IEEE Access
Multidisciplinary Rapid Review Open Access Journal

Received 4 September 2023, accepted 23 September 2023, date of publication 28 September 2023, date of current version 4 October 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3320559

RESEARCH ARTICLE

Applications of Strongly Regular Cayley Graphs to Codebooks

QIUYAN WANG[1], XIAODAN LIANG[1,2], RIZE JIN[3], AND YANG YAN[4]
[1]School of Computer Science and Technology, Tiangong University, Tianjin 300387, China
[2]Engineering Research Center of Integration and Application of Digital Learning Technology, Ministry of Education, Beijing 100039, China
[3]School of Software, Tiangong University, Tianjin 300387, China
[4]School of Information Technology and Engineering, Tianjin University of Technology and Education, Tianjin 300222, China

Corresponding author: Xiaodan Liang (lxdtjpu@163.com)

This work was supported in part by the Innovation Project of Engineering Research Center of Integration and Application of Digital Learning Technology under Grant 1221019, in part by the Humanities and Social Sciences Youth Foundation of Ministry of Education of China under Grant 22YJC870018, in part by the Science and Technology Development Fund of Tianjin Education Commission for Higher Education under Grant 2020KJ112 and Grant KYQD1817, and in part by the Haihe Laboratory of ITAI under Grant 22HHXCJC00002.

ABSTRACT In this paper, we give a construction of strongly regular Cayley graphs on the finite field $\mathbb{F}_{q^n}$. As applications of these strongly regular Cayley graphs, a class of codebooks is presented and proved to be asymptotically optimal with respect to the Welch bound. Further more, these constructed codebooks have new parameters.

INDEX TERMS Gauss sums, codebooks, strongly regular graphs, Cayley graphs.

I. INTRODUCTION

The study of Cayley graphs is an important part of modern graph theory. As a special class of Cayley graphs, strongly regular Cayley graphs have attracted increasing attention due to their important roles in algebraic graph theory and applications in many areas such as expanders [12], chemical graph theory [18] and quantum computing [1]. Let Γ be a graph with v vertices. Then Γ is said to be a (v, k, λ, μ) strongly regular graph if

1) every vertex is adjacent to exactly k other vertices, i.e., the graph is regular of valency k;
2) there are exactly λ vertices adjacent to x and y, where x and y are two adjacent vertices;
3) there are exactly μ vertices adjacent to x and y, where x and y are two nonadjacent vertices.

In [2], the structure of strongly regular graphs was studied, and general theory of strongly regular graphs could be found in [3], [5], [6], [13], and [15]. One of the most effective tools to construct strongly regular graphs is by Cayley graphs and strongly regular Cayley graphs were proposed in [4], [8], and [9].

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

Codebooks (also known as signal sets) with small inner-product correlation are commonly utilized to differentiate among signals of different users in code division multiple access (CDMA) systems, and are applied in many practical applications including space-time codes and compressed sensing. In general, constructing codebooks that achieve the Welch bound is extremely challenging. The construction of asymptotically optimal codebooks, where the ratio of their maximum cross-correlation amplitude to the corresponding bound approaches 1, is also a fascinating research topic. In this paper, we first present our construction of strongly regular Cayley graphs. Then we apply the constructed Cayley graph to obtain a class of asymptotically optimal codebooks with respect to the Welch bound. The codebooks contain new parameters. To give a comparison with known ones, we list the parameters of ours in Table 1.

This paper is organized as follows. In Section II, we briefly introduce some results which will be needed in obtaining our main results. In Section III, we present our construction of strongly regular graphs and explicitly evaluate the eigenvalues of the Cayley graph $\mathrm{Cay}(\mathbb{F}_Q, E)$, where E is given in (4). In Section IV, we describe the construction of our codebooks $\mathcal{C}$ and prove they asymptotically meet the Welch bound. In Section V, we conclude this paper.

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

Ref.	Parameters (N, K)	Constraints
[21]	$((q^s-1)^m+M, M)$	$M=\frac{(q^s-1)^m+(-1)^{m+1}}{q}$ $s>1, m>1$, q is a prime power.
[21]	$((q^s-1)^m+q^{sm-1}, q^{sm-1})$	$s>1, m>1$, q is a prime power.
[17]	(q^3+q^2, q^2)	q is a prime power.
[17]	(q^3+q^2-q, q^2-q)	q is a prime power.
[24]	$((p_{\min}+1)Q^2, Q^2)$	$Q>1$ is an integer, $p_{\min}$ is the smallest, prime factor of Q.
[24]	$((p_{\min}+1)Q^2-Q, Q(Q-1))$	$Q>2$ is an integer, $p_{\min}$ is the smallest, prime factor of Q.
[10]	$(p^{2kmp}+p^{kmp}, p^{kmp}-h)$,	$p>3$ is a prime, $k\geq 1, h\geq 1$, m is even and $h<p^m$.
[10]	$(q^2+q, q-1)$,	where $q=p^m$, $p>3$ is a prime, $m>0$ is even.
[16]	$(p^{5r}-p^{3r}, p^{3r}(p^r-1))$	p is a prime, $r\geq 1$.
[16]	$N=p^{2r}(p^{3r}-p^r-1)$, $K=p^{2r}(p^{2r}-p^r-1)$	p is a prime, $r\geq 1$.
[27]	$(p_{\min}N_1N_2, N_1N_2)$	$N_1\geq 1$, $N_2=N_1+o(N_1)$ $p_{\min}$ is the smallest, prime factor of N_2.
[27]	$(p_{\min}N_1N_2, N_1N_2)$	$N_1\geq 1$, $N_2=N_1+o(N_1)$ $p_{\min}$ is the smallest, prime factor of N_2.
Thm. IV.1	$\left(q^n, \frac{1}{2}(q-1)\left(q^{n-1}+q^{\frac{n-2}{2}}\right)\right)$	$p\equiv 1 \pmod 4$, n is even.
Thm. IV.1	$(q^n, \frac{1}{2}(q-1)(q^{n-1}+M))$	$M=(-1)^{\frac{nt}{2}}q^{\frac{n-2}{2}}$, $p\equiv 3 \pmod 4$, n is even, $t\geq 1$.

