AIMS Mathematics

http://www.aimspress.com/journal/Math

AIMS Mathematics, 9(4): 9631–9640.
DOI:10.3934/math.2024471
Received: 15 January 2024
Revised: 23 February 2024
Accepted: 01 March 2024
Published: 11 March 2024

Research article

A new construction of asymptotically optimal codebooks

Yang Yan[1], **Hanning Chen**[2,3,4,*], **Jianming Wang**[4,5] **and Gang Wang**[6]

[1] School of Information Technology and Engineering, Tianjin University of Technology and Education, Tianjin 300222, China

[2] Engineering Research Center of Integration and Application of Digital Learning Technology, Ministry of Education, Beijing 100039, China

[3] Tianjin Swom Technology Development Co., Ltd., Tianjin 300387, China

[4] School of Computer Science, Tiangong University, Tianjin 300387, China

[5] Tianjin Key Laboratory of Autonomous Intelligence Technology and Systems, Tianjin 300387, China

[6] College of Science, Civil Aviation University of China, Tianjin 300300, China

* **Correspondence:** Email: chenhanning@tiangong.edu.cn; Tel: +8618624031099.

Abstract: Codebooks with small cross-correlation amplitude have extensive applications in many fields including code division multiple access (CDMA) communications systems, space-time codes, and compressed sensing. In this paper, a class of asymptotically optimal codebooks was constructed, and the maximum inner-product of these presented codebooks was determined by using properties of character sums over finite fields. Furthermore, these codebooks provided new parameters.

Keywords: codebooks; characters; finite fields; asymptotical optimality; Welch bound
Mathematics Subject Classification: 11T23, 11T24, 12E20, 94B05

1. Introduction

Throughout this paper, let p be an odd prime and $q = p^n$ for some positive integer n. Codebooks (also known as signal sets) with low coherence are typically used to distinguish signals of different users in code division multiple access (CDMA) systems. An (N, K) codebook C is a finite set $\{\mathbf{c}_0, \mathbf{c}_1, \ldots, \mathbf{c}_{N-1}\}$, where the codeword $\mathbf{c}_i$, $0 \le i \le N-1$, is a unit norm $1 \times K$ complex vector over an alphabet $\mathcal{A}$. The maximum inner-product correlation $I_{\max}(C)$ of C is defined by

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

where $\mathbf{c}_j^H$ denotes the conjugate transpose of $\mathbf{c}_j$. The maximal cross-correlation amplitude $I_{\max}(C)$ of C is an important index of C, as it can approximately optimize many performance metrics such as outage probability and average signal-to-noise ratio. For a fixed K, researchers are highly interested in designing a codebook C with the parameter N being as large as possible and $I_{\max}(C)$ being as small as possible simultaneously. Unfortunately, there exists a bound between the parameters N, K and $I_{\max}(C)$.

Lemma 1. *([1]) For any (N, K) codebook C with $N \geq K$,*

$$I_{\max}(C) \geq \sqrt{\frac{N-K}{(N-1)K}}. \tag{1.1}$$

The bound in (1.1) is called the Welch bound of C and is denoted by $I_w(C)$. If the codebook C achieves $I_w(C)$, then C is said to be optimal with respect to the Welch bound. However, constructing codebooks achieving the Welch bound is extremely difficult. Hence, many researchers have focused their main energy on constructing asymptotically optimal codebooks, i.e., $I_{\max}(C)$ asymptotically meets the Welch bound $I_w(C)$ for sufficiently large N [2–7].

The objective of this paper is to construct a class of complex codebooks and investigate their maximum inner-product correlation. Results show that these constructed complex codebooks are nearly optimal with respect to the Welch bound, i.e., the ratio of their maximal cross-correlation amplitude to the Welch bound approaches 1. These codebooks may have applications in strongly regular graphs [8], combinatorial designs [9, 10], and compressed sensing [11, 12].

This paper is organized as follows. In Section 2, we review some essential mathematical concepts regarding characters and Gauss sums over finite fields. In Section 3, we present a class of asymptotically optimal codebooks using the trace functions and multiplicative characters over finite fields. Finally, we make a conclusion in Section 4.

