 1)^n + q^{sn-1}, q^{sn-1})$, for any $s > 1$ and $n > 1$	$\frac{\sqrt{q^{sn+1}}}{(q^s-1)^n+(-1)^{n+1}}$	[17]
$(q-1, \frac{q(r-1)}{2r})$, $r = p^t, q = r^s$, with odd p and $p \nmid s$	$\frac{\sqrt{r}}{\sqrt{q}(\sqrt{r}-1)K}$	[27]
$(q^2, \frac{q(q+1)(r-1)}{2r})$, $r = p^t, q = r^s$, with odd p	$\frac{(r+1)q}{2rK}$	[27]
$((q-1)^2, \frac{q^2-4q+5}{2})$, q is an odd prime power	$\frac{q-2+\sqrt{q}}{2K}$, when $q \geq 9$; $\frac{q+1}{2K}$, when $q < 9$,	this paper
$((q-1)^2, \frac{(q-1)(q-3)}{2})$, q is an odd prime power	$\frac{q-2+\sqrt{q}}{2K}$, when $q \geq 9$; $\frac{q+1}{2K}$, when $q < 9$,	this paper
$((q_1-1)(q_2-1), \frac{q_1q_2-2q_1-2q_2+5}{2})$, q_1 and q_2 are both odd prime powers	$\frac{q_2-2+\sqrt{q_1}}{2K}$, when $q_2 \geq q_1 \geq 9$	this paper

2.2 Jacobi sums over finite fields

Let φ_1 and φ_2 be two multiplicative characters of $\mathbb{F}_q$. The sum

$$J(\varphi_1, \varphi_2) = \sum_{x \in \mathbb{F}_q, x \neq 0,1} \varphi_1(x)\varphi_2(1-x)$$

is called a Jacobi sum in $\mathbb{F}_q$.

The values of Jacobi sums are given as follows.

Lemma 2.1. *[12, Lemma 10, Lemma 11] For the values of Jacobi sums, we have the following results.*
(1) *If φ_1 and φ_2 are trivial, then $J(\varphi_1, \varphi_2) = q - 2$.*
(2) *If one of the φ_1 and φ_2 is trivial, the other is nontrivial, $J(\varphi_1, \varphi_2) = -1$.*
(3) *If φ_1 and φ_2 are both nontrivial and $\varphi_1\varphi_2$ is nontrivial, then $|J(\varphi_1, \varphi_2)| = \sqrt{q}$.*
(4) *If φ_1 and φ_2 are both nontrivial and $\varphi_1\varphi_2$ is trivial, then $|J(\varphi_1, \varphi_2)| = 1$.*

2.3 A general construction of codebooks

Let D be a set and $K = \#D$. Let E be a set of some functions which satisfy

$$f : D \to S, \quad \text{where S is the unit circle on the complex plane.}$$

A general construction of codebooks is stated as follows in the complex plane,

$$\mathcal{C}(D; E) = \{\mathbf{c}_f := \frac{1}{\sqrt{K}}(f(x))_{x \in D}, f \in E\}.$$

3 Constructions of codebooks asymptotically achieving the Welch bound

In this section, by multiplicative characters of finite fields, we construct new series of codebooks which asymptotically achieving the Welch bound. Our constructions are inspired by the first construction in [30], and we generalize the result in [30] from one dimension to two dimensions.

Let η be the quadratic character of $\mathbb{F}_q^*$. Let $\mathbb{F}_q^* \times \mathbb{F}_q^*$ be the product of $\mathbb{F}_q^*$ and $\mathbb{F}_q^*$. Let

$$D = \{(x_1, x_2) \in \mathbb{F}_q^* \times \mathbb{F}_q^* \mid \eta(x_1 + 1)\eta(x_2 + 1) = 1\}$$

be a subset of $\mathbb{F}_q^* \times \mathbb{F}_q^*$. Then $K = \#D = (\frac{q-1}{2})(\frac{q-1}{2}) + (\frac{q-3}{2})(\frac{q-3}{2}) = \frac{q^2-4q+5}{2}$. Let

$$E = \widehat{\mathbb{F}_q^*} \times \widehat{\mathbb{F}_q^*} = \{(\varphi_1, \varphi_2) \mid \varphi_1 \in \widehat{\mathbb{F}_q^*}, \ \varphi_2 \in \widehat{\mathbb{F}_q^*}\}.$$

