IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received February 17, 2020, accepted March 4, 2020, date of publication March 12, 2020, date of current version March 27, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2980330

Asymptotically Optimal Codebooks Derived From Generalised Bent Functions

QIUYAN WANG[1] AND YANG YAN[2]

[1]School of Computer Science and Technology, Tiangong University, Tianjin 300387, China
[2]School of Information Technology and Engineering, Tianjin University of Technology and Education, Tianjin 300222, China

Corresponding author: Yang Yan (yanyangucas@126.com)

This work was supported by the Science and Technology Development Fund of Tianjin Education Commission for Higher Education under Grant 2018KJ215.

ABSTRACT Codebooks are required to have small inner-product correlation in many practical applications, such as direct spread code division multiple access communications, space-time codes and compressed sensing. In general, it is difficult to construct optimal codebooks. In this paper, two kinds of codebooks are presented and proved to be optimally optimal with respect to the Welch bound. Additionally, the constructed codebooks in this paper have new parameters.

INDEX TERMS Codebook, asymptotic optimality, Welch bound, generalised bent function.

I. INTRODUCTION

An (N, K) codebook $\mathcal{C}$ is defined to be a set of unit-norm complex vectors $\{\mathbf{c}_i\}_{i=0}^{N-1}$ in $\mathbb{C}^K$ over an alphabet A. Let

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

where $\mathbf{c}_j^H$ denotes the Hermite transpose of vector $\mathbf{c}_j$. The maximum inner-product correction $I_{\max}(\mathcal{C})$ is a performance measure of a codebook $\mathcal{C}$ in practical applications. In code division multiple access (CDMA) systems, one important problem is to minimize the codebook's maximal cross-correlation amplitude $I_{\max}(\mathcal{C})$.

For a given K, it is usually desirable that N is as large as possible and $I_{\max}(\mathcal{C})$ is as small as possible simultaneously. However, the parameters N, K and $I_{\max}(\mathcal{C})$ of a codebook have to satisfy the Welch bound [25]. That is, there is a tradeoff between the codeword length K, the set size N and $I_{\max}(\mathcal{C})$. A codebook meeting the theoretical bound with equality is said to be optimal. Searching optimal codebooks has been an interesting research topic in recent years. Many classes of optimal codebooks has been constructed [1], [3]–[7], [18], [19], [23], [26].

It is worthwhile to point out that the constructed codebooks so far have restrictive parameters N and K. Hence, many researchers attempt to research asymptotically optimal codebooks, i.e., $I_{\max}(\mathcal{C})$ asymptotically meets the theoretical bound for sufficiently large K. One important method to construct asymptotically optimal codebooks is from difference sets of finite abelian gruops which is developed by Ding and Feng [3], [4]. In [3], [4], several series of asymptotically codebooks were constructed by using almost difference sets. In [2], [8], [27], asymptotically optimal codebooks were presented by binary row selection sequences. Character sums over finite fields are considered to be useful tools for the design of asymptotically codebooks. Recently, in [9], [10], Heng *et al.* obtained two new constructions of infinitely many codebooks by Jacobi sums and their generalizations. In [15], [16], Luo and Cao defined a new character sum which is called hyper Eisenstein sum and presented two constructions of infinitely many new codebooks achieving the Wech bound. In [24], Tian presented two constructions of codebooks with additive characters over finite fields.

Bent functions are a class of Boolean functions and have important applications in cryptography, code theory and sequences for communications. In cryptography, bent vectorial functions can be used as substitution boxes in block ciphers (ensuring confusion, as explained by Shannon [20]. In code theory, they are useful for constructing error correcting codes (Kerdock codes) [17]. In sequences, they permit to construct sequences with low correlation [11].

The objective of this paper is to present two constructions of codebooks using generalised bent functions over a ring of integers modulo Q. The presented two kinds of codebooks have properties: (1) they are asymptotically optimal with respect to the Welch bound; (2) the parameters of these codebooks are new and flexible. As a comparison with the known ones, our codebooks are listed in Table 1.