2. Preliminaries

In this section, we review some essential mathematical concepts regarding characters and Gauss sums over finite fields. These concepts will play significant roles in proving the main results of this paper.

Let n be a positive integer and p an odd prime. Denote the finite field with p^n elements by $\mathbb{F}_{p^n}$. The trace function Tr_n from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ is defined by

$$\mathrm{Tr}_n(x) = \sum_{i=0}^{n-1} x^{p^i}.$$

Let ζ_p denote a primitive p-th root of complex unity and Tr_n denote the trace function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$. For $x \in \mathbb{F}_{p^n}$, it can be checked that χ_n given by $\chi_n(x) = \zeta_p^{\mathrm{Tr}_n(x)}$ is an additive character of $\mathbb{F}_{p^n}$, and χ_n is called the canonical additive character of $\mathbb{F}_{p^n}$. Assume $a \in \mathbb{F}_{p^n}$, then every additive character of $\mathbb{F}_{p^n}$ can be obtained by $\mu_a(x) = \chi_n(ax)$ where $x \in \mathbb{F}_{p^n}$. The orthogonality relation of μ_a is given by

$$\sum_{x \in \mathbb{F}_{p^n}} \mu_a(x) = \begin{cases} p^n, & \text{if } a = 0, \\ 0, & \text{otherwise.} \end{cases} \tag{2.1}$$

Let $q = p^n$ and α be a primitive element of $\mathbb{F}_q^*$, then all multiplicative characters of $\mathbb{F}_q$ are given by $\varphi_j(\alpha^i) = \zeta_{q-1}^{ij}$, where ζ_{q-1} denotes a primitive $(q-1)$-th root of unity and $0 \le i, j \le q-2$. The quadratic character of $\mathbb{F}_q$ is the character $\varphi_{(q-1)/2}$, which will be denoted by η_n in the sequel, and η_n is extended by setting $\eta_n(0) = 0$. For φ_j, its orthogonality relation is given by

$$\sum_{x\in\mathbb{F}_{p^n}} \varphi_j(x) = \begin{cases} q-1, & \text{if } j = 0, \\ 0, & \text{otherwise.} \end{cases}$$

The Gauss sum $G(\eta_n)$ over $\mathbb{F}_{p^n}$ is defined by

$$G(\eta_n) = \sum_{x\in\mathbb{F}_{p^n}^*} \eta_n(x)\chi_n(x).$$

The explicit value of $G(\eta_n)$ is given in the following lemma.

Lemma 2 ([13], Theorem 5.15)**.** *With symbols and notations above, we have*

$$G(\eta_n) = (-1)^{n-1}(-1)^{\frac{(p-1)n}{4}} q^{\frac{1}{2}}.$$

The following results on exponential sums will play an important role in proving the main results of this paper.

Lemma 3 ([13], p.195)**.** *With symbols and notations above, we have*

$$\eta_1(x) = \frac{1}{p}\sum_{a\in\mathbb{F}_p} G(\eta_1)\eta_1(-a)\chi_1(ax),$$

where η_1 denotes the quadratic character and χ_1 the canonical additive character of $\mathbb{F}_p$.

Lemma 4 ([13], Theorem 5.33)**.** *If $f(x) = a_2x^2 + a_1x + a_0 \in \mathbb{F}_{p^n}[x]$ with $a_2 \neq 0$, then*

$$\sum_{x\in\mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}_n(f(x))} = \eta_n(a_2)G(\eta_n)\zeta_p^{\mathrm{Tr}_n\left(a_0 - a_1^2(4a_2)^{-1}\right)}.$$

Lemma 5 ([14], Theorem 2)**.** *Let $n = 2m$ be an even integer and $z \in \mathbb{F}_p^*$, then*

$$\sum_{x\in\mathbb{F}_{p^n}} \zeta_p^{z\,\mathrm{Tr}_n\left(x^{p^m+1}\right)} = -p^m.$$

Lemma 6 ([15])**.** *Let $n = 2m$ be an even integer, $a \in \mathbb{F}_{p^m}^*$, and $b \in \mathbb{F}_{p^n}$, then*

$$\sum_{x\in\mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}_m\left(ax^{p^m+1}\right)+\mathrm{Tr}_n(bx)} = -p^m\zeta_p^{-\mathrm{Tr}_m\left(\frac{b^{p^m+1}}{a}\right)}.$$

Lemma 7 ([16], Lemma 3.12)**.** *If A and B are finite abelian groups, then there is an isomorphism*

$$\widehat{A\times B} \cong \widehat{A}\times\widehat{B},$$

where $\widehat{A}$ consists of all characters of A.

