



Cayley sum graphs and their applications to codebooks

Shohei Satake¹ · Yujie Gu²

Received: 27 November 2021 / Revised: 1 August 2022 / Accepted: 28 October 2022 /

Published online: 20 November 2022

© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2022

Abstract

In this paper we first provide two new constructions for Cayley sum graphs, namely, norm-coset graphs and trace-coset graphs, and determine their second largest eigenvalues using Gaussian sums. Next, a connection between Cayley sum graphs and complex codebooks is established. Based on this, infinite families of asymptotically optimal complex codebooks are explicitly constructed. The derived Cayley sum graphs and codebooks either include some known constructions as special cases or provide flexible new parameters.

Keywords Cayley sum graph · Eigenvalue · Gaussian sum · codebook · Welch bound

Mathematics Subject Classification 11T71 · 05C50

1 Introduction

The *Cayley sum graph*, also known as the *addition Cayley graph*, is a variant of the well-studied Cayley graph, see [1, 10, 21] for example.

Let $\Gamma = (V(\Gamma), E(\Gamma))$ be a graph with n vertices which might contain *loops*, i.e., edges that connect a vertex to itself. We say Γ is *K-regular* if every vertex is incident to exactly K edges, where each loop is counted only once. The *adjacency matrix* of Γ , denoted by $A(\Gamma)$, is a square matrix whose columns and rows are indexed by vertices of Γ such that the (u, v) -entry is equal to the number of edges incident to u and v . Eigenvalues of $A(\Gamma)$ are called *eigenvalues of Γ* as well. It is readily seen that $A(\Gamma)$ is a symmetric real matrix and thus all eigenvalues of Γ are real numbers. By the Perron-Frobenius theorem, it can be proved that if Γ is a K -regular graph, then all eigenvalue of Γ are in the interval $[-K, K]$

Communicated by T. Helleseth.

✉ Yujie Gu
gu@inf.kyushu-u.ac.jp

Shohei Satake
satakecomb@gmail.com

¹ School of Interdisciplinary Mathematical Sciences, Meiji University, Tokyo 164-8525, Japan

² Faculty of Information Science and Electrical Engineering, Kyushu University, Fukuoka 819-0395, Japan

and the largest eigenvalue is exactly K , which is also called the *trivial* eigenvalue of Γ . For notation convenience, let $K = \lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_n \geq -K$ denote all the eigenvalues of Γ and let

$$\lambda(\Gamma) := \max_{2 \leq i \leq n} |\lambda_i|$$

denote the second largest eigenvalue (in absolute value) of Γ . In what follows, Γ is always assumed to be a regular graph.

Here we would like to mention that the value $\lambda(\Gamma)$ can be seen as a measure of “randomness” of Γ in graph theory. Indeed, if $\lambda(\Gamma)$ is relatively smaller than the largest eigenvalue of Γ , then Γ has various properties as those of Erdős-Rényi random graphs, which is a consequence of the well-known expander-mixing lemma. This is a fundamental fact in the theory of pseudo-random graphs. For further details of pseudo-random graphs, see a survey paper [26]. On the other hand, if $\lambda(\Gamma)$ is relatively smaller than the largest eigenvalue of Γ , then accordingly the Cheeger constant of Γ is large, implying that Γ is highly-connected. To be precise, the *Cheeger constant* $h(\Gamma)$ of Γ is defined as

$$h(\Gamma) := \min_{\substack{S \subseteq V(\Gamma) \\ 0 < |S| \leq \frac{n}{2}}} \frac{|\partial S|}{|S|},$$

where ∂S denotes the set of edges such that one vertex of the edge lies in S and another vertex in $V(\Gamma) \setminus S$. A relationship between Cheeger constant and the eigenvalue $\lambda(\Gamma)$ is established by the following *Cheeger inequality* (see e.g. [24, Theorem 2.4]).

$$h(\Gamma) \geq \frac{K - \lambda(\Gamma)}{2}. \quad (1)$$

This is a significant attribution of expander graphs and has wide applications in coding theory [45]; cryptography [55]; communication networks [5]; and more. For more details on expander graphs, see e.g. [24].

Constructing regular graphs with small nontrivial eigenvalues (in absolute value) is one of the central issues in the study of pseudo-random graphs and expander graphs. It typically provides important examples (or counterexamples) to various problems in graph theory and combinatorics [2, 3, 22, 27, 37]. In fact, the Cayley sum graph is a good candidate of generically constructing such desired regular graphs.