The associate editor coordinating the review of this manuscript and approving it for publication was Matti Hämäläinen.

TABLE 1. **The parameters of codebooks asymptotically meeting the Welch bound.**

Ref.	Parameters (N, K)	Constraints
[8]	$\left(p^n, \frac{p-1}{2p}\left(p^n + p^{n/2}\right) + 1\right)$	p is an odd prime
[28]	$\left(q^2, \frac{(q-1)^2}{2}\right)$	q is an odd prime power
[13]	$\left(q(q+4), \frac{(q+3)(q+1)}{2}\right)$	q is a power of a prime
[13]	$\left(q, \frac{q+1}{2}\right)$	q is a prime power
[27]	$\left(p^n - 1, \frac{p^n-1}{2}\right)$	p is an odd prime
[29]	$(q^t + q^{t-1} - 1, q^{t-1})$	q is a prime power
[9]	$((q-1)^\ell + q^{\ell-1}, q^{\ell-1})$	$q \geq 4$ is a power of a prime, $\ell > 2$
[9]	$((q-1)^\ell + M, M)$	$M = \frac{(q-1)^\ell + (-1)^{\ell+1}}{q}$, q is a prime power, $\ell > 2$
[14]	$((q^s - 1)^m + M, M)$	$M = \frac{(q^s-1)^m + (-1)^{m+1}}{q}$, $s > 1, m > 1$, q is a prime power
[14]	$((q^s - 1)^m + q^{sm-1}, q^{sm-1})$	$s > 1, m > 1$, q is a prime power
[14]	$((q^s - 1)^m + q^{sm-1}, q^{sm-1})$	$s > 1, m > 1$, q is a prime power
[24]	$(q^3 + q^2, q^2)$	q is a prime power
[24]	$(q^3 + q^2 - q, q^2 - q)$	q is a prime power
Thm. III.1	$((p_{\min} + 1)Q^2, Q^2)$	$Q > 1$ is an integer, $p_{\min}$ is the smallest prime factor of Q
Thm. IV.1	$((p_{\min} + 1)Q^2 - Q, Q(Q-1))$	$Q > 2$ is an integer, $p_{\min}$ is the smallest prime factor of Q

This paper is organized as follows. In Section 2, we briefly recall some definitions and notations which will be needed in our discussion. In Section 3 and Section 4, we present our constructions of codebooks and prove that they are asymptotically optimal with respect to the Welch bound. In Section 5, concluding remarks of this paper is given.

II. PRELIMINARIES

In this section, we present some notations and preliminaries which are needed for the proof of the main results. Firstly, a useful lemma is given in the following.

Lemma 1 (Linear Congruence Theorem, [22]): Let a, c, and m be integers with $m > 1$, and let $g = \gcd(a, m)$.

(1) If $g \nmid c$, then the congruence $ax \equiv c \pmod{m}$ has no solutions.

(2) If $g \mid c$, then the congruence $ax \equiv c \pmod{m}$ has exactly g incongruent solutions.

The following is the well-known Welch bound on N, K and $I_{\max}(\mathcal{C})$ of a codebook $\mathcal{C}$.

Lemma 2: [25] For any (N, K) codebook $\mathcal{C}$ with $N > K$,

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

Moreover, the equality holds if and only if for all pairs of (i, j) with $i \neq j$, it holds that

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

Next, we introduce the definition of generalised bent functions. Let Q be a positive integer and $\mathbb{Z}_Q$ the ring of integers modulo Q. Assume that ξ_Q is a primitive Q-th root of unity. Denote by $\mathbb{Z}_Q^m$ the m-dimensional vector space over $\mathbb{Z}_Q$. A function mapping from $\mathbb{Z}_Q^m$ to $\mathbb{Z}_Q$ is termed a generalised Boolean function on m variables. For a generalised Boolean function f, if the complex Fourier coefficients

$$F_f(a) = \frac{1}{\sqrt{Q^m}} \sum_{x \in \mathbb{Z}_Q^m} \xi_Q^{f(x) - a^T \cdot x}$$

preserve unit magnitude for any $a \in \mathbb{Z}_Q^m$, then f is a generalised bent function.

