AIMS Mathematics, 9(7): 18236–18246.
DOI: 10.3934/math.2024890
Received: 01 February 2024
Revised: 15 May 2024
Accepted: 27 May 2024
Published: 30 May 2024

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

Research article

A class of nearly optimal codebooks and their applications in strongly regular Cayley graphs

Qiuyan Wang[1,2], Weixin Liu[1,*], Jianming Wang[1,2] and Yang Yan[3]

[1] School of Computer Science and Technology, Tiangong University, Tianjin 300387 China
[2] Tianjin Key Laboratory of Autonomous Intelligence Technology and Systems, Tiangong University, Tianjin 300387, China
[3] School of Information Technology and Engineering, Tianjin University of Technology and Education, Tianjin 300222 China

* **Correspondence:** Email: liuweixin@tiangong.edu.cn; Tel: +86-13194656595.

Abstract: Codebooks with small inner-product correlations are desirable in many fields, including compressed sensing, direct spread code division multiple access (CDMA) systems, and space-time codes. The objective of this paper is to present a class of codebooks and explore their applications in strongly regular Cayley graphs. The obtained codebooks are nearly optimal in the sense that their maximum cross-correlation amplitude nearly meets the Welch bound. As far as we know, this construction of codebooks provides new parameters.

Keywords: codebook; character; finite field; signal set; Welch bound
Mathematics Subject Classification: 94B05, 11T23, 11T24, 12E20

1. Introduction

To distinguish the signals between different users in CDMA communication systems, codebooks are required to have small inner-product correlation. An (N, K) codebook C is a vector set $\{\mathbf{c}_i\}_{i=0}^{N-1}$, where $\mathbf{c}_i$ is a unit norm $1 \times K$ complex vector over an alphabet A. As an important performance measure of a codebook, the maximum cross-correlation amplitude 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 $\mathbf{c}_j$. For a given K, it is preferable to construct codebooks with N being as large as possible and $I_{\max}(C)$ being minimal simultaneously. However, the Welch bound demonstrates that there is a tradeoff between N, K and $I_{\max}(C)$ of a codebook.

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

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

The equality in (1.1) *achieves if and only if*

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

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

If the equality in (1.1) holds, then C is called a maximum-Welch-bound-equality (MWBE) codebook. MWBE codebooks are applied in many practical fields, such as CDMA communications systems, compressed sensing and space-time codes. Unfortunately, it is very difficult to construct MWBE codebooks, and only a few MWBE codebooks are known in the literature [2–9]. Hence, a lot of attempts are made to construct codebooks which nearly meet the Welch bound, i.e., $\lim_{N\to+\infty} I_{\max}(C)/I_w(C) = 1$ for an (N, K) codebook C with $N \geq K$. Many classes of known nearly optimal codebooks have been produced for the past few years [10–18].

In this paper, we are concerned with two purposes. The first objective is to give a new construction of codebooks which are nearly optimal with respect to the Welch bound. The other objective is to provide a new construction of strongly regular Cayley graphs using the set D in (3.1). It should be pointed out that these presented codebooks have new parameters.

This paper is arranged as follows. Some basic definitions and results on exponential sums are given in Sect. II. The constructions of nearly optimal codebooks and strongly regular Cayley graphs are ordered in Sect. III. We make a conclusion in Sect. IV.

2. Preliminaries

In this section, we present some basic concepts and a number of lemmas on exponential sums. Some symbols and notations are given as follows.

- m_1 and m_2 are two integers.
- $n_1 = p^{m_1} + 1$ and $n_2 = p^{m_2} + 1$.
- $q_1 = p^{2m_1}$, $q_2 = p^{2m_2}$ and p is an odd prime.
- $\zeta_p = e^{\frac{2\pi\sqrt{-1}}{p}}$ is a primitive p-th root of unity.
- Tr_1 denotes the trace function from $\mathbb{F}_{q_1}$ to $\mathbb{F}_p$.
- Tr_2 denotes the trace function from $\mathbb{F}_{q_2}$ to $\mathbb{F}_p$.
- χ_1 denotes the canonicial additive character of $\mathbb{F}_p$.
- η_1 denotes the quadratic character of $\mathbb{F}_p$.

Let G be a finite Abelian group with order n, and U be the multiplicative group of complex numbers of absolute value 1. A character χ of G is a homomorphism from G to U with $\chi(ab) = \chi(a)\chi(b)$ for all $a, b \in G$. Given two characters χ, $\chi^{'}$ of G, we can get a product character $\chi\chi^{'}$ by letting $\chi\chi^{'}(a) = \chi(a)\chi^{'}(a)$ for all $a \in G$. It can be easily seen that the set $G^{\wedge}$ consisting of all characters of G forms an Abelian group under the multiplication of characters.

