mathematics

MDPI

Article

Four Constructions of Asymptotically Optimal Codebooks via Additive Characters and Multiplicative Characters

Xia Wu and Wei Lu *

School of Mathematics, Southeast University, Nanjing 210096, China; wuxia80@seu.edu.cn
* Correspondence: luwei1010@seu.edu.cn

Received: 23 September 2019; Accepted: 19 November 2019; Published: 23 November 2019

Abstract: In this paper, we present four new constructions of complex codebooks with multiplicative characters, additive characters, and quadratic irreducible polynomials and determine the maximal cross-correlation amplitude of these codebooks. We prove that the codebooks we constructed are asymptotically optimal with respect to the Welch bound. Moreover, we generalize the result obtained by Zhang and Feng and contain theirs as a special case. The parameters of these codebooks are new.

Keywords: codebook; asymptotic optimality; Welch bound; Gauss sum; Jacobi sum

---

1. Introduction

An (N, K) codebook $\mathcal{C} = \{\mathbf{c}_0, \mathbf{c}_1, \ldots, \mathbf{c}_{N-1}\}$ 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 magnitude of inner products between a pair of distinct vectors in $\mathcal{C}$ 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 [1] 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 [2] or an equiangular tight frame [3]. MWBE codebooks are employed in various applications including code division multiple access (CDMA) communication systems [4], communications [2], combinatorial designs [5–7], packing [8], compressed sensing [9], coding theory [10–12], and quantum computing [13]. To our knowledge, only the following MWBE codebooks have been presented as follows:

- (N, N) orthogonal MWBE codebooks for any $N > 1$ [2,7];

- $(N, N-1)$ MWBE codebooks for $N > 1$ based on discrete Fourier transformation matrices [2,7] or m-sequences [2];
- (N, K) MWBE codebooks from conference matrices [8,14], where $N = 2K = 2^{d+1}$ for a positive integer d or $N = 2K = p^d + 1$ for a prime p and a positive integer d;
- (N, K) MWBE codebooks based on (N, K, λ) difference sets in cyclic groups [7] and abelian groups [5,6];
- (N, K) MWBE codebooks from $(2, k, \nu)$-Steiner systems [15];
- (N, K) MWBE codebooks dependent on graph theory and finite geometries [16–19].

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 research works have been done instead to construct near optimal codebooks, i.e., codebook $\mathcal{C}$ whose $I_{max}(\mathcal{C})$ nearly achieves the Welch bound. In [2], Sarwate gave some nearly optimal codebooks from codes and signal sets. As an extension of the optimal codebooks based on difference sets, various types of near optimal codebooks based on almost difference sets, relative difference sets, and cyclotomic classes have been proposed; see [5,20–23]. Near optimal codebooks constructed from binary row selection sequences were presented in [24,25]. In [26–30], some near optimal codebooks were constructed via Jacobi sums and a hyper Eisenstein sum.

In [31], Mohades and Tadaion 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 use additive characters and multiplicative characters to construct four new codebooks, and we determine the maximal cross-correlation amplitude of these codebooks by the properties of characters and character sums. Moreover, we generalize the result in [21] and contain the result in [21] as a special case. All of these codebooks we constructed are new and near optimal according to the Welch bound. As a comparison, in Table 1, we list the parameters of some known classes of near optimal codebooks and the parameters of ours.

This paper is organized as follows. In Section 2, we recall some notations and basic results that will be needed in our discussion. In Section 3, we present our four constructions of near optimal codebooks. In Section 4, we give the conclusion.

