Designs, Codes and Cryptography (2020) 88:1139–1158
https://doi.org/10.1007/s10623-020-00735-w

Six constructions of asymptotically optimal codebooks via the character sums

Wei Lu[1] · Xia Wu[1] · Xiwang Cao[2] · Ming Chen[3]

Received: 29 May 2019 / Revised: 1 February 2020 / Accepted: 4 February 2020 /
Published online: 14 February 2020

Abstract
In this paper, using additive characters of finite field, we find a codebook which is equivalent to the measurement matrix in Mohades et al. (IEEE Signal Process Lett 21(7):839–843, 2014). The advantage of our construction is that it can be generalized naturally to construct the other five classes of codebooks using additive and multiplicative characters of finite field. We determine the maximum cross-correlation amplitude of these codebooks by the properties of characters and character sums. 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 · Asymptotic optimality · Welch bound · Gauss sum · Jacobi sum

Mathematics Subject Classification 94A05 · 11T24

Communicated by T. Helleseth.

This work was supported by the National Natural Science Foundation of China (Grant Nos. 11971102, 11801070, 11771007, and 61572027) and the Basic Research Foundation (Natural Science).

✉ Xia Wu
wuxia80@seu.edu.cn

Wei Lu
luwei1010@seu.edu.cn

Xiwang Cao
xwcao@nuaa.edu.cn

Ming Chen
chenming@seu.edu.cn

[1] School of Mathematics, Southeast University, Nanjing 210096, China

[2] Department of Math, Nanjing University of Aeronautics and Astronautics, Nanjing 211100, China

[3] School of Information Science and Engineering, Southeast University, Nanjing 210096, China

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 [27] 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 [20], communications [24], combinatorial designs [3,4,29], packing [2], compressed sensing [1], coding theory [5] and quantum computing [23]. To our knowledge, only the following MWBE codebooks are presented as follows:

- (N, N) orthogonal MWBE codebooks for any $N > 1$ [24,29];
- $(N, N-1)$ MWBE codebooks for $N > 1$ based on discrete Fourier transformation matrices [24,29] 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 [29] and abelian groups [3,4];
- (N, K) MWBE codebooks from $(2, k, v)$-Steiner systems [7];
- (N, K) MWBE codebooks depended on graph theory and finite geometries [6,8,9,22].

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 [3,13,31–33]. Asymptotically optimal codebooks constructed from binary row selection sequences were presented in [12,30]. In [10,11,17–19], some asymptotically optimal codebooks were constructed via Jacobi sums and hyper Eisenstein sum.

In [21], the authors combined a Reed–Solomon generator matrix with itself by the tensor product and employed this generated matrix to construct a complex measurement matrix.

They proved that this matrix is asymptotically optimal according to the Welch bound. In this paper, we find a codebook which is equivalent to the measurement matrix in [21]. The codebook is actually the first construction in Sect. 3, using additive characters of finite field. The advantage of our construction is that it can be generalized naturally to construct the other five classes of codebooks using additive and multiplicative characters of finite field. We determine the maximum cross-correlation amplitude of these codebooks by the properties of characters and character sums. All of these codebooks we constructed are asymptotically optimal according to the Welch bound. 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 Sect. 2, we recall some notations and basic results which will be needed in our discussion. In Sect. 3, we present our six constructions of asymptotically optimal codebooks. In Sect. 4, we derive another family of codebooks, which are also asymptotically optimal. In Sect. 5, 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 a 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 Characters over finite fields

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

For each $a \in \mathbb{F}_q$, an additive character of $\mathbb{F}_q$ is defined by the function $\chi_a(x) = \zeta_p^{\mathrm{Tr}_{q/p}(ax)}$, where ζ_p is a primitive p-th root of complex unity and $\mathrm{Tr}_{q/p}(\cdot)$ is the trace function from $\mathbb{F}_q$ to $\mathbb{F}_p$. By the definition, $\chi_a(x) = \chi_1(ax)$. When $a = 0$, we call χ_0 the trivial additive character of $\mathbb{F}_q$. When $a = 1$, we call χ_1 the canonical additive character of $\mathbb{F}_q$. Let $\widehat{\mathbb{F}_q}$ be the set of all additive characters of $\mathbb{F}_q$. The orthogonal relation of additive characters (see [16]) is given by

$$\sum_{x\in\mathbb{F}_q} \chi_a(x) = \begin{cases} q, & \text{if } a = 0, \\ 0, & \text{otherwise.} \end{cases}$$

As in [16], 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 α is a primitive element of $\mathbb{F}_q^*$, and $0 \le i \le q-2$. 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 [16]) 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	$\frac{(p+1)p^{n/2}}{2pK}$	[12]
$(q^2, \frac{(q-1)^2}{2}), q = p^s$ with odd p	$\frac{q+1}{(q-1)^2}$	[31]
$(q(q+4), \frac{(q+3)(q+1)}{2}), q$ is a prime power	$\frac{1}{q+1}$	[15]
$(q, \frac{q-1}{2}), q$ is a prime power	$\frac{\sqrt{q}+1}{q-1}$	[15]
$(p^n - 1, \frac{p^n-1}{2})$ with odd p	$\frac{\sqrt{p^n}+1}{p^n-1}$	[30]
$(q^l + q^{l-1} - 1, q^{l-1})$ for any $l > 2$	$\frac{1}{\sqrt{q^{l-1}}}$	[33]
$((q-1)^k + q^{k-1}, q^{k-1})$, for any $k > 2$ and $q \geq 4$	$\frac{\sqrt{q^{k+1}}}{(q-1)^k+(-1)^{k+1}}$	[11]
$((q-1)^k + K, K)$, for any $k > 2$, where $K = \frac{(q-1)^k+(-1)^{k+1}}{q}$	$\frac{\sqrt{q^{k-1}}}{K}$	[11]
$((q^s-1)^n + K, K)$, 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 $p \nmid s$	$\frac{\sqrt{r}}{\sqrt{q}(\sqrt{r}-1)}$	[28]
$(q^2, \frac{q(q+1)(r-1)}{2r}), r = p^t, q = r^s$, with odd p	$\frac{(r+1)q}{2rK}$	[28]
(q^3, q^2) and $(q^3 + q^2, q^2)$, q is a prime power	$\frac{1}{q}$	This paper
$((q-1)q^2, (q-1)q)$ and $(q^2 - 1, (q-1)q)$, q is a prime power	$\frac{1}{q-1}$	This paper
$((q-1)q^2, (q-1)^2)$ and $(q^3 - 2q + 1, (q-1)^2)$, q is a prime power	$\frac{q}{(q-1)^2}$	This paper
$((q-1)^2q, (q-1)^2)$ and $(q^3 - q^2 - q + 1, (q-1)^2)$, q is a prime power	$\frac{q}{(q-1)^2}$	This paper
$((q-1)^2q, (q-1)(q-2))$ and $(q^3 - q^2 - 2q + 2, (q-1)(q-2))$, q is a prime power	$\frac{q}{(q-1)(q-2)}$	This paper
$((q-1)^3, (q-2)^2)$ and $(q^3 - 2q^2 - q + 3, (q-2)^2)$, q is a prime power	$\frac{q}{(q-2)^2}$	This paper

2.2 Character sums over finite fields

2.2.1 Gauss sum

Let φ be a multiplicative character of $\mathbb{F}_q$ and χ an additive character of $\mathbb{F}_q$. Then the Gauss sum over $\mathbb{F}_q$ is given by

$$G(\varphi, \chi) = \sum_{x \in \mathbb{F}_q^*} \varphi(x)\chi(x).$$

For simplicity, we write $G(\varphi, \chi_1)$ over $\mathbb{F}_q$ simply as $g(\varphi)$. It is easy to see the absolute value of $G(\varphi, \chi)$ is at most $q-1$, but is much smaller in general. The following lemma shows all the cases.