Let p be an odd prime and $q = p^n$ with $n \in \mathbb{N}$. Let $\mathbb{F}_q$ be the finite field with q elements and Tr the trace function from $\mathbb{F}_q$ to $\mathbb{F}_p$. For a finite field $\mathbb{F}_q$, there are two finite abelian groups, i.e., the additive group $\mathbb{F}_q^+$ and the multiplicative group $\mathbb{F}_q^*$ of $\mathbb{F}_q$. In both cases, explicit formulas for the characters are given as follows.

Definition 1. *The canonical additive character of $\mathbb{F}_q^+$ is defined by $\chi(x) = \zeta_p^{\mathrm{Tr}(x)}$ for all $x \in \mathbb{F}_q$. For $b \in \mathbb{F}_q$, the function μ_b with $\mu_b(x) = \chi(bx)$ is an additive character of $\mathbb{F}_q$ and every additive character of $\mathbb{F}_q$ can be obtained in this way.*

Definition 2. *Let α be a fixed primitive element of $\mathbb{F}_q^*$. For each $0 \le j \le q-2$, the function φ_j with*

$$\varphi_j(\alpha^i) = \zeta_{q-1}^{ij} \text{ for } i = 0, 1, \ldots, q-2,$$

defines a multiplicative character of $\mathbb{F}_q^*$. For $j = (q-1)/2$, the character $\varphi_{(q-1)/2}$, denoted by η, is called the quadratic character of $\mathbb{F}_q$ and is extended by setting $\eta(0) = 0$.

The Gauss sum $G(\eta, \chi)$ over $\mathbb{F}_q$ is defined by

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

The explicit values of $G(\eta, \chi)$ are determined in [19].

Lemma 2. *([19], Theorem 5.15) With the symbols and notations above, we have*

$$G(\eta, \chi) = (-1)^{n-1}(-1)^{\frac{(p-1)n}{4}}\sqrt{q}.$$

Briefly, we use $G(\eta)$ to denote $G(\eta, \chi)$. The following identities on Gauss sums will be employed in the sequel.

Lemma 3. *(Theorem* 5.12*, [19]) For $y \in \mathbb{F}_q$, we obtain*

$$\sum_{z \in \mathbb{F}_q^*} \eta(z)\zeta_p^{\mathrm{Tr}(zy)} = \begin{cases} 0, & \text{if } y = 0, \\ G(\eta)\eta(y), & \text{if } y \in \mathbb{F}_q^*. \end{cases}$$

Gauss sums are the most significant types of exponential sums, since they govern the transition from the multiplicative to the additive structure.

Lemma 4. *([19], p.195) With the symbols and notations above, we have*

$$\eta(x) = \frac{1}{q}\sum_{z \in \mathbb{F}_q} G(\eta)\eta(-z)\chi(zx) \text{ for all } x \in \mathbb{F}_q.$$

The following several lemmas are useful in the next section.

Lemma 5. *([20]) Let $n = 2m$ for a positive integer m and $N = p^m + 1$ for an odd prime p. Assume $z \in \mathbb{F}_p^*$ and $a \in \mathbb{F}_q$. Then*

$$\sum_{x\in\mathbb{F}_q} \zeta_p^{\mathrm{Tr}\left(zx^N\right)+\mathrm{Tr}(ax)} = -p^m \zeta_p^{-\mathrm{Tr}\left(\frac{a^N}{4z}\right)}.$$

Lemma 6. *([21], Theorem 2) Assume that $n = 2m$ for a positive integer m and $N = p^m + 1$ for an odd prime p. For $z \in \mathbb{F}_p^*$, we have*

$$\sum_{x\in\mathbb{F}_q} \zeta_p^{z\,\mathrm{Tr}\left(x^N\right)} = -p^m.$$

Lemma 7. *([22], Lemma 3.12) Let $\mathbb{F}_{q_1}$ and $\mathbb{F}_{q_2}$ denote the finite fields with q_1 and q_2 elements, respectively. Then there is an isomorphism*

$$\left(\mathbb{F}_{q_1}^+ \times \mathbb{F}_{q_2}^+\right)^\wedge \cong (\mathbb{F}_{q_1}^+)^\wedge \times (\mathbb{F}_{q_2}^+)^\wedge.$$

From this lemma, we know

$$\left(\mathbb{F}_{q_1}^+ \times \mathbb{F}_{q_2}^+\right)^\wedge = \left\{\mu_{a,b} : a \in \mathbb{F}_{q_1}, b \in \mathbb{F}_{q_1}\right\},$$

where $\mu_{a,b}(x, y) = \zeta_p^{\mathrm{Tr}_1(ax)+\mathrm{Tr}_2(by)}$ for $(x, y) \in \mathbb{F}_{q_1} \times \mathbb{F}_{q_2}$.

3. Proofs and main results

In this section, we give a construction of nearly optimal codebooks, introduce their parameters and give the proofs. Then we analyse the strongly regular Cayley graphs derived from the presented codebooks.