By this lemma, we know that

$$\widehat{\mathbb{F}_{p^n}^+ \times \mathbb{F}_{p^n}^+} = \{\mu_{a,b} : a, b \in \mathbb{F}_{p^n}\}$$

where

$$\mu_{a,b}(x,y) = \zeta_p^{\mathrm{Tr}_n(ax+by)}$$

for $x, y \in \mathbb{F}_{p^n}$.

3. Proofs and main results

In this section, we always suppose that $n = 2m$ is an even integer and p is an odd prime. The set D is defined as follows:

$$D = \left\{(x,y) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n} : \eta_1\left(\mathrm{Tr}_n\left(x^2 + y^{p^m+1}\right)\right) = 1\right\},$$

where η_1 is the quadratic character of $\mathbb{F}_p$. A codebook C is constructed by

$$C = \left\{\mathbf{c}_{a,b} : a, b \in \mathbb{F}_{p^n}\right\}, \tag{3.1}$$

where $\mathbf{c}_{a,b} = \frac{1}{\sqrt{|D|}}\left(\mu_{a,b}(x,y)\right)_{(x,y)\in D}$, $\mu_{a,b}(x,y) = \zeta_p^{\mathrm{Tr}_n(ax+by)}$ for $(x,y) \in D$ and $|D|$ denotes the cardinality of the set D.

Lemma 8. *With symbols and notations as above, we have*

$$|D| = \frac{p-1}{2}\left(p^{2n-1} - (-1)^{\frac{n(p-1)}{4}} p^{n-1}\right).$$

Proof. Let

$$A_1 = \sum_{\substack{x,y\in\mathbb{F}_{p^n} \\ \mathrm{Tr}_n\left(x^2+y^{p^m+1}\right)=0}} 1,\ A_2 = \sum_{\substack{x,y\in\mathbb{F}_{p^n} \\ \mathrm{Tr}_n\left(x^2+y^{p^m+1}\right)\neq 0}} \eta_1\left(\mathrm{Tr}_n(x^2 + y^{p^m+1})\right).$$

Note that

$$\sum_{\substack{x,y\in\mathbb{F}_{p^n} \\ \mathrm{Tr}_n\left(x^2+y^{p^m+1}\right)=0}} 1 + \sum_{\substack{x,y\in\mathbb{F}_{p^n} \\ \mathrm{Tr}_n\left(x^2+y^{p^m+1}\right)\neq 0}} 1 = p^{2n}.$$

Together with the definition of D, we have

$$\begin{aligned}
|D| &= \sum_{\substack{x,y\in\mathbb{F}_{p^n} \\ \mathrm{Tr}_n\left(x^2+y^{p^m+1}\right)\neq 0}} \frac{\eta_1\left(\mathrm{Tr}_n\left(x^2 + y^{p^m+1}\right)\right) + 1}{2} \\
&= \frac{1}{2}\sum_{\substack{x,y\in\mathbb{F}_{p^n} \\ \mathrm{Tr}_n\left(x^2+y^{p^m+1}\right)\neq 0}} \eta_1\left(\mathrm{Tr}_n\left(x^2 + y^{p^m+1}\right)\right) + \frac{1}{2}\sum_{\substack{x,y\in\mathbb{F}_{p^n} \\ \mathrm{Tr}_n\left(x^2+y^{p^m+1}\right)\neq 0}} 1 \\
&= \frac{A_2}{2} + \frac{p^{2n}}{2} - \frac{1}{2}\sum_{\substack{x,y\in\mathbb{F}_{p^n} \\ \mathrm{Tr}_n\left(x^2+y^{p^m+1}\right)=0}} 1
\end{aligned}$$