Lemma 2.1 [16, Theorem 5.11] *Let φ be a multiplicative character and χ an additive character of $\mathbb{F}_q$. Then the Gauss sum $G(\varphi, \chi)$ over $\mathbb{F}_q$ satisfies*

$$G(\varphi, \chi) = \begin{cases} q-1, & \text{if } \varphi = \varphi_0, \chi = \chi_0, \\ -1, & \text{if } \varphi = \varphi_0, \chi \neq \chi_0, \\ 0, & \text{if } \varphi \neq \varphi_0, \chi = \chi_0. \end{cases}$$

For $\varphi \neq \varphi_0$ and $\chi \neq \chi_0$, we have $|G(\varphi, \chi)| = \sqrt{q}$.

Lemma 2.2 [16] *Gauss sums for the finite field $\mathbb{F}_q$ satisfy the following property:*
$G(\varphi, \chi_{ab}) = \overline{\varphi}(a)G(\varphi, \chi_b)$ *for $a \in \mathbb{F}_q^*$, $b \in \mathbb{F}_q$, where $\overline{\varphi}$ denotes the complex conjugate of φ.*

2.2.2 Jacobi sum

The definition of a multiplicative character φ can be extended as follows.

$$\varphi(0) = \begin{cases} 1, & \text{if } \varphi = \varphi_0, \\ 0, & \text{if } \varphi \neq \varphi_0. \end{cases}$$

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

$$J(\varphi_1, \varphi_2) = \sum_{c_1+c_2=1, c_1, c_2 \in \mathbb{F}_q} \varphi_1(c_1)\varphi_2(c_2)$$

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

The values of Jacobi sums are given as follows.

Lemma 2.3 [16, Theorem 5.19, Theorem 5.20] *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) *If one of the φ_1 and φ_2 is trivial, the other is nontrivial, $J(\varphi_1, \varphi_2) = 0$.*
(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,

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

3 Six constructions of codebooks

In [21], the authors combined a Reed–Solomon generator matrix with itself by the tensor product and employed this generated matrix to construct a complex measurement matrix. They proved that this matrix is asymptotically optimal according to the Welch bound. In this paper, we find a codebook which is equivalent to the measurement matrix in [21]. The codebook is actually the first construction in Sect. 3, which has been obtained in [26] recently. The advantage of the first construction is that it can be generalized naturally to construct the other five classes of asymptotically optimal codebooks using additive and multiplicative characters of finite field.

3.1 The first construction of codebooks

Let

$$D_1 := \{(x, y, z) \in \mathbb{F}_q \times \mathbb{F}_q \times \mathbb{F}_q : z = xy\}.$$

Then $\#D_1 = q^2$.

The codebook $\mathcal{C}_1$ is constructed as

$$\mathcal{C}_1 := \left\{ \frac{1}{q}(\chi_a(x)\chi_b(y)\chi_c(z))_{(x,y,z)\in D_1} : a, b, c \in \mathbb{F}_q \right\}.$$

We can derive the following Theorem.

Theorem 3.1 ([26, Theorem 1]) *$\mathcal{C}_1$ is a codebook with $N_1 = q^3$, $K_1 = q^2$ and $I_{max}(\mathcal{C}_1) = \frac{1}{q}$.*

Theorem 3.2 ([26, Remark 1]) *Let I_{W1} be the Welch bound equality, for the given N_1, K_1 in the current section. We have*

$$\lim_{q\to\infty} \frac{I_{max}(\mathcal{C}_1)}{I_{W1}} = 1,$$

then the codebooks we proposed are asymptotically optimal.

When codebooks employed in practical applications, only those with only a few correlation values are interesting. The distribution of correlation magnitudes of $\mathcal{C}_1$ is given as follows.

Corollary 3.3 ([26, Theorem 1])

$$|\mathbf{c}\mathbf{c}'^H| = \begin{cases} 1, & q^3 \ \textit{times}, \\ \frac{1}{q}, & q^6 - q^5 \ \textit{times}, \\ 0, & q^5 - q^3 \ \textit{times}. \end{cases}$$

3.2 The second construction of codebooks

Let

$$D_2 := \{(x, y, z) \in \mathbb{F}_q^* \times \mathbb{F}_q \times \mathbb{F}_q : z = xy\}.$$

Then $\# D_2 = (q-1)q$.

The codebook $\mathcal{C}_2$ is constructed as

$$\mathcal{C}_2 := \left\{ \frac{1}{\sqrt{(q-1)q}} (\varphi(x)\chi_b(y)\chi_c(z))_{(x,y,z)\in D_2} : \varphi \in \widehat{\mathbb{F}_q^*}, b, c \in \mathbb{F}_q \right\}.$$

We can derive the following Theorem.

Theorem 3.4 *$\mathcal{C}_2$ is a codebook with $N_2 = (q-1)q^2$, $K_2 = (q-1)q$ and $I_{max}(\mathcal{C}_2) = \frac{1}{q-1}$.*

Proof By the definition of $\mathcal{C}_2$, it contains $(q-1)q^2$ codewords of length $(q-1)q$. Then it is easy to see $N_2 = (q^2-1)q$ and $K_2 = (q-1)q$. Let $\mathbf{c}$ and $\mathbf{c}'$ be any different codewords in $\mathcal{C}_2$, $\mathbf{c} = \frac{1}{\sqrt{K_2}}(\varphi_j(x)\chi_{b_1}(y)\chi_{c_1}(z))_{(x,y,z)\in D_2}$ and $\mathbf{c}' = \frac{1}{\sqrt{K_2}}(\varphi_k(x)\chi_{b_2}(y)\chi_{c_2}(z))_{(x,y,z)\in D_2}$, where $\varphi_j, \varphi_k \in \widehat{\mathbb{F}_q^*}$, $b_1, b_2, c_1, c_2 \in \mathbb{F}_q$. Then the correlation of $\mathbf{c}$ and $\mathbf{c}'$ is as follows.

$$\begin{aligned}
&K_2\mathbf{c}\mathbf{c}'^H \\
&= \sum_{(x,y,z)\in D_2} \varphi_j(x)\chi_{b_1}(y)\chi_{c_1}(z)\overline{\varphi_k(x)\chi_{b_2}(y)\chi_{c_2}(z)} \\
&= \sum_{x\in\mathbb{F}_q^*, y\in\mathbb{F}_q} \varphi_j\overline{\varphi_k}(x)\chi((b_1-b_2)y + (c_1-c_2)xy) \\
&= \sum_{x\in\mathbb{F}_q^*, y\in\mathbb{F}_q} \varphi(x)\chi(by + cxy) \ \ (\text{where } \varphi = \varphi_j\overline{\varphi_k}, b = b_1 - b_2 \text{ and } c = c_1 - c_2) \\
&= \sum_{x\in\mathbb{F}_q^*} \varphi(x) \sum_{y\in\mathbb{F}_q} \chi((b+cx)y) \\
&= \sum_{x\in\mathbb{F}_q^*, b+cx=0} \varphi(x)q.
\end{aligned}$$

The last equation holds by the orthogonal relation of additive characters.

When $b \neq 0$ and $c \neq 0$, we have

$$K_2\mathbf{c}\mathbf{c}'^H = q\varphi\left(-\frac{b}{c}\right).$$

When $b \neq 0$, $c = 0$, or $b = 0$, $c \neq 0$, it is easy to see $\mathbf{c}\mathbf{c}'^H = 0$.

