New Constructions of Asymptotically Optimal Codebooks With Multiplicative Characters

Ziling Heng, Cunsheng Ding, *Senior Member, IEEE*, and Qin Yue

***Abstract*— In practical applications, such as direct spread code division multiple access communications, space-time codes and compressed sensing, and codebooks with small inner-product correlation are required. It is extremely difficult to construct codebooks achieving the Levenshtein bound. In this paper, two new constructions of infinitely many codebooks with multiplicative characters of finite fields are presented. These constructions produce complex codebooks asymptotically achieving the Levenshtein bound and codebooks asymptotically achieving the Welch bound. The codebooks presented in this paper have new parameters.**

***Index Terms*— Code division multiple access, codebooks, signal sets, compressed sensing, Welch bound, Levenshtein bound.**

I. Introduction

CODEBOOKS (also called signal sets) with small inner-product correlation are usually used to distinguish among the signals of different users in code division multiple access (CDMA) systems. An (N, K) codebook $\mathcal{C}$ is a set $\{\mathbf{c}_0, \mathbf{c}_1, ..., \mathbf{c}_{N-1}\}$, where each codeword $\mathbf{c}_l$, $0 \leq l \leq N-1$, is a unit norm $1 \times K$ complex vector over an alphabet. The alphabet size is the number of elements in the alphabet. The maximum cross-correlation amplitude of an (N, K) codebook $\mathcal{C}$ is defined by

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

where $\mathbf{c}^H$ denotes the conjugate transpose of a complex vector $\mathbf{c}$. $I_{\max}(\mathcal{C})$ is a performance measure of a codebook $\mathcal{C}$ in practical applications. One important problem is to minimize the codebook's maximal cross-correlation amplitude. Minimizing $I_{\max}(\mathcal{C})$ among codewords of a codebook $\mathcal{C}$ can approximately optimize various performance metrics such as outage probability, average signal-to-noise ratio and symbol error probability for multiple-antenna transmit beamforming from limited-rate feedback [15], [20]. In the context of unitary space-time modulations, minimizing $I_{\max}(\mathcal{C})$ is equivalent to minimizing the block error probability [13]. Codebooks are also called *frames*. A codebook $\mathcal{C}$ with minimal $I_{\max}(\mathcal{C})$ is referred to as a *Grassmannian frame*. Besides, minimizing $I_{\max}(\mathcal{C})$ of finite frames brings to minimal reconstruction error in multiple description coding over erasure channels [23].

For a given K, we would like to construct an (N, K) codebook with N being as large as possible and $I_{\max}(\mathcal{C})$ being as small as possible simultaneously. However, the following Welch and Levenshtein bounds demonstrate a trade-off among the parameters N, K and $I_{\max}(\mathcal{C})$ of a codebook $\mathcal{C}$.

Lemma 1 (Welch Bound): [27] For any (N, K) codebook $\mathcal{C}$ with $N \geq K$,

$$I_{\max}(\mathcal{C}) \geq \sqrt{\frac{N-K}{(N-1)K}}. \tag{I.1}$$

In addition, the equality in (I.1) is achieved if and only if

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

for all pairs (i, j) with $i \neq j$.

If a codebook $\mathcal{C}$ achieves the Welch bound in (I.1), which is denoted by I_W, we call it a maximum-Welch-bound-equality (MWBE) codebook [29]. An MWBE codebook is also called an equiangular tight frame [25]. MWBE codebooks are employed in many applications including CDMA communications [19], space-time codes [24] and compressed sensing [25]. To our knowledge, only the following constructions of MWBE codebooks were reported in literature:

(1) In [22] and [29], optimal (N, N) and $(N, N-1)$ codebooks with $N > 1$ were generated from the (inverse) discrete Fourier transform matrix or ideal two-level autocorrelation sequences.

(2) In [2] and [23], optimal (N, K) codebooks from conference matrices were given when $N = 2K = 2^{d+1}$ with d being a positive integer and $N = 2K = p^d + 1$ with p being a prime number and d being a positive integer.

(3) In [3], [4], and [29], optimal (N, K) codebooks were constructed with cyclic difference sets in the Abelian group $(\mathbb{Z}_N, +)$ or the additive group of finite fields or Abelian groups in general.

(4) In [10], optimal (N, K) codebooks from $(2, k, v)$-Steiner systems were presented.

Manuscript received December 18, 2016; revised March 22, 2017; accepted April 5, 2017. Date of publication April 12, 2017; date of current version September 13, 2017. Z. Heng and Q. Yue were supported in part by the Foundation of Science and Technology on Information Assurance Laboratory under Grant KJ-15-009 and in part by the Fundamental Research Funds for the Central Universities under Grant NZ2015102. C. Ding was supported by The Hong Kong Grants Council under Project 16301114. *(Corresponding author: Cunsheng Ding.)*

Z. Heng and Q. Yue are with the Department of Mathematics, Nanjing University of Aeronautics and Astronautics, Nanjing 211100, China (e-mail: zilingheng@163.com; yueqin@nuaa.edu.cn).

C. Ding is with the Department of Computer Scuence and Engineering, The Hong Kong University of Science and Technology, Hong Kong (email: cding@ust.hk).

Communicated by S. Mesnager, Associate Editor for Sequences.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2017.2693204

(5) In [7]-[9] and [21], graph theory and finite geometries were employed to study MWBE codebooks.

According to [23], the Welch bound on $I_{\max}(\mathcal{C})$ of a codebook $\mathcal{C}$ is not tight when $N > K(K+1)/2$ for real codebooks and $N > K^2$ for all codebooks. The following Levenshtein bound turns out to be tighter than the Welch bound when $N > K^2$.

Lemma 2 (Levenshtein Bound): [17] For any real-valued codebook $\mathcal{C}$ with $N > K(K+1)/2$,

$$I_{\max}(\mathcal{C}) \geq \sqrt{\frac{3N - K^2 - 2K}{(N-K)(K+2)}}. \tag{I.2}$$

For any complex-valued codebook $\mathcal{C}$ with $N > K^2$,

$$I_{\max}(\mathcal{C}) \geq \sqrt{\frac{2N - K^2 - K}{(N-K)(K+1)}}. \tag{I.3}$$

In general, it is very hard to construct codebooks achieving the Levenstein bound, which is denoted by I_L (the right-hand side of (I.2) or (I.3)). There are only a few constructions of codebooks achieving the Levenshtein bound. These codebooks meeting the Levenstein bound were constructed from Kerdock codes [1], [30], perfect nonlinear functions [6], bent functions over finite fields [33], and bent functions over Galois rings [11]. Codebooks achieving the Levenshtein bound are employed in quantum physics and the design of spreading sequences for CDMA and sets of mutually unbiased bases [6], [28].

Since it is very difficult to construct optimal codebooks, there have been a number of attempts to construct codebooks asymptotically (or nearly) achieving the Welch bound or the Levenshtein bound, i.e. $I_{\max}(\mathcal{C})$ is slightly higher than the Welch bound I_W or the Levenshtein bound I_L, but asymptotically achieves one of them. That is to say,

$$\lim_{K\to\infty} \frac{I_{\max}(\mathcal{C})}{I_W} = 1 \text{ or } \lim_{K\to\infty} \frac{I_{\max}(\mathcal{C})}{I_L} = 1.$$

In [22], Sarwate gave some nearly optimal codebooks from codes and signal sets. Ding [3], Ding and Feng [5], Li *et al.* [16], Zhang and Feng [32], and Zhou and Tang [34] constructed some nearly optimal codebooks based on almost or relative difference sets. Yu [31] presented some nearly optimal codebooks from binary sequences. Recently, Hu and Wu [12] proposed new constructions of nearly optimal codebooks from difference sets and the product of Abelian groups.

In this paper, we present two new constructions of complex codebooks with multiplicative characters over finite fields, and determine the maximum cross-correlation amplitude of these codebooks. We prove that our codebooks are asymptotically optimal with respect to the Levenshtein or Welch bound. The parameters of our codebooks are new.

This paper is organized as follows. In Section II, we recall some basic results on characters and Jacobi sums over finite fields. In Section III, we present our first construction of codebooks. In Section IV, we introduce our second construction of codebooks. In Section V, we conclude this paper and make some remarks.

II. Mathematical Foundations

In this section, we recall some necessary mathematical foundations on characters and Jacobi sums over finite fields. They will play important roles in our constructions of codebooks.