Definition 1 (*Cayley sum graphs*) Let (G, \oplus) be an abelian group and $D \subseteq G$. Then the *Cayley sum graph* $\text{CayS}(G, D)$ is a graph with vertex set G such that two vertices x, y are adjacent if and only if $x \oplus y \in D$.

Here we would like to follow the terminology Cayley “sum” graphs as in the literature (see e.g. [6]). However, as we mentioned before, the operation \oplus could be specifically expressed as addition “+”, multiplication “·”, or their combinations.

In this paper, we provide two new constructions for Cayley sum graphs, namely *norm-coset graphs* and *trace-coset graphs*, and determine their second largest eigenvalues using the evaluation of the modulus of Gaussian sums. It is also shown that the new constructions include some existing graphs (e.g. projective norm graph in [3]) as special cases. Furthermore we establish a connection between Cayley sum graphs and the maximum cross-correlation amplitude of complex codebooks. Based on the newly constructed graphs and newly established connection, infinite families of complex codebooks are derived. The resulted codebooks have flexible new parameters (see Table 1) and asymptotically achieve the Welch bound or Levenshtein bound accordingly. In addition, the alphabet size of these codebooks is rather small.

Table 1 The parameters of codebooks, where q is a power of a prime p

| Reference | (N, K) | I_{max} | Alphabet size |
|----------------|--|--|-----------------------|
| [40, 52] | (N, N) | 0 | N |
| [40, 52] | $(N, N - 1)$ | $\frac{1}{N-1}$ | $N - 1$ |
| [58] | $(q^l - q^{l-1} - 1, q^{l-1})$ for $l > 2$ | $\frac{1}{q^{l-1}}$ | $q^l + 1$ |
| [23] | $((q - 1)^k + m, m)$ where $m = \frac{(q-1)^k + (-1)^k}{q}, k > 2$ | $\frac{\frac{k-1}{2}}{m}$ | $q + 1$ |
| [23] | $((q - 1)^k + q^{k-1}, q^{k-1})$ for $k > 2, q \geq 4$ | $\frac{q^{\frac{k+1}{2}}}{(q-1)^k + (-1)^{k+1}}$ | $q + 1$ |
| Construction 5 | $(\frac{q^t - q^{t-1}}{v} + q^{t-1} - 1, q^{t-1} - 1)$ where $t \geq 1, v (q - 1)$ | $\frac{q^{\frac{t-1}{2}}}{q^{t-1} - 1}$ | $p \frac{q-1}{v} + 2$ |
| Construction 6 | $(\frac{q^t - q}{u} + q^{t-1} - 1, q^{t-1} - 1)$ where $t \geq 1, u q$ | $\frac{q^{\frac{t-1}{2}}}{q^{t-1} - 1}$ | $p(q^{t-1} - 1) + 2$ |

Moreover, by virtue of a number-theoretic result, we show that the provided constructions (as well as many existing constructions) can produce asymptotically optimal codebooks with *almost all* possible length.

The remainder of this paper is organized as follows. In Sect. 2, we present preliminary notations and results in finite fields. Sections 3 and 4 are devoted to explicitly constructing Cayley sum graphs and estimating their second largest eigenvalues. In Sect. 5, a relationship between complex codebooks and Cayley sum graphs is established. Asymptotically optimal complex codebooks and some discussions are provided in Sect. 6. Finally this paper is concluded in Sect. 7.

2 Preliminaries

In this section we recall some mathematical foundations which are useful in the subsequent statements.

Let (G, \oplus) be an abelian group of order $|G|$ such that $a \oplus b = b \oplus a$ for any $a, b \in G$. We also simply use G rather than (G, \oplus) to denote a group if the operation \oplus is clear or not necessarily claimed. A *character* χ on G is a group homomorphism from G to the multiplicative group of the complex field \mathbb{C}^* such that $\forall a, b \in G$, we have $\chi(a \oplus b) = \chi(a)\chi(b)$ and $|\chi(a)| = 1$. For every $a \in G$, let $\ominus a$ denote the *inverse* element of a in G and thus $a \oplus b = c$ is equivalent to $a = c \ominus b$. Moreover we have $\chi(\ominus a) = \overline{\chi(a)}$ for each character χ . If a character χ such that for any $a \in G, \chi(a) = 1$, then χ is called the *principal character* of G and denoted by χ_0 . The set of all characters of G forms an abelian group, called the *character group* of G and denoted by \widehat{G} . The inverse of χ in \widehat{G} is $\overline{\chi}$ where $\overline{\chi}(g) := \overline{\chi(g)}$ for all $g \in G$. It is well-known that $|\widehat{G}| = |G|$. The reader is also referred to [4] for more details of group theory. We remark that in the sequel the operation \oplus could specifically be addition “+”, multiplication “.”, or their combinations in the corresponding settings.