When $b = 0$ and $c = 0$, since $\mathbf{c} \neq \mathbf{c}'$, φ is nontrivial. We have

$$K_2\mathbf{c}\mathbf{c}'^H = \sum_{x\in\mathbb{F}_q^*} \varphi(x)q = 0,$$

by the orthogonal relation of multiplicative characters.

Therefore, we have

$$I_{max}(\mathcal{C}_2) = max\{|\mathbf{c}\mathbf{c}'^H| : \mathbf{c}, \mathbf{c}' \in \mathcal{C}, and\ \mathbf{c} \neq \mathbf{c}'\} = \frac{q}{K_2} = \frac{1}{q-1}.$$

□

Table 2 Parameters of the (N_2, K_2) codebook of Section III

q	N_2	K_2	$I_{max}(\mathcal{C}_2)$	I_{W2}	$\frac{I_{max}(\mathcal{C}_2)}{I_{W2}}$
3	18	6	0.5000	0.3430	1.4577
5	100	20	0.2500	0.2010	1.2437
13	2028	156	0.0833	0.0769	1.0831
49	115248	2352	0.0208	0.0204	1.0208
5^3	1937500	15500	0.0081	0.0080	1.0081
5^4	243750000	390000	0.0016	0.0016	1.0016
7^4	$1.3836e+10$	5762400	$4.1667e-04$	$4.1649e-04$	1.0004

Using Theorem 3.4, we can derive the ratio of $I_{max}(\mathcal{C}_2)$ of the proposed codebooks to that of the MWBE codebooks and show the asymptotic optimality of the proposed codebooks as in the following theorem.

Theorem 3.5 *Let I_{W2} be the Welch bound equality, for the given N_2, K_2 in the current section. We have*

$$\lim_{q\to\infty}\frac{I_{max}(\mathcal{C}_2)}{I_{W2}}=1,$$

then the codebooks we proposed are asymptotically optimal.

Proof Note that $N_2=(q-1)q^2$ and $K_2=(q-1)q$. Then the corresponding Welch bound is

$$I_{W2}=\sqrt{\frac{N_2-K_2}{(N_2-1)K_2}}=\sqrt{\frac{(q-1)q^2-(q-1)q}{((q-1)q^2-1)(q-1)q}}=\sqrt{\frac{q-1}{q^3-q^2-1}},$$

we have

$$\frac{I_{max}(\mathcal{C}_2)}{I_{W2}}=\sqrt{\frac{q^3-q^2-1}{(q-1)^3}}.$$

It is obvious that $\lim_{q\to+\infty}\frac{I_{max}(\mathcal{C}_2)}{I_{W2}}=1$. The codebook $\mathcal{C}_2$ 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 $\mathcal{C}_2$ asymptotically meet the Welch bound.

The distribution of correlation magnitudes of $\mathcal{C}_2$ is given as follows.

Corollary 3.6

$$|\mathbf{c}\mathbf{c}'^H|=\begin{cases}1, & (q-1)q^2 \ times,\\ \frac{1}{q-1}, & q-1)^4q^2 \ times,\\ 0, & q-1)q^3(2q-3) \ times.\end{cases}$$

Example 1 Let $q=p=3$. Then

$$D_2=\{(1,0,0),(1,1,1),(1,2,2),(2,0,0),(2,1,2),(2,2,1)\}$$

and $K_2 = \#D_2 = 6$. Let $\zeta = \zeta_3$. Thus, the set $\mathcal{C}_2$ consists of the following 18 codewords of length 6:

$$\mathbf{c}_0 = \frac{1}{\sqrt{6}}(1, 1, 1, 1, 1, 1), \quad \mathbf{c}_1 = \frac{1}{\sqrt{6}}(1, \zeta, \zeta^2, 1, \zeta^2, \zeta), \quad \mathbf{c}_2 = \frac{1}{\sqrt{6}}(1, \zeta^2, \zeta, 1, \zeta, \zeta^2),$$
$$\mathbf{c}_3 = \frac{1}{\sqrt{6}}(1, \zeta, \zeta^2, 1, \zeta, \zeta^2), \quad \mathbf{c}_4 = \frac{1}{\sqrt{6}}(1, \zeta^2, \zeta, 1, 1, 1), \quad \mathbf{c}_5 = \frac{1}{\sqrt{6}}(1, 1, 1, 1, \zeta^2, \zeta),$$
$$\mathbf{c}_6 = \frac{1}{\sqrt{6}}(1, \zeta^2, \zeta, 1, \zeta^2, \zeta), \quad \mathbf{c}_7 = \frac{1}{\sqrt{6}}(1, 1, 1, 1, \zeta, \zeta^2), \quad \mathbf{c}_8 = \frac{1}{\sqrt{6}}(1, \zeta, \zeta^2, 1, 1, 1),$$
$$\mathbf{c}_9 = \frac{1}{\sqrt{6}}(1, 1, 1, -1, -1, -1), \quad \mathbf{c}_{10} = \frac{1}{\sqrt{6}}(1, \zeta, \zeta^2, -1, -\zeta^2, -\zeta),$$
$$\mathbf{c}_{11} = \frac{1}{\sqrt{6}}(1, \zeta^2, \zeta, -1, -\zeta, -\zeta^2),$$
$$\mathbf{c}_{12} = \frac{1}{\sqrt{6}}(1, \zeta, \zeta^2, -1, -\zeta, -\zeta^2), \quad \mathbf{c}_{13} = \frac{1}{\sqrt{6}}(1, \zeta^2, \zeta, -1, -1, -1),$$
$$\mathbf{c}_{14} = \frac{1}{\sqrt{6}}(1, 1, 1, -1, -\zeta^2, -\zeta),$$
$$\mathbf{c}_{15} = \frac{1}{\sqrt{6}}(1, \zeta^2, \zeta, -1, -\zeta^2, -\zeta), \quad \mathbf{c}_{16} = \frac{1}{\sqrt{6}}(1, 1, 1, -1, -\zeta, -\zeta^2),$$
$$\mathbf{c}_{17} = \frac{1}{\sqrt{6}}(1, \zeta, \zeta^2, -1, -1, -1).$$

It is easy to verify that this codebook is a $(18, 6)$ codebook with $I_{max} = \frac{1}{2}$. This is consistent with the conclusion of Theorem 3.5.

3.3 The third construction of codebooks

Let

$$D_3 := \{(x, y, z) \in \mathbb{F}_q^* \times \mathbb{F}_q^* \times \mathbb{F}_q^* : z = xy\}.$$

Then $\#D_3 = (q-1)^2$.

The codebook $\mathcal{C}_3$ is constructed as

$$\mathcal{C}_3 := \left\{ \frac{1}{q-1}(\chi_a(x)\chi_b(y)\varphi(z))_{(x,y,z)\in D_3} : a, b \in \mathbb{F}_q, \varphi \in \widehat{\mathbb{F}_q^*} \right\}.$$

We can derive the following Theorem.