Throughout this section, we adopt the following notations.

- p is an odd prime.
- $q=p^t$ for some positive integer t.
- n is an even positive integer and $Q=q^n$.
- χ_1 is the canonical additive character of $\mathbb{F}_q$.
- χ_2 is the canonical additive character of $\mathbb{F}_Q$.
- $\mathrm{Tr}_{q/p}$ is the trace function from $\mathbb{F}_q$ to $\mathbb{F}_p$.
- $\mathrm{Tr}_{Q/q}$ is the trace function from $\mathbb{F}_Q$ to $\mathbb{F}_q$.
- α is a primitive element of $\mathbb{F}_Q$.
- $\beta=\alpha^{\frac{q^n-1}{q-1}}$ is a primitive element of $\mathbb{F}_q$.
- η_1 is the quadratic multiplicative character of $\mathbb{F}_q$.
- η_2 is the quadratic multiplicative character of $\mathbb{F}_Q$.
- $\zeta_n=e^{\frac{2\pi\sqrt{-1}}{n}}$ is the n-th primitive root of complex unity.

II. PRELIMINARIES

This section collects some mathematical foundations which will be used in the sequel.

A. CHARACTERS OVER FINITE FIELDS

Denote the finite field with q elements by $\mathbb{F}_q$. The trace function $\mathrm{Tr}_{q/p}$ mapping from $\mathbb{F}_q$ to $\mathbb{F}_q$ is defined by

$$\mathrm{Tr}_{q/p}(x)=x+x^p+\cdots+x^{p^{t-1}},\ x\in\mathbb{F}_q.$$

Then the function χ_1 given by

$$\chi_1(x)=\zeta_p^{\mathrm{Tr}_{q/p}(x)}=e^{\frac{2\pi i\,\mathrm{Tr}_{q/p}(x)}{p}} \quad \text{for all } x\in\mathbb{F}_q$$

is an additive character of $\mathbb{F}_q$ and the character χ_1 is called the canonical additive character of $\mathbb{F}_q$. The following lemma notes that all additive characters of $\mathbb{F}_q$ can be expressed with χ_1.

Lemma 1 ([19], Theorem 5.7): For $a\in\mathbb{F}_q$, the function with

$$\chi_a(x)=\chi_1(ax)\ \text{for all } x\in\mathbb{F}_q$$

is an additive character of $\mathbb{F}_q$, and every character of $\mathbb{F}_q$ is obtained in this way.

In particular, the character χ_0 with $a=0$ is called the trivial additive character of $\mathbb{F}_q$. For an additive character χ of $\mathbb{F}_q$, its orthogonality relation ([19], Theorem 5.4) is given by

$$\sum_{x\in\mathbb{F}_q}\chi(x)=\begin{cases} q, & \text{if } \chi=\chi_0,\\ 0, & \text{otherwise.}\end{cases} \tag{1}$$

Characters of the multiplicative group $\mathbb{F}_q^*=\mathbb{F}_q\setminus\{0\}$ of $\mathbb{F}_q$ are referred to as multiplicative characters of $\mathbb{F}_q$. Since the multiplicative group $\mathbb{F}_q^*$ is cyclic of order $q-1$, all multiplicative characters of $\mathbb{F}_q$ can be easily determined.

Lemma 2 ([19], Theorem 5.8): Let β be a primitive element of $\mathbb{F}_q$. For each $j=0,1,\ldots,q-2$, the function φ_j with

$$\varphi_j(\beta^k)=\zeta_{q-1}^{jk}=e^{\frac{2\pi ijk}{q-1}}\ \text{for } k=0,1,\ldots,q-2$$

defines a multiplicative character of $\mathbb{F}_q$, and every multiplicative character of $\mathbb{F}_q$ is obtained in this way.

Note that the character φ_0 with $j=0$ satisfies $\varphi_0(x)=1$ for all $x\in\mathbb{F}_q^*$ and φ_0 is called the trivial multiplicative character of $\mathbb{F}_q$. By setting $j=(q-1)/2$, we get the multiplicative character η_1 which is called the quadratic character of $\mathbb{F}_q$. Obviously, η_1 is defined by

$$\eta_1(\beta^i)=\begin{cases} 1, & \text{if } i \text{ is even,}\\ -1, & \text{otherwise.}\end{cases}$$

We can extend the multiplicative character φ_j $(0\leq j\leq q-2)$ of $\mathbb{F}_q$ by setting $\varphi_j(0)=1$ if $j=0$ and $\varphi_j(0)=0$ if $j\neq 0$. For a multiplicative character φ of $\mathbb{F}_q$, its orthogonality relation ([19], Theorem 5.4) is given by

$$\sum_{x\in\mathbb{F}_q}\varphi(x)=\begin{cases} q, & \text{if } \varphi=\varphi_0,\\ 0, & \text{otherwise.}\end{cases} \tag{2}$$

The Gauss sum $G(\varphi,\chi)$ is defined by [19]

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

where φ denotes a multiplicative character and χ an additive character of $\mathbb{F}_q$. Obviously, the absolute value of $G(\varphi, \chi)$ is at most $q-1$, but in general is much smaller than $q-1$, as the following lemma shows.