Let \mathbb{F}_q denote the finite field with q elements, where q is a prime power. Let \mathbb{F}_q^+ and \mathbb{F}_q^* be the additive and multiplicative group of \mathbb{F}_q respectively, where $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\} = \{g^i : 0 \leq i \leq q - 2\}$ is a cyclic group of order $q - 1$ and g is called a *primitive element* of \mathbb{F}_q . For

$t \geq 1$, let \mathbb{F}_{q^t} denote an extension field of \mathbb{F}_q , which has the same structure as a linear space over \mathbb{F}_q of dimension t . Let $\text{Tr}_{q^t/q}$ be the *trace* function from \mathbb{F}_{q^t} to \mathbb{F}_q defined as

$$\text{Tr}_{q^t/q}(x) := x + x^q + \dots + x^{q^{t-1}}$$

for any $x \in \mathbb{F}_{q^t}$. This is a linear mapping from \mathbb{F}_{q^t} to \mathbb{F}_q , that is, for any $x, y \in \mathbb{F}_{q^t}$ and $\alpha \in \mathbb{F}_q$, we have $\text{Tr}_{q^t/q}(x) \in \mathbb{F}_q$, $\text{Tr}_{q^t/q}(x + y) = \text{Tr}_{q^t/q}(x) + \text{Tr}_{q^t/q}(y)$ and $\text{Tr}_{q^t/q}(\alpha x) = \alpha \text{Tr}_{q^t/q}(x)$. Let $\text{Nr}_{q^t/q}$ denote the *norm* function from \mathbb{F}_{q^t} to \mathbb{F}_q such that

$$\text{Nr}_{q^t/q}(x) := x^{1+q+q^2+\dots+q^{t-1}}$$

for any $x \in \mathbb{F}_{q^t}$. This is a group homomorphism from $\mathbb{F}_{q^t}^*$ to \mathbb{F}_q^* , that is, for any $x, y \in \mathbb{F}_{q^t}^*$, we have $\text{Nr}_{q^t/q}(x) \in \mathbb{F}_q^*$ and $\text{Nr}_{q^t/q}(xy) = \text{Nr}_{q^t/q}(x)\text{Nr}_{q^t/q}(y)$. Notice that both $\text{Tr}_{q^t/q}$ and $\text{Nr}_{q^t/q}$ are surjective.

Definition 2 (1) An *additive character* ψ of \mathbb{F}_q is a homomorphism from \mathbb{F}_q^+ to \mathbb{C}^* such that $\psi(x + y) = \psi(x)\psi(y)$ for any $x, y \in \mathbb{F}_q$. Denote the set of all additive characters of \mathbb{F}_q as $\widehat{\mathbb{F}_q^+}$.

(2) A *multiplicative character* χ of \mathbb{F}_q is a homomorphism from \mathbb{F}_q^* to \mathbb{C}^* such that $\chi(xy) = \chi(x)\chi(y)$ for any $x, y \in \mathbb{F}_q^*$. Denote the set of all multiplicative characters of \mathbb{F}_q as $\widehat{\mathbb{F}_q^*}$.

In addition, if $\psi(x) = 1$ (resp. $\chi(x) = 1$) for all $x \in \mathbb{F}_q$, then we call it the *principal* additive (resp. multiplicative) character of \mathbb{F}_q , denoted by ψ_0 (resp. χ_0). More generally, suppose that $q = p^s$ where p is a prime and $s \geq 1$ is an integer. Let ζ_n denote a primitive n th complex root of unity and g denote a primitive element of \mathbb{F}_q . Then we have $\widehat{\mathbb{F}_q^+} = \{\psi_a(x) = \zeta_p^{\text{Tr}_{p^s/p}(ax)} : a \in \mathbb{F}_q\}$ and $\widehat{\mathbb{F}_q^*} = \{\chi_b(g^i) = \zeta_{q-1}^{bi} : 0 \leq b \leq q - 2\}$. Clearly, $|\widehat{\mathbb{F}_q^+}| = |\mathbb{F}_q^+| = q$ and $|\widehat{\mathbb{F}_q^*}| = |\mathbb{F}_q^*| = q - 1$.