$$= \frac{1}{2}\left(p^{2n} - A_1 + A_2\right). \tag{3.2}$$

By definition, we have

$$\begin{aligned} A_1 &= \frac{1}{p}\sum_{x,y\in\mathbb{F}_{p^n}}\sum_{z\in\mathbb{F}_p}\zeta_p^{z\,\mathrm{Tr}_n\left(x^2+y^{p^m+1}\right)} \\ &= p^{2n-1} + \frac{1}{p}\sum_{z\in\mathbb{F}_p^*}\sum_{x,y\in\mathbb{F}_{p^n}}\zeta_p^{\mathrm{Tr}_n\left(zx^2\right)+\mathrm{Tr}_n\left(zy^{p^m+1}\right)} \\ &= p^{2n-1} + (-1)^{\frac{n(p-1)}{4}}p^{n-1}(p-1). \end{aligned} \tag{3.3}$$

where the last equality follows from Lemmas 2, 4, and 5. Note that $\eta_n(z) = 1$ for $z \in \mathbb{F}_p^*$ if n is even. By Lemma 3, we obtain

$$A_2 = \frac{G(\eta_n)}{p}\sum_{a\in\mathbb{F}_p^*}\eta_1(-a)\sum_{x\in\mathbb{F}_{p^n}}\zeta_p^{\mathrm{Tr}_n\left(ax^2\right)}\sum_{y\in\mathbb{F}_{p^n}}\zeta_p^{\mathrm{Tr}_n\left(ay^{p^m+1}\right)}$$

Using Lemmas 4 and 5, we get

$$A_2 = -p^{m-1}G^2(\eta_n)\sum_{a\in\mathbb{F}_p^*}\eta_1(-a) = 0.$$

The desired conclusion follows from (3.2) and (3.3). □

Example 1. *Let $p = 5$ and $n = 2$. By the Magma program, we know that $|D| = 240$, which is consistent with Lemma 8.*

Theorem 9. *Let symbols and notations be the same as before, then the codebook $\mathcal{C}$ defined in* (3.1) *has parameters $[p^{2n}, K]$,*

$$K = \frac{p-1}{2}\left(p^{2n-1} - (-1)^{\frac{n(p-1)}{4}}p^{n-1}\right),$$

and

$$I_{\max}(\mathcal{C}) = (p+1)p^{n-1}/(2K).$$

Proof. By the definition of the set $\mathcal{C}$ and Lemma 8, we deduce that $\mathcal{C}$ is a $[p^{2n}, K]$ codebook. If $a, b \in \mathbb{F}_{p^n}$ and $(a, b) \neq (0, 0)$, then we have

$$\sum_{x,y\in\mathbb{F}_{p^n}}\zeta_p^{\mathrm{Tr}_n(ax+by)} = \sum_{\substack{x,y\in\mathbb{F}_{p^n} \\ \mathrm{Tr}_n\left(x^2+y^{p^m+1}\right)=0}}\zeta_p^{\mathrm{Tr}_n(ax+by)} + \sum_{\substack{x,y\in\mathbb{F}_{p^n} \\ \mathrm{Tr}_n\left(x^2+y^{p^m+1}\right)\neq 0}}\zeta_p^{\mathrm{Tr}_n(ax+by)} = 0$$

This implies that

$$\sum_{\substack{x,y\in\mathbb{F}_{p^n} \\ \mathrm{Tr}_n\left(x^2+y^{p^m+1}\right)=0}}\zeta_p^{\mathrm{Tr}_n(ax+by)} = -\sum_{\substack{x,y\in\mathbb{F}_{p^n} \\ \mathrm{Tr}_n\left(x^2+y^{p^m+1}\right)\neq 0}}\zeta_p^{\mathrm{Tr}_n(ax+by)}.$$