Lemma 3 ([19], Theorem 5.11): Let φ be a multiplicative character and χ an additive character of $\mathbb{F}_q$. Then the Gauss sum satisfies

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

Furthermore, if $\varphi \neq \varphi_0$ and $\chi \neq \chi_0$, then

$$|G(\varphi, \chi)| = q^{1/2}.$$

The following lemma describes a number of useful identities of Gauss sums.

Lemma 4 ([19], Theorem 5.12): Gauss sums for the finite field $\mathbb{F}_q$ satisfy the following properties:

(i) $G(\varphi, \chi_{ab}) = \overline{\varphi(a)}G(\varphi, \chi_b)$ *for $a \in \mathbb{F}_q^*$ and $b \in \mathbb{F}_q$;*

(ii) $G(\varphi, \overline{\chi}) = \varphi(-1)G(\varphi, \chi)$*;*

(iii) $G(\overline{\varphi}, \chi) = \varphi(-1)\overline{G(\varphi, \chi)}$*, where $\overline{\varphi}(a) = \overline{\varphi(a)}$ for all $a \in \mathbb{F}_q^*$ and the bar denotes complex conjugation.*

By the above lemma, we know $G(\varphi_j, \chi_a) = \overline{\varphi_j(a)}G(\varphi_j, \chi_1)$ for all $a \in \mathbb{F}_q^*$. For abbreviation, we use $G(\varphi_j)$ to denote $G(\varphi_j, \chi_1)$ for $0 \leq j \leq q-2$. Normally, the explicit values of $G(\varphi, \chi)$ are very difficult to determine. Fortunately, Gauss sums can be computed in some particular cases. The following lemmas state some results of Gauss sums, which will be used to obtain our main results.

Lemma 5 ([19], Theorem 5.15): Let η_1 be the quadratic character of $\mathbb{F}_q$ and χ_1 be the canonical additive character of $\mathbb{F}_q$. Then

$$G(\eta_1, \chi_1) = \begin{cases} (-1)^{t-1}q^{1/2}, & \text{if } p \equiv 1 \pmod 4, \\ (-1)^{t-1}i^t q^{1/2}, & \text{if } p \equiv 3 \pmod 4, \end{cases}$$

where $q = p^t$, p is an odd prime and t is a positive integer.

Lemma 6 ([19], P.195): Let φ be a multiplicative character of $\mathbb{F}_q$. Then we obtain

$$\varphi(x) = \frac{1}{q}\sum_{a \in \mathbb{F}_q} G(\varphi, \chi_a)\chi_a(x) \text{ for } x \in \mathbb{F}_q^*.$$

Lemma 7: Let χ be a non-trivial additive character of $\mathbb{F}_q$ with q odd and let $f(x) = a_2x^2 + a_1x + a_0 \in \mathbb{F}_q[x]$ with $a_2 \neq 0$. Then

$$\sum_{x \in \mathbb{F}_q} \chi(f(x)) = \chi\left(a_0 - a_1^2(4a_2)^{-1}\right)\eta_1(a_2)G(\eta_1, \chi),$$

where η_1 is the quadratic character of $\mathbb{F}_q$.

B. CODEBOOKS AND CAYLEY GRAPHS

An (N, K) codebook $\mathcal{C}$ is a set $\{\mathbf{c}_i\}_{i=0}^{N-1}$ of N unit-norm complex vectors, where $\mathbf{c}_i \in \mathbb{C}^K$. The maximum cross-correlation amplitude of $\mathcal{C}$ is given by

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

where $\mathbf{c_j}^H$ denotes the conjugate transpose of $\mathbf{c_j}$. Minimizing the maximum cross-correlation amplitude $I_{\max}(\mathcal{C})$ of a codebook $\mathcal{C}$ is an important problem in CDMA communication sytems, as it can approximately optimize many performance metrics such as outage probability, average signal-to-noise ratio, and symbol error probability [20].

For a given K, it is desirable to construct an (N, K) codebook with the maximizing value of N while simultaneously minimizing the magnitude of $I_{\max}(\mathcal{C})$. Nevertheless, Welch [25] has established a lower bound for $I_{\max}(\mathcal{C})$ as follows.

Lemma 8 ([25]): For any (N, K) codebook $\mathcal{C}$ with $N \geq K$,

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

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

$$|\mathbf{c}_i\mathbf{c}_j^H| = \sqrt{\frac{N-K}{(N-1)K}}. \tag{3}$$

The codebook $\mathcal{C}$ is referred to be optimal with respect to the Welch bound if the equality in (3) holds. Searching optimal codebooks is an interesting topic for the past few years. Unfortunately, Sarwate in ([14], p. 100) pointed out that constructing optimal codebooks is very difficult, and the constructed codebooks so far have restricted parameters N and K. Hence, researchers focus on studying asymptotically optimal codebooks, i.e., $I_{\max}(\mathcal{C})$ asymptotically meets the theoretical bound for sufficiently large K. In the literature, there are some constructions of asymptotically optimal codebooks with respect to the Welch bound and readers are suggested to refer to [11], [22], [23], and [26].