Theorem 3.7 *$\mathcal{C}_3$ is a codebook with $N_3 = q^2(q-1)$, $K_3 = (q-1)^2$ and $I_{max}(\mathcal{C}_3) = \frac{q}{(q-1)^2}$.*

Proof By the definition of $\mathcal{C}_3$, it contains $q^2(q-1)$ codewords of length $(q-1)^2$. Then it is easy to see $N_3 = q^2(q-1)$ and $K_3 = (q-1)^2$. Let $\mathbf{c}$ and $\mathbf{c}'$ be any different codewords in $\mathcal{C}_3$, $\mathbf{c} = \frac{1}{q-1}(\chi_{a_1}(x)\chi_{b_1}(y)\varphi_j(z))_{(x,y,z)\in D_3}$ and $\mathbf{c}' = \frac{1}{q-1}(\chi_{a_2}(x)\chi_{b_2}(y)\varphi_k(z))_{(x,y,z)\in D_3}$, where $a_1, a_2, b_1, b_2 \in \mathbb{F}_q$, $\varphi_j, \varphi_k \in \widehat{\mathbb{F}_q^*}$. Then the correlation of $\mathbf{c}$ and $\mathbf{c}'$ is as follows.

$$
\begin{aligned}
&K_3 \mathbf{c}\mathbf{c}'^H \\
&= \sum_{(x,y,z)\in D_3} \chi_{a_1}(x)\chi_{b_1}(y)\varphi_j(z)\overline{\chi_{a_2}(x)\chi_{b_2}(y)\varphi_k(z)} \\
&= \sum_{x,y\in\mathbb{F}_q^*} \chi((a_1-a_2)x+(b_1-b_2)y)\varphi_j\overline{\varphi_k}(xy) \\
&= \sum_{x,y\in\mathbb{F}_q^*} \chi(ax+by)\varphi(xy) \ \ (\text{where } a=a_1-a_2, b=b_1-b_2, \text{ and } \varphi=\varphi_j\overline{\varphi_k}) \\
&= \sum_{x\in\mathbb{F}_q^*} \chi_a(x)\varphi(x) \sum_{y\in\mathbb{F}_q^*} \chi_b(y)\varphi(y) \\
&= G(\varphi,\chi_a)G(\varphi,\chi_b).
\end{aligned}
$$

When φ is trivial, since $\mathbf{c} \neq \mathbf{c}'$, we get $a \neq 0$ or $b \neq 0$. By Lemma 2.1, we have

$$
K_3 \mathbf{c}\mathbf{c}'^H = G(\varphi,\chi_a)G(\varphi,\chi_b) = \begin{cases} -(q-1), & \text{if } a=0, b\neq 0 \text{ or } b=0, a\neq 0, \\ (-1)(-1), & \text{if } a,b\in\mathbb{F}_q^*, \end{cases}
$$

When φ is nontrivial, by Lemmas 2.1 and 2.2, we have

$$
K_3 \mathbf{c}\mathbf{c}'^H = G(\varphi,\chi_a)G(\varphi,\chi_b) = \begin{cases} 0, & \text{if } a=0 \text{ or } b=0, \\ \overline{\varphi}(ab)g^2(\varphi), & \text{if } a,b\in\mathbb{F}_q^*. \end{cases}
$$

Therefore, we have

$$
I_{max}(\mathcal{C}_3) = max\{|\mathbf{c}\mathbf{c}'^H| : \mathbf{c}, \mathbf{c}' \in \mathcal{C}, and\ \mathbf{c} \neq \mathbf{c}'\} = \frac{q}{K_3} = \frac{q}{(q-1)^2}.
$$

□

Using Theorem 3.7, we can derive the ratio of $I_{max}(\mathcal{C}_3)$ of the proposed codebooks to that of the MWBE codebooks and show the asymptotic optimality of the proposed codebooks as in the following theorem.

Theorem 3.8 *Let I_{W3} be the Welch bound equality, for the given N_3, K_3 in the current section. We have*

$$
\lim_{q\to\infty} \frac{I_{max}(\mathcal{C}_3)}{I_{W3}} = 1,
$$

then the codebooks we proposed are asymptotically optimal.

Proof Note that $N_3 = (q-1)q^2$ and $K_3 = (q-1)^2$. Then the corresponding Welch bound is

$$
I_{W3} = \sqrt{\frac{N_3 - K_3}{(N_3-1)K_3}} = \sqrt{\frac{(q-1)q^2-(q-1)^2}{((q-1)q^2-1)(q-1)^2}} = \sqrt{\frac{q^2-q+1}{(q^3-q^2-1)(q-1)}},
$$

we have

$$
\frac{I_{max}(\mathcal{C}_3)}{I_{W3}} = \frac{q}{q-1}\sqrt{\frac{q^3-q^2-1}{(q^2-q+1)(q-1)}}.
$$

It is obvious that $\lim_{q\to+\infty} \frac{I_{max}(\mathcal{C}_3)}{I_{W3}} = 1$. The codebook $\mathcal{C}_3$ asymptotically meets the Welch bound. This completes the proof. □

Table 3 Parameters of the (N_3, K_3) codebook of Section III

q	N_3	K_3	$I_{max}(\mathcal{C}_3)$	I_{W3}	$\frac{I_{max}(\mathcal{C}_3)}{I_{W3}}$
3	18	4	0.7500	0.4537	1.6529
5	100	16	0.3125	0.2303	1.3570
13	2028	144	0.0903	0.0803	1.1237
49	115248	2304	0.0213	0.0206	1.0312
5^3	1937500	15376	0.0081	0.0080	1.0121
5^4	243750000	389376	0.0016	0.0016	1.0024
7^4	$1.3830e+10$	5760000	$4.1684e-04$	$4.1658e-04$	1.0006

In Table 3, 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 $\mathcal{C}_3$ asymptotically meet the Welch bound.

The distribution of correlation magnitudes of $\mathcal{C}_3$ is given as follows.

Corollary 3.9

$$|\mathbf{c}\mathbf{c}'^H| = \begin{cases} 1, & (q-1)q^2 \ times, \\ \frac{q-1}{K_3}, & 2(q-1)^2q^2 \ times, \\ \frac{1}{K_3}, & q-1)^3q^2 \ times, \\ 0, & (q-2)(q-1)q^2(2q-1) \ times, \\ \frac{q}{K_3}, & (q-2)(q-1)^3q^2 \ times, \end{cases}$$

3.4 The fourth construction of codebooks

Let

$$D_4 := \{(x, y, z) \in \mathbb{F}_q^* \times \mathbb{F}_q^* \times \mathbb{F}_q^* : z = xy\}.$$

Then $\#D_4 = (q-1)^2$.

The codebook $\mathcal{C}_4$ is constructed as

$$\mathcal{C}_4 := \left\{ \frac{1}{q-1}(\varphi_i(x)\varphi_j(y)\chi_c(z))_{(x,y,z)\in D_4} : \varphi_i, \varphi_j \in \widehat{\mathbb{F}_q^*},\ c \in \mathbb{F}_q \right\}.$$

We can derive the following Theorem.

Theorem 3.10 *$\mathcal{C}_4$ is a codebook with $N_4 = (q-1)^2q$, $K_4 = (q-1)^2$ and $I_{max}(\mathcal{C}_4) = \frac{q}{(q-1)^2}$.*

Proof By the definition of $\mathcal{C}_4$, it contains $(q-1)^2q$ codewords of length $(q-1)^2$. Then it is easy to see $N_4 = (q-1)^2q$ and $K_4 = (q-1)^2$. Let $\mathbf{c}$ and $\mathbf{c}'$ be any different codewords in $\mathcal{C}_4$, $\mathbf{c} = \frac{1}{q-1}(\varphi_s(x)\varphi_t(y)\chi_{c_1}(z))_{(x,y,z)\in D_4}$ and $\mathbf{c}' = \frac{1}{q-1}(\varphi_s'(x)\varphi_t'(y)\chi_{c_2}(z))_{(x,y,z)\in D_4}$, where $\varphi_s, \varphi_t, \varphi_s', \varphi_t' \in \widehat{\mathbb{F}_q^*}$, $c_1, c_2 \in \mathbb{F}_q$. Then the correlation of $\mathbf{c}$ and $\mathbf{c}'$ is as follows.