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

Parameters (N,K)	I_{max}	I_{Welch}	References
(p^n, K) with odd p, where $K=\frac{p-1}{2p}(p^n+p^{n/2})+1$	$\frac{(p+1)p^{n/2}}{2pK}$	$\sqrt{\frac{p^n-K}{(p^n-1)K}}$	[24]
$(q^2, \frac{(q-1)^2}{2}), q=p^s$ with odd p	$\frac{q+1}{(q-1)^2}$	$(q-1)\sqrt{\frac{q^2+2q-1}{q^2-1}}$	[21]
$q(q+4), \frac{(q+3)(q+1)}{2}$, q is a prime power	$\frac{1}{q+1}$	$\sqrt{\frac{q^2+4q-3}{(q^2+4q-1)(q+3)(q+1)}}$	[32]
$q, \frac{q-1}{2}$, q is a prime power	$\frac{\sqrt{q}+1}{q-1}$	$\frac{\sqrt{q+1}}{q-1}$	[32]
$(p^n-1, \frac{p^n-1}{2})$ with odd p	$\frac{\sqrt{p^n}+1}{p^n-1}$	$\frac{1}{\sqrt{p^n-1}}$	[25]
$(q^l+q^{l-1}-1, q^{l-1})$ for any $l>2$	$\frac{1}{\sqrt{q^{l-1}}}$	$\sqrt{\frac{q^l-1}{(q^l+q^{l-1}-1)q^{l-1}}}$	[23]
$((q-1)^k+q^{k-1}, q^{k-1})$, for any $k>2$ and $q\geq 4$	$\frac{\sqrt{q^{k+1}}}{(q-1)^k+(-1)^{k+1}}$	$\sqrt{\frac{(q-1)^k}{((q-1)^k+q^{k-1}-1)q^{k-1}}}$	[26]
$((q-1)^k+K, K)$, for any $k>2$, where $K=\frac{(q-1)^k+(-1)^{k+1}}{q}$	$\frac{\sqrt{q^{k-1}}}{K}$	$\sqrt{\frac{(q-1)^k}{((q-1)^k+K-1)K}}$	[26]
$((q^s-1)^n+K, K)$, for any $s>1$ and $n>1$, where $K=\frac{(q^s-1)^n+(-1)^{n+1}}{q}$	$\frac{\sqrt{q^{sn+1}}}{(q^s-1)^n+(-1)^{n+1}}$	$\sqrt{\frac{(q^s-1)^n}{((q^s-1)^n+K-1)K}}$	[28]
$((q^s-1)^n+q^{sn-1}, q^{sn-1})$, for any $s>1$ and $n>1$	$\frac{\sqrt{q^{sn+1}}}{(q^s-1)^n+(-1)^{n+1}}$	$\sqrt{\frac{(q^s-1)^n}{((q^s-1)^n+q^{sn-1}-1)q^{sn-1}}}$	[28]
$(q-1, \frac{q(r-1)}{2r}), r=p^t, q=r^s$, with odd p and ps	$\frac{\sqrt{r}}{\sqrt{q}(\sqrt{r}-1)}$	$\sqrt{\frac{qr-2r+q}{q(q-2)(r-1)}}$	[33]
$(q^2, \frac{q(q+1)(r-1)}{2r}), r=p^t, q=r^s$, with odd p	$\frac{(r+1)q}{2rK}$	$\sqrt{\frac{2rq-(q+1)(r-1)}{(q+1)^2(q-1)(r-1)}}$	[33]
$((q-1)q^2, (q-1)q)$, q is a prime power	$\frac{1}{q-1}$	$\sqrt{\frac{q-1}{q^3-q^2-1}}$	[34]
$(q-1, \frac{q-1}{m}-1), q=p^t$ with odd p, $m \mid q-1$	$\leq \frac{(m-1)\sqrt{q}+1}{q-1-m}$	$\sqrt{\frac{(m-1)q+1}{(q-2)(q-1-m)}}$	this paper
$(q, \frac{q-1}{m}), q=p^t$ with odd p, $m \mid q-1$	$\leq \frac{(m-1)\sqrt{q}+1}{q-1}$	$\frac{\sqrt{(m-1)q+1}}{q-1}$	this paper
$(q_1q_2, \frac{(q_1-1)(q_2-1)}{m}), q_i=p_i^t$ with odd p_i, $m \mid q_i-1, i=1,2$	$\leq \frac{(m-1)\sqrt{q_1q_2}+1}{(q_1-1)(q_2-1)}$	$\sqrt{\frac{(m-1)q_1q_2+q_1+q_2-1}{(q_1q_2-1)(q_1-1)(q_2-1)}}$	this paper
$(q-1, \frac{q-1}{2}), q=p^t$ with odd p	$\leq \frac{2\sqrt{q}}{q-1}$	$\frac{1}{\sqrt{q-2}}$	this paper
$(q-1, \frac{q-3}{2}), q=p^t$ with odd p	$\leq \frac{2\sqrt{q}}{q-3}$	$\sqrt{\frac{q+3}{(q-2)(q-3)}}$	this paper

2. Preliminaries

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

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

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 $\lambda_a(x)=\zeta_p^{\mathrm{Tr}_{q/p}(ax)}$, where ζ_p is a primitive $p-$th root of complex unity and $\mathrm{Tr}_{q/p}(\cdot)$ is the trace functions from $\mathbb{F}_q$ to $\mathbb{F}_p$. By the definition, $\lambda_a(x) = \lambda_1(ax)$. When $a = 0$, we call λ_0 the trivial additive character of $\mathbb{F}_q$. When $a = 1$, we call λ_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 [35]) is given by:

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

As in [35], the multiplicative characters of $\mathbb{F}_q$ are defined as follows. For $j = 0, 1, \ldots, q-2$, 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 $x \in \mathbb{F}_q^*$, and 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 [35]) is given by:

$$\sum_{x\in\mathbb{F}_q^*} \varphi(x) = \begin{cases} q-1, & \text{if } \varphi = \varphi_0, \\ 0, & \text{otherwise.} \end{cases}$$

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 that 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 1. *([35], 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:*

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

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

2.2.2. Jacobi Sum

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

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

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. *([35], 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 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

There are two steps in the construction of the codebooks. In the first step, we need a set D, which determines the length of the vectors. In the second step, we choose a set of functions from D for the unit circle, which determine the number of vectors.

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

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

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

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

3. Four Constructions of Near Optimal Codebooks

In this section, by multiplicative characters, additive characters, Gauss sums, and Jacobi sums, we construct four new series of codebooks.

3.1. The First Construction of Codebooks

In this section, we propose a construction of codebooks by the group of multiplicative characters of $\mathbb{F}_q$ and a set D_1 derived by the multiplicative character of order m. The construction was inspired by [21], and we generalized the quadratic multiplicative character of a finite field to the multiplicative character of order m.