Definition 3 Let $\psi \in \widehat{\mathbb{F}_q^+}$ and $\chi \in \widehat{\mathbb{F}_q^*}$. Then the *Gaussian sum* $\mathcal{G}_q(\psi, \chi)$ is defined as

$$\mathcal{G}_q(\psi, \chi) := \sum_{x \in \mathbb{F}_q^*} \psi(x)\chi(x). \tag{2}$$

Lemma 1 [33]

- (a) If ψ and χ are principal, then $\mathcal{G}_q(\psi, \chi) = q - 1$.
- (b) If ψ is principal and χ is non-principal, then $\mathcal{G}_q(\psi, \chi) = 0$.
- (c) If ψ is non-principal and χ is principal, then $\mathcal{G}_q(\psi, \chi) = -1$.
- (d) If ψ and χ are non-principal, then $|\mathcal{G}_q(\psi, \chi)| = \sqrt{q}$.

2.1 The second largest eigenvalue of Cayley sum graphs

From Definition 1, it is readily seen that $\text{CayS}(G, D)$ is $|D|$ -regular and each vertex is involved in at most one loop. The following lemma, which is well known in graph theory (e.g. [1, 6, 29]), shows that $\lambda(\text{CayS}(G, D))$ could be expressed by character sums over G . We provide a complete proof of this result below for the reader's convenience.

Lemma 2 Let (G, \oplus) be an abelian group of order n and $D \subseteq G$. Then

$$\lambda(\text{CayS}(G, D)) = \max_{\chi \in \widehat{G} \setminus \{\chi_0\}} |\chi(D)|. \tag{3}$$

Proof We first claim that each eigenvalue of $CayS(G, D)$ can be expressed by a character sum. Let $A = A(CayS(G, D))$ be the adjacency matrix of $CayS(G, D)$ and for each character $\chi \in \widehat{G}$, let $\mathbf{v}_\chi = (\chi(g))_{g \in G}^T$. Then we have

$$A\mathbf{v}_\chi = \left(\sum_{d \in D} \chi(d \oplus g) \right)_{g \in G}^T = \left(\sum_{d \in D} \chi(d)\overline{\chi(g)} \right)_{g \in G}^T = \left(\sum_{d \in D} \chi(d) \right) \overline{\mathbf{v}_\chi} = \chi(D)\overline{\mathbf{v}_\chi} \tag{4}$$

where $\overline{\mathbf{v}_\chi} = (\overline{\chi(g)})_{g \in G}^T$. Similarly,

$$A\overline{\mathbf{v}_\chi} = \left(\sum_{d \in D} \overline{\chi(d)} \right) \mathbf{v}_\chi = \overline{\chi(D)}\mathbf{v}_\chi. \tag{5}$$

Now we obtain

$$A^2\mathbf{v}_\chi = A(A\mathbf{v}_\chi) \stackrel{(4)}{=} \chi(D)A\overline{\mathbf{v}_\chi} \stackrel{(5)}{=} |\chi(D)|^2\mathbf{v}_\chi,$$

which means that $|\chi(D)|^2$ is an eigenvalue of A^2 and \mathbf{v}_χ is an eigenvector with respect to $|\chi(D)|^2$. Notice that A^2 is symmetric and the set of vectors $\{\mathbf{v}_\chi\}_{\chi \in \widehat{G}}$ forms an orthogonal basis of \mathbb{C}^n . This implies that the multiset $\{|\chi(D)|^2 : \chi \in \widehat{G}\}$ comprises all eigenvalues of A^2 . Equivalently, every eigenvalue of A (in absolute value) could be expressed in the form of $|\chi(D)|$. Also notice that $\chi_0(D) = |D|$ corresponds to the largest eigenvalue, then the lemma follows. \square

As a consequence of the proof of Lemma 2 we can obtain the whole spectrum of $CayS(G, D)$ (see also [29, Propositions 1 and 2]).

Corollary 1 *Let $I_1 = \{\chi \in \widehat{G} : \chi(D) = 0\}$, $I_2 = (\widehat{G} \setminus \{\chi_0\}) \setminus I_1$. Then the multiset of all eigenvalues of $CayS(G, D)$ are*

$$\{\chi_0(D)\} \cup \{\chi(D) = 0 : \chi \in I_1\} \cup \{\pm|\chi(D)| : \chi \in I_2\}.$$

Here for $\chi \in I_1$, eigenvectors corresponding to $\chi(D)$ are \mathbf{v}_χ and $\overline{\mathbf{v}_\chi}$, and for $\chi \in I_2$, eigenvectors corresponding to $\pm|\chi(D)|$ are $\mathbf{u}_\chi^\pm := |\chi(D)|\mathbf{v}_\chi \pm \chi(D)\overline{\mathbf{v}_\chi}$ respectively.