Bent functions are a hot research topic due to their wide applications in cryptography, information theory and coding theory. Kumar *et al.* [12] introduced the definition of generalised bent functions from $\mathbb{Z}_Q^m$ to $\mathbb{Z}_Q$ and gave a class of generalised bent functions in the following lemma.

Lemma 3 ([12]): Assume that Q is a positive integer. Let $\Omega(x)$ be an arbitrary permutation and $\Theta(x)$ an arbitrary function on $\mathbb{Z}_Q$. Then the function

$$f(x_1, x_2) = x_2 \Omega(x_1) + \Theta(x_1)$$

is generalised bent, where $x_1, x_2 \in \mathbb{Z}_Q$.

For more details on bent functions and generalised bent functions, we refer readers to [21]. Inspired by the generalised bent functions given in Lemma 3, we propose two constructions of codebooks in the following two sections.

III. THE FIRST CONSTRUCTION OF ASYMPTOTICALLY OPTIMAL CODEBOOKS

In this section, we present a construction of codebooks and show that the maximum inner-product correction of these codebooks asymptotically achieves the Welch bound. Before proposing our construction, we need to do some preparations.

Suppose that $Q > 1$ is an integer and p_{min} is the smallest prime factor of Q. Denote the standard basis of the Q^2-dimensional Hilbert space by $\mathcal{E}_{Q^2}$ which is formed by Q^2 vectors of length Q^2 as follow:

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

In the following theorem, we give a new construction of infinite many codebooks and evaluate their maximum inner-product correction.

Theorem 1: Let symbols be the same as above. For any $a \in \mathbb{Z}_{p_{\min}}$, $b, u \in \mathbb{Z}_Q$, define a unit-norm complex vector *of length Q^2 by*

$$\mathbf{c}_{a,b,u} = \frac{1}{Q}\left(\xi_Q^{j(a\pi(i)+b)+u\sigma(i)}\right)_{i,j\in\mathbb{Z}_Q},$$

where $\pi(x)$ and $\sigma(x)$ are permutations on $\mathbb{Z}_Q$. Let

$$\begin{aligned}\mathcal{F} &= \left\{\mathbf{c}_{a,b,u} : a \in \mathbb{Z}_{p_{\min}}, b, u \in \mathbb{Z}_Q\right\},\\ \mathcal{C} &= \mathcal{F} \cup \mathcal{E}_{Q^2}.\end{aligned} \tag{1}$$

Then the set $\mathcal{C}$ is a $\left((p_{\min}+1)Q^2, Q^2\right)$ codebook with $I_{\max}(\mathcal{C}) = \frac{1}{Q}$.

Proof: According to the definition of codebooks, we deduce that $\mathcal{C}$ is consisted of $(p_{min}+1)Q^2$ codewords with length Q^2. In other words, $\mathcal{C}$ is a codebook with parameters $\left((p_{\min}+1)Q^2, Q^2\right)$. Now we turn to the computation of $I_{\max}(\mathcal{C})$. Let $\mathbf{c}_1, \mathbf{c}_2 \in \mathcal{C}$ be two distinct codewords. We distinguish among the following three cases to calculate the correlation of $\mathbf{c}_1$ and $\mathbf{c}_2$.

(1) If $\mathbf{c}_1, \mathbf{c}_2 \in \mathcal{E}_{Q^2}$, it is easy to verify that $\left|\mathbf{c}_1\mathbf{c}_2^H\right| = 0$.

(2) If $\mathbf{c}_1 \in \mathcal{E}_{Q^2}$ and $\mathbf{c}_2 \in \mathcal{F}$, it is obvious that $\left|\mathbf{c}_1\mathbf{c}_2^H\right| = \frac{1}{Q}$.