Then

$$\mathcal{C} = \mathcal{C}(D; E) = \{\mathbf{c}_{\varphi_1,\varphi_2} = \frac{1}{\sqrt{K}}(\varphi_1(x_1)\varphi_2(x_2))_{(x_1,x_2) \in D}, \ \varphi_1, \varphi_2 \in \widehat{\mathbb{F}_q^*}\}.$$

For $x_1, x_2 \in \mathbb{F}_q^*$, we set

$$\delta(x_1, x_2) = \begin{cases} \frac{1+\eta(x_1+1)\eta(x_2+1)}{2}, & \text{if } x_1 \neq -1 \text{ and } x_2 \neq -1, \\ 0, & \text{if } x_1 = -1 \text{ or } x_2 = -1. \end{cases}$$

Through the definition of D, we known that

$$\delta(x_1, x_2) = \begin{cases} 1, & \text{if } x \in D, \\ 0, & \text{otherwise.} \end{cases}$$

We can derive the following Theorem.

Theorem 3.1. *With the above notations, $\mathcal{C}$ is a codebook with $N = (q-1)^2$, $K = \frac{q^2-4q+5}{2}$ and*

$$I_{max}(\mathcal{C}) \leq \begin{cases} \frac{q-2+\sqrt{q}}{2K}, & \textit{when } q > 9, \\ \frac{q+1}{2K}, & \textit{otherwise.} \end{cases}$$

Proof. By the definition of $\mathcal{C}$, we know that $K = \frac{q^2-4q+5}{2}$. Let $\mathbf{c}_1 = \mathbf{c}_{\varphi_{11},\varphi_{12}}$, $\mathbf{c}_2 = \mathbf{c}_{\varphi_{21},\varphi_{22}}$, where $\varphi_{11}, \varphi_{12}, \varphi_{21}, \varphi_{22}$ are multiplicative characters of $\mathbb{F}_q$. Then the correlation of $\mathbf{c}_1$ and $\mathbf{c}_2$ is as follows.

