Mathematics

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

AIMS Mathematics, 9(2): 2672–2683.
DOI: 10.3934/math.2024132
Received: 15 November 2023
Revised: 12 December 2023
Accepted: 21 December 2023
Published: 27 December 2023

Research article

A construction of strongly regular Cayley graphs and their applications to codebooks

Yang Yan[1], **Xingguo Zhang**[2,3,*], **Rize Jin**[4,5] **and Limin Zhou**[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] School of Humanities, Tiangong University, Tianjin 300387, China

[4] School of Software, Tiangong University, Tianjin 300387, China

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

[6] Department of Mathematics, Binzhou University, Binzhou 256600, Shandong Province, China

* **Correspondence:** Email: zhangxingguo@tiangong.edu.cn; Tel: +86-13920918713.

Abstract: In this paper, we give a kind of strongly regular Cayley graphs and a class of codebooks. Both constructions are based on choosing subsets of finite fields, and the main tools that we employed are Gauss sums. In particular, these obtained codebooks are asymptotically optimal with respect to the Welch bound and they have new parameters.

Keywords: codebooks; strongly regular Cayley graphs; finite fields; Gauss sums; Welch bound
Mathematics Subject Classification: 94B05, 11T23, 11T24, 12E20

1. Introduction

Let Γ be a strongly regular graph with v vertices and parameters k, λ and μ. Then Γ is defined as follows: (1) For any two adjacent vertices x and y, there are exactly λ vertices adjacent to both x and y; (2) for any two nonadjacent vertices x and y, there are exactly μ vertices adjacent to both x and y. For a more detailed introduction on strongly regular graphs, please refer to [1, 2].

Cayley graphs are an effective tool constructing strongly regular graphs. Let $(G, +)$ be a finite abelian group and S be a subset of $G \setminus \{0\}$ such that $S = -S$, where 0 is the identity of G. The Cayley graph $\mathrm{Cay}(G, S)$ is defined as the graph $\Gamma(G, E)$ where two vertices a and b are adjacent if and only if $a - b \in S$. Let $\widehat{G}$ be the character group of G consisting of all characters of G. The eigenvalues of $\mathrm{Cay}(G, S)$ are given by $\phi(S) = \sum_{x \in S} \phi(x)$, where $\phi \in \widehat{G}$. It is well known that $\mathrm{Cay}(G, S)$ is strongly regular if and only if $\phi(S)$ with $\phi \in \widehat{G} \setminus \{1_{\widehat{G}}\}$ take exactly two values, where $1_{\widehat{G}}$ is the identity of $\widehat{G}$. By the determination of Cayley graphs in the additive groups of finite fields, strongly regular cayley graphs were proposed in [3–6].

It should be noted that strongly regular graphs are related to some combinational objects, such as linear codes, two-intersection sets and partial difference set [7, 8]. For these connections, we are inspired to construct asymptotically optimal codebooks by using the connection set S of $\mathrm{Cay}(G, S)$. An (N, K) codebook C is defined to be a set $\{\mathbf{c}_i\}_{i=0}^{N-1}$ of N units norm $1 \times K$ complex vectors $\mathbf{c}_i$, and $\mathbf{c}_i$ $(0 \le i \le N-1)$ are called codewords of the codebook C. As an important measure of performance of a codebook C in code-division multiple access system, the maximum correlation amplitudes $I_{\max}(C)$ 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 a complex vector $\mathbf{c}_j$.

Minimizing $I_{\max}(C)$ is a meaningful problem as it can optimize some performance metrics such as average signal-to-noise ratio and outage probability. Hence, for a given K, it is desirable to construct codebooks with N as large as possible and $I_{\max}(C)$ as small as possible simultaneously. Unfortunately, there is a tradeoff among the parameters N, K and $I_{\max}(C)$. Let $I_w(C) = \sqrt{(N-K)/((N-1)K)}$, we know $I_{\max}(C) \ge I_w(C)$ [9]. If C achieves the Welch bound, that is, $I_{\max}(C) = I_w(C)$, then C is referred to as a Welch-bound-equality codebook. In ordinary circumstance, it is extremely difficult to construct codebooks achieving the Welch bound. As a consequence, researchers attempt to construct codebooks asymptotically meeting the Welch bound, that is, $I_{\max}(C)$ is slightly higher than $I_w(C)$, but $\lim_{N \to \infty} I_{\max}(C)/I_w(C) = 1$ [10–12].

This paper is organized as follows. Some interesting mathematical foundations will be introduced in Section II. Based on these related character sums, a class of strongly regular graphs and nearly optimal codebooks are presented in Section III. In addition, these constructed codebooks have new parameters.

For convenience, we use the following notations in the following sequel.