In this paper, we always assume that p is a prime number and $q = p^m$ with m being a positive integer. Let $\mathbb{F}_q$ denote the finite field with q elements. Let α be a primitive element of $\mathbb{F}_q$. Let $\mathrm{Tr}_{q/p}$ be the trace function from $\mathbb{F}_q$ to $\mathbb{F}_p$ defined by

$$\mathrm{Tr}_{q/p}(x) = \sum_{j=0}^{m-1} x^{p^j}.$$

A. Characters Over Finite Fields

In this section, we recall both additive and multiplicative characters over finite fields.

Definition 3: An additive character of $\mathbb{F}_q$ is a mapping χ from $\mathbb{F}_q$ to the set $\mathbb{C}^*$ of nonzero complex numbers such that $\chi(x+y) = \chi(x)\chi(y)$ for any $(x, y) \in \mathbb{F}_q \times \mathbb{F}_q$.

Every additive character of $\mathbb{F}_q$ can be expressed as

$$\chi_a(x) = \zeta_p^{\mathrm{Tr}_{q/p}(ax)}, \quad x \in \mathbb{F}_q,$$

where ζ_p is a primitive p-th root of complex unity. If $a = 0$, we call χ_0 the trivial additive character of $\mathbb{F}_q$. If $a = 1$, we denote $\chi = \chi_1$ which is called the canonical additive character of $\mathbb{F}_q$. The orthogonal relation of additive characters (see [14]) is given by

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

Definition 4: A multiplicative character of $\mathbb{F}_q$ is a nonzero function ψ from $\mathbb{F}_q^*$ to the set $\mathbb{C}^*$ of nonzero complex numbers such that $\psi(xy) = \psi(x)\psi(y)$ for any $x, y \in \mathbb{F}_q^*$, where $\mathbb{F}_q^* = \mathbb{F}_q \backslash \{0\}$.

The multiplicative characters of $\mathbb{F}_q$ can be expressed as follows [14]. Let $\zeta_h = e^{\frac{2\pi\sqrt{-1}}{h}}$ denote the h-th root of complex unity. For $j = 0, 1, \cdots, q-2$, the functions ψ_j defined by

$$\psi_j(\alpha^k) = \zeta_{q-1}^{jk}, \text{ for } k = 0, 1, \cdots, q-2,$$

are all the multiplicative characters of $\mathbb{F}_q$. If $j = 0$, we have $\psi_0(x) = 1$ for any $x \in \mathbb{F}_q^*$. We call ψ_0 the trivial multiplicative character of $\mathbb{F}_q$.

For two multiplicative characters ψ, ψ', we define their multiplication by setting $\psi\psi'(x) = \psi(x)\psi'(x)$ for all $x \in \mathbb{F}_q^*$. Let $\widehat{\mathbb{F}_q^*}$ be the set of all multiplicative characters of $\mathbb{F}_q$. Let $\overline{\psi}$ denote the conjugate character of ψ by setting $\overline{\psi}(x) = \overline{\psi(x)}$, where $\overline{\psi(x)}$ denotes the complex conjugate of $\psi(x)$. It is easy to verify that $\psi^{-1} = \overline{\psi}$. Then $\widehat{\mathbb{F}_q^*}$ forms a group under the multiplication of characters. Furthermore, $\widehat{\mathbb{F}_q^*}$ is isomorphic to $\mathbb{F}_q^*$. Then by Definition 4, we have the following lemma.

Lemma 5: For any $x \in \mathbb{F}_q^*$ and $j_1, j_2 \in \{0, 1, \cdots, q-2\}$, we have

$$\psi_{j_1}(x)\overline{\psi_{j_2}(x)} = \psi_{j_1 - j_2}(x).$$

For a multiplicative character ψ of $\mathbb{F}_q$, the orthogonal relation (see [14]) of it is given by

$$\sum_{x\in\mathbb{F}_q^*}\psi(x)=\begin{cases}q-1, & \text{if } \psi=\psi_0,\\ 0 & \text{otherwise.}\end{cases}$$

B. Jacobi Sums

We now extend the definition of a multiplicative character ψ by setting

$$\psi(0)=\begin{cases}1, & \text{if } \psi=\psi_0,\\ 0, & \text{if } \psi\neq\psi_0.\end{cases}$$

As a result, the property that $\psi(xy)=\psi(x)\psi(y)$ holds for all $x,y\in\mathbb{F}_q$.

Definition 6: [14, p. 205] Let $\lambda_1,\ldots,\lambda_k$ be k multiplicative characters of $\mathbb{F}_q$. The sum

$$J(\lambda_1,\ldots,\lambda_k)=\sum_{\substack{c_1+\cdots+c_k=1\\ c_1,\cdots,c_k\in\mathbb{F}_q}}\lambda_1(c_1)\cdots\lambda_k(c_k),$$

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

Jacobi sums are very useful in coding theory, sequence design and cryptography. A well-known result on the value of Jacobi sums is the following.

Lemma 7: [14, Ths. 5.19, 5.22] For the values of the Jacobi sums, we have the following results.

(1) *If $\lambda_1,\ldots,\lambda_k$ are trivial, then $J(\lambda_1,\ldots,\lambda_k)=q^{k-1}$.*

(2) *If some, but not all, of the λ_i are trivial, then $J(\lambda_1,\ldots,\lambda_k)=0$.*

(3) *If all of $\lambda_1,\ldots,\lambda_k$ are nontrivial characters and $\lambda_1\cdots\lambda_k$ is nontrivial, then $|J(\lambda_1,\ldots,\lambda_k)|=q^{\frac{k-1}{2}}$.*

(4) *If all of $\lambda_1,\ldots,\lambda_k$ are nontrivial characters and $\lambda_1\cdots\lambda_k$ is trivial, then $|J(\lambda_1,\ldots,\lambda_k)|=q^{\frac{k-2}{2}}$.*

For any $a\in\mathbb{F}_q^*$, we define the sum

$$J_a(\lambda_1,\ldots,\lambda_k)=\sum_{c_1+\cdots+c_k=a}\lambda_1(c_1)\cdots\lambda_k(c_k), \qquad \text{(II.1)}$$

where the summation extends over all k-tuples $(c_1,\ldots,c_k)$ of elements of $\mathbb{F}_q$ satisfying $c_1+\cdots+c_k=a$. Hence, $J_1(\lambda_1,\ldots,\lambda_k)=J(\lambda_1,\ldots,\lambda_k)$. It was shown in [14, p. 205] that

$$J_a(\lambda_1,\ldots,\lambda_k)=(\lambda_1\cdots\lambda_k)(a)J(\lambda_1,\ldots,\lambda_k). \qquad \text{(II.2)}$$

Therefore, $|J_a(\lambda_1,\ldots,\lambda_k)|=|J(\lambda_1,\ldots,\lambda_k)|$. That is to say, Lemma 7 also holds for $J_a(\lambda_1,\ldots,\lambda_k)$ for $a\in\mathbb{F}_q^*$.

For $a=0$ in Equation (II.1), we recall the following results.

Lemma 8: [14, Ths. 5.19, 5.20, 5.23] Let $J_0(\lambda_1,\ldots,\lambda_k)$ be the character sum defined in Equation (II.1) with $a=0$.

(1) *If $\lambda_1,\ldots,\lambda_k$ are trivial, then $J_0(\lambda_1,\ldots,\lambda_k)=q^{k-1}$.*

(2) *If some, but not all, of the λ_i are trivial, then $J_0(\lambda_1,\ldots,\lambda_k)=0$.*

(3) *If all of $\lambda_1,\ldots,\lambda_k$ are nontrivial characters and $\lambda_1\cdots\lambda_k$ is nontrivial, then $|J_0(\lambda_1,\ldots,\lambda_k)|=0$.*

(4) *If all of $\lambda_1,\ldots,\lambda_k$ are nontrivial characters and $\lambda_1\cdots\lambda_k$ is trivial, then $|J_0(\lambda_1,\ldots,\lambda_k)|=(q-1)q^{\frac{k-2}{2}}$.*

III. The First Construction of Codebooks

In this section, we present our first construction of codebooks with multiplicative characters of finite fields, and prove that our codebooks are asymptotically optimal.

A. Some Character Sums Related to Jacobi Sums

In this subsection, we evaluate some character sums related to Jacobi sums. These character sums will be employed later.

Let k be a positive integer. Now we count the number of solutions $(c_1,\ldots,c_k)\in(\mathbb{F}_q^*)^k$ of the diagonal equation

$$c_1+c_2+\cdots+c_k=a \text{ with } a\in\mathbb{F}_q. \qquad \text{(III.1)}$$

The number of its solutions may be known. For completeness, we present a simple proof in the following lemma.