Let $q = p^t$, where p is an odd prime number and $t \geq 1$ is a positive integer. Let φ be the multiplicative character of order m of $\mathbb{F}_q$, where $m|q-1$. Let:

$$D_1 := \{x \in \mathbb{F}_q^* \mid \varphi(x+1) = 1\},$$

Then, $K = \#D_1 = \frac{q-1}{m} - 1$.

A codeword of length K is defined as:

$$\mathbf{c}_\chi = \frac{1}{\sqrt{K}}(\chi(x))_{x \in D_1},$$

where $\chi \in \widehat{\mathbb{F}_q^*}$.

Then, we construct the following (N, K) codebook $\mathcal{C}(D_1)$ as:

$$\mathcal{C}(D_1) = \{\frac{1}{\sqrt{K}}(\chi(x))_{x \in D_1} \mid \chi \in \widehat{\mathbb{F}_q^*}\}.$$

It is easy to see that $N = q - 1$.

We set:

$$\delta_1(x) = \begin{cases} \frac{1+\varphi(x+1)+\ldots+\varphi^{m-1}(x+1)}{m}, & \text{if } x \in \mathbb{F}_q^* \text{ and } x \neq -1, \\ 0, & \text{if } x = -1; \end{cases}$$

through the definition of D_1, we known that:

$$\delta_1(x) = \begin{cases} 1, & \text{if } x \in D_1, \\ 0, & \text{otherwise.} \end{cases}$$

Lemma 3. *With the above notation, we have:*

$$I_{max}(\mathcal{C}(D_1)) \leq \frac{(m-1)\sqrt{q}+1}{q-1-m}.$$

Proof. For any characters χ_i and χ_j in $\widehat{\mathbb{F}_q^*}$, where $1 \leq i \neq j \leq q-1$, we have:

$$\begin{aligned}
& K(\mathbf{c}_{\chi_i}\mathbf{c}_{\chi_j}^H) \\
= \ & K\frac{1}{\sqrt{K}}(\chi_i(x))_{x\in D_1}\frac{1}{\sqrt{K}}(\chi_j(x))_{x\in D_1}^H \\
= \ & \textstyle\sum_{x\in D_1}\chi_i(x)\overline{\chi_j(x)} = \sum_{x\in D_1}\chi(x), \ \ (\text{where } \chi = \chi_i\overline{\chi_j}) \\
= \ & \textstyle\sum_{x\in\mathbb{F}_q^*}\chi(x)\delta_1(x) \\
= \ & \textstyle\sum_{x\in\mathbb{F}_q^*, x\neq -1}\chi(x)\frac{1+\varphi(x+1)+\ldots+\varphi^{m-1}(x+1)}{m} \\
= \ & \textstyle\frac{1}{m}[\sum_{x\in\mathbb{F}_q^*}\chi(x)+\sum_{x\in\mathbb{F}_q^*}\chi(x)\varphi(x+1)\ldots+\sum_{x\in\mathbb{F}_q^*}\chi(x)\varphi^{m-1}(x+1)] - \frac{1}{m}\chi(-1) \\
= \ & \textstyle\frac{1}{m}[\sum_{x\in\mathbb{F}_q^*}\chi(x)+\sum_{x\in\mathbb{F}_q^*}\chi(-x)\varphi(-x+1)+\ldots+\sum_{x\in\mathbb{F}_q^*}\chi(-x)\varphi^{m-1}(-x+1)] - \frac{1}{m}\chi(-1) \\
= \ & \textstyle\frac{1}{m}\chi(-1)[\sum_{x\in\mathbb{F}_q^*}\chi(x)+\sum_{x\in\mathbb{F}_q^*}\chi(x)\varphi(1-x)+\ldots+\sum_{x\in\mathbb{F}_q^*}\chi(x)\varphi^{m-1}(1-x)] - \frac{1}{m}\chi(-1) \\
= \ & \textstyle\frac{1}{m}\chi(-1)[J(\chi,\varphi)+\ldots+J(\chi,\varphi^{m-1})-1],
\end{aligned}$$

the equations hold since $\sum_{x\in\mathbb{F}_q^*}\chi(x) = 0$, where χ is a nontrivial character as $\chi_i \neq \chi_j$. By the results in Lemma 2, we get $|J(\chi,\varphi^i)| = \sqrt{q}$, $1 \leq i \leq m-1$, so $|[J(\chi,\varphi)+\ldots+J(\chi,\varphi^{m-1})-1]| \leq (m-1)\sqrt{q}+1$. It follows that:

$$\begin{aligned}
I_{max}(\mathcal{C}(D_1)) &= max\{|\mathbf{c}_{\chi_i}\mathbf{c}_{\chi_j}^H| : 1 \leq i \neq j \leq q-1\} \\
&\leq \tfrac{(m-1)\sqrt{q}+1}{q-1-m}.
\end{aligned}$$

□

Remark 1. (1) *Since $N = q-1$ and $K = \frac{q-1}{m} - 1$ in this construction, the corresponding Welch bound is:*

$$I_{Welch} = \sqrt{\frac{N-K}{(N-1)K}} = \sqrt{\frac{(m-1)q+1}{(q-2)(q-1-m)}}.$$

Thus,

$$I_{max}(\mathcal{C}(D_1)) - I_{Welch} \to 0,$$

and:

$$1 \leq \frac{I_{max}(\mathcal{C}(D_1))}{I_{Welch}} \leq \sqrt{m-1},$$

as $q \to \infty$.