Remark 1 To enumerate all eigenvalues with multiplicity, we shall enumerate characters consisting of (1) χ_0 , (2) χ with $\chi(D) = 0$, (3) χ such that $\chi = \overline{\chi}$, (4) one of $\{\chi, \overline{\chi}\}$ with $\chi \neq \overline{\chi}$. In fact, when I_2 contains a character χ with $\chi = \overline{\chi}$, then $\chi(D)$ is a non-zero real number and only one of $\{|\chi(D)|, -|\chi(D)|\}$ can be an eigenvalue since if $\chi(D) > 0$ (resp. $\chi(D) < 0$) then $-|\chi(D)|$ (resp. $|\chi(D)|$) cannot be an eigenvalue since the corresponding eigenvector is $\mathbf{0}$. Also if $\chi \neq \overline{\chi}$ then \mathbf{u}_χ^\pm and $\mathbf{u}_{\overline{\chi}}^\pm$ are in fact linearly dependent since

$$\begin{aligned} \mathbf{u}_\chi^+ &= |\chi(D)|\overline{\mathbf{v}_\chi} + \overline{\chi(D)}\mathbf{v}_\chi = |\chi(D)|\overline{\mathbf{v}_\chi} + \overline{\chi(D)}\mathbf{v}_\chi = \frac{|\chi(D)|}{\chi(D)}\mathbf{u}_{\overline{\chi}}^+, \\ \mathbf{u}_{\overline{\chi}}^- &= |\chi(D)|\mathbf{v}_{\overline{\chi}} - \overline{\chi(D)}\overline{\mathbf{v}_\chi} = |\chi(D)|\overline{\mathbf{v}_\chi} - \overline{\chi(D)}\mathbf{v}_\chi = -\frac{|\chi(D)|}{\chi(D)}\mathbf{u}_{\overline{\chi}}^-. \end{aligned}$$

3 Norm-coset graphs

In this section, we present our first construction of Cayley sum graphs, namely, norm-coset graphs, and investigate their second largest eigenvalues.

First we define norm-coset graphs and then prove that they are Cayley sum graphs. For notations, we will use the capital letter to denote an element in the extension field (i.e. $Y \in \mathbb{F}_{q^{t-1}}$) in order to distinguish it with the lowercase letter denoting $x \in \mathbb{F}_q$.

Definition 4 Let q be a prime power and $t \geq 2$ be an integer. Let v be a divisor of $q - 1$ and H^\times be a subgroup of order v of the multiplicative group \mathbb{F}_q^* . Then the *norm-coset graph* $N\Gamma_{q,v,t,H^\times}^\times$ is a graph with vertex set $(\mathbb{F}_q^*/H^\times) \times \mathbb{F}_{q^{t-1}}^+ = \{(\bar{x}, Y) : \bar{x} \in \mathbb{F}_q^*/H^\times, Y \in \mathbb{F}_{q^{t-1}}^+\}$ such that two vertices $(\bar{x}_1, Y_1), (\bar{x}_2, Y_2)$ are adjacent if and only if $\text{Nr}_{q^{t-1}/q}(Y_1 + Y_2) \in \overline{x_1 x_2} = \overline{x_1 x_2}$.

We would like to mention that the norm-coset graphs defined above actually include several known graphs as special cases, as described below.

- (1) If the subgroup H^\times is of order one (i.e., $v = 1$), the graph $N\Gamma_{q,v,t,H^\times}^\times$ turns out to be the so-called *projective norm graph* $NG_{q,t}$, which was introduced by Alon, Ronyai and Szabó [3] and provides good bounds for Turán numbers and Ramsey numbers [2, 3].
- (2) If $t = 2$, the graph $N\Gamma_{q,v,t,H^\times}^\times$ turns out to be the so-called *product-coset graph* G^\times , which was introduced by Lentz and Mubayi and used to prove sharp bounds for multi-colored Ramsey numbers [27].
- (3) If $t = 2$ and H^\times is of order one (i.e., $v = 1$), the graph $N\Gamma_{q,v,t,H^\times}^\times$ turns out to be the so-called *sum-product graph* SP_q , which was defined by Solymosi [46] and employed to prove Garaev’s theorem [19] in additive combinatorics.

To the best of our knowledge, these known graphs have been independently considered in graph theory and additive combinatorics, which have not yet been pointed out and investigated in terms of Cayley sum graphs. In the following Proposition 1 we will show that these known graphs (as special cases of norm-coset graphs) are in fact Cayley sum graphs over the corresponding abelian groups, which provides a unified view to compute their eigenvalues as well. In particular, our result improves upon the existing eigenvalue estimation on $\lambda(SP_q)$ for sum-product graphs. Precisely, Solymosi proved that $\lambda(SP_q) < \sqrt{3q}$ in [46], while the Proposition 1 below yields that $\lambda(SP_q) = \sqrt{q}$.