Define

$$D = \left\{(x, y) \in \mathbb{F}_{q_1} \times \mathbb{F}_{q_2} : \mathrm{Tr}_1(x^{n_1}) + \mathrm{Tr}_2(y^{n_2}) \in \mathbb{F}_p^{*2}\right\}, \tag{3.1}$$

where $\mathbb{F}_p^{*2} = \langle\beta^2\rangle$ and β is a primitive element of $\mathbb{F}_p^*$.

The codebook C_D is given by

$$C_D = \left\{\mathbf{c}_{a,b} : a \in \mathbb{F}_{q_1}, b \in \mathbb{F}_{q_2}\right\}, \tag{3.2}$$

where

$$\mathbf{c}_{a,b}(x, y) = \frac{1}{\sqrt{|D|}} \left(\mu_{a,b}(x, y)\right)_{(x,y)\in D},$$
$$\mu_{a,b}(x, y) = \zeta_p^{\mathrm{Tr}_1(ax)+\mathrm{Tr}_2(by)},$$

and $|D|$ denotes the cardinality of the set D.

To prove the main results of this paper, we introduce the sets E and F, which are defined by (3.3) and (3.4), respectively. Let

$$E = \left\{(x, y) \in \mathbb{F}_{q_1} \times \mathbb{F}_{q_2} : \mathrm{Tr}_1(x^{n_1}) + \mathrm{Tr}_2(y^{n_2}) \neq 0\right\}, \tag{3.3}$$

$$F = \left\{(x, y) \in \mathbb{F}_{q_1} \times \mathbb{F}_{q_2} : \mathrm{Tr}_1(x^{n_1}) + \mathrm{Tr}_2(y^{n_2}) = 0\right\}. \tag{3.4}$$

Regarding the set D, we have the following two lemmas.

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

$$|D| = \frac{1}{2}(p-1)\left(p^{2m_1+2m_2-1} - p^{m_1+m_2-1}\right).$$

Proof. From Lemma 6, we obtain

$$\begin{aligned} |F| &= \frac{1}{p}\sum_{z\in\mathbb{F}_p}\sum_{x\in\mathbb{F}_{q_1}}\zeta_p^{\mathrm{Tr}_1(zx^{n_1})}\sum_{y\in\mathbb{F}_{q_2}}\zeta_p^{\mathrm{Tr}_2(zy^{n_2})} \\ &= p^{2m_1+2m_2-1} + \frac{1}{p}\sum_{z\in\mathbb{F}_p^*}(-p^{m_1})(-p^{m_2}) \\ &= p^{2m_1+2m_2-1} + (p-1)p^{m_1+m_2-1}. \end{aligned}$$

Hence, we have

$$|E| = \sum_{x\in\mathbb{F}_{q_1},y\in\mathbb{F}_{q_2}} 1 - |F| = (p-1)\left(p^{2m_1+2m_2-1} - p^{m_1+m_2-1}\right). \tag{3.5}$$

It can be easily checked that

$$\begin{aligned} |D| &= \sum_{(x,y)\in E}\frac{\eta_1\left(\mathrm{Tr}_1\left(x^{n_1}\right)+\mathrm{Tr}_2\left(y^{n_2}\right)\right)+1}{2} \\ &= \frac{1}{2}\sum_{(x,y)\in E}1 + \frac{1}{2}\sum_{x\in\mathbb{F}_{q_1},y\in\mathbb{F}_{q_2}}\eta_1\left(\mathrm{Tr}_1\left(x^{n_1}\right)+\mathrm{Tr}_2\left(y^{n_2}\right)\right). \end{aligned} \tag{3.6}$$

By Lemma 4, we obtain

$$\begin{aligned} \sum_{x\in\mathbb{F}_{q_1},y\in\mathbb{F}_{q_2}}\eta_1\left(\mathrm{Tr}_1\left(x^{n_1}\right)+\mathrm{Tr}_2\left(y^{n_2}\right)\right) &= \frac{1}{p}\sum_{x\in\mathbb{F}_{q_1},y\in\mathbb{F}_{q_2}}\sum_{z\in\mathbb{F}_p}G(\eta_1)\eta_1(-z)\chi_1\left(z\,\mathrm{Tr}_1(x^{n_1})+z\,\mathrm{Tr}_2(x^{n_2})\right) \\ &= \frac{G(\eta_1)}{p}\sum_{z\in\mathbb{F}_p^*}\eta_1(-z)(-p^{m_1})(-p^{m_2}), \end{aligned}$$

where the last equality follows from Lemma 6. From the fact that $\sum_{z\in\mathbb{F}_p^*}\eta_1(z) = 0$, we have

$$\sum_{x\in\mathbb{F}_{q_1},y\in\mathbb{F}_{q_2}}\eta_1\left(\mathrm{Tr}_1\left(x^{n_1}\right)+\mathrm{Tr}_2\left(y^{n_2}\right)\right) = 0. \tag{3.7}$$