$$
\begin{aligned}
& K\mathbf{c}_1\mathbf{c}_2^H \\
= & \sum_{(x_1,x_2)\in D} \varphi_{11}(x_1)\varphi_{12}(x_2)\overline{\varphi_{21}(x_1)\varphi_{22}(x_2)} \\
= & \sum_{(x_1,x_2)\in D} (\varphi_{11}\overline{\varphi_{21}})(x_1)(\varphi_{12}\overline{\varphi_{22}})(x_2) \\
= & \sum_{(x_1,x_2)\in D} \varphi_1(x_1)\varphi_2(x_2), \quad (\text{where } \varphi_1 = \varphi_{11}\overline{\varphi_{21}},\ \varphi_2 = \varphi_{12}\overline{\varphi_{22}}) \\
= & \sum_{x_1\in\mathbb{F}_q^*, x_2\in\mathbb{F}_q^*} \varphi_1(x_1)\varphi_2(x_2)\delta(x_1,x_2) \\
= & \sum_{\substack{x_1\in\mathbb{F}_q^*, x_2\in\mathbb{F}_q^* \\ x_1,x_2\neq -1}} \varphi_1(x_1)\varphi_2(x_2)\frac{1+\eta(x_1+1)\eta(x_2+1)}{2} \\
= & \frac{1}{2}\Big(\sum_{\substack{x_1\in\mathbb{F}_q^*, x_2\in\mathbb{F}_q^* \\ x_1,x_2\neq -1}} \varphi_1(x_1)\varphi_2(x_2) + \sum_{\substack{x_1\in\mathbb{F}_q^*, x_2\in\mathbb{F}_q^* \\ x_1,x_2\neq -1}} \varphi_1(x_1)\varphi_2(x_2)\eta(x_1+1)\eta(x_2+1)\Big) \\
= & \frac{1}{2}\Big(\sum_{x_1\in\mathbb{F}_q^*, x_2\in\mathbb{F}_q^*} \varphi_1(x_1)\varphi_2(x_2) - \sum_{x_1=-1, x_2\in\mathbb{F}_q^*} \varphi_1(x_1)\varphi_2(x_2) - \sum_{x_1\in\mathbb{F}_q^*, x_2=-1} \varphi_1(x_1)\varphi_2(x_2) \\
& +\varphi_1(-1)\varphi_2(-1) + \sum_{x_1\in\mathbb{F}_q^*, -x_1\neq 1} \varphi_1(x_1)\eta(x_1+1) \sum_{x_2\in\mathbb{F}_q^*, -x_2\neq 1} \varphi_2(x_2)\eta(x_2+1)\Big) \\
= & \frac{1}{2}\Big(\sum_{x_1\in\mathbb{F}_q^*} \varphi_1(x_1) \sum_{x_2\in\mathbb{F}_q^*} \varphi_2(x_2) - \varphi_1(-1)\sum_{x_2\in\mathbb{F}_q^*} \varphi_2(x_2) - \varphi_2(-1)\sum_{x_1\in\mathbb{F}_q^*} \varphi_1(x_1) + \\
& +\varphi_1(-1)\varphi_2(-1) + \sum_{x_1\in\mathbb{F}_q^*, x_1\neq 1} \varphi_1(-x_1)\eta(-x_1+1) \sum_{x_2\in\mathbb{F}_q^*, x_2\neq 1} \varphi_2(-x_2)\eta(-x_2+1)\Big) \\
= & \frac{1}{2}\Big(\sum_{x_1\in\mathbb{F}_q^*} \varphi_1(x_1) \sum_{x_2\in\mathbb{F}_q^*} \varphi_2(x_2) - \varphi_1(-1)\sum_{x_2\in\mathbb{F}_q^*} \varphi_2(x_2) - \varphi_2(-1)\sum_{x_1\in\mathbb{F}_q^*} \varphi_1(x_1) + \\
& +\varphi_1(-1)\varphi_2(-1) + \varphi_1(-1)\varphi_2(-1) \sum_{x_1\in\mathbb{F}_q^*, x_1\neq 1} \varphi_1(x_1)\eta(-x_1+1) \sum_{x_2\in\mathbb{F}_q^*, x_2\neq 1} \varphi_2(x_2)\eta(-x_2+1)\Big) \\
= & \frac{1}{2}\Big(\sum_{x_1\in\mathbb{F}_q^*} \varphi_1(x_1) \sum_{x_2\in\mathbb{F}_q^*} \varphi_2(x_2) - \varphi_1(-1)\sum_{x_2\in\mathbb{F}_q^*} \varphi_2(x_2) - \varphi_2(-1)\sum_{x_1\in\mathbb{F}_q^*} \varphi_1(x_1) + \\
& +\varphi_1(-1)\varphi_2(-1) + \varphi_1(-1)\varphi_2(-1)J(\varphi_1,\eta)J(\varphi_2,\eta)\Big).
\end{aligned}
$$

By Lemma 2.1 and the orthogonal relation of multiplicative characters, we have the following results. When φ_1 is trivial and φ_2 is nontrivial,

$$K\mathbf{c}_1\mathbf{c}_2^H = -\frac{1}{2}\varphi_2(-1)(q-2+J(\varphi_2,\eta)).$$

Thus

$$|\mathbf{c}\mathbf{c}'^H| \leq \frac{q-2+\sqrt{q}}{2K}.$$

When φ_1 is nontrivial and φ_2 is trivial,

$$K\mathbf{c}_1\mathbf{c}_2^H = -\frac{1}{2}\varphi_1(-1)(q-2+J(\varphi_1,\eta)).$$

Thus

$$|\mathbf{c}\mathbf{c}'^H| \leq \frac{q-2+\sqrt{q}}{2K}.$$

When φ_1 is nontrivial and φ_2 is nontrivial,

$$K\mathbf{c}_1\mathbf{c}_2^H = -\frac{1}{2}\varphi_1\varphi_2(-1)(1+J(\varphi_1,\eta)J(\varphi_2,\eta)).$$