In the following proposition, we claim that $N\Gamma_{q,v,t,H^\times}^\times$ is a Cayley sum graph and determine the exact value of $\lambda(N\Gamma_{q,v,t,H^\times}^\times)$ accordingly.

Proposition 1 Suppose that $G = (\mathbb{F}_q^*/H^\times) \times \mathbb{F}_{q^{t-1}}^+$ and $D = \{(\bar{x}, Y) \in (\mathbb{F}_q^*/H^\times) \times \mathbb{F}_{q^{t-1}}^+ : \text{Nr}_{q^{t-1}/q}(Y) \in \bar{x}\}$. Then $N\Gamma_{q,v,t,H^\times}^\times$ is a Cayley sum graph $\text{CayS}(G, D)$, and $\lambda(N\Gamma_{q,v,t,H^\times}^\times) = q^{\frac{t-1}{2}}$.

Proof It is easy to see that $G = (\mathbb{F}_q^*/H^\times) \times \mathbb{F}_{q^{t-1}}^+$ is an abelian group of order $q^{t-1}(q - 1)/v$ under the operation $(\bar{x}_1, Y_1) \oplus (\bar{x}_2, Y_2) = (\overline{x_1 x_2}, Y_1 + Y_2) = (\overline{x_1 x_2}, Y_1 + Y_2)$. By Definition 4, two vertices (\bar{x}_1, Y_1) and (\bar{x}_2, Y_2) are adjacent if and only if $(\bar{x}_1, Y_1) \oplus (\bar{x}_2, Y_2) = (\overline{x_1 x_2}, Y_1 + Y_2) \in D$, that is, $\text{Nr}_{q^{t-1}/q}(Y_1 + Y_2) \in \overline{x_1 x_2}$. Thus according to Definition 1, $N\Gamma_{q,v,t,H^\times}^\times$ is a Cayley sum graph $\text{CayS}(G, D)$. Now we claim that for each non-zero $Y \in \mathbb{F}_{q^{t-1}}^+$, there exists a unique corresponding $(\bar{x}, Y) \in D$. Indeed, given Y , the value $y = \text{Nr}_{q^{t-1}/q}(Y) \in \mathbb{F}_q^*$ could be first uniquely determined; next, for each $y \in \mathbb{F}_q^*$, there exists a unique coset $\bar{x} = \bar{y} \in \mathbb{F}_q^*/H^\times$ containing y , since all the cosets in \mathbb{F}_q^*/H^\times form a partition of \mathbb{F}_q^* . Based on this, we have $|D| = |\mathbb{F}_{q^{t-1}}^+ \setminus \{0\}| = q^{t-1} - 1$, which is the degree of each vertex in $N\Gamma_{q,v,t,H^\times}^\times$.

Next we are going to determine the value of $\lambda(N\Gamma_{q,v,t,H^\times}^\times)$. Notice that $\widehat{G} = \{(\nu \otimes \psi) : \nu \in \widehat{\mathbb{F}_q^*/H^\times}, \psi \in \widehat{\mathbb{F}_{q^{t-1}}^+}\}$ where $(\nu \otimes \psi)(\bar{x}, Y) = \nu(\bar{x})\psi(Y)$ for all $(\bar{x}, Y) \in G$. According

to Lemma 2, we have

$$\lambda(N\Gamma_{q,v,t,H^\times}^\times) = \max \left\{ \left| \sum_{(\bar{x}, Y) \in D} (\nu \otimes \psi)(\bar{x}, Y) \right| : \nu \in \widehat{\mathbb{F}_q^*/H^\times}, \psi \in \widehat{\mathbb{F}_{q^{t-1}}^+}, \nu \otimes \psi \neq \nu_0 \otimes \psi_0 \right\}.$$

By the assumption of D ,

$$\begin{aligned} \sum_{(\bar{x}, Y) \in D} (\nu \otimes \psi)(\bar{x}, Y) &= \sum_{(\bar{x}, Y) \in D} \nu(\bar{x})\psi(Y) \\ &= \sum_{\substack{Y \in \mathbb{F}_{q^{t-1}}^+ \setminus \{0\}, \\ y = \text{Nr}_{q^{t-1}/q}(Y)}} \nu(\bar{y})\psi(Y) \\ &= \sum_{Y \in \mathbb{F}_{q^{t-1}}^*} \nu(\overline{\text{Nr}_{q^{t-1}/q}(Y)})\psi(Y). \end{aligned}$$