Then the desired conclusion follows from (3.5)–(3.7). □

Example 1. *Let $p = 5$ and $(m_1, m_2) = (2, 1)$. By the Magma program, we get that the cardinality $|D|$ of the set D is* 6200*, which accords with Lemma 8.*

Example 2. *Let $p = 7$ and $(m_1, m_2) = (2, 2)$. By Lemma 8, we get $|D| =$* 2469600*, which is consistent with the numerical computation by Magma.*

Lemma 9. *For $(a,b) \in \mathbb{F}_{q_1} \times \mathbb{F}_{q_2}$ and $(a,b) \neq (0,0)$, we have*

$$\sum_{(x,y)\in D} \mu_{a,b}(x,y) = \begin{cases} -\frac{1}{2}p^{m_1+m_2-1}(p-1), & \text{if } \mathrm{Tr}_1(a^{n_1}) + \mathrm{Tr}_2(b^{n_2}) = 0, \\ \frac{1}{2}p^{m_1+m_2-1} + \frac{1}{2}(-1)^{\frac{p-1}{2}}p^{m_1+m_2}, & \text{if } \mathrm{Tr}_1(a^{n_1}) + \mathrm{Tr}_2(b^{n_2}) \in \mathbb{F}_p^{*2}, \\ \frac{1}{2}p^{m_1+m_2-1} - \frac{1}{2}(-1)^{\frac{p-1}{2}}p^{m_1+m_2}, & \text{if } \mathrm{Tr}_1(a^{n_1}) + \mathrm{Tr}_2(b^{n_2}) \in \mathbb{F}_p^* \setminus \mathbb{F}_p^{*2}. \end{cases}$$

Proof. By definition, we have

$$\sum_{(x,y)\in D} \mu_{a,b}(x,y) = \sum_{(x,y)\in E} \frac{\eta_1(\mathrm{Tr}_1(x^{n_1}) + \mathrm{Tr}_2(y^{n_2})) + 1}{2} \zeta_p^{\mathrm{Tr}_1(ax)+\mathrm{Tr}_2(by)},$$

where the set E is given in (3.3). Note that

$$\sum_{x\in\mathbb{F}_{q_1}, y\in\mathbb{F}_{q_2}} \zeta_p^{\mathrm{Tr}_1(ax)+\mathrm{Tr}_2(by)} = 0,$$

if $(a,b) \in \mathbb{F}_{q_1} \times \mathbb{F}_{q_2} \setminus \{(0,0)\}$. Hence, we get

$$\sum_{(x,y)\in D} \mu_{a,b}(x,y) = -\frac{1}{2} \sum_{(x,y)\in F} \zeta_p^{\mathrm{Tr}_1(ax)+\mathrm{Tr}_2(by)} + \frac{1}{2} \sum_{x\in\mathbb{F}_{q_1}, y\in\mathbb{F}_{q_2}} \eta_1(\mathrm{Tr}_1(x^{n_1}) + \mathrm{Tr}_2(y^{n_2}))\zeta_p^{\mathrm{Tr}_1(ax)+\mathrm{Tr}_2(by)}, \tag{3.8}$$

where the set F is given in (3.4). Together with Lemma 5, we derive

$$\begin{aligned} \sum_{(x,y)\in F} \zeta_p^{\mathrm{Tr}_1(ax)+\mathrm{Tr}_2(by)} &= \frac{1}{p} \sum_{x\in\mathbb{F}_{q_1}, y\in\mathbb{F}_{q_2}} \zeta_p^{\mathrm{Tr}_1(ax)+\mathrm{Tr}_2(by)} \sum_{z\in\mathbb{F}_p} \zeta_p^{z\,\mathrm{Tr}_1(x^{n_1})+z\,\mathrm{Tr}_2(y^{n_2})} \\ &= \frac{1}{p} \sum_{z\in\mathbb{F}_p^*} \sum_{x\in\mathbb{F}_{q_1}} \zeta_p^{\mathrm{Tr}_1(zx^{n_1}+ax)} \sum_{y\in\mathbb{F}_{q_2}} \zeta_p^{\mathrm{Tr}_2(zy^{n_2}+by)} \\ &= p^{m_1+m_2-1} \sum_{z\in\mathbb{F}_p^*} \zeta_p^{-\mathrm{Tr}_1\left(\frac{a^{n_1}}{4z}\right)-\mathrm{Tr}_2\left(\frac{b^{n_2}}{4z}\right)}. \end{aligned}$$