(2) *When $m = 2$, we get $\frac{I_{max}(\mathcal{C}(D_1))}{I_{Welch}} = 1$, when $q \to \infty$, which is similar to the first construction in [21].*

3.2. The Second Construction of Codebooks

In this section, we propose a construction of codebooks by the group of additive characters and a set D_2 derived by the multiplicative character of order m. In the first construction, we use the multiplicative characters, which lead to the Jacobi sums. In this section, we use the additive characters, which will lead to Gauss sums.

Let $q = p^t$, where p is an odd prime number and $t \geq 1$ is a positive integer. Let φ be the multiplicative character of order m of $\mathbb{F}_q$, where $m|q-1$. Let:

$$D_2 := \{x \in \mathbb{F}_q^* \mid \varphi(x) = 1\}.$$

Then, $K = \#D_2 = \frac{q-1}{m}$.

A codeword of length K is defined as:

$$\mathbf{c}_\lambda = \frac{1}{\sqrt{K}}(\lambda(x))_{x \in D_2}.$$

where $\lambda \in \widehat{\mathbb{F}_q}$.

Then, we construct the following (N, K) codebook $\mathcal{C}(D_2)$ as:

$$\mathcal{C}(D_2) = \{\frac{1}{\sqrt{K}}(\lambda(x))_{x \in D_2} \mid \lambda \in \widehat{\mathbb{F}_q}\}.$$

It is easy to see that $N = q$.

Let:

$$\delta_2(x) = \frac{1 + \varphi(x) + \ldots + \varphi^{m-1}(x)}{m},\ x \in \mathbb{F}_q^*$$

Through the definition of D_2, we known that:

$$\delta_2(x) = \begin{cases} 1, & \text{if } x \in D_2, \\ 0, & \text{otherwise.} \end{cases}$$

Theorem 1. *With the above notation, we have:*

$$I_{max}(\mathcal{C}(D_2)) \leq \frac{(m-1)\sqrt{q}+1}{q-1}.$$

Proof. For any characters λ_i and λ_j in $\widehat{\mathbb{F}_q}$, where $0 \leq i \neq j \leq q-1$, we have:

$$\begin{array}{rl} & K(\mathbf{c}_{\lambda_i}\mathbf{c}_{\lambda_j}^H) \\ = & \sum_{x \in D_2} \lambda_i(x)\overline{\lambda_j(x)} = \sum_{x \in D_2} \lambda(x), \\ & (\text{where } \lambda = \lambda_i\overline{\lambda_j}) \\ = & \sum_{x \in \mathbb{F}_q^*} \lambda(x)\delta_2(x) \\ = & \sum_{x \in \mathbb{F}_q^*} \lambda(x)\frac{1+\varphi(x)+\ldots+\varphi^{m-1}(x)}{m} \\ = & \frac{1}{m}[\sum_{x \in \mathbb{F}_q^*} \lambda(x) + \sum_{x \in \mathbb{F}_q^*} \lambda(x)\varphi(x) \ldots + \sum_{x \in \mathbb{F}_q^*} \lambda(x)\varphi^{m-1}(x)] \\ = & \frac{1}{m}[-1 + G(\varphi, \lambda) + \ldots + G(\varphi, \lambda^{m-1})], \end{array}$$

and the last equation holds since $\sum_{x \in \mathbb{F}_q^*} \lambda(x) = -1$, where λ is a nontrivial character as $\lambda_i \neq \lambda_j$.

By the results in Lemma 1, we get $|G(\varphi, \lambda^i)| = \sqrt{q}$, $1 \leq i \leq m-1$, then:

$$\begin{array}{rcl} I_{max}(\mathcal{C}(D_2)) & = & max\{|\mathbf{c}_{\lambda_i}\mathbf{c}_{\lambda_j}^H| : 0 \leq i \neq j \leq q-1\} \\ & \leq & \frac{(m-1)\sqrt{q}+1}{q-1}. \end{array}$$

□

Remark 2. (1) *Since* $N = q$ *and* $K = \frac{q-1}{m}$ *in this construction, the corresponding Welch bound is:*

$$I_{Welch} = \sqrt{\frac{N-K}{(N-1)K}} = \frac{\sqrt{(m-1)q+1}}{q-1}.$$

Thus,

$$I_{max}(\mathcal{C}(D_2)) - I_{Welch} \to 0,$$

and:

$$1 \le \frac{I_{max}(\mathcal{C}(D_2))}{I_{Welch}} \le \sqrt{m-1},$$

as $q \to \infty$.

(2) *When* $m = 2$, *we get* $\frac{I_{max}(\mathcal{C}(D_2))}{I_{Welch}} = 1$ *when* $q \to \infty$.

3.3. The Third Construction of Codebooks

In this section, we propose a construction of codebooks by the group of additive characters of $\mathbb{F}_{q_1} \oplus \mathbb{F}_{q_2}$ and a set D_3 derived by the multiplicative characters of order m. We generalized the quadratic multiplicative character of a finite field in [21] to the multiplicative character of order m, and we contain the second construction in [21] as a special case. The third construction seems very close to [27,29]; however, the set D in our construction is defined by multiplicative characters, and the sets in their construction are defined by trace functions.