Now we define a new multiplicative character χ' of \mathbb{F}_q by letting $\chi'(x) := \nu(\bar{x})$. This is well-defined since for any $x, y \in \mathbb{F}_q^*$ and $\nu \in \widehat{\mathbb{F}_q^*/H^\times}$, we have $\chi'(xy) = \nu(\overline{xy}) = \nu(\bar{x} \cdot \bar{y}) = \nu(\bar{x})\nu(\bar{y}) = \chi'(x)\chi'(y)$. It follows by the definition of D that the condition $(\bar{x}, Y) \in D$ implies that $\bar{x} = \overline{\text{Nr}_{q^{t-1}/q}(Y)}$ in the quotient group \mathbb{F}_q^*/H^\times . Then we have

$$\begin{aligned} \sum_{Y \in \mathbb{F}_{q^{t-1}}^*} \nu(\overline{\text{Nr}_{q^{t-1}/q}(Y)})\psi(Y) &= \sum_{Y \in \mathbb{F}_{q^{t-1}}^*} \chi'(\text{Nr}_{q^{t-1}/q}(Y))\psi(Y) \\ &= \sum_{Y \in \mathbb{F}_{q^{t-1}}^*} (\chi' \circ \text{Nr}_{q^{t-1}/q})(Y)\psi(Y) \end{aligned}$$

which is a Gaussian sum $\mathcal{G}_{q^{t-1}}(\psi, \chi' \circ \text{Nr}_{q^{t-1}/q})$ since $\chi' \circ \text{Nr}_{q^{t-1}/q}$ is a multiplicative character of $\mathbb{F}_{q^{t-1}}$ as well. Notice that the character $\chi' \circ \text{Nr}_{q^{t-1}/q}$ is principal if and only if χ' is principal. According to the definition of χ' , the multiplicative character $\chi' \circ \text{Nr}_{q^{t-1}/q}$ is non-principal if and only if ν is non-principal. Thus by Lemma 1, we have $\lambda(N\Gamma_{q,v,t,H^\times}^\times) = \max\{0, 1, q^{\frac{t-1}{2}}\} = q^{\frac{t-1}{2}}$, as required. □

According to the discussion in the proof, we can determine the whole spectrum of $N\Gamma_{q,v,t,H^\times}^\times$, which immediately follows from Lemma 1 and Corollary 1 (with Remark 1).

Corollary 2 *Let q be an odd prime power. Then the graph $N\Gamma_{q,v,t,H^\times}^\times$ has eigenvalues $q^{t-1} - 1$ (with multiplicity 1), $\pm q^{\frac{t-1}{2}}$ (with multiplicity $\frac{1}{2}(q^{t-1} - 1)(\frac{q-1}{v} - 1)$, respectively), 0 (with multiplicity $\frac{q-1}{v} - 1$) and ± 1 (with multiplicity $\frac{1}{2}(q^{t-1} - 1)$, respectively).*

By Proposition 1 we obtain the following propositions regarding graph-theoretic properties of norm-coset graphs such as *diameter* (i.e. the maximum length of the shortest path) and Cheeger constant.

Proposition 2 *The diameter of $N\Gamma_{q,v,t,H^\times}^\times$ is 2.*

Proof Chung [10] proved that if Γ is a K -regular graph with n vertices then the diameter of Γ is at most $\log(n - 1) / \log(K / \lambda(\Gamma))$. Since $N\Gamma_{q,v,t,H^\times}^\times$ is a $(q^{t-1} - 1)$ -regular graph with $q^{t-1}(q - 1)/v$ vertices and $\lambda(N\Gamma_{q,v,t,H^\times}^\times) = q^{\frac{t-1}{2}}$, the diameter is at most

$$\frac{t - \log(v)}{\frac{t-1}{2} + o(1)} = 2 \cdot \frac{t - \log(v)}{t - 1 + o(1)} < 3.$$

Notice that a graph Γ has diameter 1 if and only if Γ is a complete graph, and hence the diameter of $N\Gamma_{q,v,t,H^\times}^\times$ is 2 since it is not a complete graph. □

The following bound of $h(N\Gamma_{q,v,t,H^\times}^\times)$ immediately follows from the Cheeger inequality (1).

Proposition 3 *For the Cheeger constant we have*

$$h(N\Gamma_{q,v,t,H^\times}^\times) \geq \frac{q^{t-1} - q^{\frac{t-1}{2}} - 1}{2}.$$

4 Trace-coset graphs

In this section, we present our second construction of Cayley sum graphs, namely, trace-coset graphs, and determine their second largest eigenvalues.