- m, s are positive integers and $n = ms$.
- p is an odd prime and $q = p^n$.
- Tr_m^n denotes the trace function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$.
- β is a primitive element of $\mathbb{F}_{p^n}$.
- $\zeta_p = e^{\frac{2\pi\sqrt{-1}}{p}}$ is a p-th primitive root of complex unity.
- η_n and η_m denote the quadratic characters of $\mathbb{F}_{p^n}$ and $\mathbb{F}_{p^m}$, separately.
- χ_n and χ_m denote the canonical additive characters of $\mathbb{F}_{p^n}$ and $\mathbb{F}_{p^m}$, separately.
- μ_a denotes an additive character of $\mathbb{F}_{p^n}$ for $a \in \mathbb{F}_{p^n}$.

2. Preliminaries

In this section, we start with characters of finite fields. To prove the main results of this letter, we need a number of results on exponential sums that are derived for the proofs.

For an odd prime p, let $q = p^n$ and $\mathbb{F}_q$ denote the finite field with q elements. Then Tr_m^n is defined by

$$\mathrm{Tr}_m^n(x) = \sum_{j=0}^{n/m-1} x^{(p^m)^j}$$

and Tr_m^n is called the trace function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$.

An additive character of $\mathbb{F}_{p^n}$ is a homomorphism χ from the additive group of $\mathbb{F}_{p^n}$ to the multiplicative group of complex numbers of absolute value 1. The function

$$\chi_n(x) = \zeta_p^{\mathrm{Tr}_1^n(x)}, \ x \in \mathbb{F}_{p^n},$$

defines an additive character of $\mathbb{F}_{p^n}$ and χ_n is called the canonical additive character of $\mathbb{F}_{p^n}$. For $a \in \mathbb{F}_{p^n}$, define

$$\mu_a(x) = \chi_n(ax) = \zeta_p^{\mathrm{Tr}_1^n(ax)}, \quad x \in \mathbb{F}_{p^n}.$$

Obviously, μ_a is also an additive character of $\mathbb{F}_{p^n}$. And every additive character of $\mathbb{F}_{p^n}$ can be obtained in this way [13]. Its orthogonality relation is given by

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

Let β be a primitive element of $\mathbb{F}_q$. For a fixed integer j, $0 \le j \le q-2$, the function

$$\chi_j(\beta^i) = e^{\frac{2\pi\sqrt{-1}ji}{q-1}}, \ i = 0, 1, \cdots, q-2,$$

defines a multiplicative character of $\mathbb{F}_q$. In this paper, we use η_n to denote the quadratic character $\chi_{(q-1)/2}$ of $\mathbb{F}_q$. And the quadratic character η_n is extended by letting $\eta_n(0) = 0$. The orthogonality relation for quadratic characters is given by

$$\sum_{x\in\mathbb{F}_{p^k}} \eta_k(x) = 0,$$

where η_k is the quadratic character of $\mathbb{F}_{p^k}$ and k is a positive integer.

The Gauss sum $G(\eta_m, \chi_m)$ over $\mathbb{F}_{p^m}$ is defined by [13]

$$G(\eta_m, \chi_m) = \sum_{x\in\mathbb{F}_{p^m}^*} \eta_m(x)\chi_m(x),$$

where η_m and χ_m are the quadratic and canonical additive characters of $\mathbb{F}_{p^m}$, respectively.

The Gauss sum $G(\eta_m, \chi_m)$ can be evaluated explicitly and the result on $G(\eta_m, \chi_m)$ is given in the following lemma.

Lemma 1. *[13, Theorem 5.15] Let $\mathbb{F}_{p^m}$ be the finite field with p^m element, where p is an odd prime. Then*

$$G(\eta_m, \chi_m) = (-1)^{m-1}(p^*)^{\frac{m}{2}},$$

where $p^* = \left(\frac{-1}{p}\right)p$.

Hence, we shall abbreviate $G(\eta_m, \chi_m)$ to G_m. The following lemma establishes a relationship between the quadratic character η_m and the canonical additive character χ_m of $\mathbb{F}_{p^m}$.

Lemma 2. *[13, p. 195] With symbols and notations above, we have*

$$\eta_m(x) = \frac{1}{p^m} \sum_{a \in \mathbb{F}_{p^m}} G_m \eta_m(-a) \chi_m(ax).$$

Let $f(x)$ be a function from $\mathbb{F}_q$ to $\mathbb{F}_p$. The Walsh transform of f is defined by

$$\mathcal{W}_f(\beta) := \sum_{x \in \mathbb{F}_q} \zeta_p^{f(x) + \mathrm{Tr}_1^n(\beta x)},$$

for $\beta \in \mathbb{F}_q$. The following lemma states a property of the Walsh transform of $f(x) = \alpha x^2$, where $\alpha \in \mathbb{F}_q^*$.