Let $q_1 = p_1^{t_1}$, $q_2 = p_2^{t_2}$, where p_1, p_2 are odd primes and $t_1, t_2 \ge 1$ are positive integers. Let $R = \mathbb{F}_{q_1} \oplus \mathbb{F}_{q_2}$, $R^* = \mathbb{F}_{q_1}^* \oplus \mathbb{F}_{q_2}^*$. Let φ_1 and φ_2 be the multiplicative character of order m of $\mathbb{F}_{q_1}$ and $\mathbb{F}_{q_2}$, respectively, where $m|(q_1-1, q_2-1)$. The character group of the additive group $R = \mathbb{F}_{q_1} \oplus \mathbb{F}_{q_2}$ is:

$$\widehat{R} = \{\lambda_b : b = (b_1, b_2) \in R\},$$

where $\lambda_b(x) = \lambda_{b_1}(x_1)\lambda_{b_2}(x_2)$, for $x = (x_1, x_2) \in R$.

We set:

$$D_3 = \{x = (x_1, x_2) \in R^* \mid \varphi_1(x_1)\varphi_2(x_2) = 1\}.$$

Then, $K = \#D_3 = \frac{(q_1-1)(q_2-1)}{m}$.

A codeword of length K is defined as:

$$\mathbf{c}_b = \frac{1}{\sqrt{K}}(\lambda_b(x))_{x \in D_3}.$$

where $b \in R$.

Then, we construct the following (N, K) codebook $\mathcal{C}(D_3)$ as:

$$\mathcal{C}(D_3) = \{\mathbf{c}_b = \frac{1}{\sqrt{K}}(\lambda_b(x))_{x \in D_3} \mid b \in R\}.$$

It is easy to see that $N = q_1 q_2$.

We set:

$$\delta_3(x) = \frac{1 + \varphi_1(x_1)\varphi_2(x_2) + \ldots + \varphi_1^{m-1}(x_1)\varphi_2^{m-1}(x_2)}{m},$$

where $x \in R^*$ through the definition of D_3, we known that:

$$\delta_3(x) = \begin{cases} 1, & \text{if } x \in D_3, \\ 0, & \text{otherwise.} \end{cases}$$

Theorem 2. *With the above notation, we have:*

$$I_{max}(\mathcal{C}(D_3)) \leq \frac{(m-1)\sqrt{q_1q_2}+1}{m}.$$

Proof. For any characters λ_i and λ_j in $\widehat{R}$, where $\lambda_i \neq \lambda_j$, we have:

$$\begin{aligned}
& K(\mathbf{c}_{\lambda_i}\mathbf{c}_{\lambda_j}^H) \\
= & \sum_{x\in D_3}\lambda_i(x)\overline{\lambda_j(x)} = \sum_{x\in D_3}\lambda_b(x) = \sum_{x\in R^*}\lambda_b(x)\delta_3(x) \ \ (\text{where } \lambda_b = \lambda_i\overline{\lambda_j}) \\
= & \sum_{x\in R^*}\lambda_{b_1}(x_1)\lambda_{b_2}(x_2)\frac{1+\varphi_1(x_1)\varphi_2(x_2)+\ldots+\varphi_1^{m-1}(x_1)\varphi_2^{m-1}(x_2)}{m} \\
= & \frac{1}{m}[\sum_{x_1\in\mathbb{F}_{q_1}^*}\lambda_{b_1}(x_1)\sum_{x_2\in\mathbb{F}_{q_2}^*}\lambda_{b_2}(x_2)+\sum_{x_1\in\mathbb{F}_{q_1}^*}\lambda_{b_1}(x_1)\varphi_1(x_1)\sum_{x_2\in\mathbb{F}_{q_2}^*}\lambda_{b_2}(x_2)\varphi_2(x_2) \\
& +\ldots+\sum_{x_1\in\mathbb{F}_{q_1}^*}\lambda_{b_1}(x_1)\varphi_1^{m-1}(x_1)\sum_{x_2\in\mathbb{F}_{q_2}^*}\lambda_{b_2}(x_2)\varphi_2^{m-1}(x_2)],
\end{aligned}$$

since $\lambda_i \neq \lambda_j$, λ_b is a nontrivial character, which means not both b_1 and b_2 are equal to zero.

By the orthogonal relation of additive characters, we get:

$$\sum_{x_i\in\mathbb{F}_{q_i}^*}\lambda_{b_i}(x_i) = \begin{cases} q_i-1, & \text{for } b_i = 0, \\ -1, & \text{for } b_i \neq 0. \end{cases} \tag{1}$$

and:

$$\sum_{x_i\in\mathbb{F}_{q_i}^*}\lambda_{b_i}(x_i)\varphi_i^k(x_i) = G(\varphi_i^k,\lambda_{b_i}) = \begin{cases} 0, & \text{for } b_i = 0, \\ \sqrt{q_i}, & \text{for } b_i \neq 0, \end{cases} \tag{2}$$

where $i = 1, 2$ and $0 \leq k \leq m-1$.