Motivated by the construction in [7], we employ strongly regular Cayley graphs to give a class of asymptotically optimal codebooks. Let G be a finite abelian group and D be a subset of $G \setminus \{0\}$ such that $D = -D$, where 0 is the identity of G and $-D = \{-d : d \in D\}$. The Cayley graph $\mathrm{Cay}(G, D)$ on G with connection set D is the graph with elements of G as vertices; two vertices are adjacent if and only if their difference belongs to D [8]. Let $\widehat{G}$ be the character group of G, i.e., $\widehat{G}$ is consist of all characters of G. Then the eigenvalues of $\mathrm{Cay}(G, D)$ are given by $\phi(D) = \sum_{x \in D}\phi(x)$, where $\phi \in \widehat{G}\backslash\{e\}$ and e denotes the identity of $\widehat{G}$. It is well known that $\mathrm{Cay}(G, D)$ is strongly regular if and only if $\phi(D)$ with $\phi \in \widehat{G} \setminus \{e\}$ takes exactly two values.

III. A CONSTRUCTION OF STRONGLY REGULAR CAYLEY GRAPHS

In this section, we provide a construction of strongly regular Cayley graphs. Let symbols be the same as before. Then a subset E of $\mathbb{F}_Q$ is defined by

$$E = \left\{x \in \mathbb{F}_Q : \eta_1(\mathrm{Tr}_{Q/q}(x^2)) = 1\right\}. \tag{4}$$

In order to compute the eigenvalues of Cay$(\mathbb{F}_Q, E)$, we begin with the following lemma which gives the cardinality of E.

Lemma 9: Let E be the subset defined by (4). Then the cardinality $|E|$ of E is

$$|E| = \begin{cases} \frac{q-1}{2}\left(q^{n-1} + q^{\frac{n-2}{2}}\right), & \text{if } p \equiv 1 \pmod 4, \\ \frac{q-1}{2}\left(q^{n-1} + (-1)^{\frac{nt}{2}} q^{\frac{n-2}{2}}\right), & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Proof: By the definition of the quadratic multiplicative character η_1 of $\mathbb{F}_q$, we deduce that

$$\begin{aligned} |E| &= \sum_{\substack{x\in\mathbb{F}_Q \\ \mathrm{Tr}_{Q/q}(x^2)\neq 0}} \frac{\eta_1\left(\mathrm{Tr}_{Q/q}(x^2)\right)+1}{2} \\ &= \frac{1}{2}\sum_{\substack{x\in\mathbb{F}_Q \\ \mathrm{Tr}_{Q/q}(x^2)\neq 0}} 1 + \frac{1}{2}\sum_{x\in\mathbb{F}_Q}\eta_1\left(\mathrm{Tr}_{Q/q}(x^2)\right) \\ &= \frac{q^n}{2} - \frac{1}{2}\sum_{\substack{x\in\mathbb{F}_Q \\ \mathrm{Tr}_{Q/q}(x^2)= 0}} 1 + \frac{1}{2}\sum_{x\in\mathbb{F}_Q}\eta_1\left(\mathrm{Tr}_{Q/q}(x^2)\right), \end{aligned} \tag{5}$$

where $Q = q^n$ and n is an even positive integer. Let

$$A_1 = \sum_{\substack{x\in\mathbb{F}_Q \\ \mathrm{Tr}_{Q/q}(x^2)= 0}} 1,$$
$$A_2 = \sum_{x\in\mathbb{F}_Q}\eta_1\left(\mathrm{Tr}_{Q/q}(x^2)\right).$$

Next we compute the values of A_1 and A_2 separately. By the orthogonal relationship in (1) and Lemma 7, we have

$$\begin{aligned} A_1 &= \frac{1}{q}\sum_{x\in\mathbb{F}_Q}\sum_{z\in\mathbb{F}_q}\chi_1\left(z\,\mathrm{Tr}_{Q/q}(x^2)\right) \\ &= q^{n-1} + \frac{1}{q}\sum_{z\in\mathbb{F}_q^*}\sum_{x\in\mathbb{F}_Q}\chi_2(zx^2) \\ &= q^{n-1} + \frac{1}{q}\sum_{z\in\mathbb{F}_q^*}\eta_2(z)G(\eta_2). \end{aligned}$$

where χ_1 and χ_2 denote the additive characters of the finite field $\mathbb{F}_q$ and $\mathbb{F}_Q$, respectively, and η_2 denotes the quadratic multiplicative character of $\mathbb{F}_Q$. Let α be a primitive element of $\mathbb{F}_Q$. For each $z \in \mathbb{F}_q^*$, we have

$$z = \alpha^{\frac{q^n-1}{q-1}j} \text{ for some } 0 \le j \le q-2.$$

Since n is even, the number $(q^n-1)/(q-1)$ is even. Then we have

$$\eta_2(z) = 1 \text{ for each } z \in \mathbb{F}_q^*. \tag{6}$$

It follows from Lemma 5 that

$$A_1 = \begin{cases} q^{n-1} - (q-1)q^{\frac{n-2}{2}}, & \text{if } p \equiv 1 \pmod 4, \\ q^{n-1} - (-1)^{\frac{nt}{2}}(q-1)q^{\frac{n-2}{2}}, & \text{if } p \equiv 3 \pmod 4. \end{cases} \tag{7}$$