Lemma 3. *[14] For $\alpha \in \mathbb{F}_q^*$, the Walsh transform coefficient of $\mathrm{Tr}_1^n(\alpha x^2)$ is equal to*

$$\omega_\alpha(\beta) = \sum_{x \in \mathbb{F}_q} \zeta_p^{\mathrm{Tr}_1^n(\alpha x^2) + \mathrm{Tr}_1^n(\beta x)} = (-1)^{n-1} \eta_n(\alpha) (p^*)^{\frac{n}{2}} \zeta_p^{-\mathrm{Tr}_1^n\left(\frac{\beta^2}{4\alpha}\right)},$$

where $\beta \in \mathbb{F}_q$ and $p^* = \left(\frac{-1}{p}\right) p$.

Below we give a few results which are used to obtain the main results of this paper.

Lemma 4. *Let symbols be the same as before. Then we have:*

(1) If $s \geq 2$ is even, then $\eta_n(z) = 1$, for $z \in \mathbb{F}_{p^m}^*$.

(2) If $s \geq 2$ is odd, then $\eta_n(z) = \eta_m(z)$, for $z \in \mathbb{F}_{p^m}^*$.

Proof. Assume that $\mathbb{F}_{p^n}^* = \langle \beta \rangle$, we get $\mathbb{F}_{p^m}^* = \langle \beta^{\frac{p^n-1}{p^m-1}} \rangle$. For $n = ms$, we have

$$\frac{p^n - 1}{p^m - 1} = p^{m(s-1)} + p^{m(s-2)} + \cdots + p^m + 1.$$

This means that the parity of $(p^n - 1)/(p^m - 1)$ is the same as s. Hence, we have

$$\eta_n(z) = \begin{cases} 1, & \text{if } s \text{ is even}, \\ \eta_m(z), & \text{if } s \text{ is odd}, \end{cases}$$

for $z \in \mathbb{F}_{p^m}^*$. □

Lemma 5. *[13, Theorem 5.12] For $y \in \mathbb{F}_{p^m}$, we obtain*

$$\sum_{z \in \mathbb{F}_{p^m}^*} \eta_m(z) \zeta_p^{\mathrm{Tr}_1^m(zy)} = \begin{cases} 0, & \text{if } y = 0, \\ G_m \eta_m(y), & \text{if } y \in \mathbb{F}_{p^m}^*. \end{cases}$$

3. Proofs and main results

In this section, we provide a construction of strongly regular Cayley graphs and a family of asymptotically optimal codebooks. For $\alpha \in \mathbb{F}_q^*$, let

$$D_\alpha = \left\{x \in \mathbb{F}_q : \eta_m\left(\mathrm{Tr}_m^n(\alpha x^2)\right) = 1\right\}. \tag{3.1}$$

The following lemma gives the cardinality of the special subset D_α of $\mathbb{F}_q$.

Lemma 6. *Let symbols be the same as before. Then the cardinality $|D_\alpha|$ of D_α is given by:*

(1) If s is even, then

$$|D_\alpha| = \frac{1}{2p^m}(p^m - 1)\left(p^n + \eta_n(\alpha)(p^*)^{\frac{n}{2}}\right).$$

(2) If s is odd, then

$$|D_\alpha| = \frac{1}{2}\left(p^n - p^{n-m} + (p^m - 1)\frac{(-1)^{n+\frac{(p+1)m}{2}}(p^*)^{\frac{m+n}{2}}\eta_n(\alpha)}{p^m}\right).$$

Proof. In order to determine the cardinality of D_α, we firstly compute the values of the following two equalities:

$$A_1 = \sum_{\substack{x\in\mathbb{F}_{p^n} \\ \mathrm{Tr}_m^n(\alpha x^2)=0}} 1,\ \alpha \in \mathbb{F}_q^*,$$
$$A_2 = \sum_{\substack{x\in\mathbb{F}_{p^n} \\ \mathrm{Tr}_m^n(\alpha x^2)\neq 0}} \eta_m\left(\mathrm{Tr}_m^n(\alpha x^2)\right),\ \alpha \in \mathbb{F}_q^*.$$

It is clear that

$$\begin{aligned} A_1 &= \frac{1}{p^m}\sum_{x\in\mathbb{F}_{p^n}}\sum_{z\in\mathbb{F}_{p^m}}\chi_m\left(z\,\mathrm{Tr}_m^n(\alpha x^2)\right) \\ &= \frac{1}{p^m}\left(p^n + \sum_{z\in\mathbb{F}_{p^m}^*}\sum_{x\in\mathbb{F}_{p^n}}\chi_m\left(\mathrm{Tr}_m^n\left(z\alpha x^2\right)\right)\right). \end{aligned} \tag{3.2}$$