(3) If $\mathbf{c}_1, \mathbf{c}_2 \in \mathcal{F}$, write $\mathbf{c}_1 = \mathbf{c}_{a,b,u}$ and $\mathbf{c}_2 = \mathbf{c}_{\widehat{a},\widehat{b},\widehat{u}}$, where $(a-\widehat{a}, b-\widehat{b}, u-\widehat{u}) \neq (0,0,0)$. Then we deduce that

$$\begin{aligned}\mathbf{c}_1\mathbf{c}_2^H &= \frac{1}{Q^2}\sum_{i=0}^{Q-1}\sum_{j=0}^{Q-1}\xi_Q^{j(a\pi(i)+b)+u\sigma(i)-j\left(\widehat{a}\pi(i)+\widehat{b}\right)-\widehat{u}\sigma(i)}\\ &= \frac{1}{Q^2}\sum_{i=0}^{Q-1}\xi_Q^{(u-\widehat{u})\sigma(i)}\sum_{j=0}^{Q-1}\xi_Q^{j\left((a-\widehat{a})\pi(i)+b-\widehat{b}\right)}.\end{aligned}$$

If $a-\widehat{a}=0$, we obtain

$$\begin{aligned}\mathbf{c}_1\mathbf{c}_2^H &= \frac{1}{Q^2}\sum_{i=0}^{Q-1}\xi_Q^{(u-\widehat{u})\sigma(i)}\sum_{j=0}^{Q-1}\xi_Q^{j(b-\widehat{b})}\\ &= 0,\end{aligned}$$

where the second identity follows from the fact that $(b-\widehat{b}, u-\widehat{u}) \neq (0,0)$.

If $a-\widehat{a} \neq 0$, then $\gcd(a-\widehat{a}, Q) = 1$. By Lemma 1, the congruence $(a-\widehat{a})\pi(x)+b-\widehat{b} \equiv 0 \pmod{Q}$ has only one integer solution i' in $\mathbb{Z}_Q$. In this case, we have

$$\begin{aligned}\mathbf{c}_1\mathbf{c}_2^H &= \frac{1}{Q^2}\sum_{i=0}^{Q-1}\xi_Q^{(u-\widehat{u})\sigma(i)}\sum_{j=0}^{Q-1}\xi_Q^{j\left((a-\widehat{a})\pi(i)+b-\widehat{b}\right)}\\ &= \frac{1}{Q^2}\sum_{i=0, i\neq i'}^{Q-1}\xi_Q^{(u-\widehat{u})\sigma(i)}\sum_{j=0}^{Q-1}\xi_Q^{j\left((a-\widehat{a})\pi(i)+b-\widehat{b}\right)}\\ &\quad + \frac{1}{Q^2}\xi_Q^{(u-\widehat{u})\sigma(i')}\sum_{j=0}^{Q-1}1\\ &= \frac{1}{Q}\xi_Q^{(u-\widehat{u})\sigma(i')},\end{aligned}$$

where the last equality is derived from the fact that $\sum_{j=0}^{Q-1}\xi_Q^{\ell j} = 0$ for any $\ell \not\equiv 0 \pmod{Q}$. Therefore, we obtain $\left|\mathbf{c}_1\mathbf{c}_2^H\right| \in \{0, \frac{1}{Q}\}$.

TABLE 2. The parameters of the (N, K) codebook in Theorem 1.

$p_{\min}$	N	K	$I_{\max}$	I_W	$\frac{I_W}{I_{\max}}$
5	7350	1225	0.02857	0.02608	0.91293
13	683774	48841	0.45249×10^{-2}	0.43603×10^{-2}	0.96362
17	4374882	243049	0.20284×10^{-2}	0.19712×10^{-2}	0.97183
31	114428192	3575881	0.52882×10^{-3}	0.52049×10^{-3}	0.98425
43	410115596	9320809	0.32755×10^{-3}	0.32380×10^{-3}	0.98857
61	1229410598	19829209	0.22345×10^{-3}	0.22275×10^{-2}	0.99190
73	3123614666	42211009	0.15392×10^{-3}	0.15287×10^{-3}	0.99322
83	4583692596	54567796	0.13537×10^{-3}	0.13456×10^{-3}	0.99403
97	11774065058	120143521	0.91230×10^{-4}	0.90766×10^{-4}	0.99488

The analysis above shows that $I_{\max}(\mathcal{C}) = \frac{1}{Q}$. This completes the proof of this theorem. □

The next theorem deals with the asymptotical optimality of the codebooks defined in Theorem 1.