It follows that:

$$mKCC^{\cdot H} = \begin{cases} 1-q_1, & \text{for } b_1 = 0, b_2 \neq 0 \\ 1-q_2, & \text{for } b_1 \neq 0, b_2 = 0 \\ 1+G_1(\varphi_1,\lambda_{b_1})G_2(\varphi_2,\lambda_{b_2})+\ldots & \\ +G_1(\varphi_1^{m-1},\lambda_{b_1})G_2(\varphi_2^{m-1},\lambda_{b_2}), & \text{for } b_1 \neq 0, b_2 \neq 0. \end{cases} \tag{3}$$

Thus:

$$\begin{aligned}
I_{max}(\mathcal{C}(D_3)) &= max\{|\mathbf{c}_{\lambda_i}\mathbf{c}_{\lambda_j}^H| : 0 \leq i \neq j \leq q-1\} \\
&\leq \frac{(m-1)\sqrt{q_1q_2}+1}{(q_1-1)(q_2-1)}.
\end{aligned}$$

□

Remark 3. (1) *Since* $N = q_1q_2$ *and* $K = \frac{(q_1-1)(q_2-1)}{m}$ *in this construction, the corresponding Welch bound is:*

$$I_{Welch} = \sqrt{\frac{N-K}{(N-1)K}} = \sqrt{\frac{(m-1)q_1q_2+q_1+q_2-1}{(q_1q_2-1)(q_1-1)(q_2-1)}}.$$

Thus,

$$I_{max}(\mathcal{C}(D_2)) - I_{Welch} \to 0,$$

and:

$$1 \le \frac{I_{max}(\mathcal{C}(D_2))}{I_{Welch}} \le \sqrt{m-1},$$

as $q_1, q_2 \to \infty$ *and* $|q_1 - q_2| = O(1)$.

(2) *When* $m = 2$*, we get* $\frac{I_{max}(\mathcal{C}(D_3))}{I_{Welch}} = 1$*, when* $q_1, q_2 \to \infty$ *and* $|q_1 - q_2| = O(1)$*, which is similar to the second construction in [21].*

3.4. The Fourth Construction of Codebooks

In this section, we propose a construction of codebooks by the group of multiplicative characters and a set D_4 derived by the quadratic character and a quadratic irreducible polynomial.

Let $q = p^t$, where p is an odd prime number and t is a positive integer. Let η be the quadratic character of $\mathbb{F}_q$. Let $f(x) = x^2 + a_1x + a_0 \in \mathbb{F}_q[x]$ be a quadratic irreducible polynomial. We set:

$$D_4 := \{x \in \mathbb{F}_q^* \mid \eta(f(x)) = 1\},$$

and $\#D_4$ = K.

Lemma 4. *([35], Theorem 5.48) Let* $f(x) = a_2x^2 + a_1x + a_0 \in \mathbb{F}_q[x]$ *with* q *odd and* $a_2 \neq 0$*. Put* $b = a_1^2 - 4a_2a_0$*, and let* η *be the quadratic character of* $\mathbb{F}_q$*. Then:*

$$\sum_{c \in \mathbb{F}_q} \eta(f(c)) = \begin{cases} -\eta(a_2), & \text{if } d \neq 0, \\ (q-1)\eta(a_2), & \text{if } d = 0. \end{cases}$$

Lemma 5. *With the above notations, we get:*

$$K = \begin{cases} \frac{q-1}{2}, & \text{if } \eta(a_0) = -1, \\ \frac{q-3}{2}, & \text{if } \eta(a_0) = 1. \end{cases}$$

Proof. Let $K_1 = \#\{x \in \mathbb{F}_q^* : \eta(f(x)) = 1\}$. Since f is irreducible, we get:

$$K + K_1 = q - 1.$$

On the other hand, by Lemma 4, it is easy to see:

$$K - K_1 + \eta(a_0) = K - K_1 + \eta(f(0)) = \sum_{c \in \mathbb{F}_q} \eta(f(c)) = -\eta(1) = -1.$$

The result then follows. □

A codeword of length K is defined as:

$$\mathbf{c}_\chi = \frac{1}{\sqrt{K}}(\chi(x))_{x \in D_4}.$$

where $\chi \in \widehat{\mathbb{F}_q^*}$.

Then, we construct the following (N, K) codebook $\mathcal{C}(D_4)$ as:

$$\mathcal{C}(D_4) = \{\frac{1}{\sqrt{K}}(\chi(x))_{x \in D_4} \mid \chi \in \widehat{\mathbb{F}_q^*}\},$$

and it is easy to see $N = q - 1$.