Note that

$$\sum_{z\in\mathbb{F}_{p^m}^*}\sum_{x\in\mathbb{F}_{p^n}}\chi_m\left(\mathrm{Tr}_m^n\left(z\alpha x^2\right)\right) = \sum_{z\in\mathbb{F}_{p^m}^*}\sum_{x\in\mathbb{F}_{p^n}}\chi_n(z\alpha x^2).$$

By Lemmas 3 and 4, we get

$$\sum_{z\in\mathbb{F}_{p^m}^*}\sum_{x\in\mathbb{F}_{p^n}}\chi_n(z\alpha x^2) = \begin{cases} (-1)^{n-1}\eta_n(\alpha){p^*}^{\frac{n}{2}}(p^m - 1), & \text{if } s \text{ even}, \\ 0, & \text{if } s \text{ odd}. \end{cases} \tag{3.3}$$

Hence, we obtain

$$A_1 = \begin{cases} \frac{p^n+(-1)^{n-1}\eta_n(\alpha)(p^*)^{\frac{n}{2}}(p^m-1)}{p^m}, & \text{if } s \text{ even},\\ p^{n-m}, & \text{if } s \text{ odd}. \end{cases} \tag{3.4}$$

Now we determine the values of A_2. By Lemma 2, we have

$$\begin{aligned} A_2 &= \frac{G_m}{p^m}\sum_{a\in\mathbb{F}_{p^m}}\eta_m(-a)\sum_{x\in\mathbb{F}_{p^n}}\chi_n\left(a\alpha x^2\right)\\ &= \frac{\eta_n(\alpha)G_mG_n}{p^m}\sum_{a\in\mathbb{F}_{p^m}^*}\eta_m(-a)\eta_n(a)\\ &= \begin{cases} 0, & \text{if } s \text{ even},\\ \frac{(-1)^{\frac{(p-1)m}{2}}(p^m-1)\eta_n(\alpha)(-1)^{n+m}(p^*)^{\frac{n+m}{2}}}{p^m}, & \text{if } s \text{ odd}, \end{cases} \end{aligned} \tag{3.5}$$

where the last equality follows from the fact that $\sum_{a\in\mathbb{F}_{p^m}^*}\eta_m(a) = 0$ and Lemma 4. By definition, we deduce that

$$|D_\alpha| = \sum_{\substack{x\in\mathbb{F}_{p^n}\\ \mathrm{Tr}_m^n(\alpha x^2)\neq 0}}\frac{\eta_m\left(\mathrm{Tr}_m^n(\alpha x^2)\right)+1}{2} = \frac{p^n}{2}-\frac{1}{2}\sum_{\substack{x\in\mathbb{F}_{p^n}\\ \mathrm{Tr}_m^n(\alpha x^2)=0}}1+\frac{1}{2}\sum_{\substack{x\in\mathbb{F}_{p^n}\\ \mathrm{Tr}_m^n(\alpha x^2)\neq 0}}\eta_m\left(\mathrm{Tr}_m^n(\alpha x^2)\right), \tag{3.6}$$

The results of this lemma follow from (3.4)–(3.6). □

Example 1. *Let $p = 5$, $n = 4$, $m = 2$ and $s = 2$. If α is a primitive element of $\mathbb{F}_{5^4}^*$, by Lemma 6 we get $|D_\alpha| = 288$, which agrees with numerical computations by Magma. If $\alpha = 1$, then $|D_1| = 240$, which is consistent with Magma program computation.*

Example 2. *Let $p = 7$, $n = 3$, $m = 1$ and $s = 3$. If α is a primitive element of $\mathbb{F}_{7^3}^*$, by Lemma 6 we get $|D_\alpha| = 168$, which agrees with Magma program. If $\alpha = 1$, then $|D_1| = 126$, which coincides with numerical results by Magma program computation.*

Lemma 7. *For $a,\alpha\in\mathbb{F}_{p^n}^*$, define*

$$E_{\alpha,a} = \sum_{\substack{x\in\mathbb{F}_{p^n}\\ \mathrm{Tr}_m^n(\alpha x^2)\neq 0}}\mu_a(x).$$

(1) If s is an even integer, then

$$E_{\alpha,a} = \begin{cases} -A(p^m-1), & \textit{if } \mathrm{Tr}_m^n\left(\frac{a^2}{4\alpha}\right)=0,\\ A, & \textit{if } \mathrm{Tr}_m^n\left(\frac{a^2}{4\alpha}\right)\neq 0, \end{cases}$$

where $A = \frac{(-1)^{n-1}\eta_n(-\alpha)(p^*)^{\frac{n}{2}}}{p^m}$.