Theorem 2: Let symbols be the same as before. Then the maximum inner-product correction $I_{\max}(\mathcal{C})$ of the codebook $\mathcal{C}$ defined in (1) *asymptotically meets the Welch bound.*

Proof: From Theorem 1, we know $\mathcal{C}$ is a $\left((p_{\min}+1)Q^2, Q^2\right)$ codebook. Note that the corresponding Welch bound of $\mathcal{C}$ is

$$I_W = \sqrt{\frac{p_{\min}}{p_{\min}Q^2+Q^2-1}}.$$

Then we obtain

$$\begin{aligned}\frac{I_{\max}(\mathcal{C})}{I_W} &= \sqrt{\frac{p_{\min}Q^2+Q^2-1}{Q^2p_{\min}}}\\ &= \sqrt{1+\frac{1}{p_{\min}}-\frac{1}{Q^2p_{\min}}}.\end{aligned}$$

Observe that

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

which implies that the codebook $\mathcal{C}$ asymptotically meets the Welch bound. □

In Table 2, we list some examples of codebooks generated by Theorem 1. The numerical results indicate that the codebooks defined in Theorem 1 asymptotically achieve the Welch bound as $p_{\min}$ increases, as predicted in Theorem 2.

IV. THE SECOND CONSTRUCTION OF ASYMPTOTICALLY OPTIMAL CODEBOOKS

In this section, we propose a construction of codebooks by slightly modifying the construction of codebooks in Section III. In addition, we show that these codebooks are asymptotically optimal with respect to the Welch bound.

Let $Q > 1$ be an integer and $p_{\min}$ the smallest prime factor of Q. Assume that $\mathcal{E}_{Q(Q-1)}$ is a set consisted of all rows of the identity matrix $I_{Q(Q-1)}$. That is to say, $\mathcal{E}_{Q(Q-1)}$ is the standard basis of the Hilbert space with dimension $Q(Q-1)$. Let $\pi(x)$ and $\sigma(x)$ be permutations on $\mathbb{Z}_Q$. For any $\ell \in \mathbb{Z}_Q$, we define a set by

$$\mathcal{F} = \left\{\mathbf{c}_{a,b,u} : a \in \mathbb{Z}_{p_{min}}, b, u \in \mathbb{Z}_Q\right\}, \tag{2}$$

where

$$\mathbf{c}_{a,b,u} = \frac{1}{\sqrt{Q(Q-1)}} \left(\xi_Q^{j(a\pi(i)+b)+u\sigma(i)}\right)_{i\in\mathbb{Z}_Q\setminus\{\ell\}, j\in\mathbb{Z}_Q}.$$

Let

$$\mathcal{C} = \mathcal{F} \bigcup \mathcal{E}_{Q(Q-1)}. \tag{3}$$

Then parameters of $\mathcal{C}$ and the the maximum inner-product correction $I_{\max}(\mathcal{C})$ of $\mathcal{C}$ can be obtained in the following theorem.

Theorem 3: Assume that $Q > 1$ is an integer and p_{min} is the smallest prime factor of Q. Then $\mathcal{C}$ defined by (3) is a $\left(p_{\min}Q^2 + Q^2 - Q, Q(Q-1)\right)$ codebook with $I_{\max}(\mathcal{C}) = \frac{1}{\sqrt{Q(Q-1)}}$.

Proof: Let $\mathbf{c}_1, \mathbf{c}_2$ be two distinct codewords in $\mathcal{C}$. Now we calculate the correlation of $\mathbf{c}_1$ and $\mathbf{c}_2$ by distinguishing among the following cases.