For $a, b \in \mathbb{F}_{p^n}$ and $(a, b) \neq (0, 0)$, we have that

$$\begin{aligned}
\sum_{(x,y)\in D} \mu_{a,b}(x, y) = & \sum_{\substack{x,y\in\mathbb{F}_{p^n} \\ \mathrm{Tr}_n\left(x^2+y^{p^m+1}\right)\neq 0}} \zeta_p^{\mathrm{Tr}_n(ax+by)} \frac{\eta_1\left(\mathrm{Tr}_n\left(x^2+y^{p^m+1}\right)\right)+1}{2} \\
= & -\frac{1}{2} \sum_{\substack{x,y\in\mathbb{F}_{p^n} \\ \mathrm{Tr}_n\left(x^2+y^{p^m+1}\right)=0}} \zeta_p^{\mathrm{Tr}_n(ax+by)} + \frac{1}{2} \sum_{\substack{x,y\in\mathbb{F}_{p^n} \\ \mathrm{Tr}_n\left(x^2+y^{p^m+1}\right)\neq 0}} \zeta_p^{\mathrm{Tr}_n(ax+by)} \eta_1\left(\mathrm{Tr}_n\left(x^2+y^{p^m+1}\right)\right) \\
= & \frac{1}{2}(-B_1 + B_2),
\end{aligned} \tag{3.4}$$

where

$$B_1 = \sum_{\substack{x,y\in\mathbb{F}_{p^n} \\ \mathrm{Tr}_n\left(x^2+y^{p^m+1}\right)=0}} \zeta_p^{\mathrm{Tr}_n(ax+by)},\ B_2 = \sum_{x,y\in\mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}_n(ax+by)} \eta_1\left(\mathrm{Tr}_n\left(x^2+y^{p^m+1}\right)\right).$$

By (2.1), we derive that

$$\sum_{z\in\mathbb{F}_p} \zeta_p^{z\,\mathrm{Tr}_n\left(x^2+y^{p^m+1}\right)} = \begin{cases} p, & \text{if } \mathrm{Tr}_n\left(x^2+y^{p^m+1}\right)=0, \\ 0, & \text{otherwise.} \end{cases}$$

Combining Lemmas 4 and 6, we get that

$$\begin{aligned}
B_1 = & \frac{1}{p} \sum_{x,y\in\mathbb{F}_{p^n}} \sum_{z\in\mathbb{F}_p} \zeta_p^{\mathrm{Tr}_n(ax+by)} \zeta_p^{z\,\mathrm{Tr}_n\left(x^2+y^{p^m+1}\right)} \\
= & \frac{1}{p} \sum_{z\in\mathbb{F}_p^*} \sum_{x,y\in\mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}_n\left(zx^2+ax\right)} \zeta_p^{\mathrm{Tr}_n\left(zy^{p^m+1}+by\right)} \\
= & -p^{m-1} G(\eta_n) \sum_{z\in\mathbb{F}_p^*} \eta_n(z) \zeta_p^{\mathrm{Tr}_n\left(a^2+b^{p^m+1}\right)z} \\
= & \begin{cases} -p^{m-1}(p-1)G(\eta_n), & \text{if } \mathrm{Tr}_n\left(a^2+b^{p^m+1}\right)=0, \\ p^{m-1}G(\eta_n), & \text{if } \mathrm{Tr}_n\left(a^2+b^{p^m+1}\right)\neq 0, \end{cases}
\end{aligned} \tag{3.5}$$

where $G(\eta_n)$ is given in Lemma 2. By Lemma 3, we have that

$$B_2 = \frac{G(\eta_1)}{p} \sum_{z\in\mathbb{F}_p^*} \eta_1(-z) \sum_{x\in\mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}_n\left(zx^2+ax\right)} \sum_{y\in\mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}_n\left(zy^{p^m+1}+by\right)}.$$

Moreover, by Lemmas 4 and 6, we obtain

$$\begin{aligned}
B_2 = & -p^{m-1} G(\eta_1) G(\eta_n) \sum_{z\in\mathbb{F}_p^*} \eta_1(z) \zeta_p^{z\,\mathrm{Tr}_n\left(a^2+b^{p^m+1}\right)} \\
= & \begin{cases} 0, & \text{if } \mathrm{Tr}_n\left(a^2+b^{p^m+1}\right)=0, \\ -p^m\left(\frac{-1}{p}\right) G(\eta_n) \eta_1\left(\mathrm{Tr}_n\left(a^2+b^{p^m+1}\right)\right), & \text{if } \mathrm{Tr}_n\left(a^2+b^{p^m+1}\right)\neq 0. \end{cases}
\end{aligned} \tag{3.6}$$