(2) If s is an odd integer, then

$$E_{\alpha,a} = \begin{cases} 0, & \textit{if } \mathrm{Tr}_m^n\left(\frac{a^2}{4\alpha}\right)=0,\\ -B, & \textit{if } \mathrm{Tr}_m^n\left(\frac{a^2}{4\alpha}\right)\in\mathbb{F}_{p^m}^{*2},\\ B, & \textit{if } \mathrm{Tr}_m^n\left(\frac{a^2}{4\alpha}\right)\in\mathbb{F}_{p^m}^{*}\setminus\mathbb{F}_{p^m}^{*2}, \end{cases}$$

where $B = \frac{(-1)^{n+m}(p^*)^{\frac{m+n}{2}}\eta_n(-\alpha)}{p^m}$.

Proof. For $a \in \mathbb{F}_{p^n}^*$, by the orthogonality relation of μ_a we get

$$\begin{aligned} E_{\alpha,a} &= - \sum_{\substack{x \in \mathbb{F}_{p^n} \\ \mathrm{Tr}_m^n(\alpha x^2)=0}} \mu_a(x) \\ &= -\frac{1}{p^m} \sum_{x \in \mathbb{F}_{p^n}} \sum_{z \in \mathbb{F}_{p^m}} \chi_m\left(z\,\mathrm{Tr}_n^m(\alpha x^2)\right)\mu_a(x) \\ &= -\frac{1}{p^m} \sum_{z \in \mathbb{F}_{p^m}^*} \sum_{x \in \mathbb{F}_{p^n}} \chi_n(z\alpha x^2 + ax). \end{aligned}$$

By Lemma 3, we get

$$E_{\alpha,a} = -\frac{1}{p^m} \sum_{z \in \mathbb{F}_{p^m}^*} (-1)^{n-1}\eta_n(z\alpha)(p^*)^{\frac{n}{2}} \zeta_p^{-\mathrm{Tr}_1^n\left(\frac{a^2}{4z\alpha}\right)}.$$

From the map $z \mapsto -\frac{1}{z}$, we obtain

$$E_{\alpha,a} = -\frac{1}{p^m} \sum_{z \in \mathbb{F}_{p^m}^*} (-1)^{n-1}\eta_n(-z\alpha)(p^*)^{\frac{n}{2}} \zeta_p^{\mathrm{Tr}_1^n\left(\frac{za^2}{4\alpha}\right)}. \tag{3.7}$$

When s is even, from Lemmas 4 and 5, we have the result (1) of this lemma.
When s is odd, the desired result follows from Lemmas 4 and 5.

□

Lemma 8. *For $a, \alpha \in \mathbb{F}_{p^n}^*$, let*

$$N_{\alpha,a} = \sum_{\substack{x \in \mathbb{F}_{p^n} \\ \mathrm{Tr}_m^n(\alpha x^2)\neq 0}} \eta_m\left(\mathrm{Tr}_m^n(\alpha x^2)\right)\mu_a(x).$$

(1) If s is even, then

$$N_{\alpha,a} = \begin{cases} 0, & \text{if } \mathrm{Tr}_m^n\left(\frac{a^2}{4\alpha}\right) = 0, \\ (p^*)^m A, & \text{if } \mathrm{Tr}_m^n\left(\frac{a^2}{4\alpha}\right) \in \mathbb{F}_{p^m}^{*2}, \\ -(p^*)^m A, & \text{if } \mathrm{Tr}_m^n\left(\frac{a^2}{4\alpha}\right) \in \mathbb{F}_{p^m}^{*} \backslash \mathbb{F}_{p^m}^{*2}, \end{cases}$$

where $A = \frac{(-1)^{n-1}(p^*)^{\frac{n}{2}}\eta_n(-\alpha)}{p^m}$.

(2) If s is odd, then

$$N_{\alpha,a} = \begin{cases} (p^m-1)B, & \text{if } \mathrm{Tr}_m^n\left(\frac{a^2}{4\alpha}\right) = 0, \\ -B, & \text{if } \mathrm{Tr}_m^n\left(\frac{a^2}{4\alpha}\right) \neq 0, \end{cases}$$

where $B = \frac{(-1)^{n+m}(p^*)^{\frac{m+n}{2}}\eta_n(-\alpha)}{p^m}$.

Proof. It follows from Lemma 2 that

$$p^m N_{\alpha,a} = G_m \sum_{x\in\mathbb{F}_{p^n}} \sum_{z\in\mathbb{F}_{p^m}^*} \chi_n(ax)\eta_m(-z)\chi_n\left(z\alpha x^2\right)$$
$$= G_n G_m \sum_{z\in\mathbb{F}_{p^m}^*} \eta_m(-z)\eta_n(z\alpha)\zeta_p^{-\mathrm{Tr}_1^n\left(\frac{a^2}{4z\alpha}\right)}.$$

From the map $z \mapsto -\frac{1}{z}$, we derive that

$$p^m N_{\alpha,a} = G_n G_m \sum \eta_m(z)\eta_n(-z\alpha)\zeta_p^{\mathrm{Tr}_1^m\left(z\,\mathrm{Tr}_m^n\left(\frac{a^2}{4\alpha}\right)\right)}. \tag{3.8}$$

The desired result follows from (3.8), Lemmas 4 and 5.