(1) If $\mathbf{c}_1, \mathbf{c}_2 \in \mathcal{E}_{Q(Q-1)}$, it is obvious that $\left|\mathbf{c}_1\mathbf{c}_2^H\right| = 0$.

(2) If $\mathbf{c}_1 \in \mathcal{E}_{Q(Q-1)}$ and $\mathbf{c}_2 \in \mathcal{F}$, we have

$$\left|\mathbf{c}_1\mathbf{c}_2^H\right| = \frac{1}{\sqrt{Q(Q-1)}}.$$

(3) If $\mathbf{c}_1, \mathbf{c}_2 \in \mathcal{F}$, we assume that $\mathbf{c}_1 = \mathbf{c}_{a,b,u}$ and $\mathbf{c}_2 = \mathbf{c}_{\widehat{a},\widehat{b},\widehat{u}}$, where $(a-\widehat{a}, b-\widehat{b}, u-\widehat{u}) \neq (0,0,0)$. Then we have

$$\begin{aligned} &Q(Q-1)\mathbf{c}_1\mathbf{c}_2^H \\ &= \sum_{i=0,i\neq\ell}^{Q-1}\sum_{j=0}^{Q-1} \xi_Q^{j(a\pi(i)+b)+u\sigma(i)-j(\widehat{a}\pi(i)+\widehat{b})-\widehat{u}\sigma(i)} \\ &= \sum_{i=0,i\neq\ell}^{Q-1} \xi_Q^{(u-\widehat{u})\sigma(i)} \sum_{j=0}^{Q-1} \xi_Q^{j((a-\widehat{a})\pi(i)+b-\widehat{b})}. \end{aligned}$$

If $a-\widehat{a}=0$ and $b-\widehat{b}\neq 0$, we obtain

$$\begin{aligned} \mathbf{c}_1\mathbf{c}_2^H &= \frac{1}{Q(Q-1)} \sum_{i=0,i\neq\ell}^{Q-1} \xi_Q^{(u-\widehat{u})\sigma(i)} \sum_{j=0}^{Q-1} \xi_Q^{j(b-\widehat{b})} \\ &= 0. \end{aligned}$$

If $a-\widehat{a}=0$ and $b-\widehat{b}=0$, it follows from the fact that $u-\widehat{u}\not\equiv 0 \pmod{Q}$ that

$$\begin{aligned} \mathbf{c}_1\mathbf{c}_2^H &= \frac{1}{Q(Q-1)} \sum_{i=0,i\neq\ell}^{Q-1} \xi_Q^{(u-\widehat{u})\sigma(i)} \sum_{j=0}^{Q-1} 1 \\ &= \frac{1}{Q-1} \sum_{i=0}^{Q-1} \xi_Q^{(u-\widehat{u})\sigma(i)} - \frac{1}{Q-1}\xi_Q^{(u-\widehat{u})\sigma(\ell)} \\ &= -\frac{1}{Q-1}\xi_Q^{(u-\widehat{u})\sigma(\ell)}. \end{aligned}$$

TABLE 3. The parameters of the (N, K) codebook in Theorem 3.

$p_{\min}$	N	K	$I_{\max}$	I_W	$\frac{I_W}{I_{\max}}$
7	47355	5852	0.013072	0.01224	0.93618
19	3818943	190532	0.22906×10^{-2}	0.22331×10^{-2}	0.97474
29	34538797	1150256	0.93240×10^{-3}	0.91674×10^{-3}	0.98321
41	198318845	4719756	0.46023×10^{-3}	0.45479×10^{-3}	0.98803
59	777164461	12949202	0.27789×10^{-3}	0.27557×10^{-3}	0.99163
67	1538770575	22624292	0.21024×10^{-3}	0.20869×10^{-2}	0.99262
79	3439533363	42987692	0.15252×10^{-3}	0.15156×10^{-3}	0.99373
89	6707573377	74520056	0.11584×10^{-3}	0.11520×10^{-3}	0.99443
101	12362193253	121187072	0.90839×10^{-4}	0.90393×10^{-4}	0.99509

If $a-\widehat{a}\neq 0$, then $\gcd(a-\widehat{a}, Q) = 1$. According to Lemma 1, the congruence $(a-\widehat{a})\pi(x)+b-\widehat{b}\equiv 0 \pmod{Q}$ has only one integer solution i' in $\mathbb{Z}_Q$.