Lemma 9: The number of solutions $(c_1,\ldots,c_k)\in(\mathbb{F}_q^*)^k$ of Equation (III.1) is given by $n:=\frac{1}{q}((q-1)^k+(-1)^{k+1})$ if $a\in\mathbb{F}_q^*$ and $n:=\frac{1}{q}((q-1)^k+(-1)^k(q-1))$ if $a=0$.

Proof: Denote by χ the canonical additive character of $\mathbb{F}_q$. It follows from the orthogonal relation of additive characters that

$$\begin{aligned} n&=\frac{1}{q}\sum_{y\in\mathbb{F}_q}\sum_{c_1,\ldots,c_k\in\mathbb{F}_q^*}\chi(y(c_1+\cdots+c_k-a))\\ &=\frac{1}{q}\left((q-1)^k+\left(\sum_{y\in\mathbb{F}_q^*}\chi(-ay)\right)\prod_{j=1}^{k}\sum_{c_j\in\mathbb{F}_q^*}\chi(c_jy)\right)\\ &=\begin{cases}\frac{(q-1)^k+(-1)^{k+1}}{q}, & \text{if } a\in\mathbb{F}_q^*,\\ \frac{(q-1)^k+(-1)^k(q-1)}{q}, & \text{if } a=0.\end{cases}\end{aligned}$$

□

For a positive integer k and $a\in\mathbb{F}_q$, we define a new character sum by

$$\widetilde{J}_a(\lambda_1,\ldots,\lambda_k)=\sum_{\substack{c_1+\cdots+c_k=a\\ (c_1,\ldots,c_k)\in(\mathbb{F}_q^*)^k}}\lambda_1(c_1)\cdots\lambda_k(c_k), \qquad \text{(III.2)}$$

where $\lambda_1,\ldots,\lambda_k$ are k multiplicative characters of $\mathbb{F}_q$. By Lemma 9, this sum contains n terms, where n is the number of solutions of Equation (III.1). Note that if all of $\lambda_1,\ldots,\lambda_k$ are nontrivial characters, we have $\lambda_i(0)=0$ for $1\leq i\leq k$ and then

$$\widetilde{J}_a(\lambda_1,\ldots,\lambda_k)=J_a(\lambda_1,\ldots,\lambda_k).$$

1) The Case $a\in\mathbb{F}_q^*$: We first consider the case $a\in\mathbb{F}_q^*$. By Lemmas 7, 9 and (II.2), we directly have the following results.

Lemma 10: Let $\widetilde{J}_a(\lambda_1,\ldots,\lambda_k)$ be the character sum defined before.

(1) *If $\lambda_1,\ldots,\lambda_k$ are trivial, then $\widetilde{J}_a(\lambda_1,\ldots,\lambda_k)=\frac{1}{q}((q-1)^k+(-1)^{k+1})$.*

(2) *If all of $\lambda_1,\ldots,\lambda_k$ are nontrivial characters and $\lambda_1\cdots\lambda_k$ is nontrivial, then $|\widetilde{J}_a(\lambda_1,\ldots,\lambda_k)|=q^{\frac{k-1}{2}}$.*

(3) *If all of $\lambda_1,\ldots,\lambda_k$ are nontrivial characters and $\lambda_1\cdots\lambda_k$ is trivial, then $|\widetilde{J}_a(\lambda_1,\ldots,\lambda_k)|=q^{\frac{k-2}{2}}$.*

In the following, we mainly consider the case that some, but not all, of the λ_i are trivial.

Lemma 11: Assume that $\lambda_1, \lambda_2, \ldots, \lambda_h$ are nontrivial and $\lambda_{h+1}, \ldots, \lambda_k$ are trivial for $1 \le h \le k-1$.

(1) *If $\lambda_1 \cdots \lambda_h$ is nontrivial, then $|\widetilde{J}_a(\lambda_1, \ldots, \lambda_k)| = q^{\frac{h-1}{2}}$.*

(2) *If $\lambda_1 \cdots \lambda_h$ is trivial, then $|\widetilde{J}_a(\lambda_1, \ldots, \lambda_k)| = q^{\frac{h-2}{2}}$.*

Proof: Assume that $\lambda_1, \lambda_2, \ldots, \lambda_h$ are nontrivial and $\lambda_{h+1}, \ldots, \lambda_k$ are trivial for $1 \le h \le k-1$. Then

$$\begin{aligned}\widetilde{J}_a(\lambda_1, \ldots, \lambda_k) &= \sum_{\substack{c_1+\cdots+c_k=a \\ (c_1,\ldots,c_k)\in(\mathbb{F}_q^*)^k}} \lambda_1(c_1)\cdots\lambda_k(c_k) \\ &= \sum_{\substack{c_1+\cdots+c_k=a \\ (c_1,\ldots,c_k)\in(\mathbb{F}_q^*)^k}} \lambda_1(c_1)\cdots\lambda_h(c_h).\end{aligned}$$

For a fixed $(c_1, \ldots, c_h) \in (\mathbb{F}_q^*)^h$, we now consider the solutions $(c_{h+1}, \ldots, c_k) \in (\mathbb{F}_q^*)^{k-h}$ of the equation

$$c_{h+1} + \cdots + c_k = a - (c_1 + \cdots + c_h).$$

By Lemma 9, it has $\frac{1}{q}((q-1)^{k-h} + (-1)^{k-h}(q-1))$ solutions if $c_1 + \cdots + c_h = a$ or $\frac{1}{q}((q-1)^{k-h} + (-1)^{k-h+1})$ solutions if $c_1 + \cdots + c_h \ne a$. Hence,

$$\begin{aligned}&\widetilde{J}_a(\lambda_1, \ldots, \lambda_k) \\ &= \frac{1}{q}((q-1)^{k-h} + (-1)^{k-h}(q-1)) \\ &\quad \times \sum_{\substack{c_1+\cdots+c_h=a \\ (c_1,\ldots,c_h)\in(\mathbb{F}_q^*)^h}} \lambda_1(c_1)\cdots\lambda_h(c_h) \\ &\quad + \frac{1}{q}((q-1)^{k-h} + (-1)^{k-h+1}) \\ &\quad \times \sum_{\substack{c_1+\cdots+c_h\ne a \\ (c_1,\ldots,c_h)\in(\mathbb{F}_q^*)^h}} \lambda_1(c_1)\cdots\lambda_h(c_h) \\ &= \frac{1}{q}((q-1)^{k-h} + (-1)^{k-h+1}) \\ &\quad \times \sum_{(c_1,\ldots,c_h)\in(\mathbb{F}_q^*)^h} \lambda_1(c_1)\cdots\lambda_h(c_h) \\ &\quad + (-1)^{k-h} \sum_{\substack{c_1+\cdots+c_h=a \\ (c_1,\ldots,c_h)\in(\mathbb{F}_q^*)^h}} \lambda_1(c_1)\cdots\lambda_h(c_h) \\ &= \frac{1}{q}((q-1)^{k-h} + (-1)^{k-h+1}) \prod_{j=1}^{h} \left(\sum_{c_j\in\mathbb{F}_q^*} \lambda_j(c_j) \right) \\ &\quad + (-1)^{k-h} \sum_{\substack{c_1+\cdots+c_h=a \\ (c_1,\ldots,c_h)\in(\mathbb{F}_q^*)^h}} \lambda_1(c_1)\cdots\lambda_h(c_h) \\ &= (-1)^{k-h} \sum_{\substack{c_1+\cdots+c_h=a \\ (c_1,\ldots,c_h)\in(\mathbb{F}_q^*)^h}} \lambda_1(c_1)\cdots\lambda_h(c_h) \\ &= (-1)^{k-h} \widetilde{J}_a(\lambda_1, \ldots, \lambda_h),\end{aligned}$$

where the fourth equation holds due to the orthogonal relation of multiplicative characters. This implies that

$$|\widetilde{J}_a(\lambda_1, \ldots, \lambda_k)| = |\widetilde{J}_a(\lambda_1, \ldots, \lambda_h)|.$$

Since $\lambda_1, \lambda_2, \ldots, \lambda_h$ are nontrivial, the desired conclusions follow from Lemma 10. □

2) The Case $a = 0$: We now consider the case $a = 0$. By Lemmas 8 and 9, we directly have the following result.

Lemma 12: Let $\widetilde{J}_0(\lambda_1, \ldots, \lambda_k)$ be the character sum defined before.