For $z \in \mathbb{F}_p^*$, from the map $-\frac{1}{4z} \to z$, we get

$$\begin{aligned} \sum_{(x,y)\in F} \zeta_p^{\mathrm{Tr}_1(ax)+\mathrm{Tr}_2(by)} &= p^{m_1+m_2-1} \sum_{z\in\mathbb{F}_p^*} \zeta_p^{z(\mathrm{Tr}_1(a^{n_1})+\mathrm{Tr}_2(b^{n_2}))} \\ &= \begin{cases} p^{m_1+m_2-1}(p-1), & \text{if } \mathrm{Tr}_1(a^{n_1}) + \mathrm{Tr}_2(b^{n_2}) = 0, \\ -p^{m_1+m_2-1}, & \text{if } \mathrm{Tr}_1(a^{n_1}) + \mathrm{Tr}_2(b^{n_2}) \neq 0. \end{cases} \end{aligned} \tag{3.9}$$

From Lemma 4, we obtain

$$\begin{aligned} &\sum_{x\in\mathbb{F}_{q_1}, y\in\mathbb{F}_{q_2}} \eta_1(\mathrm{Tr}_1(x^{n_1}) + \mathrm{Tr}_2(y^{n_2}))\zeta_p^{\mathrm{Tr}_1(ax)+\mathrm{Tr}_2(by)} \\ =&\frac{1}{p} \sum_{x\in\mathbb{F}_{q_1}, y\in\mathbb{F}_{q_2}} \zeta_p^{\mathrm{Tr}_1(ax)+\mathrm{Tr}_2(by)} \sum_{z\in\mathbb{F}_p} G(\eta_1)\eta_1(-z)\chi_1(\mathrm{Tr}_1(zx^{n_1}) + \mathrm{Tr}_2(zy^{n_2})) \\ =&\frac{G(\eta_1)}{p} \sum_{z\in\mathbb{F}_p^*} \eta_1(-z) \sum_{x\in\mathbb{F}_{q_1}} \zeta_p^{\mathrm{Tr}_1(zx^{n_1}+ax)} \sum_{y\in\mathbb{F}_{q_2}} \zeta_p^{\mathrm{Tr}_2(zy^{n_2}+by)} \end{aligned}$$

$$=\frac{G(\eta_1)}{p}\sum_{z\in\mathbb{F}_p^*}\eta_1(-z)\left(-p^{m_1}\zeta_p^{-\mathrm{Tr}_1\left(\frac{a^{n_1}}{4z}\right)}\right)\left(-p^{m_2}\zeta_p^{-\mathrm{Tr}_2\left(\frac{b^{n_2}}{4z}\right)}\right),$$

where the last equality follows from Lemma 5. For $z \in \mathbb{F}_p^*$, from the map $-\frac{1}{4z} \to z$, we get

$$\begin{aligned}
&\sum_{x\in\mathbb{F}_{q_1},y\in\mathbb{F}_{q_2}}\eta_1\left(\mathrm{Tr}_1\left(x^{n_1}\right)+\mathrm{Tr}_2\left(y^{n_2}\right)\right)\zeta_p^{\mathrm{Tr}_1(ax)+\mathrm{Tr}_2(by)}\\
&=p^{m_1+m_1-1}G(\eta_1)\sum_{z\in\mathbb{F}_p^*}\eta_1(z)\zeta_p^{z(\mathrm{Tr}_1(a^{n_1})+\mathrm{Tr}_2(b^{n_2}))}\\
&=\begin{cases}0, & \text{if } \mathrm{Tr}_1\left(a^{n_1}\right)+\mathrm{Tr}_2\left(b^{n_2}\right)=0,\\ (-1)^{\frac{p-1}{2}}p^{m_1+m_2}\eta_1\left(\mathrm{Tr}_1\left(a^{n_1}\right)+\mathrm{Tr}_2\left(b^{n_2}\right)\right), & \text{if } \mathrm{Tr}_1\left(a^{n_1}\right)+\mathrm{Tr}_2\left(b^{n_2}\right)\neq 0,\end{cases}
\end{aligned} \tag{3.10}$$

where the last equality follows from Lemmas 2 and 3. The desired conclusion follows from (3.8)–(3.10). □

Theorem 10. *Let*

$$K=\frac{1}{2}(p-1)\left(p^{2m_1+2m_2-1}-p^{m_1+m_2-1}\right). \tag{3.11}$$

Then the set C_D defined in (3.2) *is a $[p^{2m_1+2m_2}, K]$ codebook with $I_{\max}(C_D) = p^{m_1+m_2-1}(p+1)/(2K)$.*

Proof. From the definition of the codebook C_D and Lemma 8, we deduce that C_D is a $[p^{2m_1+2m_2}, K]$ codebook. Given two codewords $\mathbf{c}_{a,b}$ and $\mathbf{c}_{c,d}$ with $(a-c, b-d) \neq (0,0)$, we have

$$\left|\mathbf{c}_{a,b}\mathbf{c}_{c,d}^H\right|=\frac{1}{K}\left|\sum_{(x,y)\in D}\mu_{a-c,b-d}(x,y)\right|.$$