Thus

$$|\mathbf{c}\mathbf{c}'^H| \le \frac{1+q}{2K}.$$

Therefore, we have $N=(q-1)^2$ and

$$I_{max}(\mathcal{C}) = \max\{|\mathbf{c}_1\mathbf{c}_2^H| : \mathbf{c}_1,\mathbf{c}_2 \in \mathcal{C}, \text{and } \mathbf{c}_1 \ne \mathbf{c}_2\} \le \begin{cases} \frac{q-2+\sqrt{q}}{2K}, & \text{when } q>9,\\ \frac{q+1}{2K}, & \text{otherwise.}\end{cases}$$

□

Using Theorem 3.1, we can derive the ratio of $I_{max}(\mathcal{C})$ of the proposed codebooks to that of the Welch bound and show the asymptotic optimality of the proposed codebooks as in the following theorem.

Theorem 3.2. *We have*

$$\lim_{q\to\infty}\frac{I_{max}(\mathcal{C})}{I_W}=1,$$

then the codebooks we proposed are asymptotically optimal.

Proof. Note that $N=(q-1)^2$ and $K=\frac{q^2-4q+5}{2}$. Then the corresponding Welch bound is

$$I_W=\sqrt{\frac{N-K}{(N-1)K}}=\sqrt{\frac{(q-1)^2-\frac{q^2-4q+5}{2}}{((q-1)^2-1)\frac{q^2-4q+5}{2}}}=\sqrt{\frac{q^2-3}{q(q-2)(q^2-4q+5)}},$$

it is obvious that

$$\lim_{q\to+\infty}\frac{I_{max}(\mathcal{C})}{I_W} \le \lim_{q\to+\infty}\frac{\frac{q-2+\sqrt{q}}{(q^2-4q+5)}}{\sqrt{\frac{q^2-3}{q(q-2)(q^2-4q+5)}}}=1.$$

The codebook $\mathcal{C}$ asymptotically meets the Welch bound. This completes the proof. □

In Table 2, we provide some explicit values of the parameters of the codebooks we proposed for some given q, and corresponding numerical data of the Welch bound for comparison. The numerical results show that the codebooks asymptotically meet the Welch bound.

Table 2: Parameters of the (N,K) codebook

q	N	K	$I_{max}(\mathcal{C})$	I_W	$\frac{I_{max}(\mathcal{C})}{I_W}$
3	4	1	2	1	2
5	16	5	0.6	0.3830	1.5667
13	144	61	0.1197	0.0975	1.2273
49	2304	1105	0.0244	0.0217	1.1257
5^3	15376	7565	0.0089	0.0082	1.0822
5^4	389376	194065	0.0017	0.0016	1.0385
7^4	5760000	2877601	$4.2535e-04$	$4.1701e-04$	1.0200
11^4	214329600	107150161	$6.8875e-05$	$6.8315e-05$	1.0082

Similarly, we have the following two constructions.

Theorem 3.3. *Let*

$$D=\{(x_1,x_2)\in\mathbb{F}_q^*\times\mathbb{F}_q^* \mid \eta(x_1+1)\eta(x_2+1)=-1\}$$

be a subset of $\mathbb{F}_q^*\times\mathbb{F}_q^*$. *Let*

$$E=\widehat{\mathbb{F}_q^*}\times\widehat{\mathbb{F}_q^*}=\{(\varphi_1,\varphi_2)\mid \varphi_1\in\widehat{\mathbb{F}_q^*},\ \varphi_2\in\widehat{\mathbb{F}_q^*}\}.$$

Then

$$\mathcal{C}=\mathcal{C}(D;E)=\{\mathbf{c}_{\varphi_1,\varphi_2}=\frac{1}{\sqrt{K}}(\varphi_1(x_1)\varphi_2(x_2))_{(x_1,x_2)\in D},\ \varphi_1,\varphi_2\in\widehat{\mathbb{F}_q^*}\},$$

is a (N,K) *codebook with* $N=(q-1)^2$ *and* $K=\frac{(q-1)(q-3)}{2}$.