Using Lemma 6, we deduce that

$$\begin{aligned} A_2 &= \frac{1}{q}\sum_{x\in\mathbb{F}_Q}\sum_{z\in\mathbb{F}_q} G(\eta_1, \overline{\chi_z})\chi_z(\mathrm{Tr}_{Q/q}(x^2)) \\ &= \frac{1}{q}\sum_{z\in\mathbb{F}_q^*} G(\eta_1, \overline{\chi_z})\sum_{x\in\mathbb{F}_Q}\chi_2(zx^2) \\ &= \frac{1}{q}\sum_{z\in\mathbb{F}_q^*}\overline{\eta_1}(z)G(\eta_1)G(\eta_2) \end{aligned} \tag{8}$$

where the second equality follows from Lemma 1, and the third equality follows from (6), Lemmas 4 and 7. Combining (8) and (2), We know

$$A_2 = 0. \tag{9}$$

The desired result follows from (5), (7) and (14). ☐

We now propose the construction of strongly regular Cayley graphs.

Theorem 10: Let symbols be the same as before. Then

1) *if $p \equiv 1 \pmod 4$, then the Cayley graph Cay$(\mathbb{F}_Q, E)$ is strongly regular with eigenvalues $-(q+1)q^{\frac{n-2}{2}}/2$ and $(q-1)q^{\frac{n-2}{2}}/2$;*
2) *if $p \equiv 3 \pmod 4$, then the Cayley graph Cay $(\mathbb{F}_Q, E)$ is strongly regular with eigenvalues $(-1)^{\frac{nt}{2}}(q+1)q^{\frac{n-2}{2}}/2$ and $-(-1)^{\frac{nt}{2}}(q-1)q^{\frac{n-2}{2}}/2$.*

Proof: For each $y \in \mathbb{F}_Q^*$, we deduce that

$$\begin{aligned} \sum_{x\in E}\chi_2(yx) &= \sum_{\substack{x\in\mathbb{F}_Q \\ \mathrm{Tr}_{Q/q}(x^2)\neq 0}} \chi_2(yx)\frac{\eta_1\left(\mathrm{Tr}_{Q/q}(x^2)\right)+1}{2} \\ &= \frac{1}{2}(B_1 + B_2) \end{aligned} \tag{10}$$

where

$$B_1 = \sum_{x\in\mathbb{F}_Q}\chi_2(yx)\eta_1\left(\mathrm{Tr}_{Q/q}(x^2)\right),$$
$$B_2 = \sum_{\substack{x\in\mathbb{F}_Q \\ \mathrm{Tr}_{Q/q}(x^2)\neq 0}}\chi_2(yx).$$

Next we will determine the explicit values of B_1 and B_2. It follows from Lemma 6 that

$$\begin{aligned} B_1 =& \frac{1}{q}\sum_{x\in\mathbb{F}_Q}\chi_2(yx)\sum_{z\in\mathbb{F}_q}G(\eta_1,\overline{\chi_z})\chi_z(\mathrm{Tr}_{Q/q}(x^2)) \\ =& \frac{1}{q}\sum_{z\in\mathbb{F}_q^*}G(\eta_1,\overline{\chi_z})\sum_{x\in\mathbb{F}_Q}\chi_2(zx^2+yx) \\ =& \frac{G(\eta_1)G(\eta_2)}{q}\sum_{z\in\mathbb{F}_q^*}\eta_1\left(-\frac{1}{z}\right)\chi_2\left(-\frac{y^2}{4z}\right), \end{aligned} \tag{11}$$

where the second equality follows from Lemma 1, the third equality is obtained by Lemmas 4 and 7. By (11), we have

$$\begin{aligned} B_1 =& \frac{G(\eta_1)G(\eta_2)}{q}\sum_{z\in\mathbb{F}_q^*}\eta_1(z)\chi_1\left(z\,\mathrm{Tr}_{Q/q}\left(\frac{y^2}{4}\right)\right) \\ =& \begin{cases} \eta_1\left(\mathrm{Tr}_{Q/q}\left(\frac{y^2}{4}\right)\right)G(\eta_2), & \text{if } \mathrm{Tr}_{Q/q}\left(\frac{y^2}{4}\right)\neq 0, \\ 0, & \text{if } \mathrm{Tr}_{Q/q}\left(\frac{y^2}{4}\right)= 0, \end{cases} \end{aligned} \tag{12}$$

where the second equality is derived from Lemmas 3 and 4.

Now our task is to determine the values of B_2. For each $y \in \mathbb{F}_Q^*$, by (1) we have that

$$\sum_{x\in\mathbb{F}_Q}\chi_2(yx) = 0,$$

which means that

$$B_2 = -\sum_{\substack{x\in\mathbb{F}_Q \\ \mathrm{Tr}_{Q/q}(x^2)=0}}\chi_2(yx). \tag{13}$$