It follows from Lemma 2 and (3.4) that

$$\sum_{(x,y)\in D} \mu_{a,b}(x,y) \in \left\{\frac{1}{2}(p-1)p^{m-1}G(\eta_n), -\frac{1}{2}(p+1)p^{m-1}G(\eta_n)\right\}. \tag{3.7}$$

For any two distinct codewords $\mathbf{c}_{z_1,z_2}, \mathbf{c}_{z_1',z_2'} \in C$, i.e., $(z_1,z_2) \neq (z_1',z_2')$, it is easy to check that

$$\left|\mathbf{c}_{z_1,z_2}\mathbf{c}^H_{z_1',z_2'}\right| = \frac{1}{K}\left|\sum_{(x,y)\in D} \mu_{z_1-z_1',z_2-z_2'}(x,y)\right|. \tag{3.8}$$

Combining (3.7) and (3.8), we get that $I_{\max}(C) = (p+1)p^{n-1}/(2K)$. □

Example 2. *Let $f(x)$ be an irreducible polynomial over the field $\mathbb{F}_3$ and $f(x) = x^2 + x + 2$ in $\mathbb{F}_3[x]$. Suppose that $p = 3$, $n = 2$, and α is a root of $f(x)$ over $\mathbb{F}_3$, then $m = 1$, $q = 3^2$, and $\mathbb{F}_9 = \mathbb{F}_3(\alpha)$. It can be verified that the set D consists of the following* 30 *elements:*

$$\begin{aligned} D &= \left\{(x,y) \in \mathbb{F}_9 \times \mathbb{F}_9 : \mathrm{Tr}_2\left(x^2+y^4\right) = 1\right\} \\ &= \left\{\begin{array}{lllll} (1+2\alpha,0), & (2+\alpha,0), & (1,1), & (1,2), & (1,1+2\alpha), \\ (1,2+\alpha), & (2,1), & (2,2), & (2,1+2\alpha), & (2,2+\alpha), \\ (\alpha,\alpha), & (\alpha,2\alpha), & (\alpha,1+\alpha), & (\alpha,2+2\alpha), & (2\alpha,\alpha), \\ (2\alpha,2\alpha), & (2\alpha,1+\alpha), & (2\alpha,2+2\alpha), & (0,\alpha), & (0,2\alpha), \\ (0,1+\alpha), & (0,2+2\alpha), & (1+\alpha,\alpha), & (1+\alpha,2\alpha), & (1+\alpha,1+\alpha), \\ (1+\alpha,2+2\alpha), & (2+2\alpha,\alpha), & (2+2\alpha,2\alpha), & (2+2\alpha,1+\alpha), & (2+2\alpha,2+2\alpha) \end{array}\right\}. \end{aligned}$$

The corresponding codebook C is given by

$$C = \left\{\frac{1}{\sqrt{30}}\left(\zeta_3^{\mathrm{Tr}_2(ax+by)}\right)_{(x,y)\in D} : a,b \in \mathbb{F}_9\right\},$$

where $\zeta_3 = e^{\frac{2\pi\sqrt{-1}}{3}}$ and Tr_2 denotes the trace function from $\mathbb{F}_9$ to $\mathbb{F}_3$.

Corollary 10. *The codebook C constructed in* (3.1) *is asymptotically optimal with respect to the Welch bound.*

Proof. The corresponding Welch bound is

$$I_w(C) = \sqrt{\frac{p^{2n-1}(p+1) + (-1)^{\frac{n(p-1)}{4}}p^{n-1}(p-1)}{(p^{2n}-1)(p-1)\left(p^{2n-1} - (-1)^{\frac{n(p-1)}{4}}p^{n-1}\right)}}.$$

We deduce that

$$\lim_{p^n\to+\infty}\frac{I_w(C)}{I_{\max}(C)} = \lim_{p^n\to+\infty}\sqrt{\frac{4K\left(p^{2n}-K\right)}{(p^{2n}-1)(p+1)^2p^{2n-2}}} = 1,$$

which implies that C asymptotically meets the Welch bound. □

In Table 1, we show some parameters of some specific codebooks defined in (3.1). From this table, we conclude that $I_{\max}(C)$ is very close to $I_w(C)$ for largely enough p, which ensures the correctness of Theorem 9 and Corollary 10.