Moreover,

$$I_{max}(\mathcal{C})\le\begin{cases}\frac{q-2+\sqrt{q}}{2K}, & \text{when } q>9,\\ \frac{q+1}{2K}, & \text{otherwise.}\end{cases}$$

and

$$\lim_{q\to\infty}\frac{I_{max}(\mathcal{C})}{I_W}=1,$$

that is to say the codebooks are asymptotically optimal.

Theorem 3.4. *Let* q_1 *and* q_2 *be powers of odd primes. Let*

$$D=\{(x_1,x_2)\in\mathbb{F}_{q_1}^*\times\mathbb{F}_{q_2}^*\mid\eta_1(x_1+1)\eta_2(x_2+1)=1\}$$

be a subset of $\mathbb{F}_{q_1}^*\times\mathbb{F}_{q_2}^*$. *Let*

$$E=\widehat{\mathbb{F}_{q_1}^*}\times\widehat{\mathbb{F}_{q_2}^*}=\{(\varphi_1,\varphi_2)\mid\varphi_1\in\widehat{\mathbb{F}_{q_1}^*},\ \varphi_2\in\widehat{\mathbb{F}_{q_2}^*}\}.$$

Then

$$\mathcal{C}=\mathcal{C}(D;E)=\{\mathbf{c}_{\varphi_1,\varphi_2}=\frac{1}{\sqrt{K}}(\varphi_1(x_1)\varphi_2(x_2))_{(x_1,x_2)\in D},\ \varphi_1\in\widehat{\mathbb{F}_{q_1}^*},\varphi_2\in\widehat{\mathbb{F}_{q_2}^*}\},$$

is a (N,K) *codebook with* $N=(q_1-1)(q_2-1)$, $K=\frac{q_1q_2-2q_1-2q_2+5}{2}$.

Moreover,

$$I_{max}(\mathcal{C})\le\max\{\frac{q_1-2+\sqrt{q_2}}{2K},\ \frac{q_2-2+\sqrt{q_1}}{2K},\ \frac{1+\sqrt{q_1q_2}}{2K}\}.$$

If $q_1,q_2\longrightarrow\infty$ *and* $|q_1-q_2|=O(1)$, *then* $I_{max}(\mathcal{C})$ *is asymptotically meet the Welch bound.*

The proofs of the above two theorems are similar as those of Theorem 3.1 and 3.2.

4 Concluding remarks

In this paper, we described three constructions of codebooks asymptotically achieving the Welch bounds with multiplicative characters of finite fields. Our constructions generalize the first construction in [30] from one dimension to two dimensions. The parameters of the codebooks in this paper and those of known asymptotically optimal codebooks with respect to the Welch bound are summarized in Table 1. The parameters of our asymptotic codebooks are new. The analysis of the parameters of our codebooks is mainly based on Jacobi sums and orthogonal relation of multiplicative characters.

References

[1] Candes E. and Wakin M.: An introduction to compressive sampling, IEEE Signal Process. Mag. **25**(2), 21-30 (2008).

[2] Conway J., Harding R., and Sloane N.: Packing lines, planes, etc.: Packings in Grassmannian spaces. Exp. Math. **5**(2), 139-159 (1996).

[3] Ding C.: Complex codebooks from combinatorial designs. IEEE Trans. Inf. Theory **52**(9), 4229-4235 (2006).

[4] Ding C. and Feng T.: A generic construction of complex codebooks meeting the Welch bound. IEEE Trans. Inf. Theory **53**(11), 4245-4250 (2007).

[5] Delsarte P., Goethals J., and Seidel J.: Spherical codes and designs. Geometriae Dedicate **67**(3), 363-388 (1997).

[6] Fickus M., Mixon D., and Tremain J.: Steiner equiangular tight frames. Linear Algebra Appl. **436**(5), 1014-1027 (2012).

[7] Fickus M. and Mixon D.: Tables of the existence of equiangular tight frames. arxiv:1504.00253v2, (2016).

[8] Fickus M., Mixon D. and Jasper J.: Equiangular tight frames from hyperovals. IEEE Trans. Inf. Theory **62**(9), 5225-5236 (2016).