$$
\begin{aligned}
&K_4\mathbf{c}\mathbf{c}'^H\\
&= \sum_{(x,y,z)\in D_4} \varphi_s(x)\varphi_t(y)\chi_{c_1}(z)\overline{\varphi'_s(x)\varphi'_t(y)\chi_{c_2}(z)}\\
&= \sum_{(x,y,z)\in D_4} \varphi_s\overline{\varphi'_s}(x)\varphi_t\overline{\varphi'_t}(y)\chi((c_1-c_2)z)\\
&= \sum_{x,y\in\mathbb{F}_q^*} \varphi(x)\varphi'(y)\chi(cxy)\ \ (\text{where } \varphi=\varphi_s\overline{\varphi'_s},\ \varphi'=\varphi_t\overline{\varphi'_t},\ \text{and } c=c_1-c_2)\\
&= \sum_{x\in\mathbb{F}_q^*} \varphi(x)\chi_c(x)\sum_{y\in\mathbb{F}_q^*} \varphi'(y)\chi_c(y)\\
&= G(\varphi,\chi_c)G(\varphi',\chi_c).
\end{aligned}
$$

When $c=0$, since $\mathbf{c}\neq\mathbf{c}'$, at least one of φ and φ' is nontrivial. By Lemma 2.1, we have

$$K_4\mathbf{c}\mathbf{c}'^H = G(\varphi,\chi_c)G(\varphi',\chi_c)=0.$$

When $c\neq 0$, by Lemmas 2.1 and 2.2, we have

$$
K_4\mathbf{c}\mathbf{c}'^H = G(\varphi,\chi_c)G(\varphi',\chi_c) = \begin{cases}(-1)(-1), & \text{both } \varphi \text{ and } \varphi' \text{ are trivial},\\ (-1)\overline{\varphi'(c)}g(\varphi'), & \varphi \text{ is trivial, and } \varphi' \text{ is nontrivial},\\ (-1)\overline{\varphi(c)}g(\varphi), & \varphi \text{ is nontrivial, and } \varphi' \text{ is trivial},\\ \overline{\varphi\varphi'}(c)g(\varphi)g(\varphi'), & \text{both } \varphi \text{ and } \varphi' \text{ are nontrivial}.\end{cases}
$$

Therefore, we have

$$I_{max}(\mathcal{C}_4) = max\{|\mathbf{c}\mathbf{c}'^H| : \mathbf{c},\mathbf{c}'\in\mathcal{C}_4, and\ \mathbf{c}\neq\mathbf{c}'\} = \frac{q}{K_4} = \frac{q}{(q-1)^2}.$$

□

Using Theorem 3.10, we can derive the ratio of $I_{max}(\mathcal{C}_4)$ of the proposed codebooks to that of the MWBE codebooks and show the asymptotic optimality of the proposed codebooks as in the following theorem.

Theorem 3.11 *Let I_{W4} be the Welch bound equality, for the given N_4, K_4 in the current section. We have*

$$\lim_{q\to\infty}\frac{I_{max}(\mathcal{C}_4)}{I_{W4}} = 1,$$

then the codebooks we proposed are asymptotically optimal.

Proof Note that $N_4=(q-1)^2q$ and $K_4=(q-1)^2$. Then the corresponding Welch bound is

$$I_{W4} = \sqrt{\frac{N_4-K_4}{(N_4-1)K_4}} = \sqrt{\frac{(q-1)^2q-(q-1)^2}{((q-1)^2q-1)(q-1)^2}} = \sqrt{\frac{q-1}{(q-1)^2q-1}},$$

we have

$$\frac{I_{max}(\mathcal{C}_4)}{I_{W4}} = \frac{q}{q-1}\sqrt{\frac{(q-1)^2q-1}{(q-1)^3}}.$$

It is obvious that $\lim_{q\to+\infty}\frac{I_{max}(\mathcal{C}_4)}{I_{W4}} = 1$. The codebook $\mathcal{C}_4$ asymptotically meets the Welch bound. This completes the proof. □

Table 4 Parameters of the (N_4, K_4) codebook of Section III

q	N_4	K_4	$I_{max}(\mathcal{C}_4)$	I_{W4}	$\frac{I_{max}(\mathcal{C}_4)}{I_{W4}}$
3	12	4	0.7500	0.4264	1.7589
5	80	16	0.3125	0.2250	1.3888
13	1872	144	0.0903	0.0801	1.1273
49	112896	2304	0.0213	0.0206	1.0314
5^3	1922000	15376	0.0081	0.0080	1.0121
5^4	243360000	389376	0.0016	0.0016	1.0024
7^4	$1.3830e+10$	5760000	$4.1684e-04$	$4.1658e-04$	1.0006

In Table 4, 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 $\mathcal{C}_4$ asymptotically meet the Welch bound.

The distribution of correlation magnitudes of $\mathcal{C}_4$ is given as follows.

Corollary 3.12

$$|\mathbf{c}\mathbf{c}'^H| = \begin{cases} 1, & (q-1)^2 q \ \textit{times}, \\ 0, & (q-2)(q-1)^2 q^2 \ \textit{times}, \\ \frac{1}{K_4}, & (q-1)^3 q \ \textit{times}, \\ \frac{\sqrt{q}}{K_4}, & 2(q-2)(q-1)^3 q \ \textit{times}, \\ \frac{q}{K_4}, & (q-2)^2(q-1)^3 q \ \textit{times}. \end{cases}$$

3.5 The fifth construction of codebooks

Let

$$D_5 := \{(x, y, z) \in \mathbb{F}_q^* \times \mathbb{F}_q^* \times \mathbb{F}_q^* : z = x(1-y)\}.$$

Then $\#D_5 = (q-1)(q-2)$.

The codebook $\mathcal{C}_5$ is constructed as

$$\mathcal{C}_5 := \left\{ \frac{1}{\sqrt{(q-1)(q-2)}} (\chi_a(x)\varphi_i(y)\varphi_j(z))_{(x,y,z)\in D_5} : \varphi_i, \varphi_j \in \widehat{\mathbb{F}_q^*},\ a \in \mathbb{F}_q \right\}.$$

We can derive the following Theorem.

Theorem 3.13 *$\mathcal{C}_5$ is a codebook with $N_5 = (q-1)^2 q$, $K_5 = (q-1)(q-2)$ and $I_{max}(\mathcal{C}_5) = \frac{q}{(q-1)(q-2)}$.*

Proof By the definition of $\mathcal{C}_5$, it contains $(q-1)^2 q$ codewords of length $(q-1)(q-2)$. Then it is easy to see $N_5 = (q-1)^2 q$ and $K_5 = (q-1)(q-2)$. Let $\mathbf{c}$ and $\mathbf{c}'$ be any different codewords in $\mathcal{C}_5$, $\mathbf{c} = \frac{1}{\sqrt{(q-1)(q-2)}}(\chi_{a_1}(x)\varphi_s(y)\varphi_t(z))_{(x,y,z)\in D_5}$ and $\mathbf{c}' = \frac{1}{\sqrt{(q-1)(q-2)}}(\chi_{a_2}(x)\varphi_s'(y)\varphi_t'(z))_{(x,y,z)\in D_5}$, where $\varphi_s, \varphi_t, \varphi_s', \varphi_t' \in \widehat{\mathbb{F}_q^*}$, $a_1, a_2 \in \mathbb{F}_q$. Then the correlation of $\mathbf{c}$ and $\mathbf{c}'$ is as follows.