It follows from (1) that

$$\begin{aligned} \sum_{\substack{x\in\mathbb{F}_Q \\ \mathrm{Tr}_{Q/q}(x^2)=0}}\chi_2(yx) =& \frac{1}{q}\sum_{x\in\mathbb{F}_Q}\sum_{z\in\mathbb{F}_q}\chi_1(z\,\mathrm{Tr}_{Q/q}(x^2))\chi_2(yx) \\ =& \frac{1}{q}\sum_{z\in\mathbb{F}_q^*}\sum_{x\in\mathbb{F}_Q}\chi_2(zx^2+yx) \\ =& \frac{G(\eta_2)}{q}\sum_{z\in\mathbb{F}_q^*}\chi_2\left(-\frac{y^2}{4z}\right) \\ =& \frac{G(\eta_2)}{q}\sum_{z\in\mathbb{F}_q^*}\chi_1\left(z\,\mathrm{Tr}_{Q/q}\left(\frac{y^2}{4}\right)\right) \\ =& \begin{cases} -\frac{G(\eta_2)}{q}, & \text{if } \mathrm{Tr}_{Q/q}\left(\frac{y^2}{4}\right)\neq 0, \\ \frac{(q-1)G(\eta_2)}{q}, & \text{if } \mathrm{Tr}_{Q/q}\left(\frac{y^2}{4}\right)= 0, \end{cases} \end{aligned} \tag{14}$$

where the second and fourth equalities derive from Lemma 1, and the third equality follows from Lemma 7.

By (13) and (14), we have

$$B_2 = \begin{cases} \frac{G(\eta_2)}{q}, & \text{if } \mathrm{Tr}_{Q/q}\left(\frac{y^2}{4}\right)\neq 0, \\ -\frac{(q-1)G(\eta_2)}{q}, & \text{if } \mathrm{Tr}_{Q/q}\left(\frac{y^2}{4}\right)= 0, \end{cases} \tag{15}$$

For $y \in \mathbb{F}_Q^*$, by (10), (12) and (15) we have

$$\sum_{x\in E}\chi_2(yx) = \begin{cases} \frac{(q+1)G(\eta_2)}{2q}, & \text{if } \mathrm{Tr}_{Q/q}\left(\frac{y^2}{4}\right)\neq 0 \text{ and } \\ & \eta_1\left(\mathrm{Tr}_{Q/q}\left(\frac{y^2}{4}\right)\right)=1, \\ -\frac{(q-1)G(\eta_2)}{2q}, & \text{if } \mathrm{Tr}_{Q/q}\left(\frac{y^2}{4}\right)\neq 0 \text{and} \\ & \eta_1\left(\mathrm{Tr}_{Q/q}\left(\frac{y^2}{4}\right)\right)=-1, \\ -\frac{(q-1)G(\eta_2)}{2q}, & \text{if } \mathrm{Tr}_{Q/q}\left(\frac{y^2}{4}\right)= 0. \end{cases} \tag{16}$$

Therefore, the Cayley graph $\mathrm{Cay}(\mathbb{F}_Q, E)$ has exactly two eigenvalues and the explicit eigenvalues of $\mathrm{Cay}(\mathbb{F}_Q, E)$ derive from Lemma 5. □

IV. A CONSTRUCTION OF ASYMPTOTICALLY OPTIMAL CODEBOOKS

In this section, we propose a construction of asymptotically optimal codebooks based on the strongly regular Cayley graph $\mathrm{Cay}(\mathbb{F}_Q, E)$ defined in Theorem 10. We begin with the connection between strongly regular Cayley graphs and codebooks.

Let $\mathrm{Cay}(G, S)$ be a strongly regular Cayley graph with two restricted eigenvalues δ_1 and δ_2. For each $\phi \in \widehat{G}$, define the vector $\mathbf{c}_\phi$ by

$$\mathbf{c}_\phi = \left(\frac{1}{\sqrt{|S|}}\phi(x)\right)_{x\in S},$$

where $|S|$ denotes the cardinality of S. A codebook $\mathcal{C}$ is given by

$$\mathcal{C} = \{\mathbf{c}_\phi : \phi \in \widehat{G}\}.$$

It can be easily to be checked that

$$\begin{aligned} I_{\max}(\mathcal{C}) =& \max_{\phi\neq\tau\in\widehat{G}}\left\{|\mathbf{c}_\phi\mathbf{c}_\tau^H|\right\} \\ =& \frac{1}{|S|}\max_{\phi\neq\tau\in\widehat{G}}\{|\phi\overline{\tau}(S)|\} \\ =& \frac{1}{|S|}\max_{\phi\in\widehat{G}\setminus\{e\}}\{|\phi(S)|\} \\ =& \frac{1}{|S|}\max\{|\delta_1|, |\delta_2|\}. \end{aligned}$$

Let

$$E = \left\{x \in \mathbb{F}_Q : \eta_1\left(\mathrm{Tr}_{Q/q}(x^2)\right) = 1\right\}.$$

For each $a \in \mathbb{F}_Q$, we define a vector $\mathbf{c}_a$ by

$$\mathbf{c}_a = \left(\frac{1}{\sqrt{|E|}}\chi_2(ax)\right)_{x\in E}.$$

In this paper, the codebook $\mathcal{C}$ is given by

$$\mathcal{C} = \{\mathbf{c}_a : a \in \mathbb{F}_Q\}. \tag{17}$$

Theorem 11: Let symbols be the same as before. Then we have

1) if $p \equiv 1 \pmod 4$, then $\mathcal{C}$ is a (q^n, K) codebook with

$$I_{\max}(\mathcal{C}) = \frac{(q+1)q^{\frac{n}{2}}}{2qK},$$

where $K = \frac{q-1}{2}\left(q^{n-1} + q^{\frac{n-2}{2}}\right)$;

2) if $p \equiv 3 \pmod 4$, then $\mathcal{C}$ is a (q^n, K) codebook with

$$I_{\max}(\mathcal{C}) = \frac{(q+1)q^{\frac{n}{2}}}{2qK},$$

where $K = \frac{q-1}{2}\left(q^{n-1} + (-1)^{\frac{nt}{2}}q^{\frac{n-2}{2}}\right)$.