Table 1. The parameters of the codebook C in (3.1) for $n = 4$.

p	N	K	$I_{\max}(C)$	$I_w(C)$	$I_{\max}(C)/I_w(C)$
3	3^8	2160	1/40	1.762×10^{-2}	1.4185
7	7^8	2469600	1/1800	4.811×10^{-4}	1.1548
11	11^8	97429200	1/12200	7.483×10^{-5}	1.0955
13	13^8	376477920	1/24480	3.782×10^{-5}	1.0801
17	17^8	3282670080	1/74240	1.2699×10^{-5}	1.0607

4. Concluding remarks

This paper presented a family of codebooks by the combination of additive characters and multiplicative characters over finite fields. Results show that the constructed codebooks are asymptotically optimal in the sense that the maximum cross correlation amplitude of the codebooks asymptotically achieves the Welch bound. As a comparison, parameters of some known nearly optimal codebooks and the constructed ones are listed in Table 2. From this table, we can conclude that the parameters of C are not covered by those in [2–6, 17–19]. This means the presented codebooks have new parameters.

Table 2. The parameters of codebooks asymptotically meeting the Welch bound.

Ref.	Parameters (N, K)	Constraints
[2]	$\left((q-1)^{\ell} + M, M\right)$, $M = \frac{(q-1)^{\ell}+(-1)^{\ell+1}}{q}$.	q is a prime power, $\ell > 2$.
[3]	$\left(2K + (-1)^{ln}, K\right)$, $K = \frac{(q_1-1)^n \cdots (q_l-1)^n - (-1)^{ln}}{2}$.	$1 \le i \le l$, $s_i > 1$, $q_i = 2^{s_i}$, $l > 1$ and $n > 1$.
[4]	$\left((q^s - 1)^m + q^{sm-1}, q^{sm-1}\right)$	$s > 1$, $m > 1$, q is a prime power.
[5]	$\left((p_{\min} + 1)Q^2, Q^2\right)$	$Q > 1$ is an integer, $p_{\min}$ is the smallest prime factor of Q.
[6]	$(p_{\min} N_1 N_2, N_1 N_2)$	$N_1 \ge 1$, $N_2 = N_1 + o(N_1)$, $p_{\min}$ is the smallest prime factor of N_2.
[6]	$(p_{\min} N_1 N_2, N_1 N_2)$	$N_1 \ge 1$, $N_2 = N_1 + o(N_1)$, $p_{\min}$ is the smallest prime factor of N_2.
[17]	$(q_1 q_2 \cdots q_l, (q_1 q_2 \cdots q_l - 1)/2)$	$1 \le i \le l$, q_i is a prime power, $q_i \equiv 3 \pmod 4$
[18]	$\left(q, \frac{q+1}{2}\right)$	q is a prime power.
[19]	$\left(q^3 + q^2, q^2\right)$ or $\left(q^3 + q^2 - q, q^2 - q\right)$	q is a prime power.
Thm. 9	$\left(p^{2n}, \frac{p-1}{2}\left(p^{2n-1} - (-1)^{\frac{n(p-1)}{4}} p^{n-1}\right)\right)$	p is an odd prime, $n = 2m$, m is a positive integer.

Use of AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

Acknowledgments

This work was supported by the Innovation Project of Engineering Research Center of Integration and Application of Digital Learning Technology (No.1221003), Humanities and Social Sciences Youth Foundation of Ministry of Education of China (No. 22YJC870018), the Science and Technology Development Fund of Tianjin Education Commission for Higher Education (No. 2020KJ112, 2022KJ075, KYQD1817), the National Natural Science Foundation of China (Grant No. 12301670), the Natural Science Foundation of Tianjin (Grant No. 23JCQNJC00050), Haihe Lab. of Information Technology Application Innovation (No. 22HHXCJC00002), Fundamental Research Funds for the Central Universities, China (Grant No. ZY2301, BH2316), the Open Project of Tianjin Key Laboratory of Autonomous Intelligence Technology and Systems (No. TJKL-AITS-20241004, No. TJKL-AITS-20241006).

Conflict of interest

The authors declare no conflicts of interest.