By Lemma 9, we obtain that

$$\left|\mathbf{c}_{a,b}\mathbf{c}_{c,d}^H\right|\in\left\{\frac{1}{2K}p^{m_1+m_2-1}(p+1),\frac{1}{2K}p^{m_1+m_2-1}(p-1)\right\}.$$

Hence, we have

$$I_{\max}(C_D)=\frac{p^{m_1+m_2-1}(p+1)}{2K}.$$

□

Theorem 11. *The codebook C_D constructed in Theorem 10 is nearly optimal with respect to the Welch bound.*

Proof. By Theorem 10, we derive that

$$I_w(C_D)=\sqrt{\frac{p^{m_1+m_2+1}+p^{m_1+m_2}+p-1}{(p-1)\left(p^{m_1+m_2}-1\right)\left(p^{2m_1+2m_2}-1\right)}}.$$

Therefore, we deduce that

$$\frac{I_{\max}(C_D)}{I_w(C_D)} = \sqrt{\frac{(p+1)^2(p^{m_1+m_2}+1)}{(p-1)(p^{m_1+m_2+1}+p^{m_1+m_2}+p-1)}}.$$

Obviously,

$$\lim_{p\to+\infty} \frac{I_{\max}(C_D)}{I_w(C_D)} = 1,$$

which implies that C_D is nearly optimal with respect to the Welch bound. □

Table 1 lists some parameters of the codebooks defined in (3.2). From this table, we can derive that $I_{\max}(C_D)$ is very close to $I_w(C_D)$, as the odd prime p increases. This accords with Theorems 10 and 11 and also guarantees the correctness of our main results.

Table 1. The parameters of the codebook C_D in (3.2).

p	(m_1, m_2)	N	K	$I_{\max}(C)$	$I_w(C)$	$I_{\max}/I_w$
3	(1,1)	3^4	24	1/4	1.7230×10^{-1}	1.4600
5	(2,1)	5^6	6200	3/248	9.8639×10^{-3}	1.2264
5	(2,2)	5^8	156000	1/416	1.9622×10^{-3}	1.2251
7	(3,2)	7^{10}	121053618	2/25209	6.8707×10^{-5}	1.1547
11	(3,3)	11^{12}	1426557547800	1/1476300	6.1835×10^{-7}	1.0954
13	(5,5)	13^{20}	$6(13^{19}-13^9)$	1/118164421584	7.8350×10^{-12}	1.0801
17	(6,6)	17^{24}	$8(17^{23}-17^{11})$	1/517886433093120	1.8205×10^{-15}	1.0607

For $(p, m_1, m_2) = (199, 6, 6)$, it can be easily checked that $I_{\max}/I_w = 1.0050$. This implies that the ratio $I_{\max}/I_w$ is much closer to 1, if p is a larger prime.

Motivated by the work in [23], we use the set D defined in (3.1) to give a construction of strongly regular Cayley graphs. The definition of strongly regular graphs is given below.

Definition 3. *([4]) A strongly regular graph (v, k, λ, μ) is a graph with v vertices which is not complete or edgeless and which has the following properties:*

(1) The graph is regular of valency k, i.e., each vertex is adjacent to k vertices.

(2) There are exactly λ vertices adjacent to both x and y, if x and y are two adjacent vertices.

(3) There are exactly μ vertices adjacent to both x and y, if x and y are two nonadjacent vertices.

One of the most efficient approaches to construct strongly regular graphs is the Cayley graph construction. Let G be a finite Abelian group and D be a subset of G satisfying that $0 \notin D$ and $-D = \{-d : d \in D\} = D$. The Cayley graph on G with connection set D, written as $\mathrm{Cay}(G, D)$, is the graph with the elements of G as vertices; two vertices x and y are adjacent if and only if $x - y \in D$.

For the set D given in (3.1), it is clear that $0 \notin D$ and $-D = D$. Here and hereafter, we use $\mathrm{Cay}(\mathbb{F}_{q_1}\times\mathbb{F}_{q_2}, D)$ to denote the Cayley graph on $\mathbb{F}_{q_1}\times\mathbb{F}_{q_2}$ with connection set D. For $(a, b) \in \mathbb{F}_{q_1}\times\mathbb{F}_{q_2}$, let

$$\mu_{a,b}(D) = \sum_{(x,y)\in D} \mu_{a,b}(x, y),$$

where $\mu_{a,b} \in \left(\mathbb{F}_{q_1} \times \mathbb{F}_{q_2}\right)^{\wedge}$. The eigenvalues of $\mathrm{Cay}(\mathbb{F}_{q_1} \times \mathbb{F}_{q_2}, D)$ are defined by $\mu_{a,b}(D)$. When $(a,b) = (0,0)$, we have $\mu_{0,0}(D) = |D| = K$, which is called the trivial eigenvalue of $\mathrm{Cay}(\mathbb{F}_{q_1} \times \mathbb{F}_{q_2}, D)$. It is known that $\mathrm{Cay}(\mathbb{F}_{q_1} \times \mathbb{F}_{q_2}, D)$ is strongly regular if and only if $\mu_{a,b}(D)$ with $(a,b) \neq (0,0)$ has exactly two distinct values.