Let:

$$\delta_4(x) = \frac{1+\eta(f(x))}{2}.$$

Through the definition of D_4, we known that:

$$\delta_4(x) = \begin{cases} 1, & \text{if } x \in D_4, \\ 0, & \text{otherwise.} \end{cases}$$

Theorem 3. *With the above notation, we have:*

$$I_{max}(\mathcal{C}(D_4)) \leq \frac{\sqrt{q}}{K} = \begin{cases} \frac{2\sqrt{q}}{q-1}, & \text{if } \eta(a_0) = -1, \\ \frac{2\sqrt{q}}{q-3}, & \text{if } \eta(a_0) = 1. \end{cases}$$

Proof. For any characters χ_i and χ_j in $\widehat{\mathbb{F}_q^*}$, where $1 \leq i \neq j \leq q-1$, let $\chi = \chi_i\overline{\chi_j}$, then we have:

$$\begin{aligned} & K(\mathbf{c}_{\chi_i}\mathbf{c}_{\chi_j}^H) \\ = & \sum_{x\in D_4} \chi_i(x)\overline{\chi_j(x)} = \sum_{x\in D_4} \chi(x) = \sum_{x\in\mathbb{F}_q^*} \chi(x)\delta_4(x) \ \ (\text{where } \chi = \chi_i\overline{\chi_j}) \\ = & \sum_{x\in\mathbb{F}_q^*} \chi(x)\frac{1+\eta(f(x))}{2} \\ = & \frac{1}{2}\sum_{x\in\mathbb{F}_q^*} \chi(x) + \frac{1}{2}\sum_{x\in\mathbb{F}_q^*} \chi(x)\eta(f(x)) \\ = & \frac{1}{2}\sum_{x\in\mathbb{F}_q^*} \chi(x)\eta(f(x)). \end{aligned}$$

By the result in Lemma 6, we get:

$$|\sum_{x\in\mathbb{F}_q^*} \chi(x)\eta(f(x))| \leq (3-1)\sqrt{q} = 2\sqrt{q}$$

Then:

$$I_{max}(\mathcal{C}(D_4)) \leq \frac{\sqrt{q}}{K} = \begin{cases} \frac{2\sqrt{q}}{q-1}, & \text{if } \eta(a_0) = -1, \\ \frac{2\sqrt{q}}{q-3}, & \text{if } \eta(a_0) = 1. \end{cases}$$

□

Lemma 6. ([36]) *Let $f_1(x), \ldots, f_h(x)$ be h monic, distinct, and irreducible polynomials in $\mathbb{F}_q[x]$, which have the positive degrees $d_1, \ldots, d_h$, respectively. Let d be the number of distinct roots of $f(x) = \prod_{i=1}^h f_i(x)$ in its splitting field over $\mathbb{F}_q$. Let $\psi_1, \ldots, \psi_h$ be the multiplicative characters of $\mathbb{F}_q$. Assume that the product character $\prod_{i=1}^h \psi_i(f_i(x))$ is nontrivial for some $x \in \mathbb{F}_q$. Then, for every $a_i \in \mathbb{F}_q^*$, $i = 1, \ldots, h$,*

$$|\sum_{x\in\mathbb{F}_q} \psi_1(a_1 f_1(x)), \ldots, \psi_h(a_h f_h(x))| \leq (d-1)\sqrt{q}.$$

Remark 4. *Since $N = q-1$, combining the result in Lemma 5 about K, the corresponding Welch bound is:*

$$I_{Welch} = \begin{cases} \frac{1}{\sqrt{q-2}}, & \text{if } \eta(a_0) = -1, \\ \sqrt{\frac{q+3}{(q-2)(q-3)}}, & \text{if } \eta(a_0) = 1. \end{cases}$$

Thus,

$$I_{max}(\mathcal{C}(D_4)) - I_{Welch} \to 0,$$

and:

$$\lim_{q\to\infty} \frac{I_{max}(\mathcal{C}(D_2))}{I_{Welch}} = 2.$$

4. Concluding Remarks

In this paper, we proposed four constructions of codebooks and determined the maximum cross-correlation amplitude of codebooks generated by these four constructions. We verified that the codebooks generated by these four constructions were asymptotically optimal with respect to the Welch bound. Notably, the parameters of our codebooks were new and flexible. The technique of our paper was the properties of the Gauss sum, Jacobi sum, and some conclusions about the upper bound of the multiplicative characters acting on irreducible polynomials. The parameters of our codebooks were flexible and new, and the p in our constructions could be any odd prime.

Author Contributions: Conceptualization, W.L.; Formal analysis, X.W.; Investigation, X.W; Writing original draft, W.L.