(1) *If $\lambda_1, \ldots, \lambda_k$ are trivial, then $\widetilde{J}_0(\lambda_1, \ldots, \lambda_k) = \frac{1}{q}((q-1)^k + (-1)^k(q-1))$.*

(2) *If all of $\lambda_1, \ldots, \lambda_k$ are nontrivial characters and $\lambda_1 \cdots \lambda_k$ is nontrivial, then $|\widetilde{J}_0(\lambda_1, \ldots, \lambda_k)| = 0$.*

(3) *If all of $\lambda_1, \ldots, \lambda_k$ are nontrivial characters and $\lambda_1 \cdots \lambda_k$ is trivial, then $|\widetilde{J}_0(\lambda_1, \ldots, \lambda_k)| = (q-1)q^{\frac{k-2}{2}}$.*

With similar arguments as those in the proof of Lemma 11, one can prove the following results.

Lemma 13: Assume that $\lambda_1, \lambda_2, \ldots, \lambda_h$ are nontrivial and $\lambda_{h+1}, \ldots, \lambda_k$ are trivial for $1 \le h \le k-1$.

(1) *If $\lambda_1 \cdots \lambda_h$ is nontrivial, then $|\widetilde{J}_0(\lambda_1, \ldots, \lambda_k)| = 0$.*

(2) *If $\lambda_1 \cdots \lambda_h$ is trivial, then $|\widetilde{J}_0(\lambda_1, \ldots, \lambda_k)| = (q-1)q^{\frac{h-2}{2}}$.*

B. The First Construction of Asymptotically Optimal Codebooks

In this subsection, we present a construction of codebooks, which is based on multiplicative characters of $\mathbb{F}_q$. Throughout this subsection, we let $a \in \mathbb{F}_q^*$ and $n = \frac{1}{q}((q-1)^k + (-1)^{k+1})$ unless otherwise stated.

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

$$\begin{array}{c}(1, 0, 0, \cdots, 0, 0), \\ (0, 1, 0, \cdots, 0, 0), \\ \vdots \\ (0, 0, 0, \cdots, 0, 1).\end{array}$$

Let $\psi_{j_1}, \psi_{j_2}, \ldots, \psi_{j_k}$ be k multiplicative characters of $\mathbb{F}_q$ defined in Definition 4, where $j_1, \ldots, j_k \in \{0, 1, \ldots, q-2\}$. Define a set

$$\mathcal{S} = \{(c_1, \ldots, c_k) \in (\mathbb{F}_q^*)^k : c_1 + \ldots + c_k = a\}$$

for $a \in \mathbb{F}_q^*$. Note that $|\mathcal{S}| = n$ by Lemma 9. Then we define a codeword of length n by

$$\mathbf{c}_{(j_1,\ldots,j_k)} = \frac{1}{\sqrt{n}}(\psi_{j_1}(c_1)\cdots\psi_{j_k}(c_k))_{(c_1,\ldots,c_k)\in\mathcal{S}}.$$

This codeword is a unit norm $1 \times n$ complex vector.

Now we construct a complex codebook $\mathcal{C}$ as

$$\mathcal{C} = \{\mathbf{c}_{(j_1,\ldots,j_k)} : j_1, \ldots, j_k \in \{0, 1, \ldots, q-2\}\} \cup \mathcal{E}_n. \quad \text{(III.3)}$$

The alphabet size of the codebook $\mathcal{C}$ is $q+1$. By definition, $\mathcal{C}$ has $N = (q-1)^k + n$ codewords of length $K = n = \frac{1}{q}((q-1)^k + (-1)^{k+1})$. Consequently, we have the following conclusion.

Lemma 14: If $k = 2$, we have $N > K^2$. If $k > 2$, we have $K < N < K^2$.

Theorem 15: Let $\mathcal{C}$ be the codebook in Equation (III.3). Then it is a $((q-1)^k + n, n)$ codebook with

$$I_{\max}(\mathcal{C}) = \frac{q^{\frac{k+1}{2}}}{(q-1)^k + (-1)^{k+1}},$$

where $n = \frac{1}{q}((q-1)^k + (-1)^{k+1})$.

Proof: Let $\mathbf{c}, \mathbf{c}' \in \mathcal{C}$ be two distinct codewords. Denote $\mathcal{F} = \mathcal{C} \backslash \mathcal{E}_n$. Now we calculate the correlation of $\mathbf{c}$ and $\mathbf{c}'$ in the following cases.

(1) If $\mathbf{c}, \mathbf{c}' \in \mathcal{E}_n$, it is obvious that $|\mathbf{c}\mathbf{c}'^H| = 0$.

(2) If $\mathbf{c} \in \mathcal{F}, \mathbf{c}' \in \mathcal{E}_n$ or $\mathbf{c} \in \mathcal{E}_n, \mathbf{c}' \in \mathcal{F}$, we have

$$|\mathbf{c}\mathbf{c}'^H| = \frac{1}{\sqrt{n}} |\psi_{j_1}(c_1) \cdots \psi_{j_k}(c_k)| = \frac{1}{\sqrt{n}}$$

for some $(c_1, \ldots, c_k) \in \mathcal{S}$ and $j_1, \ldots, j_k \in \{0, 1, \ldots, q-2\}$.

(3) If $\mathbf{c}, \mathbf{c}' \in \mathcal{F}$, we assume that $\mathbf{c} = \mathbf{c}_{(j_1,\ldots,j_k)}$ and $\mathbf{c}' = \mathbf{c}_{(j'_1,\ldots,j'_k)}$ with $(j_1, \ldots, j_k) \neq (j'_1, \ldots, j'_k)$ where $j_1, \ldots, j_k \in \{0, 1, \ldots, q-2\}$ and $j'_1, \ldots, j'_k \in \{0, 1, \ldots, q-2\}$. By Lemma 5, $\psi_{j_t}\overline{\psi'_{j_t}} = \psi_{j_t - j'_t}$ for all $t = 0, 1, \ldots, q-2$. Denote $\lambda_t = \psi_{j_t - j'_t}$ for all $t = 0, 1, \ldots, q-2$. Then we have

$$\begin{aligned} \mathbf{c}\mathbf{c}'^H &= \frac{1}{n} \sum_{\substack{c_1+\cdots+c_k=a \\ (c_1,\ldots,c_k) \in (\mathbb{F}_q^*)^k}} \lambda_1(c_1) \cdots \lambda_k(c_k) \\ &= \frac{1}{n} \widetilde{J}_a(\lambda_1, \ldots, \lambda_k). \end{aligned}$$

Since $(j_1, \ldots, j_k) \neq (j'_1, \ldots, j'_k)$, not all of λ_t are trivial characters. Hence, by Lemmas 10 and 11, we deduce

$$\begin{aligned} |\mathbf{c}\mathbf{c}'^H| \in & \left\{ \frac{q^{\frac{k-1}{2}}}{n}, \frac{q^{\frac{k-2}{2}}}{n} \right\} \cup \left\{ \frac{q^{\frac{h-1}{2}}}{n} : 1 \leq h \leq k-1 \right\} \\ & \cup \left\{ \frac{q^{\frac{h-2}{2}}}{n} : 2 \leq h \leq k-1 \right\}. \end{aligned}$$

We remark that $|\mathbf{c}\mathbf{c}'^H|$ can take all the values in the sets on the right hand of the above expression. Furthermore, $|\mathbf{c}\mathbf{c}'^H| = \frac{q^{\frac{k-1}{2}}}{n}$ if and only if all of $\lambda_1, \ldots, \lambda_k$ are nontrivial characters and $\lambda_1 \cdots \lambda_k$ is nontrivial.

Summarizing the conclusions in the three cases above, we obtain

$$\begin{aligned} |\mathbf{c}\mathbf{c}'^H| \in & \left\{ 0, \frac{1}{\sqrt{n}}, \frac{q^{\frac{k-1}{2}}}{n}, \frac{q^{\frac{k-2}{2}}}{n} \right\} \cup \left\{ \frac{q^{\frac{h-1}{2}}}{n} : 1 \leq h \leq k-1 \right\} \\ & \cup \left\{ \frac{q^{\frac{h-2}{2}}}{n} : 2 \leq h \leq k-1 \right\}. \end{aligned}$$

As a result, we have

$$I_{\max}(\mathcal{C}) = \frac{q^{\frac{k-1}{2}}}{n}$$

where $n = \frac{1}{q}((q-1)^k + (-1)^{k+1})$. This completes the proof. □

Theorem 16: When $k = 2$, the codebook in Theorem 15 is asymptotically optimal with respect to the Levenshtein bound in Equation (I.3).