Theorem 12. *Let D be the set given in* (3.1)*, and K is the integer given in* (3.11)*. Then we have*

(1) $Cay(\mathbb{F}_{q_1} \times \mathbb{F}_{q_2}, D)$ has two distinct nontrivial eigenvalues, $p^{m_1+m_2-1}(1+p)/2$ and $p^{m_1+m_2-1}(1-p)/2$.

(2) $Cay(\mathbb{F}_{q_1} \times \mathbb{F}_{q_2}, D)$ is strongly regular with parameters

$$\left(p^{2m_1+2m_2}, K, \frac{1}{4}p^{m_1+m_2-1}\left(p^{m_1+m_2-1}(1-p)^2 - 2p + 6\right), \frac{1}{4}p^{m_1+m_2-1}\left(p^{m_1+m_2-1}(1-p)^2 - 2p + 2\right)\right).$$

Proof. (1) By Lemma 9, we know

$$\mu_{a,b}(D) = \frac{1}{2}p^{m_1+m_2-1}(1+p) \text{ or } \mu_{a,b}(D) = \frac{1}{2}p^{m_1+m_2-1}(1-p),$$

for $(a,b) \in \mathbb{F}_{q_1} \times \mathbb{F}_{q_2} \setminus \{(0,0)\}$. This implies that $\mathrm{Cay}(\mathbb{F}_{q_1} \times \mathbb{F}_{q_2}, D)$ has precisely two distinct nontrivial eigenvalues $p^{m_1+m_2-1}(1+p)/2$ and $p^{m_1+m_2-1}(1-p)/2$.

(2) From the definition of $\mathrm{Cay}(\mathbb{F}_{q_1} \times \mathbb{F}_{q_2}, D)$ and the first part of this theorem, we get that $\mathrm{Cay}(\mathbb{F}_{q_1} \times \mathbb{F}_{q_2}, D)$ has $p^{2m_1+2m_2}$ vertices and $\mathrm{Cay}(\mathbb{F}_{q_1} \times \mathbb{F}_{q_2}, D)$ is regular of valency $|D|$. Let k denote the valency of $\mathrm{Cay}(\mathbb{F}_{q_1} \times \mathbb{F}_{q_2}, D)$. Then

$$k = |D| = \frac{1}{2}(p-1)\left(p^{2m_1+2m_2-1} - p^{m_1+m_2-1}\right).$$

Let r and s denote the two nontrivial eigenvalues of $\mathrm{Cay}(\mathbb{F}_{q_1} \times \mathbb{F}_{q_2}, D)$. By Theorem 9.1.2 in [24], the parameters λ and μ of the strongly regular graph can be computed by $\lambda = s + r + k + sr$ and $\mu = k + sr$. Then the second part of this theorem follows. □

As a comparison, the parameters of some known strongly regular graphs and the newly presented ones are listed in Table 2.

Table 2. The parameters of some strongly regular graphs.

(p, m_1, m_2)	v	k	λ	μ	r	s	References
	81	16	7	2	7	-2	[25]
(3,1,1)	81	24	9	6	6	-3	Theorem 12
	14080	3159	918	648	279	-9	[25]
(5,2,1)	15625	6200	2475	2450	75	-50	Theorem 12

4. Conclusions

In this paper, a class of codebooks is constructed using the combination of the quadratic character over $\mathbb{F}_p$ and the trace functions over finite fields. Main results show that they are nearly optimal with respect to the Welch bound. Their applications in Cayley graphs are investigated and a kind of strongly regular Cayley graphs is obtained by the use of set D. Some interesting nearly optimal codebooks were presented in [10, 12–18]. The parameters of the codebooks obtained in this paper were not found in the literature. This means that C_D has new parameters.

Author contributions

The authors contributed equally to the writing of this paper. All authors have read and agreed to the published version of the manuscript.