When $i'\neq\ell$, we can deduce that

$$\begin{aligned} \mathbf{c}_1\mathbf{c}_2^H &= \frac{1}{Q(Q-1)} \sum_{i=0,i\neq\ell}^{Q-1} \xi_Q^{(u-\widehat{u})\sigma(i)} \sum_{j=0}^{Q-1} \xi_Q^{j((a-\widehat{a})\pi(i)+b-\widehat{b})} \\ &= \frac{1}{Q(Q-1)} \sum_{i=0,i\neq i',\ell}^{Q-1} \xi_Q^{(u-\widehat{u})\sigma(i)} \sum_{j=0}^{Q-1} \xi_Q^{j((a-\widehat{a})\pi(i)+b-\widehat{b})} \\ &\quad + \frac{1}{Q(Q-1)}\xi_Q^{(u-\widehat{u})\sigma(i')} \sum_{j=0}^{Q-1} 1 \\ &= \frac{1}{Q-1}\xi_Q^{(u-\widehat{u})\sigma(i')}. \end{aligned}$$

When $i'=\ell$, we have

$$\begin{aligned} \mathbf{c}_1\mathbf{c}_2^H &= \frac{1}{Q(Q-1)} \sum_{i=0,i\neq\ell}^{Q-1} \xi_Q^{(u-\widehat{u})\sigma(i)} \sum_{j=0}^{Q-1} \xi_Q^{j((a-\widehat{a})\pi(i)+b-\widehat{b})} \\ &= 0. \end{aligned}$$

Hence, we get that

$$\left|\mathbf{c}_1\mathbf{c}_2^H\right| \in \left\{0, \frac{1}{Q-1}\right\}.$$

Summarizing the conclusions in the three cases above, we obtain

$$I_{\max}(\mathcal{C}) = \frac{1}{Q-1}.$$

This completes the proof. □

Theorem 4: Let symbols be the same as before. If $Q > 2$, then the codebook $\mathcal{C}$ is asymptotically optimal with respect to the Welch bound.

Proof: For $N = p_{\min}Q^2 + Q^2 - Q$ and $K = Q(Q-1)$, by Lemma 2 we have

$$I_W = \sqrt{\frac{p_{\min}Q}{(p_{\min}Q^2 + Q^2 - Q - 1)(Q-1)}}.$$

Hence,

$$\frac{I_{\max}(\mathcal{C})}{I_W} = \sqrt{\frac{p_{\min}Q^2 + Q^2 - Q - 1}{Q(Q-1)p_{\min}}} = \sqrt{\frac{Q}{Q-1} + \frac{Q^2 - Q - 1}{Q(Q-1)p_{\min}}}.$$

Consequently,

$$\lim_{p_{\min}\to+\infty} \frac{I_{\max}(\mathcal{C})}{I_W} = 1.$$

This completes the proof of this theorem. □

Table 3 presents some parameters of codebooks derived from Theorem 3. From Table 3, we can see that I_W is very close to $I_{\max}(\mathcal{C})$ as $p_{\min}$ increases. This means that the codebooks defined in Theorem 3 are asymptotically optimal with respect to the Welch bound for large $p_{\min}$, as predicted in Theorem 4.

V. CONCLUDING REMARKS

Employing generalised bent functions, we presented two classes of codebooks and proved that these constructed codebooks nearly meet the Welch bound. As a comparison, the parameters of some known classes of asymptotically optimal codebooks with respect to the Welch bound and the new ones are listed in Table 1. Obviously, the parameters of our classes of codebooks have not been covered in the literature.