Proof: For $N = (q-1)^2 + (q-2)$ and $K = q-2$, by Lemma 2, we have

$$I_L = \sqrt{\frac{q^2 + q - 4}{(q-1)^3}}.$$

Hence, by Theorem 15,

$$\frac{I_L}{I_{\max}} = \sqrt{\frac{(q^2 + q - 4)(q-2)^2}{q(q-1)^3}}.$$

Consequently, $\lim_{q \to \infty} \frac{I_L}{I_{\max}} = 1$. This completes the proof. □

Theorem 17: When $k > 2$, the codebook in Theorem 15 is asymptotically optimal with respect to the Welch bound in Equation (I.1).

Proof: By Lemma 14, $N < K^2$. For $N = (q-1)^k + n$ and $K = n = \frac{1}{q}((q-1)^k + (-1)^{k+1})$, by Lemma 1, we have

$$I_W = \sqrt{\frac{(q-1)^k}{n((q-1)^k + n - 1)}}.$$

Hence, by Theorem 15,

$$\begin{aligned} \frac{I_W}{I_{\max}} &= \sqrt{\frac{(q-1)^k n}{q^{k-1}((q-1)^k + n - 1)}} \\ &= \sqrt{\frac{(q-1)^k}{(q-1)^k + n - 1}} \cdot \sqrt{\frac{(q-1)^k + (-1)^{k+1}}{q^k}}. \end{aligned}$$

It then follows that $\lim_{q \to \infty} \frac{I_W}{I_{\max}} = 1$. This completes the proof. □

Example 18: Let $p = q = 5, a = 1$ and $k = 2$, then $N = 19$, $K = 3$. Let α be a primitive element of $\mathbb{F}_q$ with $\alpha^2 + 1 = 0$. Then $\mathbb{F}_q = \{0, 1, \alpha, \alpha^2, \alpha^3\}$. Without loss of generality, we assume that $\alpha = 2$. It is easy to verify that all the 2-tuple $(c_1, c_2) \in (\mathbb{F}_q^*)^2$ satisfying $c_1 + c_2 = 1$ are the following:

$$(\alpha, \alpha^2) \text{ or } (\alpha^2, \alpha) \text{ or } (\alpha^3, \alpha^3).$$

Thus, $\mathcal{S} = \{(\alpha, \alpha^2), (\alpha^2, \alpha), (\alpha^3, \alpha^3)\}$. The set $\mathcal{F} = \mathcal{C} \backslash \mathcal{E}_3$ consists of the following 16 codewords of length 3:

$$\begin{aligned} &\mathbf{c}_0 = \frac{1}{\sqrt{3}}(1, 1, 1), \quad \mathbf{c}_1 = \frac{1}{\sqrt{3}}(-1, i, -i), \\ &\mathbf{c}_2 = \frac{1}{\sqrt{3}}(i, -1, -i), \quad \mathbf{c}_3 = \frac{1}{\sqrt{3}}(-1, 1, -1), \\ &\mathbf{c}_4 = \frac{1}{\sqrt{3}}(1, -1, -1), \quad \mathbf{c}_5 = \frac{1}{\sqrt{3}}(-i, -1, i), \\ &\mathbf{c}_6 = \frac{1}{\sqrt{3}}(-1, -i, i), \quad \mathbf{c}_7 = \frac{1}{\sqrt{3}}(1, i, i), \\ &\mathbf{c}_8 = \frac{1}{\sqrt{3}}(-i, -i, -1), \quad \mathbf{c}_9 = \frac{1}{\sqrt{3}}(-1, -1, 1), \\ &\mathbf{c}_{10} = \frac{1}{\sqrt{3}}(i, i, -1), \quad \mathbf{c}_{11} = \frac{1}{\sqrt{3}}(i, 1, i), \\ &\mathbf{c}_{12} = \frac{1}{\sqrt{3}}(i, -i, 1), \quad \mathbf{c}_{13} = \frac{1}{\sqrt{3}}(-i, i, 1), \\ &\mathbf{c}_{14} = \frac{1}{\sqrt{3}}(1, -i, -i), \quad \mathbf{c}_{15} = \frac{1}{\sqrt{3}}(-i, 1, -i), \end{aligned}$$

where $i = \sqrt{-1}$. It is easy to verify that the codebook $\mathcal{C} = \mathcal{F} \cup \mathcal{E}_3$ of Theorem 15 is a $(19, 3)$ codebook with $I_{\max} = \frac{\sqrt{5}}{3}$. This is consistent with the conclusion of Theorem 15.

In Table I, we provide the parameters of examples of the codebook of Theorem 16. The numerical data shows the asymptotic optimality of the codebook. In Table II, we provide

TABLE I

PARAMETERS OF THE (N, K) CODEBOOK IN THEOREM 16

q	N	K	$I_{\max}$	I_L	$I_L/I_{\max}$
11	109	9	0.368514	0.357771	0.970845
13	155	11	0.327777	0.320951	0.979175
16	239	14	0.285714	0.281793	0.986276
17	271	15	0.274874	0.271534	0.987849
23	505	21	0.228373	0.226859	0.993370
41	1639	39	0.164183	0.163841	0.997917
64	4031	62	0.129032	0.128922	0.999147
121	14,519	119	0.092437	0.092415	0.999762
128	16,255	126	0.089791	0.089772	0.999788

TABLE II

PARAMETERS OF THE (N, K) CODEBOOK IN THEOREM 17

q	N	K	$I_{\max}$	I_W	$I_W/I_{\max}$
11	1091	91	0.120879	0.100407	0.830641
16	3586	211	0.075829	0.066791	0.880877
17	4337	241	0.070539	0.062608	0.887566
23	11,111	463	0.049676	0.045497	0.915875
41	65,561	1561	0.026265	0.025007	0.952104
64	253,954	3907	0.016381	0.015875	0.969111
121	1,742,281	14,281	0.008473	0.008334	0.983595
128	2,064,386	16,003	0.007999	0.007874	0.984373
256	16,646,146	64,771	0.003952	0.003922	0.992409

the parameters of examples of the codebook of Theorem 17 for the case $k = 3$. The numerical data demonstrates the asymptotic optimality of the codebook.

When $a = 0$, one can similarly prove that the codebook in (III.3) has parameters $((q-1)^k + n, n)$ and $I_{\max} = \frac{(q-1)q^{\frac{k-2}{2}}}{n}$, where $n = \frac{1}{q}((q-1)^k + (-1)^k(q-1))$. The codebook in this case has relatively poor parameters with respect to the Welch and Levenshtein bounds. Hence, we are not interested in the codebook defined by $a = 0$.

IV. THE SECOND CONSTRUCTION OF CODEBOOKS

We are now ready to present another construction of codebooks with the multiplicative characters of $\mathbb{F}_q$. In this section, let $K = q^{k-1}$, where k is a positive integer.

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

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

Let $\psi_{j_1}, \psi_{j_2}, \ldots, \psi_{j_k}$ be k multiplicative characters of $\mathbb{F}_q$ defined in Definition 4, where $j_1, \ldots, j_k \in \{0, 1, \ldots, q-2\}$. Define a set

$$\mathcal{S} = \{(c_1, \ldots, c_k) \in (\mathbb{F}_q)^k : c_1 + \ldots + c_k = a\}$$

for $a \in \mathbb{F}_q^*$. Then we have $K := |\mathcal{S}| = q^{k-1}$. We define a codeword of length K by

$$\mathbf{c}_{(j_1,\ldots,j_k)} = \frac{1}{\sqrt{n_{\overline{\mathbf{c}}}}}(\psi_{j_1}(c_1) \cdots \psi_{j_k}(c_k))_{(c_1,\ldots,c_k)\in\mathcal{S}},$$

where $n_{\overline{\mathbf{c}}}$ denotes the Euclidean norm of the vector $\overline{\mathbf{c}}_{(j_1,\ldots,j_k)} := (\psi_{j_1}(c_1) \cdots \psi_{j_k}(c_k))_{(c_1,\ldots,c_k)\in\mathcal{S}}$. When $q = 2$ and k is odd or $q \geq 3$ and $k \geq 1$, Lemma 9 tells that the diagonal equation of (III.1) has at least one solution $(c_1, c_2, \ldots, c_k) \in (\mathbb{F}_q^*)^k$ for $a \in \mathbb{F}_q^*$. Note that $\psi_{j_i}(0)$ means the extended value defined before. Hence, any codeword $\mathbf{c}_{(j_1,\ldots,j_k)}$ is a unit norm $1 \times K$ complex vector. It follows from Lemma 9 that

$$\frac{(q-1)^k + (-1)^{k+1}}{q} \leq n_{\overline{\mathbf{c}}} \leq K = q^{k-1}. \qquad \text{(IV.1)}$$

Furthermore, $n_{\overline{\mathbf{c}}} = K$ if all of ψ_{j_i} for $1 \leq i \leq k$ are trivial and $n_{\overline{\mathbf{c}}} = \frac{(q-1)^k+(-1)^{k+1}}{q}$ if all of ψ_{j_i} for $1 \leq i \leq k$ are nontrivial.