Funding: This work was supported by the National Natural Science Foundation of China (Grant Nos. 11971102 and 11801070).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Welch, L. Lower bounds on the maximum cross correlation of signals. *IEEE Trans. Inf. Theory* **1974**, *20*, 397–399.
2. Sarwate, D. *Meeting the Welch Bound with Equality*; Springer: New York, NY, USA, 1999; pp. 63–79.
3. Kovacevic, J.; Chebira, A. An introduction to frames. *Found. Trends Signal Process.* **2008**, *2*, 1–94.
4. Massey, J.; Mittelholzer, T. *Welch's Bound and Sequence Sets for Code-Division Multiple-Access Systems*; Sequences II; Springer: New York, NY, USA, 1999; pp. 63–78.
5. Ding, C. Complex codebooks from combinatorial designs. *IEEE Trans. Inf. Theory* **2006**, *52*, 4229–4235.
6. Ding, C.; Feng, T. A generic construction of complex codebooks meeting the Welch bound. *IEEE Trans. Inf. Theory* **2007**, *53*, 4245–4250.
7. Xia, P.; Zhou, S.; Giannakis, G. Achieving the Welch bound with difference sets. *IEEE Trans. Inf. Theory* **2005**, *51*, 1900–1907.
8. Conway, J.; Harding, R.; Sloane, N. Packing lines, planes, etc.: Packings in Grassmannian spaces. *Exp. Math.* **1996**, *5*, 139–159.
9. Candes, E.; Wakin, M. An introduction to compressive sampling. *IEEE Signal Process* **2008**, *25*, 21–30.
10. Delsarte, P.; Goethals, J.; Seidel, J. Spherical codes and designs. *Geom. Dedicate* **1997**, *67*, 363–388.
11. Kim, Y.S.; Park, H.; No, J.S. Construction of New Fractional Repetition Codes from Relative Difference Sets with lambda=1. *Entropy* **2017**, *19*, 563.
12. Phu, T.T.; Nguyen, T.N.; Sang, N.Q. Rateless Codes-Based Secure Communication Employing Transmit Antenna Selection and Harvest-To-Jam under Joint Effect of Interference and Hardware Impairments. *Entropy* **2019**, *21*, 700.
13. Renes, J.; Blume-Kohout, R.; Scot, A.; Caves, C. Symmetric informationally complete quantum measurements. *J. Math. Phys.* **2004**, *45*, 2171–2180.
14. Strohmer, T.; Heath, R. Grassmannian frames with applications to coding and communication. *Appl. Comput. Harmon. Anal.* **2003**, *14*, 257–275.
15. Fickus, M.; Mixon, D.; Tremain, J. Steiner equiangular tight frames. *Linear Algebra Appl.* **2012**, *436*, 1014–1027.
16. Fickus, M.; Mixon, D. Tables of the existence of equiangular tight frames. *arXiv* **2016**, arXiv:1504.00253v2.
17. Fickus, M.; Mixon, D.; Jasper, J. Equiangular tight frames from hyperovals. *IEEE Trans. Inf. Theory* **2016**, *62*, 5225–5236.

18. Fickus, M.; Jasper, J.; Mixon, D.; Peterson, J. Tremain equiangular tight frames. *arXiv* **2016**, arXiv:1602.03490v1.
19. Rahimi, F. Covering Graphs and Equiangular Tight Frames. Ph.D. Thesis, University of Waterloo, Waterloo, ON, Canada, 2016. Available online: http://hdl.handle.net/10012/10793 (accessed on 20 November 2019).
20. Hu, H.; Wu, J. New constructions of codebooks nearly meeting the Welch bound with equality. *IEEE Trans. Inf. Theory* **2014**, *60*, 1348–1355.
21. Zhang, A.; Feng, K. Two classes of codebooks nearly meeting the Welch bound. *IEEE Trans. Inf. Theory* **2012**, *58*, 2507–2511.
22. Zhang, A.; Feng, K. Construction of cyclotomic codebooks nearly meeting the Welch bound. *Des. Codes Cryptogr.* **2013**, *63*, 209–224.
23. Zhou, Z.; Tang, X. New nearly optimal codebooks from relative difference sets. *Adv. Math. Commun.* **2011**, *5*, 521–527.
24. 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* **2014**, *60*, 3698–3705.
25. Yu, N. A construction of codebooks associated with binary sequences. *IEEE Trans. Inf. Theory* **2012**, *58*, 5522–5533.
26. Heng, Z.; Ding, C.; Yue, Q. New constructions of asymptotically optimal codebooks with multiplicative characters. *IEEE Trans. Inf. Theory* **2017**, *63*, 6179–6187.
27. Heng, Z. Nearly optimal codebooks based on generalized Jacobi sums. *Discrete Appl. Math.* **2018**, *250*, 227–240.
28. Luo, G.J.; Cao, X.W. Two constructions of asymptotically optimal codebooks via the hyper Eisenstein sum. *IEEE Trans. Inf. Theory* **2018**, *64*, 6498–6505.
29. Luo, G.J.; Cao, X.W. New constructions of codebooks asymptotically achieving the Welch bound. In Proceedings of the 2018 IEEE International Symposium on Information Theory (ISIT), Vail, CO, USA, 17–22 June 2018; pp. 2346–2349.
30. Luo, G.J.; Cao, X.W. Two constructions of asymptotically optimal codebooks. *Crypt. Commun.* **2019**, *11*, 825–838, doi:10.1007/s12095-018-0331-4.
31. Mohades, M.M.; Mohades, A.; Tadaion, A. A Reed-Solomom Code Based Measurement Matrix with Small Coherence. *IEEE Signal Process. Lett.* **2014**, *21*, 839–843.
32. Li, C.J.; Qin, Y.; Huang, Y.W. Two families of nearly optimal codebooks. *Des. Codes Cryptogr.* **2015**, *75*, 43–57.
33. Wu, X.; Lu, W.; Cao, X.W.; Chen, M. Two constructions of asymptotically optimal codebooks via the trace functions. *arXiv* **2019**, arXiv:1905.01815.
34. Lu, W.; Wu, X.; Cao, X.W. Six constructions of asymptotically optimal codebooks via the character sums. *arXiv* **2019**, arXiv:1911.00506.
35. Lidl, R.; Niederreiter, H. *Finite Fields*; Cambridge University Press: Cambridge, UK, 1997.
36. Wan, D. Generators and irreducible polynomials over finite fields. *Math. Comput.* **1997**, *66*, 1195–1212.