REFERENCES

[1] 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, Jan. 1996.

[2] X. Cao, W. Chou, and X. Zhang, "More constructions of near optimal codebooks associated with binary sequences," *Adv. Math. Commun.*, vol. 11, no. 1, pp. 187–202, 2017.

[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] M. Fickus and D. Mixon, "Tables of the existence of equiangular tight frames," 2016, *arXiv:1504.00253*. [Online]. Available: https://arxiv.org/abs/1504.00253

[6] 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.

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

[8] S. Hong, H. Park, J.-S. No, T. Helleseth, and Y.-S. Kim, "Near-optimal partial Hadamard codebook construction using binary sequences obtained from quadratic residue mapping," *IEEE Trans. Inf. Theory*, vol. 60, no. 6, pp. 3698–3705, Jun. 2014.

[9] Z. Heng, C. Ding, and Q. Yue, "New constructions of asymptotically optimal codebooks with multiplicative characters," *IEEE Trans. Inf. Theory*, vol. 63, no. 10, pp. 6179–6187, Oct. 2017.

[10] Z. Heng, "Nearly optimal codebooks based on generalized Jacobi sums," *Discrete Appl. Math.*, vol. 250, pp. 227–240, Dec. 2018.

[11] M. G. Karpovsky, K. J. Kulikowski, and Z. Wang, "On-line self error detection with equal protection against all errors," *Int. J. High. Reliab. Electron. Syst. Des.*, pp. 124–130, Dec. 2008.

[12] P. V. Kumar, R. A. Scholtz, and L. R. Welch, "Generalized bent functions and their properties," *J. Combinat. Theory A*, vol. 40, no. 1, pp. 90–107, 1985.

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

[14] G. Luo and X. Cao, "Two constructions of asymptotically optimal codebooks via the hyper eisenstein sum," *IEEE Trans. Inf. Theory*, vol. 64, no. 10, pp. 6498–6505, Oct. 2018.

[15] G. Luo and X. Cao, "New constructions of codebooks asymptotically achieving the welch bound," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Vail, CO, USA, Jun. 2018, pp. 2346–2349.

[16] G. Luo and X. Cao, "Two constructions of asymptotically optimal codebooks," *Cryptogr. Commun.*, vol. 11, no. 4, pp. 825–838, Jul. 2019.

[17] F. J. MacWilliams, N. J. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North Holland, 1977.

[18] F. Rahimi, "Covering graphs and equiangular tight frames," M.S. thesis, Univ. Waterloo, Waterloo, ON, Canada, 2016.

[19] D. Sarwate, "Meeting the Welch bound with equality," in *Sequences and their Applications*. London, U.K.: Springer, 1999, pp. 79–102.

[20] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, pp. 379–423, Jul. 1948.

[21] S. Mesnager, *Bent Functions: Fundamentals and Results*. Cham, Switzerland: Springer, 2016.

[22] J. H. Silverman, *A Friendly Introduction to Number Theory*. Upper Saddle River, NJ, USA: Prentice-Hall, 2006.

[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] L. Tian, Y. Li, T. Liu, and C. Xu, "Constructions of codebooks asymptotically achieving the welch bound with additive characters," *IEEE Signal Process. Lett.*, vol. 26, no. 4, pp. 622–626, Apr. 2019.

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

[26] 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.

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

[28] 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.

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

QIUYAN WANG received the B.Sc. degree in mathematics from Capital Normal University, Beijing, China, in 2012, and the Ph.D. degree from the University of Chinese Academy of Sciences, in 2016. She is currently a Lecturer with the School of Computer Sciences and Technology, Tiangong University. Her research interests include coding theory and cryptography.

YANG YAN received the B.Sc. degree in computer science and technology from Shandong Normal University, Jinan, China, in 2012, and the Ph.D. degree from the University of Chinese Academy of Sciences, in 2018. He is currently a Lecturer with the School of Information Technology Engineering, Tianjin University of Technology and Education. His research interests include social networks, data mining, coding theory, and cryptography.