□

Theorem 9. *Let symbols be the same as before and $s \geq 2$ be even. Then the Cayley graph Cay$(\mathbb{F}_{p^n}, D_\alpha)$ is strongly regular with non-trivial eigenvalues $-(p^*)^{\frac{n}{2}}(p^m+1)\eta_n(-\alpha)/(2p^m)$ and $(p^*)^{\frac{n}{2}}(p^m-1)\eta_n(-\alpha)/(2p^m)$.*

Proof. For $a \in \mathbb{F}_{p^n}^*$, we deduce that

$$\sum_{x\in D_\alpha} \mu_a(x) = \sum_{\substack{x\in\mathbb{F}_{p^n} \\ \mathrm{Tr}_m^n(\alpha x^2)\neq 0}} \mu_a(x)\cdot\frac{\eta_m\left(\mathrm{Tr}_m^n\left(\alpha x^2\right)\right)+1}{2}$$
$$= \frac{1}{2}\sum_{\substack{x\in\mathbb{F}_{p^n} \\ \mathrm{Tr}_m^n(\alpha x^2)\neq 0}} \mu_a(x) + \frac{1}{2}\sum_{\substack{x\in\mathbb{F}_{p^n} \\ \mathrm{Tr}_m^n(\alpha x^2)\neq 0}} \mu_a(x)\eta_m\left(\mathrm{Tr}_m^n\left(\alpha x^2\right)\right),$$

where the last equality follows from that $\eta_m(0) = 0$. Then the desired conclusions follow from Lemmas 7 and 8. □

Remark 1. *Let $s > 1$ be an odd integer. Then the eigenvalues of the Cayley graph Cay$(\mathbb{F}_{p^n}, D_\alpha)$ can also be computed by a similar method given in Theorem 9. It can be easily checked that*

$$\sum_{x\in D_\alpha} \mu_a(x) \in \left\{0, \frac{(p^m-1)B}{2}, -B\right\},$$

where $a \in \mathbb{F}_{p^n}^*$ and $B = (-1)^{n+m}\eta_n(-\alpha)(p^*)^{\frac{m+n}{2}}/p^m$. This means that the Cayley graph Cay$(\mathbb{F}_{p^n}, D_\alpha)$ is not strong regular if s is odd.

Motivated by the work in [15], we give a construction of asymptotically optimal codebooks based on the strongly regular Cayley graph Cay$(\mathbb{F}_{p^n}, D_\alpha)$ defined in Theorem 9. For $\alpha \in \mathbb{F}_{p^n}^*$, let

$$C_\alpha = \{\mathbf{c}_{\alpha,a} : a \in \mathbb{F}_{p^n}\}, \tag{3.9}$$

where $\mathbf{c}_{\alpha,a} = \left(\frac{1}{\sqrt{|D_\alpha|}}\mu_a(x)\right)_{x\in D_\alpha}$.

Theorem 10. *Let*

$$K = \frac{1}{2p^m}(p^m - 1)\left(p^n + \eta_n(\alpha)(p^*)^{\frac{n}{2}}\right),$$

and let $s \geq 2$ be a fixed even integer. Then C_α defined by (3.9) *is an asymptotically optimal codebook with parameters $[p^n, K]$.*

Proof. By the definition of C_α and Lemma 6, we deduce that C_α is a $[p^n, K]$ codebook. For any two distinct codewords $\mathbf{c}_a$ and $\mathbf{c}_b$ in C_α (i.e., $a \neq b \in \mathbb{F}_{p^n}$), it can be easily checked that

$$|\mathbf{c}_a\mathbf{c}_b^H| = \frac{1}{K}\left|\sum_{x \in D_\alpha} \mu_a(x)\overline{\mu_b(x)}\right| = \frac{1}{K}\left|\sum_{x \in D_\alpha} \mu_{a-b}(x)\right|.$$