Use of AI tools declaration

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

Acknowledgments

This work is supported by the 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, KYQD1817), and Science and Technology Project of Putian City (No. 2021R4001-10), Haihe Lab. of Information Technology Application Innovation (No. 22HHXCJC00002), 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 T. Inform. Theory*, **20** (1974), 397–399. https://doi.org/10.1109/TIT.1974.1055219
2. J. H. Conway, R. H. Harding, N. J. A. Sloane, Packing lines, planes, etc.: Packings in Grassmannian spaces, *Exp. Math.*, **5** (1996), 139–159. https://doi.org/10.1080/10586458.1996.10504585
3. C. Ding, Complex codebooks from combinatorial designs, *IEEE T. Inform. Theory*, **52** (2006), 4229–4235. https://doi.org/10.1109/TIT.2006.880058
4. M. Fickus, D. G. Mixon, J. Jasper, Equiangular tight frames from hyperovals, *IEEE T. Inform. Theory*, **62** (2016), 5225–5236. https://doi.org/10.1109/TIT.2016.2587865
5. M. Fickus, D. G. Mixon, J. C. Tremain, Steiner equiangular tight frames, *Linear Algebra Appl.*, **436** (2012), 1014–1027. https://doi.org/10.1016/j.laa.2011.06.027
6. F. Rahimi, Covering graphs and equiangular tight frames, *Univ. Waterloo*, 2016. Available from: `http://hdl.handle.net/10012/10793`
7. D. Sarwate, Meeting the Welch bound with equality, *Sequences their Appl.*, 1999, 63–79. Available from: `https://link.springer.com/chapter/10.1007/978-1-4471-0551-0_6`
8. T. Strohmer, J. R. W. Heath, Grassmannian frames with applications to coding and communication, *Appl. Comput. Harmon. Anal.*, **14** (2003), 257–275. https://doi.org/10.1016/S1063-5203(03)00023-X

9. P. Xia, S. Zhou, G. Giannakis, Achieving the Welch bound with difference sets, *IEEE T. Inf. Theory*, **51** (2005), 1900–1907. https://doi.org/10.1109/TIT.2005.846411
10. S. Hong, H. Park, T. Helleset, Y. Kim, Near optimal partial Hadamard codebook construction using binary sequences obtained from quadratic residue mapping, *IEEE T. Inf. Theory*, **60** (2014), 3698–3705. https://doi.org/10.1109/TIT.2014.2314298
11. Z. Heng, C. Ding, Q. Yue, New constructions of asymptotically optimal codebooks with multiplicative characters, *IEEE T. Inf. Theory*, **63** (2017), 6179–6187. https://doi.org/10.1109/TIT.2017.2693204
12. H. Hu, J. Wu, New constructions of codebooks nearly meeting the Welch bound with equality, *IEEE T. Inf. Theory,* **60** (2014), 1348–1355. https://doi.org/10.1109/TIT.2013.2292745
13. G. Luo, X. Cao, Two constructions of asymptotically optimal codebooks via the hyper eisenstein sum, *IEEE T. Inf. Theory*, **64** (2018), 6498–6505. https://doi.org/10.1109/TIT.2017.2777492
14. S. Satake, Y. Gu, Constructions of complex codebooks asymptotically meeting the Welch bound: A graph theoretic approach, *IEEE Int. Symposium Inf. Theory*, 2020, 48–53. 10.1109/ISIT44484.2020.9174496
15. X. Wu, W. Lu, X. Cao, Two constructions of asymptotically optimal codebooks via the trace functions, *Cryptogr. Commun.*, **12** (2020), 1195–1211. https://doi.org/10.1007/s12095-020-00448-w
16. 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
17. Y. Yan, Y. Yao, Z. Chen, Q. Wang, Two new families of asymptotically optimal codebooks from characters of cyclic groups, *IEICE Trans. Fundament. Electr. Commun. Comput. Sci.*, **E104** (2021), 1027–1032. https://doi.org/10.1587/transfun.2020EAP1124
18. N. Yu, A construction of codebooks associated with binary sequences, *IEEE T. Inf. Theory,* **58** (2012), 5522–5533. https://doi.org/10.1109/TIT.2012.2196021
19. R. Lidl, H. Niederreiter, *Finite fields*, Cambridge: Cambridge University Press, 1997. Available from: `https://dl.acm.org/doi/10.5555/248301`
20. R. S. Coulter, Further evaluation of some Weil sums, *Acta Arith.*, **86** (1998), 217–226. Available from: `http://matwbn.icm.edu.pl/ksiazki/aa/aa86/aa8633.pdf`
21. R. S. Coulter, Explicit evaluations of some Weil sums, *Acta Arith.*, **83** (1998), 241–251. Available from: `http://matwbn.icm.edu.pl/ksiazki/aa/aa83/aa8334.pdf`
22. K. Conrad, Characters of finite abelian groups, *Lect. Notes*, **17** (2010). Available from: `https://kconrad.math.uconn.edu/blurbs/grouptheory/charthy.pdf`
23. 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
24. A. E. Brouwer, W. H. Haemers, *Spectra of graphs*, Springer Science & Business Media, 2011.
25. **Online content:** *Parameters of Strongly Regular Graphs*, Eindhoven: The University, 2024. Available from: `https://www.win.tue.nl/~aeb/graphs/srg/srgtab.html`

AIMS Press