[9] Fickus M., Jasper J., Mixon D. and Peterson J.: Tremain equiangular tight frames. arxiv:1602.03490v1, (2016).

[10] Hu H. and Wu J.: New constructions of codebooks nearly meeting the Welch bound with equality. IEEE Trans. Inf. Theory **60**(2), 1348-1355 (2014).

[11] Hong S., Park H., Helleseth T., and Kim Y.: Near optimal partial Hadamard codebook construction using binary sequences obtained from quadratic residue mapping. IEEE Trans. Inf. Theory **60**(6), 3698-3705 (2014).

[12] Heng Z., Ding C., Yue Q.: New constructions of asymptotically optimal codebooks with multiplicative characters. IEEE Trans. Inf. Theory **63**(10), 6179-6187 (2017).

[13] Heng Z.: Nearly optimal codebooks based on generalized Jacobi sums. Discrete Appl. Math. **250**, 227-240 (2018).

[14] Kovacevic J.and Chebira A.: An introduction to frames. Found. Trends Signal Process. **2**(1), 1-94 (2008).

[15] Li C., Qin Y., Huang Y.: Two families of nearly optimal codebooks. Des. Codes Cryptogr. **75**(1), 43- 57 (2015).

[16] Lu W., Wu X., Cao X., Chen M.: Six constructions of asymptotically optimal codebooks via the character sums. Des. Codes Cryptogr. **88**(6), 1139- 1158 (2020).

[17] Luo G., Cao X.: Two constructions of asymptotically optimal codebooks via the hyper Eisenstein sum. IEEE Trans. Inf. Theory **64**(10), 6498-6505 (2018).

[18] Luo G., Cao X.: New constructions of codebooks asymptotically achieving the Welch bound. in Proc. IEEE Int. Symp. Inf. Theory, Vail, CO, USA, 2346-2349 (2018).

[19] Luo G., Cao X.: Two constructions of asymptotically optimal codebooks. Crypt. Commun. **11**(4), 825-838 (2019).

[20] Lidl R. and Niederreiter H., Finite fields. Cambridge university press, (1997).

[21] Massey J. and Mittelholzer T.: Welch's bound and sequence sets for code-division multiple-access systems. Sequences II, Springer New York, 63-78 (1999).

[22] Renes J., Blume-Kohout R., Scot A., and Caves C.: Symmetric informationally complete quantum measurements. J. Math. Phys. **45**(6), 2171-2180 (2004).

[23] Rahimi F.: Covering graphs and equiangular tight frames. Ph.D. Thesis, University of Waterloo, Ontario, (2016) (available at http://hdl.handle.net/10012/10793).

[24] Sarwate D.: Meeting the Welch bound with equality. New York, NY, USA:Springer-Verlag, 63-79 (1999).

[25] Strohmer T. and Heath R.: Grassmannian frames with applications to coding and communication. Appl. Comput. Harmon. Anal. **14**(3), 257-275 (2003).

[26] Welch L.: Lower bounds on the maximum cross correlation of signals. IEEE Trans. Inf. Theory **20**(3), 397-399 (1974).

[27] Wu X., Lu W., Cao X.: Two constructions of asymptotically optimal codebooks via the trace functions. Crypt. Commun. (2020). [online]. Available:https://doi.org/10.1007/s12095-020-00448-w.

[28] Xia P., Zhou S., and Giannakis G.: Achieving the Welch bound with difference sets. IEEE Trans. Inf. Theory **51**(5), 1900-1907 (2005).

[29] Yu N.: A construction of codebooks associated with binary sequences. IEEE Trans. Inf. Theory **58**(8), 5522-5533 (2012).

[30] Zhang A. and Feng K.: Two classes of codebooks nearly meeting the Welch bound. IEEE Trans. Inf. Theory **58**(4), 2507-2511 (2012).

[31] Zhang A. and Feng K.: Construction of cyclotomic codebooks nearly meeting the Welch bound," Des. Codes Cryptogr. **63**(2), 209-224 (2013).

[32] Zhou Z., Tang X.: New nearly optimal codebooks from relative difference sets. Adv. Math. Commun. **5**(3), 521-527 (2011).