It follows from Theorem 9 that

$$|\mathbf{c}_a\mathbf{c}_b^H| \in \left\{\frac{p^{\frac{n}{2}}(p^m+1)}{2Kp^m}, \frac{p^{\frac{n}{2}}(p^m-1)}{2Kp^m}\right\},$$

which implies that

$$I_{\max}(C_\alpha) = \frac{p^{\frac{n}{2}}(p^m+1)}{2Kp^m}.$$

According to the Welch bound, we have

$$I_w(C_\alpha) = \sqrt{\frac{p^n + p^{n-m} + \eta_n(\alpha)\left(\frac{-1}{p}\right)^{\frac{n}{2}}\left(p^{\frac{n-2m}{2}} - p^{\frac{n}{2}}\right)}{2(p^n-1)K}}.$$

It is easy to check that

$$\lim_{p^n \to +\infty} \frac{I_{\max}(C_\alpha)}{I_w(C_\alpha)} = 1,$$

which means that the codebook C_α is asymptotically optimal with respect to the Welch bound. $\square$

Remark 2. *Many readers may wonder what parameters the codebook C_α has when s is an odd integer and whether it is asymptotically optimal. If s is odd, then by Theorems 6 and 9 we know the codebook C_α defined in* (3.9) *has parameters*

$$N = p^n,\ K = \frac{1}{2}\left(p^n - p^{n-m} + (p^m - 1)\frac{(-1)^{n+\frac{(p+1)m}{2}}(p^*)^{\frac{m+n}{2}}\eta_n(\alpha)}{p^m}\right),$$
$$I_{\max}(C_\alpha) = \frac{(p^m-1)B}{2K}.$$

It can be verified that

$$\lim_{p^n \to +\infty} \frac{I_{\max}(C_\alpha)}{I_w(C_\alpha)} \neq 1,$$

which implies that C *is not asymptotically optimal.*

In Table 1, we assume that α is a primitive element of $\mathbb{F}_{p^n}^*$, $p = 3$ and $s = 4$. And we show some parameters of the codebook C_α in this table. From Table 1, it can be seen that C_α is asymptotically optimal with respect to the Welch bound for sufficiently large N. This also agrees with the result of Theorem 10.

To give a comparison, we present the parameters (N, K) of some known asymptotically optimal codebooks and the codebook defined in (3.9) in Table 2. From this table, we can conclude that C_α has new parameters.

Table 1. The parameters of the codebook C_α in (3.9) for $p = 3$ and $s = 4$.

m	N	K	$I_{\max}(C_\alpha)$	$I_W(C_\alpha)$	$I_{\max}/I_w$
2	6561	2808	5/312	1.4273×10^{-2}	1.2273
3	531441	254826	7/4719	1.4292×10^{-3}	1.0379
4	43046721	21228480	41/262080	1.5452×10^{-4}	1.0124
5	348684401	1735953120	61/3571920	1.7008×10^{-5}	1.0041
6	282429536481	141013893384	365/193434696	1.884×10^{-6}	1.0014

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

Constraints	Ref.	Parameters (N, K)
q is a prime power	[16]	$\left(q, \frac{q+1}{2}\right)$
$n > 1$, $1 \le i \le l$, $s_i > 1$ $q_i = 2^{s_i}$ $l > 1$	[17]	$\left(2K + (-1)^{ln}, K\right)$, $K = \frac{(q_1-1)^n \cdots (q_l-1)^n - (-1)^{ln}}{2}$
$1 \le i \le l$, q_i is a prime power, $q_i \equiv 3 \pmod 4$	[18]	$(q_1q_2\cdots q_l, (q_1q_2\cdots q_l - 1)/2)$
q is a prime power, $\ell > 2$	[19]	$\left((q-1)^\ell + M, M\right)$ $M = \frac{(q-1)^\ell + (-1)^{\ell+1}}{q}$,
q is a prime power	[20]	$\left(q^3 + q^2 - q, q^2 - q\right)$
q is a prime power	[20]	$\left(q^3 + q^2, q^2\right)$
$s > 1$, $m > 1$, q is a prime power	[21]	$\left((q^s - 1)^m + q^{sm-1}, q^{sm-1}\right)$
$s > 1$, $m > 1$, q is a prime power	[21]	$((q^s - 1)^m + M, M)$ $M = \frac{(q^s-1)^m + (-1)^{m+1}}{q}$
$\alpha \in \mathbb{F}_{p^n}^*$, p is an odd prime, $n = ms$, s is even	Thm. 10	$\left(p^n, \frac{p^m-1}{2p^m}C\right)$ $C = p^n + \eta_n(\alpha)\left(\frac{-1}{p}\right)^{\frac{n}{2}} p^{\frac{n}{2}}$

4. Conclusions

In this paper, we propose a method for constructing strongly regular graphs. Then we use the connection set D_α ($\alpha \in \mathbb{F}_{p^n}^*$) of the strongly regular graph $\mathrm{Cay}(\mathbb{F}_{p^n}^*, D_\alpha)$ to give a class of codebook C_α.