Now we construct a complex codebook $\mathcal{C}$ as

$$\mathcal{C} = \{\mathbf{c}_{(j_1,\ldots,j_k)} : j_1, \ldots, j_k \in \{0, 1, \ldots, q-2\}\} \cup \mathcal{E}_K. \quad \text{(IV.2)}$$

The alphabet size of the codebook $\mathcal{C}$ is $q + 1$. By definition, $\mathcal{C}$ has $N = (q-1)^k + q^{k-1}$ codewords of length $K = q^{k-1}$. Consequently, we have the following conclusion.

Theorem 19: Let $q \geq 4$ and $k > 1$ be any positive integer. Then the set $\mathcal{C}$ in Equation (IV.2) is a $((q-1)^k + q^{k-1}, q^{k-1})$ codebook with

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

Proof: Let $\mathbf{c}, \mathbf{c}' \in \mathcal{C}$ be two distinct codewords. Denote $\mathcal{F} = \mathcal{C} \backslash \mathcal{E}_K$. Now we calculate the correlation of $\mathbf{c}$ and $\mathbf{c}'$ by distinguishing among the following cases.

(1) If $\mathbf{c}, \mathbf{c}' \in \mathcal{E}_K$, it is obvious that $|\mathbf{c}\mathbf{c}'^H| = 0$.

(2) If $\mathbf{c} \in \mathcal{F}, \mathbf{c}' \in \mathcal{E}_K$ or $\mathbf{c} \in \mathcal{E}_K, \mathbf{c}' \in \mathcal{F}$, we have

$$|\mathbf{c}\mathbf{c}'^H| = \frac{1}{\sqrt{n_{\overline{\mathbf{c}}}}}|\psi_{j_1}(c_1) \cdots \psi_{j_k}(c_k)| = \frac{1}{\sqrt{n_{\overline{\mathbf{c}}}}}$$

for some $(c_1, \ldots, c_k) \in \mathcal{S}$ and $j_1, \ldots, j_k \in \{0, 1, \ldots, q-2\}$. Hence,

$$\frac{1}{\sqrt{q^{k-1}}} \leq |\mathbf{c}\mathbf{c}'^H| \leq \sqrt{\frac{q}{(q-1)^k + (-1)^{k+1}}}$$

due to Equation (IV.1).

(3) If $\mathbf{c}, \mathbf{c}' \in \mathcal{F}$, we assume that

$$\mathbf{c} = \mathbf{c}_{(j_1,\ldots,j_k)} = \frac{1}{\sqrt{n_{\overline{\mathbf{c}}}}}\overline{\mathbf{c}}_{(j_1,\ldots,j_k)}$$

and

$$\mathbf{c}' = \mathbf{c}_{(j'_1,\ldots,j'_k)} = \frac{1}{\sqrt{n_{\overline{\mathbf{c}}'}}}\overline{\mathbf{c}}'_{(j'_1,\ldots,j'_k)}$$

with $(j_1, \ldots, j_k) \neq (j'_1, \ldots, j'_k)$, where $j_1, \ldots, j_k \in \{0, 1, \ldots, q-2\}$ and $j'_1, \ldots, j'_k \in \{0, 1, \ldots, q-2\}$. By Lemma 5, $\psi_{j_t}\overline{\psi'_{j_t}} = \psi_{j_t - j'_t}$ for all $t = 0, 1, \ldots, q-2$. Denote $\lambda_t = \psi_{j_t - j'_t}$ for all $t = 0, 1, \ldots, q-2$. Then we have

$$\begin{aligned}\mathbf{c}\mathbf{c}'^H &= \frac{1}{\sqrt{n_{\overline{\mathbf{c}}}}} \cdot \frac{1}{\sqrt{n_{\overline{\mathbf{c}}'}}} \sum_{\substack{c_1+\cdots+c_k=a\\(c_1,\ldots,c_t)\in(\mathbb{F}_q)^k}} \lambda_1(c_1) \cdots \lambda_k(c_k)\\ &= \frac{1}{\sqrt{n_{\overline{\mathbf{c}}}}} \cdot \frac{1}{\sqrt{n_{\overline{\mathbf{c}}'}}} J_a(\lambda_1, \ldots, \lambda_k).\end{aligned}$$

Since $(j_1, \ldots, j_k) \neq (j'_1, \ldots, j'_k)$, not all of λ_t are trivial characters. Hence, by Lemma 7 and Equation (II.2), we deduce

$$|\mathbf{c}\mathbf{c}'^H| \in \left\{0, \frac{q^{\frac{k-1}{2}}}{\sqrt{n_{\overline{\mathbf{c}}}} \cdot \sqrt{n_{\overline{\mathbf{c}}'}}}, \frac{q^{\frac{k-2}{2}}}{\sqrt{n_{\overline{\mathbf{c}}}} \cdot \sqrt{n_{\overline{\mathbf{c}}'}}}\right\}.$$

Then

$$|\mathbf{c}\mathbf{c}'^H| \leq \frac{q^{\frac{k+1}{2}}}{(q-1)^k + (-1)^{k+1}} \qquad \text{(IV.3)}$$

due to Equation (IV.1).

We now prove that there are two codewords $\mathbf{c}, \mathbf{c}' \in \mathcal{F}$ such that the equality in (IV.3) holds by distinguishing the following two cases. In the first case, we assume that $k = 2t + 1$ for some nonnegative integer t. In this case, we put

$$\begin{aligned}(j_1, \cdots, j_t, j_{t+1}, \cdots, j_{2t}, j_{2t+1}) \\ = (2, \cdots, 2, 1, \cdots, 1, 2)\end{aligned}$$

and

$$\begin{aligned}(j'_1, \cdots, j'_t, j'_{t+1}, \cdots, j'_{2t}, j'_{2t+1}) \\ = (1, \cdots, 1, 2, \cdots, 2, 1).\end{aligned}$$

We have then

$$\begin{aligned}&(j_1, \cdots, j_t, j_{t+1}, \cdots, j_{2t}, j_{2t+1}) \\ &\quad - (j'_1, \cdots, j'_t, j'_{t+1}, \cdots, j'_{2t}, j'_{2t+1}) \\ &= (1, \cdots, 1, -1, \cdots, -1, 1).\end{aligned}$$

Consequently,

$$\lambda_i = \begin{cases} \psi_1 & \text{if } i \in \{1, 2, \cdots, t\}, \\ \psi_{q-2} & \text{if } i \in \{t+1, t+2, \cdots, 2t\}, \\ \psi_1 & \text{if } i = 2t+1. \end{cases}$$

Clearly, all λ_i are nontrivial and

$$\lambda_1 \lambda_2 \cdots \lambda_k = \psi_1,$$

which is nontrivial.

By definition, all ψ_{j_i} and $\psi_{j'_i}$ are nontrivial. We then deduce that

$$n_{\overline{\mathbf{c}}'} = n_{\overline{\mathbf{c}}} = \frac{(q-1)^k + (-1)^{k+1}}{q}.$$

It then follows from Lemma 7 that

$$|\mathbf{c}\mathbf{c}'^H| = \frac{q^{\frac{k+1}{2}}}{(q-1)^k + (-1)^{k+1}}$$

We now consider the second case that $k = 2t$ for some $t \geq 1$. In this case, we put

$$\begin{aligned}(j_1, \cdots, j_{t-1}, j_t, \cdots, j_{2t-2}, j_{2t-1}, j_{2t}) \\ = (2, \cdots, 2, 1, \cdots, 1, 2, 2)\end{aligned}$$

and

$$\begin{aligned}(j'_1, \cdots, j'_{t-1}, j'_t, \cdots, j'_{2t-2}, j'_{2t-1}, j'_{2t}) \\ = (1, \cdots, 1, 2, \cdots, 2, 1, 1).\end{aligned}$$

We have then

$$\begin{aligned}&(j_1, \cdots, j_{t-1}, j_t, \cdots, j_{2t-2}, j_{2t-1}, j_{2t}) \\ &\quad - (j'_1, \cdots, j'_{t-1}, j'_t, \cdots, j'_{2t-2}, j'_{2t-1}, j'_{2t}) \\ &= (1, \cdots, 1, -1, \cdots, -1, 1, 1).\end{aligned}$$

Consequently,

$$\lambda_i = \begin{cases} \psi_1 & \text{if } i \in \{1, 2, \cdots, t-1\}, \\ \psi_{q-2} & \text{if } i \in \{t, t+1, \cdots, 2t-2\}, \\ \psi_1 & \text{if } i \in \{2t-1, 2t\}. \end{cases}$$

Clearly, all λ_i are nontrivial and

$$\lambda_1 \lambda_2 \cdots \lambda_k = \psi_2,$$

which is nontrivial.