$$
\begin{aligned}
&K_5\mathbf{c}\mathbf{c}'^H\\
&= \sum_{(x,y,z)\in D_5} \chi_{a_1}(x)\varphi_s(y)\varphi_t(z)\overline{\chi_{a_2}(x)\varphi_s'(y)\varphi_t'(z)}\\
&= \sum_{(x,y,z)\in D_5} \chi((a_1-a_2)x)\varphi_s\overline{\varphi_s'}(y)\varphi_t\overline{\varphi_t'}(z)\\
&= \sum_{x,y\in\mathbb{F}_q^*, y\neq 1} \chi(ax)\varphi(y)\varphi'(x(1-y)) \ \ (\text{where } a=a_1-a_2, \varphi=\varphi_s\overline{\varphi_s'}, \text{ and } \varphi'=\varphi_t\overline{\varphi_t'})\\
&= \sum_{x\in\mathbb{F}_q^*} \chi(ax)\varphi'(x) \sum_{y\in\mathbb{F}_q^*, y\neq 1} \varphi(y)\varphi'(1-y)\\
&= G(\varphi',\chi_a)(J(\varphi,\varphi')-\varphi(0)\varphi'(1)-\varphi(1)\varphi'(0)).
\end{aligned}
$$

When $a=0$, since $\mathbf{c}\neq\mathbf{c}'$, at least one of φ and φ' is nontrivial, by Lemmas 2.1 and 2.3, we have

$$
K_5\mathbf{c}\mathbf{c}'^H = \begin{cases} (-1)(q-1), & \varphi' \text{ is trivial, and } \varphi \text{ is nontrivial,}\\ 0, & \varphi' \text{ are nontrivial.} \end{cases}
$$

When $a\neq 0$, by Lemmas 2.1 and 2.3, we have

$$
K_5\mathbf{c}\mathbf{c}'^H = \begin{cases} (-1)(q-2), & \text{both } \varphi' \text{ and } \varphi \text{ are trivial,}\\ (-1)(-1), & \varphi' \text{ is trivial, and } \varphi \text{ is nontrivial,}\\ \overline{\varphi'}(a)g(\varphi')(-1), & \varphi' \text{ is nontrivial, and } \varphi \text{ is trivial,}\\ \overline{\varphi'}(a)g(\varphi')J(\varphi,\varphi'), & \text{both } \varphi' \text{ and } \varphi \text{ are nontrivial.} \end{cases}
$$

Therefore, we have

$$
I_{max}(\mathcal{C}_5) = max\{|\mathbf{c}\mathbf{c}'^H| : \mathbf{c},\mathbf{c}'\in\mathcal{C}, and\ \mathbf{c}\neq\mathbf{c}'\} = \frac{q}{K_5} = \frac{q}{(q-1)(q-2)},
$$

the maximal value obtained when all of φ, φ' and $\varphi\varphi'$ are nontrivial. □

Using Theorem 3.13, we can derive the ratio of $I_{max}(\mathcal{C}_5)$ of the proposed codebooks to that of the MWBE codebooks and show the asymptotic optimality of the proposed codebooks as in the following theorem.

Theorem 3.14 *Let I_{W5} be the Welch bound equality, for the given N_5, K_5 in the current section. We have*

$$
\lim_{q\to\infty} \frac{I_{max}(\mathcal{C}_5)}{I_{W5}} = 1,
$$

then the codebooks we proposed are asymptotically optimal.

Proof Note that $N_5=(q-1)^2q$ and $K_5=(q-1)(q-2)$. Then the corresponding Welch bound is

$$
I_{W5} = \sqrt{\frac{N_5-K_5}{(N_5-1)K_5}} = \sqrt{\frac{(q-1)^2q-(q-1)(q-2)}{((q-1)^2q-1)(q-1)(q-2)}} = \sqrt{\frac{q^2-2q+2}{(q(q-1)^2-1)(q-2)}},
$$

we have

$$
\frac{I_{max}(\mathcal{C}_5)}{I_{W5}} = \frac{q}{q-1}\sqrt{\frac{q(q-1)^2-1}{(q^2-2q+2)(q-2)}}.
$$

Table 5 Parameters of the (N_5, K_5) codebook of Section III

q	N_5	K_5	$I_{max}(\mathcal{C}_5)$	I_{W5}	$\frac{I_{max}(\mathcal{C}_5)}{I_{W5}}$
3	12	2	1.5000	0.6742	2.2249
5	80	12	0.4167	0.2678	1.5557
13	1872	132	0.0985	0.0839	1.1733
49	112896	2256	0.0217	0.0208	1.0421
5^3	1922000	15252	0.0082	0.0081	1.0162
5^4	243360000	388752	0.0016	0.0016	1.0032
7^4	$1.3830e+10$	5757600	$4.1701e-04$	$4.1667e-04$	1.0008

It is obvious that $\lim_{q\to+\infty}\frac{I_{max}(\mathcal{C}_5)}{I_{W5}}=1$. The codebook $\mathcal{C}_5$ asymptotically meets the Welch bound. This completes the proof. □

In Table 5, 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 $\mathcal{C}_5$ asymptotically meet the Welch bound.

The distribution of correlation magnitudes of $\mathcal{C}_5$ is given as follows.

Corollary 3.15

$$|\mathbf{c}\mathbf{c}'^H| = \begin{cases} 1, & (q-1)^2 q \ times, \\ \frac{q-1}{K_5}, & (q-2)(q-1)^2 q \ times, \\ 0, & (q-2)(q-1)^3 q \ times, \\ \frac{q-2}{K_5}, & (q-1)^3 q \ times, \\ \frac{1}{K_5}, & (q-2)(q-1)^3 q \ times, \\ \frac{\sqrt{q}}{K_5}, & 2(q-2)(q-1)^3 q \ times, \\ \frac{q}{K_5}, & (q-3)(q-2)(q-1)^3 q \ times. \end{cases}$$

3.6 The sixth construction of codebooks

Let

$$D_6 := \{(x, y, z) \in \mathbb{F}_q^* \times \mathbb{F}_q^* \times \mathbb{F}_q^* : z = (1-x)(1-y)\}.$$

Then $\#D_6 = (q-2)^2$.

The codebook $\mathcal{C}_6$ is constructed as

$$\mathcal{C}_6 := \left\{\frac{1}{q-2}(\varphi_i(x)\varphi_j(y)\varphi_k(z))_{(x,y,z)\in D_6} : \varphi_i, \varphi_j, \varphi_k \in \widehat{\mathbb{F}_q^*}\right\}.$$

We can derive the following Theorem.

Theorem 3.16 *$\mathcal{C}_6$ is a codebook with $N_6 = (q-1)^3$, $K_6 = (q-2)^2$ and $I_{max}(\mathcal{C}_6) = \frac{q}{(q-2)^2}$.*

Proof By the definition of $\mathcal{C}_6$, it contains $(q-1)^3$ codewords of length $(q-2)^2$. Then it is easy to see $N_6=(q-1)^3$ and $K_6=(q-2)^2$. Let $\mathbf{c}$ and $\mathbf{c}'$ be any different codewords in $\mathcal{C}_6$, $\mathbf{c}=\frac{1}{q-2}(\varphi_s(x)\varphi_u(y)\varphi_v(z))_{(x,y,z)\in D_6}$ and $\mathbf{c}'=\frac{1}{q-2}(\varphi'_s(x)\varphi'_u(y)\varphi'_v(z))_{(x,y,z)\in D_6}$, where $\varphi_s,\varphi_u,\varphi_v,\varphi'_s,\varphi'_u,\varphi'_v\in\widehat{\mathbb{F}_q^*}$. Then the correlation of $\mathbf{c}$ and $\mathbf{c}'$ is as follows.