References

1. L. Welch, Lower bounds on the maximum cross correlation of signals, *IEEE Trans. Inform. Theory*, **20** (1974), 397–399. https://doi.org/10.1109/TIT.1974.1055219
2. Z. Heng, C. Ding, Q. Yue, New constructions of asymptotically optimal codebooks with multiplicative characters, *IEEE Trans. Inform. Theory*, **63** (2017), 6179–6187. https://doi.org/10.1109/TIT.2017.2693204
3. G. Luo, X. Cao, Two constructions of asymptotically optimal codebooks, *Cryptogr. Commun.*, **11** (2019), 825–838. https://doi.org/10.1007/s12095-018-0331-4
4. G. Luo, X. Cao, Two constructions of asymptotically optimal codebooks via the hyper eisenstein sum, *IEEE Trans. Inform. Theory*, **64** (2018), 6498–6505. https://doi.org/10.1109/TIT.2017.2777492
5. Q. Wang, Y. Yan, Asymptotically optimal codebooks derived from generalised bent functions, *IEEE Access*, **8** (2020), 54905–54909. https://doi.org/10.1109/ACCESS.2020.2980330
6. Y. Yan, Y. Yao, Z. Chen, Q. Wang, Two new families of asymptotically optimal codebooks from characters of cyclic groups, *IEICE Trans. Fund. Electr.*, **E104** (2021), 1027–1032. https://doi.org/10.1587/transfun.2020EAP1124
7. W. Lu, X. Wu, X. Cao, Three constructions of asymptotically optimal codebooks via multiplicative characters of finite fields, *Adv. Math. Commun.*, **2022** (2022), 1–9. https://doi.org/10.3934/amc.2022091
8. Q. Wang, X. Liang, R. Jin, Y. Yan, Applications of strongly regular Cayley graphs to codebooks, *IEEE Access*, **11** (2023), 106980–106986. https://doi.org/10.1109/ACCESS.2023.3320559
9. C. Ding, Complex codebooks from combinatorial designs, *IEEE Trans. Inform. Theory*, **52** (2006), 4229–4235. https://doi.org/10.1109/TIT.2006.880058

10. P. Xia, S. Zhou, G. Giannakis, Achieving the Welch bound with difference sets, *IEEE Trans. Inform. Theory*, **51** (2005), 1900–1907. https://doi.org/10.1109/TIT.2005.846411

11. E. Candes, M. Wakin, An introduction to compressive sampling, *IEEE Signal Proc. Mag.*, **25** (2008), 21–30. https://doi.org/10.1109/MSP.2007.914731

12. S. Li, G. Ge, Deterministic sensing matrices arising from near orthogonal systems, *IEEE Trans. Inform. Theory*, **60** (2014), 2291–2302. https://doi.org/10.1109/TIT.2014.2303973

13. R. Lidl, H. Niederreiter, *Finite fields*, Cambridge: Cambridge University Press, 1997.

14. R. S. Coulter, Explicit evaluations of some Weil sums, *Acta Arith.*, **83** (1998), 241–251. https://doi.org/10.4064/aa-83-3-241-251

15. R. S. Coulter, Further evaluation of some Weil sums, *Acta Arith.*, **86** (1998), 217–226. https://doi.org/10.4064/aa-86-3-217-226

16. K. Conrad, Characters of finite abelian groups, Lecture Notes, Vol. 17, 2010. Available from: `https://kconrad.math.uconn.edu/blurbs/grouptheory/charthy.pdf`.

17. H. Hu, J. Wu, New constructions of codebooks nearly meeting the Welch bound with equality, *IEEE Trans. Inform. Theory*, **60** (2014), 1348–1355. https://doi.org/10.1109/TIT.2013.2292745

18. C. Li, Q. Yue, Y. Huang, Two families of nearly optimal codebooks, *Des. Codes Cryptogr.*, **75** (2015), 43–57. https://doi.org/10.1007/s10623-013-9891-7

19. L. Tian, Y. Li, T. Liu, C. Xu, Constructions of codebooks asymptotically achieving the welch bound with additive characters, *IEEE Signal Proc. Lett.*, **26** (2019), 622–626. https://doi.org/10.1109/LSP.2019.2891896