In addition, the parameters $[N, K]$ and $I_{\max}(C_\alpha)$ of the codebook C_α are determined in Theorem 10. Table 1 demonstrates that these proposed codebooks are asymptotically optimal according to the Welch bound.

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 was supported by the Innovation Project of Engineering Research Center of Integration and Application of Digital Learning Technology (No.1221049), 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, 2022KJ075), Haihe Laboratory of Information Technology Application Innovation (No. 22HHXCJC00002), the National Natural Science Foundation of China (Grant No. 12301670).

Conflict of interest

The authors declare no conflicts of interest.

References

1. R. C. Bose, Strongly regular graphs, partial geometries and partially balanced designs, *Pac. J. Math.*, **13** (1963), 389–419. Available from: https://msp.org/pjm/1963/13-2/pjm-v13-n2-p04-s.pdf.
2. P. J. Cameron, *Strongly regular graphs*, Selected Topics in Graph Theory, New York: Academic Press, 1978, 337–360. Available from: http://vlsicad.eecs.umich.edu/BK/SAUCY/papers/srg_cameron.pdf.
3. A. E. Brouwer, J. H. Van Lint, *Strongly regular graphs and partial geometries, Enumeration and Designs*, New York: Academic Press, 2022. Available from: https://pure.tue.nl/ws/files/2394798/595248.pdf.
4. A. E. Brouwer, R. M. Wilson, Q. Xiang, Cyclotomy and strongly regular graphs, *J. Algebr. Comb.*, **10** (1999), 25–28. https://doi.org/10.1023/A:1018620002339
5. T. Feng, Q. Xiang, Strongly regular graphs from unions of cyclotomic classes, *J. Combin. Theory B*, **102** (2012), 982–995. https://doi.org/10.1016/j.jctb.2011.10.006
6. T. Feng, K. Momihara, Q. Xiang, Constructions of strongly regular Cayley graphs and skew Hadamard difference sets from cyclotomic classes, *Combinatorica*, **35** (2015), 413–434. https://doi.org/10.1007/s00493-014-2895-8
7. P. J. Cameron, J. H. van Lint, *Designs, graphs, codes and their links*, Cambridge: Cambridge University Press, 1991.

8. J. M. Goethals, J. J. Seidel, Strongly regular graphs derived from combinatorial design, *Geom. Combin.*, 1991, 44–61.
9. 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
10. 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
11. W. Lu, X. Wu, X. Cao, Three constructions of asymptotically optimal codebooks via multiplicative characters of finite fields, *Adv. Math. Commun.*, 2022, 1–9. https://doi.org/10.3934/amc.2022091
12. Y. Yan, Y. Yao, Z. Chen, Q. Wang, Two new families of asymptotically optimal codebooks from characters of cyclic groups, *IEICE T. Fund. Electr.*, **E104** (2021), 1027–1032. https://doi.org/10.1587/transfun.2020EAP1124
13. R. Lidl, H. Niederreiter, *Finite fields*, Cambridge: Cambridge University Press, 1997. Available from: `https://dl.acm.org/doi/10.5555/248301`.
14. T. Helleseth, A. Kholosha, Monomial and quadratic bent functions over the finite fields of odd characteristic, *IEEE T. Inform. Theory*, **52** (2006), 2018–2032. Available from: `http://www.ii.uib.no/publikasjoner/texrap/ps/2005-310.ps`.
15. C. Ding, T. Feng, A generic construction of complex codebooks meeting the Welch bound, *IEEE T. Inform. Theory*, **53** (2007), 4245–4250. https://doi.org/10.1109/TIT.2007.907343
16. C. Li, Q. Yue, Y. Huang, Two families of nearly optimal codebooks, *Design. Code. Cryptogr.*, **75** (2015), 43–57. https://doi.org/10.1007/s10623-013-9891-7
17. 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
18. H. Hu, J. Wu, New constructions of codebooks nearly meeting the Welch bound with equality, *IEEE T. Inform. Theory*, **60** (2014), 1348–1355. https://doi.org/10.1109/TIT.2013.2292745
19. Z. Heng, C. Ding, Q. Yue, New constructions of asymptotically optimal codebooks with multiplicative characters, *IEEE T. Inform. Theory*, **63** (2017), 6179–6187. https://doi.org/10.1109/TIT.2017.2693204
20. L. Tian, Y. Li, T. Liu, C. Xu, Constructions of codebooks asymptotically achieving the welch bound with additive characters, *IEEE Signal Proc. Let.*, **26** (2019), 622–626. https://doi.org/10.1109/LSP.2019.2891896
21. G. Luo, X. Cao, Two constructions of asymptotically optimal codebooks via the hyper eisenstein sum, *IEEE T. Inform. Theory*, **64** (2018), 6498–6505. https://doi.org/10.1109/TIT.2017.2777492