$$\begin{aligned}
&K\mathbf{c}\mathbf{c}'^H\\
&=\sum_{(x,y,z)\in D_6}\varphi_s(x)\varphi_u(y)\varphi_v(z)\overline{\varphi'_s(x)\varphi'_u(y)\varphi'_v(z)}\\
&=\sum_{(x,y,z)\in D_6}\varphi_s\overline{\varphi'_s}(x)\varphi_u\overline{\varphi'_u}(y)\varphi_v\overline{\varphi'_v}(z)\\
&=\sum_{x,y\in\mathbb{F}_q^*,x\neq1,y\neq1}\varphi_i(x)\varphi_j(y)\varphi_k((1-x)(1-y))\\
&\qquad(\text{where } \varphi_i=\varphi_s\overline{\varphi'_s},\ \varphi_j=\varphi_u\overline{\varphi'_u},\ \text{and } \varphi_k=\varphi_v\overline{\varphi'_v})\\
&=\sum_{x\in\mathbb{F}_q^*,x\neq1}\varphi_i(x)\varphi_k(1-x)\sum_{y\in\mathbb{F}_q^*,y\neq1}\varphi_j(y)\varphi_k(1-y)\\
&=(J(\varphi_i,\varphi_k)-\varphi_i(0)\varphi_k(1)-\varphi_i(1)\varphi_k(0))(J(\varphi_j,\varphi_k)-\varphi_j(0)\varphi_k(1)-\varphi_j(1)\varphi_k(0)).
\end{aligned}$$

When φ_k is trivial, since $\mathbf{c}\neq\mathbf{c}'$, at least one of φ_i and φ_j is nontrivial. By Lemma 2.3, we have

$$K_6\mathbf{c}\mathbf{c}'^H=\begin{cases}(-1)(q-2), & \varphi_i \text{ is trivial, and } \varphi_j \text{ is nontrivial,}\\ (-1)(q-2), & \varphi_i \text{ is nontrivial, and } \varphi_j \text{ is trivial,}\\ (-1)(-1), & \text{both } \varphi_i \text{ and } \varphi_j \text{ are nontrivial.}\end{cases}$$

When φ_k is nontrivial, by Lemma 2.3, we have

$$K_6\mathbf{c}\mathbf{c}'^H=\begin{cases}(-1)(-1), & \text{both } \varphi_i \text{ and } \varphi_j \text{ are trivial,}\\ (-1)J(\varphi_j,\varphi_k), & \varphi_i \text{ is trivial, and } \varphi_j \text{ is nontrivial,}\\ (-1)J(\varphi_i,\varphi_k), & \varphi_i \text{ is nontrivial, and } \varphi_j \text{ is trivial,}\\ J(\varphi_i,\varphi_k)J(\varphi_j,\varphi_k), & \text{both } \varphi_i \text{ and } \varphi_j \text{ are nontrivial.}\end{cases}$$

Therefore, we have

$$I_{max}(\mathcal{C}_6)=max\{|\mathbf{c}\mathbf{c}'^H|:\mathbf{c},\mathbf{c}'\in\mathcal{C}, and\ \mathbf{c}\neq\mathbf{c}'\}=\frac{q}{K_6}=\frac{q}{(q-2)^2},$$

the maximal value obtained when all of $\varphi_i,\varphi_j,\varphi_k,\varphi_i\varphi_k$ and $\varphi_j\varphi_k$ are nontrivial. □

Using Theorem 3.16, we can derive the ratio of $I_{max}(\mathcal{C}_6)$ of the proposed codebooks to that of the MWBE codebooks and show the asymptotic optimality of the proposed codebooks as in the following theorem.

Theorem 3.17 *Let I_{W6} be the Welch bound equality, for the given N_6, K_6 in the current section. We have*

$$\lim_{q\to\infty}\frac{I_{max}(\mathcal{C}_6)}{I_{W6}}=1,$$

then the codebooks we proposed are asymptotically optimal.

Table 6 Parameters of the (N_6, K_6) codebook of Section III

q	N_6	K_6	$I_{max}(\mathcal{C}_6)$	I_{W6}	$\frac{I_{max}(\mathcal{C}_6)}{I_{W6}}$
3	8	1	3	1	3
5	64	9	0.5556	0.3115	1.7838
13	1728	121	0.1074	0.0877	1.2251
49	110592	2209	0.0222	0.0211	1.0531
5^3	1906624	15129	0.0083	0.0081	1.0203
5^4	242970624	388129	0.0016	0.0016	1.0040
7^4	$1.3824e+10$	5755201	$4.1719e-04$	$4.1675e-04$	1.0010

Proof Note that $N_6 = (q-1)^3$ and $K_6 = (q-2)^2$. Then the corresponding Welch bound is

$$I_{W6} = \sqrt{\frac{N_6 - K_6}{(N_6 - 1)K_6}} = \sqrt{\frac{(q-1)^3 - (q-2)^2}{((q-1)^3 - 1)(q-2)^2}} = \frac{1}{q-2}\sqrt{\frac{q^3 - 4q^2 + 7q - 5}{q^3 - 3q^2 + 3q - 2}},$$

we have

$$\frac{I_{max}(\mathcal{C}_6)}{I_{W6}} = \frac{q}{q-2}\sqrt{\frac{q^3 - 3q^2 + 3q - 2}{q^3 - 4q^2 + 7q - 5}}.$$

It is obvious that $\lim_{q\to+\infty} \frac{I_{max}(\mathcal{C}_6)}{I_{W6}} = 1$. The codebook $\mathcal{C}$ asymptotically meets the Welch bound. This completes the proof. □

In Table 6, 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 $\mathcal{C}_6$ asymptotically meet the Welch bound.

The distribution of correlation magnitudes of $\mathcal{C}_6$ is given as follows.

Corollary 3.18

$$|\mathbf{c}\mathbf{c}'^H| = \begin{cases} 1, & (q-1)^3 \textit{ times}, \\ \frac{q-2}{K_6}, & 2(q-2)(q-1)^3 \textit{ times}, \\ \frac{1}{K_6}, & (q-2)(q-1)^3(q+2) \textit{ times}, \\ \frac{\sqrt{q}}{K_6}, & 4(q-3)(q-2)(q-1)^3 \textit{ times}, \\ \frac{q}{K_6}, & (q-3)^2(q-2)(q-1)^3 \textit{ times}. \end{cases}$$

4 Another family of codebooks

Based on the six constructions of codebooks in Sect. 3, more new codebooks can be derived, which are also asymptotically optimal.

Let $\mathcal{E}_n$ denote the set formed by the standard basis of the n-dimensional Hilbert space:

$$\begin{gathered}(1, 0, 0, ..., 0, 0),\\ (0, 1, 0, ..., 0, 0),\\ ......\\ (0, 0, 0, ..., 0, 1).\end{gathered}$$

Combining with the preceding six constructions, we get the following result.

Theorem 4.1 *Let $\mathcal{C}_i' = \mathcal{C}_i \cup \mathcal{E}_{K_i}$. Then the codebooks $\mathcal{C}_i'$ are all asymptotically optimal, $i = 1, 2, 3, 4, 5, 6$, and the parameters of the new codebooks are as follows:*
$N_i' = N_i + K_i$, $K_i' = K_i$ and $I_{max}(\mathcal{C}_i') = I_{max}(\mathcal{C}_i)$. Specifically,

(1) $N_1' = N_1 + K_1 = q^3 + q^2$, $K_1' = K_1 = q^2$ *and* $I_{max}(\mathcal{C}_1') = I_{max}(\mathcal{C}_1) = \frac{1}{q}$;
(2) $N_2' = N_2 + K_2 = (q^2 - 1)$, $K_2' = K_2 = (q-1)q$ *and* $I_{max}(\mathcal{C}_2') = I_{max}(\mathcal{C}_2) = \frac{1}{q-1}$;
(3) $N_3' = N_3 + K_3 = q^3 - 2q + 1$, $K_3' = K_3 = (q-1)^2$ *and* $I_{max}(\mathcal{C}_3') = I_{max}(\mathcal{C}_3) = \frac{q}{(q-1)^2}$;
(4) $N_4' = N_4 + K_4 = q^3 - q^2 - q + 1$, $K_4' = K_4 = (q-1)^2$ *and* $I_{max}(\mathcal{C}_4') = I_{max}(\mathcal{C}_4) = \frac{q}{(q-1)^2}$;
(5) $N_5' = N_5 + K_5 = q^3 - q^2 - 2q + 2$, $K_5' = K_5 = (q-1)(q-2)$ *and* $I_{max}(\mathcal{C}_5') = I_{max}(\mathcal{C}_5) = \frac{q}{(q-1)(q-2)}$;
(6) $N_5' = N_6 + K_6 = q^3 - 2q^2 - q + 3$, $K_6' = K_6 = (q-2)^2$ *and* $I_{max}(\mathcal{C}_5') = I_{max}(\mathcal{C}_5) = \frac{q}{(q-2)^2}$.