By definition, all ψ_{j_i} and $\psi_{j'_i}$ are nontrivial. We then deduce that

$$n_{\overline{\mathbf{c}}'} = n_{\overline{\mathbf{c}}} = \frac{(q-1)^k + (-1)^{k+1}}{q}.$$

It then follows from Lemma 7 that

$$|\mathbf{c}\mathbf{c}'^H| = \frac{q^{\frac{k+1}{2}}}{(q-1)^k + (-1)^{k+1}}$$

Summarizing the conclusions in the three cases above, we obtain

$$I_{\max}(\mathcal{C}) \frac{q^{\frac{k+1}{2}}}{(q-1)^k + (-1)^{k+1}}.$$

This completes the proof. □

Theorem 20: When $k \geq 2$ and $q \geq 4$, the codebook in Theorem 19 is asymptotically optimal with respect to the Welch bound in Equation (I.1).

Proof: Recall that $N = (q-1)^k + q^{k-1}$ and $K = q^{k-1}$, then $N < K^2$ for $k > 2$. By Lemma 1, we have

$$I_W = \sqrt{\frac{(q-1)^k}{q^{k-1}((q-1)^k + q^{k-1} - 1)}}.$$

By Theorem 19, we recall that

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

It then follows that

$$\lim_{q \to \infty} \frac{I_W}{\frac{q^{\frac{k+1}{2}}}{(q-1)^k + (-1)^{k+1}}} = 1.$$

This completes the proof. □

Example 21: Let $p = q = 5, a = 1$ and $k = 2$, then $N = 21$, $K = 5$. Let α be a primitive element of $\mathbb{F}_q$ with $\alpha^2 + 1 = 0$. Then $\mathbb{F}_q = \{0, 1, \alpha, \alpha^2, \alpha^3\}$. It is easy to verify that

$$\mathcal{S} = \{(\alpha, \alpha^2), (\alpha^2, \alpha), (\alpha^3, \alpha^3), (0, 1), (1, 0)\}.$$

TABLE III
PARAMETERS OF THE CODEBOOKS OF THEOREMS 17 AND 20 AND SOME OTHERS

Parameters	$I_{\max}$	Reference
(N, N)	0	[22], [29]
$(N, N-1)$	$\frac{1}{N-1}$	[22], [29]
$(2^{d+1}, 2^d)$	$\sqrt{\frac{1}{2^{d+1}-1}}$	[2], [23]
$(p^d+1, \frac{p^d+1}{2})$ with odd p	$\frac{1}{p^d}$	[2], [23]
(N, K) (from difference set)	$\sqrt{\frac{N-K}{(N-1)K}}$	[3], [4], [29]
(N, K) (from Steiner systems)	$\frac{\sqrt{p^m}}{p^m-1}$	[26]
$((q-1)^k+n, n)$, $k>2$, where$n = \frac{(q-1)^k+(-1)^{k+1}}{q}$	$\frac{q^{\frac{k-1}{2}}}{n}$	Theorem III.9
$(q^l - q^{l-1} - 1, q^{l-1})$ with any $l > 2$	$\frac{1}{\sqrt{q^{l-1}}}$	[34]
$((q-1)^k + q^{k-1}, q^{k-1})$ with any $k > 2, q \geq 4$	$\frac{q^{\frac{k+1}{2}}}{(q-1)^k+(-1)^{k+1}}$	Theorem IV.2

TABLE IV
PARAMETERS OF THE CODEBOOKS IN THEOREM 16 AND SOME OTHERS

Parameters	$I_{\max}$	Reference
$(2^{2m-1}+2^m, 2^m)$	$\frac{1}{\sqrt{2^m}}$	[1], [28], [30], [33]
$(p^{2m}+p^m, p^m)$ with odd p	$\frac{1}{\sqrt{p^m}}$	[6], [28], [33]
$(2^{2m}+2^m, 2^m)$	$\frac{1}{\sqrt{2^m}}$	[1], [11]
$(p^{2m}-1, p^m-1)$ with any p	$\frac{\sqrt{p^m}}{p^m-1}$	[26]
$(p^{2m}-p^m-1, p^m-2)$ with any p	$\frac{\sqrt{p^m}}{p^m-2}$	Theorem III.8
$(p^{2m}+p^m-1, p^m)$ with any p	$\frac{1}{\sqrt{p^m}}$	[34]

The set $\mathcal{F} = \mathcal{C}\backslash\mathcal{E}_5$ *consists of the following* 16 *codewords of length* 5*:*

$$\boldsymbol{c}_0 = \frac{1}{\sqrt{5}}(1,1,1,1,1), \quad \boldsymbol{c}_1 = \frac{1}{2}(-1,i,-i,1,0),$$

$$\boldsymbol{c}_2 = \frac{1}{2}(i,-1,-i,0,1), \quad \boldsymbol{c}_3 = \frac{1}{2}(-1,1,-1,0,1),$$

$$\boldsymbol{c}_4 = \frac{1}{2}(1,-1,-1,1,0), \quad \boldsymbol{c}_5 = \frac{1}{2}(-i,-1,i,0,1),$$

$$\boldsymbol{c}_6 = \frac{1}{2}(-1,-i,i,1,0), \quad \boldsymbol{c}_7 = \frac{1}{\sqrt{3}}(1,i,i,0,0),$$

$$\boldsymbol{c}_8 = \frac{1}{\sqrt{3}}(-i,-i,-1,0,0), \quad \boldsymbol{c}_9 = \frac{1}{\sqrt{3}}(-1,-1,1,0,0),$$

$$\boldsymbol{c}_{10} = \frac{1}{\sqrt{3}}(i,i,-1,0,0), \quad \boldsymbol{c}_{11} = \frac{1}{\sqrt{3}}(i,1,i,0,0),$$

$$\boldsymbol{c}_{12} = \frac{1}{\sqrt{3}}(i,-i,1,0,0), \quad \boldsymbol{c}_{13} = \frac{1}{\sqrt{3}}(-i,i,1,0,0),$$

$$\boldsymbol{c}_{14} = \frac{1}{\sqrt{3}}(1,-i,-i,0,0), \quad \boldsymbol{c}_{15} = \frac{1}{\sqrt{3}}(-i,1,-i,0,0),$$

where $i = \sqrt{-1}$*. One can easily verify that the codebook* $\mathcal{C} = \mathcal{F} \cup \mathcal{E}_5$ *of Theorem 19 is a* $(21, 5)$ *codebook with* $I_{\max} = \frac{\sqrt{5}}{3}$*. This is consistent with the conclusion of Theorem 19.*

V. CONCLUSIONS AND REMARKS

In this paper, two new constructions of asymptotically optimal codebooks with multiplicative characters of finite fields were presented. They produce asymptotically optimal codebooks with respect to the Welch bound or the Levenshtein bound. The parameters of the codebooks in Theorems 17 and 20 and those of known (nearly) optimal codebooks with respect to the Welch bound are summarized in Table III. The parameters of the codebooks in Theorem 16 and those of known (nearly) optimal codebooks with respect to the Levenshtein bound are summarized in Table IV, where $q = p^m$. The parameters of our asymptotic codebooks are new and flexible. The analysis of the parameters of our codebooks is mainly based on Jacobi sums and related character sums.

As pointed out in [15], constructing optimal codebooks with minimal $I_{\max}$ is very difficult in general. This problem is equivalent to line packing in Grassmannian spaces [2]. In frame theory, such a codebook with $I_{\max}$ minimized is referred to as a Grassmannian frame [23]. The codebooks presented in this paper should have applications in these areas. With the framework developed in [18], our codebooks can be used to obtain deterministic sensing matrices with small coherence for compressed sensing.

ACKNOWLEDGMENTS

The authors are very grateful to the reviewers and the Associate Editor, Prof. Sihem Mesnager, for their comments and suggestions that improved the quality and presentation of this paper. Part of this paper was done when the first author was visiting the second one in 2016.