Proof: By the definition of the codebook $\mathcal{C}$ in (17) and Lemma 9, we deduce that (1) if $p \equiv 1 \pmod 4$, then

$$N = q^n,$$
$$K = |E| = \frac{q-1}{2}\left(q^{n-1} + q^{\frac{n-2}{2}}\right);$$

(2) if $p \equiv 3 \pmod 4$, then

$$N = q^n,$$
$$K = |E| = \frac{q-1}{2}\left(q^{n-1} + (-1)^{\frac{nt}{2}}q^{\frac{n-2}{2}}\right).$$

Given two distinct codewords $\mathbf{c}_a$ and $\mathbf{c}_b$ in $\mathcal{C}$, it is easy to check that

$$\begin{aligned}|\mathbf{c}_a\mathbf{c}_b^H| &= \frac{1}{K}\left|\sum_{x\in E}\chi_2(ax)\overline{\chi_2(bx)}\right| \\ &= \frac{1}{K}\left|\sum_{x\in E}\chi_2((a-b)x)\right|,\end{aligned} \tag{18}$$

where $a \neq b$ and $a, b \in \mathbb{F}_Q$. Combining (16) and (18), we obtain that

$$|\mathbf{c}_a\mathbf{c}_b^H| \in \left\{\frac{(q+1)q^{\frac{n}{2}}}{2qK}, \frac{(q-1)q^{\frac{n}{2}}}{2qK}\right\}.$$

Therefore, we get

$$I_{\max}(\mathcal{C}) = \frac{(q+1)q^{\frac{n}{2}}}{2qK},$$

where K is the cardinality of the set E and is given in Lemma 9.

Theorem 12: The codebook $\mathcal{C}$ defined by (17) is asymptotically optimal with respect to the Welch bound.

Proof: If $p \equiv 1 \pmod 4$, we have

$$I_W = \sqrt{\frac{q^n - q^{\frac{n}{2}} + q^{n-1} + q^{\frac{n-2}{2}}}{(q^n-1)(q-1)(q^{n-1} + q^{\frac{n-2}{2}})}}.$$

Then we deduce that

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

It is easy to check that

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

which implies that the codebook $\mathcal{C}$ is asymptotically optimal with respect to the Welch bound. If $p \equiv 3 \pmod 4$, using a similar argument, we can prove that the codebook $\mathcal{C}$ is asymptotically optimal with respect to the Welch bound.

In Table 2, we give some parameters of codebooks given in (17). As Table 2 shows, we know that I_W approaches $I_{\max}(\mathcal{C})$ as p increases. This implies that the codebooks presented in this paper are asymptotically optimal with respect to the Welch bound for sufficiently large p, which is consistent with Theorem 12.

TABLE 2. The parameters (N, K) of the codebook $\mathcal{C}$ in (17).

p	(n,t)	N	K	$I_{\max}$	I_W	$I_{\max}/I_W$
5	(2,1)	25	12	1/4	0.21246	1.1767
23	(2,1)	529	242	1/121	0.04739	1.0463
31	(2,1)	961	450	8/225	0.03439	1.0338
41	(2,1)	1681	840	1/40	0.02412	1.0241
59	(2,1)	3481	1682	15/841	0.01753	1.0174
71	(2,1)	5041	2450	18/225	0.01449	1.0144
101	(2,1)	10201	5100	1/100	0.00990	1.0099
109	(2,1)	11881	5940	1/108	0.00918	1.0091

Remark 1: In this paper, we limit the integer n to be an even positive integer. Readers may wonder what results will be obtained when n is an odd number. Using a similar method in Theorems 10 and 11, we can calculate the eigenvalues of $Cay(\mathbb{F}_Q, E)$ given in Theorem 10 and $I_{\max}(\mathcal{C})$ of the codebook $\mathcal{C}$ constructed in (17). Unfortunately, it can be easily verified that $Cay(\mathbb{F}_Q, E)$ is not a strongly regular graph and the codebook $\mathcal{C}$ is not asymptotically optimal with respect to the Welch bound, if n is odd.

V. CONCLUDING REMARKS

In this paper, we have given a construction of strongly regular graphs and asymptotically optimal codebooks. As a consequence, we get one infinite series of strongly regular graphs. And the results on strongly regular graphs have applications on codebooks. Table 2 confirms that these presented codebooks are nearly optimal with respect to the Welch bound.