Proof We only prove the case when $i = 2$, the other cases can be proved as a similar way. It is easy to see $N_2' = N_2 + K_2 = (q^2 - 1)q$ and $K_2' = K_2 = (q-1)q$. Let $\mathbf{c}$ and $\mathbf{c}'$ be any different codewords in $\mathcal{C}_2'$, the correlation of $\mathbf{c}$ and $\mathbf{c}'$ can be discussed in the following cases.

Case 1: If $\mathbf{c}, \mathbf{c}' \in \mathcal{C}_2$, by Theorem 3.4, we have

$$max\{|\mathbf{c}\mathbf{c}'^H| : \mathbf{c}, \mathbf{c}' \in \mathcal{C}_2, and\ \mathbf{c} \neq \mathbf{c}'\} = \frac{1}{q-1}.$$

Case 2: If $\mathbf{c} \in \mathcal{C}_2$ and $\mathbf{c}' \in \mathcal{E}_{(q-1)q}$ (or $\mathbf{c}' \in \mathcal{C}_2$ and $\mathbf{c} \in \mathcal{E}_{(q-1)q}$), it is easy to see

$$|\mathbf{c}\mathbf{c}'^H| = \frac{1}{\sqrt{(q-1)q}}.$$

Case 3: If $\mathbf{c}$ and $\mathbf{c}' \in \mathcal{E}_{(q-1)q}$, it is obvious that $\mathbf{c}\mathbf{c}'^H = 0$.

From the above three cases, we have

$$I_{max}(\mathcal{C}_2') = \frac{1}{q-1}.$$

Note that $N_2' = (q^2 - 1)q$ and $K_2' = (q-1)q$, then the corresponding Welch bound is

$$I_W = \sqrt{\frac{N_2' - K_2'}{(N_2' - 1)K_2'}} = \sqrt{\frac{q}{q^3 - q - 1}},$$

we have

$$\frac{I_{max}(\mathcal{C}_2')}{I_W} = \sqrt{\frac{q^3 - q - 1}{(q-1)^2 q}}.$$

It is obvious that $\lim_{q \to +\infty} \frac{I_{max}(\mathcal{C}_2')}{I_W} = 1$. The codebook $\mathcal{C}_2'$ asymptotically meets the Welch bound. This completes the proof. □

5 Concluding remarks

In this paper, we presented six constructions of codebooks asymptotically achieve the Welch bounds with additive characters, multiplicative characters and character sums of finite fields. Actually, the first construction in our paper is equivalent to the measurement matrix in [21]. The advantage of our construction is that it can be generalized naturally to the other five constructions of codebooks which are also asymptotically optimal.

References

1. Candes E., Wakin M.: An introduction to compressive sampling. IEEE Signal Process. Mag. **25**(2), 21–30 (2008).
2. Conway J., Harding R., 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., 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., Seidel J.: Spherical codes and designs. Geom. Dedic. **67**(3), 363–388 (1997).
6. Fickus M., Mixon D.: Tables of the existence of equiangular tight frames (2016). arXiv:1504.00253v2.
7. Fickus M., Mixon D., Tremain J.: Steiner equiangular tight frames. Linear Algebr. Appl. **436**(5), 1014–1027 (2012).
8. Fickus M., Mixon D., Jasper J.: Equiangular tight frames from hyperovals. IEEE Trans. Inf. Theory **62**(9), 5225–5236 (2016).
9. Fickus M., Jasper J., Mixon D., Peterson J.: Tremain equiangular tight frames (2016). arXiv:1602.03490v1.
10. Heng Z.: Nearly optimal codebooks based on generalized Jacobi sums. Discret. Appl. Math. **250**, 227–240 (2018).
11. Heng Z., Ding C., Yue Q.: New constructions of asymptotically optimal codebooks with multiplicative characters. IEEE Trans. Inf. Theory **63**(10), 6179–6187 (2017).
12. Hong S., Park H., Helleseth T., 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).
13. Hu H., Wu J.: New constructions of codebooks nearly meeting the Welch bound with equality. IEEE Trans. Inf. Theory **60**(2), 1348–1355 (2014).
14. Kovacevic J., 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. Lidl R., Niederreiter H.: Finite Fields. Cambridge University Press, Cambridge (1997).
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: Proceedings of IEEE International Symposium on Information Theory, Vail, CO, pp. 2346–2349 (2018).
19. Luo G., Cao X.: Two constructions of asymptotically optimal codebooks. Crypt. Commun. (2018). https://doi.org/10.1007/s12095-018-0331-4.
20. Massey J., Mittelholzer T.: Welch's Bound and Sequence Sets for Code-Division Multiple-Access Systems: Sequences II, pp. 63–78. Springer, New York (1999).
21. Mohades M., Mohades A., Tadaion A.: A Reed-Solomom code based measurement matrix with small coherence. IEEE Signal Process. Lett. **21**(7), 839–843 (2014).
22. Rahimi F.: Covering graphs and equiangular tight frames. Ph.D. Thesis, University of Waterloo, Ontario (2016). http://hdl.handle.net/10012/10793.
23. Renes J., Blume-Kohout R., Scot A., Caves C.: Symmetric informationally complete quantum measurements. J. Math. Phys. **45**(6), 2171–2180 (2004).
24. Sarwate D.: Meeting the Welch Bound with Equality, pp. 63–79. Springer, New York (1999).
25. Strohmer T., Heath R.: Grassmannian frames with applications to coding and communication. Appl. Comput. Harmon. Anal. **14**(3), 257–275 (2003).

26. Tian L., Li Y., Liu T., Xu C.: Constructions of codebooks asymptotically achieving the Welch bound with additive characters. IEEE Signal Process. Lett. **26**(4), 622–626 (2019).
27. Welch L.: Lower bounds on the maximum cross correlation of signals. IEEE Trans. Inf. Theory **20**(3), 397–399 (1974).
28. Wu X., Lu W., Cao X., Chen M.: Two constructions of asymptotically optimal codebooks via the trace functions (2019). arXiv:1905.01815.
29. Xia P., Zhou S., Giannakis G.: Achieving the Welch bound with difference sets. IEEE Trans. Inf. Theory **51**(5), 1900–1907 (2005).
30. Yu N.: A construction of codebooks associated with binary sequences. IEEE Trans. Inf. Theory **58**(8), 5522–5533 (2012).
31. Zhang A., Feng K.: Two classes of codebooks nearly meeting the Welch bound. IEEE Trans. Inf. Theory **58**(4), 2507–2511 (2012).
32. Zhang A., Feng K.: Construction of cyclotomic codebooks nearly meeting the Welch bound. Des. Codes Cryptogr. **63**(2), 209–224 (2013).
33. Zhou Z., Tang X.: New nearly optimal codebooks from relative difference sets. Adv. Math. Commun. **5**(3), 521–527 (2011).