REFERENCES

[1] A. R. Calderbank, P. J. Cameron, W. M. Kantor, and J. J. Seidel, "$\mathbb{Z}_4$-Kerdock codes, orthogonal spreads, and extremal Euclidean line-sets," *Proc. London Math. Soc.*, vol. 75, no. 2, pp. 436–480, 1997.

[2] J. H. Conway, R. H. Hardin, and N. J. A. Sloane, "Packing lines, planes, etc.: Packings in Grassmannian spaces," *Experim. Math.*, vol. 5, no. 2, pp. 139–159, 1996.

[3] C. Ding, "Complex codebooks from combinatorial designs," *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 4229–4235, Sep. 2006.

[4] C. Ding and T. Feng, "A generic construction of complex codebooks meeting the Welch bound," *IEEE Trans. Inf. Theory*, vol. 53, no. 11, pp. 4245–4250, Nov. 2007.

[5] C. Ding and T. Feng, "Codebooks from almost difference sets," *Design Codes Cryptogr.*, vol. 46, no. 1, pp. 113–126, Jan. 2008.

[6] C. Ding and J. Yin, "Signal sets from functions with optimum nonlinearity," *IEEE Trans. Commun.*, vol. 55, no. 5, pp. 936–940, May 2007.

[7] M. Fickus and D. G. Mixon. (Jun. 2016). "Tables of the existence of equiangular tight frames." [Online]. Available: https://arxiv.org/abs/1504.00253

[8] M. Fickus, D. G. Mixon, and J. Jasper, "Equiangular tight frames from hyperovals," *IEEE Trans. Inf. Theory*, vol. 62, no. 9, pp. 5225–5236, Sep. 2016.

[9] M. Fickus, J. Jasper, D. G. Mixon, and J. Peterson. (Feb. 2016). "Tremain equiangular tight frames." [Online]. Available: https://arxiv.org/abs/1602.03490

[10] M. Fickus, D. G. Mixon, and J. C. Tremain, "Steiner equiangular tight frames," *Linear Algebra Appl.*, vol. 436, no. 5, pp. 1014–1027, 2012.

[11] Z. Heng and Q. Yue, "Optimal codebooks achieving the Levenshtein bound from generalized bent functions over $\mathbb{Z}_4$" *Cryptogr. Commun.*, vol. 9, no. 1, pp. 41–53, Jan. 2017.

[12] H. Hu and J. Wu, "New constructions of codebooks nearly meeting the Welch bound with equality," *IEEE Trans. Inf. Theory*, vol. 60, no. 2, pp. 1348–1355, Feb. 2014.

[13] B. M. Hochwald, T. L. Marzetta, T. J. Richardson, W. Sweldens, and R. Urbanke, "Systematic design of unitary space-time constellations," *IEEE Trans. Inf. Theory*, vol. 46, no. 6, pp. 1962–1973, Sep. 2000.

[14] R. Lidl and H. Niederreiter, *Finite Fields*. Cambridge, U.K.: Cambridge Univ. Press, 1984.

[15] D. J. Love, R. W. Heath, and T. Strohmer, "Grassmannian beamforming for multiple-input multiple-output wireless systems," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2735–2747, Oct. 2003.

[16] C. Li, Q. Yue, and Y. Huang, "Two families of nearly optimal codebooks," *Des. Codes Cryptograph.*, vol. 75, no. 1, pp. 43–57, Apr. 2015.

[17] V. I. Levenshtein, "Bounds for packing of metric spaces and some of their applications," *Problem Cybern.*, vol. 40, pp. 43–110, 1983.

[18] S. Li and G. Ge, "Deterministic sensing matrices arising from near orthogonal systems," *IEEE Trans. Inf. Theory*, vol. 60, no. 4, pp. 2291–2302, Apr. 2014.

[19] J. L. Massey and T. Mittelholzer, "Welch's bound and sequence sets for code-division multiple-access systems," in *Sequences II*. New York, NY, USA: Springer-verlag, 1993, pp. 63–78.

[20] K. K. Mukkavilli, A. Sabharwal, E. Erkip, and B. A. Aazhang, "On beamforming with finite rate feedback in multiple-antenna systems," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2562–2579, Oct. 2003.

[21] F. Rahimi, "Covering graphs and equiangular tight frames," Ph.D. dissertation, Dept. Combinat. Optim., Univ. Waterloo, Ontario, ON, USA, 2016. [Online]. Available: http://hdl.handle.net/10012/10793

[22] D. V. Sarwate, *Meeting the Welch Bound With Equality*. New York, NY, USA: Springer-Verlag, 1999, pp. 63–79.

[23] T. Strohmer and R. W. Heath, "Grassmannian frames with applications to coding and communication," *Appl. Comput. Harmon. Anal.*, vol. 14, no. 3, pp. 257–275, May 2003.

[24] V. Tarokh and I.-M. Kim, "Existence and construction of noncoherent unitary space-time codes," *IEEE Trans. Inf. Theory*, vol. 48, no. 12, pp. 3112–3117, Dec. 2002.

[25] E. V. Tsiligianni, L. P. Kondi, and A. K. Katsaggelos, "Construction of incoherent unit norm tight frames with application to compressed sensing," *IEEE Trans. Inf. Theory*, vol. 60, no. 4, pp. 2319–2330, Apr. 2014.

[26] P. Tan, Z. Zhou, and D. Zhang, "A construction of codebooks nearly achieving the levenstein bound," *IEEE Signal Process. Lett.*, vol. 23, no. 10, pp. 1306–1309, Oct. 2016.

[27] L. Welch, "Lower bounds on the maximum cross correlation of signals," *IEEE Trans. Inf. Theory*, vol. 20, no. 3, pp. 397–399, May 1974.

[28] W. K. Wootters and B. D. Fields, "Optimal state-determination by mutually unbiased measurements," *Ann. Phys.*, vol. 191, no. 2, pp. 363–381, 1989.

[29] P. Xia, S. Zhou, and G. B. Giannakis, "Achieving the Welch bound with difference sets," *IEEE Trans. Inf. Theory*, vol. 51, no. 5, pp. 1900–1907, May 2005.

[30] C. Xiang, C. Ding, and S. Mesnager, "Optimal codebooks from binary codes meeting the levenshtein bound," *IEEE Trans. Inf. Theory*, vol. 61, no. 12, pp. 6526–6535, Dec. 2015.

[31] N. Y. Yu, "A construction of codebooks associated with binary sequences," *IEEE Trans. Inf. Theory*, vol. 58, no. 8, pp. 5522–5533, Aug. 2012.

[32] A. Zhang and K. Feng, "Two classes of codebooks nearly meeting the Welch bound," *IEEE Trans. Inf. Theory*, vol. 58, no. 4, pp. 2507–2511, Apr. 2012.

[33] Z. Zhou, C. Ding, and N. Li, "New families of codebooks achieving the levenstein bound," *IEEE Trans. Inf. Theory*, vol. 60, no. 11, pp. 7382–7387, Nov. 2014.

[34] Z. Zhou and X. Tang, "New nearly optimal codebooks from relative difference sets," *Adv. Math. Commun.*, vol. 5, no. 3, pp. 521–527, Aug. 2011.

Ziling Heng received the B.Sci. degree in mathematics from Henan Normal University, Xinxiang, China, in 2012. Currently, he is a Ph.D. candidate in Fundamental Mathematics at Nanjing University of Aeronautics and Astronautics, Nanjing, China. His research interests include coding theory and sequences.

Cunsheng Ding (M'98–SM'05) was born in 1962 in Shaanxi, China. He received the M.Sc. degree in 1988 from the Northwestern Telecommunications Engineering Institute, Xian, China; and the Ph.D. in 1997 from the University of Turku, Turku, Finland.

From 1988 to 1992 he was a Lecturer of Mathematics at Xidian University, China. Before joining the Hong Kong University of Science and Technology in 2000, where he is currently a Professor of Computer Science and Engineering, he was an Assistant Professor of Computer Science at the National University of Singapore.

His research fields are combinatorial designs, cryptography and coding theory. He has coauthored four research monographs, and served as a guest editor or editor for ten journals. Dr. Ding co-received the State Natural Science Award of China in 1989.

Qin Yue received the Ph.D. degree in mathematics from The University of Science and Technology of China, Hefei, China, in 1999. He is currently a Professor in the Department of Mathematics, Nanjing University of Aeronautics and Astronautics, Nanjing, China. His research interests include algebraic number theory, cryptography, and coding theory.