REFERENCES

[1] A. Bernasconi, C. D. Godsil, and S. Severini, "Quantum networks on cubelike graphs," *Phys. Rev. A, Gen. Phys.*, vol. 78, no. 5, 2008, Art. no. 052320.
[2] R. C. Bose, "Strongly regular graphs, partial geometries and partially balanced designs," *Pacific J. Math.*, vol. 13, pp. 389–419, Feb. 1963.
[3] A. E. Brouwer and J. H. van Lint, "Strongly regular graphs and partial geometries," in *Enumeration and Designs*. New York, NY, USA: Academic, 1984, pp. 85–122.
[4] A. E. Brouwer, R. M. Wilson, and Q. Xiang, "Cyclotomy and strongly regular graphs," *J. Algebr. Combin.*, vol. 10, pp. 25–28, Jul. 1999.
[5] P. J. Cameron, *Strongly Regular Graphs. Selected Topics in Graph Theory*. New York, NY, USA: Academic, 1978, pp. 337–360.
[6] P. J. Cameron and J. H. van Lint, *Designs, Graphs, Codes and Their Links*. Cambridge, U.K.: Cambridge Univ. Press, 1991.
[7] C. Ding and T. Feng, "A generic construction of complex codebooks meeting the Welch bound," *IEEE Trans. Inf. Theory*, vol. 53, no. 11, pp. 4245–4250, Nov. 2007.
[8] T. Feng, K. Momihara, and Q. Xiang, "Constructions of strongly regular Cayley graphs and skew Hadamard difference sets from cyclotomic classes," *Combinatorica*, vol. 35, pp. 413–434, Sep. 2015.
[9] T. Feng and Q. Xiang, "Strongly regular graphs from unions of cyclotomic classes," *J. Combin. Theory Ser. B*, vol. 102, pp. 982–995, Jul. 2012.
[10] L. Han, S. Sun, Y. Yan, and Q. Wang, "A new construction of codebooks meeting the Levenshtein bound," *IEEE Access*, vol. 8, pp. 77598–77603, 2020.
[11] Z. Heng, C. Ding, and Q. Yue, "New constructions of asymptotically optimal codebooks with multiplicative characters," *IEEE Trans. Inf. Theory*, vol. 63, no. 10, pp. 6179–6187, Oct. 2017.
[12] S. Hoory, N. Linial, and A. Wigderson, "Expander graphs and their applications," *Bull. Amer. Math. Soc.*, vol. 43, no. 4, pp. 439–561, 2006.
[13] X. L. Hubaut, "Strongly regular graphs," *Discrete Math.*, vol. 13, no. 4, pp. 357–381, 1975.
[14] D. Sarwate, "Meeting the Welch bound with equality," in *Proc. SETA*, vol. 98. London, U.K.: Springer, 1999, pp. 79–102.
[15] J. J. Seidel, *Strongly Regular Graphs. Surveys in Combinatorics*, Cambridge, U.K.: Cambridge Univ. Press, 1979, pp. 157–180.
[16] S. Sun, L. Han, Y. Yan, and Y. Yao, "Two new classes of codebooks asymptotically achieving the Welch bound," *IEEE Access*, vol. 9, pp. 5881–5886, 2021.
[17] L. Tian, Y. Li, T. Liu, and C. Xu, "Constructions of codebooks asymptotically achieving the Welch bound with additive characters," *IEEE Signal Process. Lett.*, vol. 26, no. 4, pp. 622–626, Apr. 2019.
[18] N. Trinajstić, *Chemical Graph Theory. Mathematical Chemistry Series*, 2nd ed. Boca Raton, FL, USA: CRC Press, 1992.
[19] R. Lidl and H. Niederreiter, *Finite Fields*. Cambridge, U.K.: Cambridge Univ. Press, 1997.
[20] D. J. Love, R. W. Heath, and T. Strohmer, "Grassmannian beamforming for multiple-input multiple-output wireless systems," *IEEE Trans. Inform. Theory*, vol. 49, no. 10, pp. 2735–2747, Oct. 2003.
[21] G. Luo and X. Cao, "Two constructions of asymptotically optimal codebooks via the hyper Eisenstein sum," *IEEE Trans. Inf. Theory*, vol. 64, no. 10, pp. 6498–6505, Oct. 2018.
[22] G. Luo and X. Cao, "Two classes of near-optimal codebooks with respect to the Welch bound," *Adv. Math. Commun.*, vol. 15, no. 2, pp. 279–289, 2021.
[23] H. Wang, L. Fan, G. Wang, and L. Shen, "Optimal and asymptotically optimal codebooks as regards the Levenshtein bounds," *IEICE Trans. Fundamentals Electron., Commun. Comput. Sci.*, vol. E104.A, no. 7, pp. 979–983, 2021.
[24] Q. Wang and Y. Yan, "Asymptotically optimal codebooks derived from generalised bent functions," *IEEE Access*, vol. 8, pp. 54905–54909, 2020.
[25] L. Welch, "Lower bounds on the maximum cross correlation of signals," *IEEE Trans. Inf. Theory*, vol. IT-20, no. 3, pp. 397–399, May 1974.
[26] W. Lu, X. Wu, X. Cao, and M. Chen, "Six constructions of asymptotically optimal codebooks via the character sums," 2019, *arXiv:1911.00506*.
[27] Y. Yan, Y. Yao, Z. Chen, and Q. Wang, "Two new families of asymptotically optimal codebooks from characters of cyclic groups," *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, vol. E104.A, no. 8, pp. 1027–1032, 2021.

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

XIAODAN LIANG received the B.Sc. degree in technology for computer applications from the Taiyuan University of Science and Technology, Shanxi, China, in 2002, and the Ph.D. degree from Tiangong University, in 2016. She is currently a Professor with the School of Computer Sciences and Technology, Tiangong University. Her research interests include seismic wave analysis and processing, intelligent optimization algorithm and its application in RFID network planning, artificial intelligence, and heuristic computation.

RIZE JIN received the M.S. and Ph.D. degrees in computer engineering from Ajou University (AU), Republic of Korea, in February 2011 and February 2015, respectively. He was an Assistant Professor with the Software Department, AU. Before joining AU, he was a Postdoctoral Researcher with the Department of Computer Engineering, KAIST, Republic of Korea. He is currently a Professor with the School of Software, Tiangong University, China. His research interests include databases, deep learning, and natural language processing.

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