We first define trace-coset graphs and then show that they are Cayley sum graphs.

Definition 5 Let q be a prime power and $t \geq 2$ be an integer. Let u be a divisor of q and H^+ be a subgroup of order u of the additive group \mathbb{F}_q^+ . Then the *trace-coset graph* $T\Gamma_{q,u,t,H^+}^+$ is a graph with vertex set $(\mathbb{F}_q^+ / H^+) \times \mathbb{F}_{q^{t-1}}^* = \{(\bar{x}, Y) : \bar{x} \in \mathbb{F}_q^+ / H^+, y \in \mathbb{F}_{q^{t-1}}^*\}$ such that two vertices $(\bar{x}_1, Y_1), (\bar{x}_2, Y_2)$ are adjacent if and only if $\text{Tr}_{q^{t-1}/q}(Y_1 Y_2) \in \overline{\bar{x}_1 + \bar{x}_2} = \overline{\bar{x}_1 + \bar{x}_2}$.

The trace-coset graph defined above can deduce some known graphs as described below.

- (1) If $t = 2$, the trace-coset graph $T\Gamma_{q,u,t,H^+}^+$ turns out to be a *sum-coset graph* G^+ , which was introduced by Lentz and Mubayi and used to prove sharp bounds for multicolored Ramsey numbers [27].
- (2) If $t = 2$ and H^+ is trivial (i.e., $u = 1$), the graph $T\Gamma_{q,v,t,H^+}^+$ turns out to be the *sum-product graph* SP_q [46].

In the following, we claim that $T\Gamma_{q,u,t,H^+}$ is a Cayley sum graph and determine the exact value of $\lambda(T\Gamma_{q,u,t,H^+})$ as well.

Proposition 4 *Suppose that $G = (\mathbb{F}_q^+ / H^+) \times \mathbb{F}_{q^{t-1}}^*$ and $D = \{(\bar{x}, Y) \in (\mathbb{F}_q^+ / H^+) \times \mathbb{F}_{q^{t-1}}^* : \text{Tr}_{q^{t-1}/q}(Y) \in \bar{x}\}$. Then $T\Gamma_{q,v,t,H^+}^+$ is a Cayley sum graph $\text{CayS}(G, D)$, and $\lambda(T\Gamma_{q,u,t,H^+}^+) = q^{\frac{t-1}{2}}$.*

Proof It is easy to see that $G = (\mathbb{F}_q^+ / H^+) \times \mathbb{F}_{q^{t-1}}^*$ is an abelian group of order $q(q^{t-1} - 1)/u$ under the operation $(\bar{x}_1, Y_1) \oplus (\bar{x}_2, Y_2) = (\overline{\bar{x}_1 + \bar{x}_2}, Y_1 Y_2) = (\overline{\bar{x}_1 + \bar{x}_2}, Y_1 Y_2)$. By Definition 5, two vertices (\bar{x}_1, y_1) and (\bar{x}_2, y_2) are adjacent if and only if $(\bar{x}_1, y_1) \oplus (\bar{x}_2, y_2) = (\overline{\bar{x}_1 + \bar{x}_2}, y_1 y_2) \in D$, that is, $y_1 y_2 \in \overline{\bar{x}_1 + \bar{x}_2}$. Thus according to Definition 1, $T\Gamma_{q,u,t,H^+}^+$ is a Cayley sum graph $\text{CayS}(G, D)$. Next we claim that for each $Y \in \mathbb{F}_{q^{t-1}}^*$, there exists a unique

corresponding $(\bar{x}, Y) \in D$. In fact, given Y , the value $y = \text{Tr}_{q^{t-1}/q}(Y) \in \mathbb{F}_q^+$ is uniquely determined; also for each $y \in \mathbb{F}_q^+$, there exists a unique coset $\bar{x} = \bar{y} = \mathbb{F}_q^+/H^+$ containing y , since all the cosets in \mathbb{F}_q^+/H^+ form a partition of \mathbb{F}_q^+ . This implies $|D| = |\mathbb{F}_{q^{t-1}}^*| = q^{t-1} - 1$, which is the degree of each vertex in $T\Gamma_{q,u,t,H^+}^+$ as well.

Now we would like to determine $\lambda(T\Gamma_{q,u,t,H^+}^+)$. Notice that $\widehat{G} = \{(\mu \otimes \chi) : \mu \in \widehat{\mathbb{F}_q^+/H^+}, \chi \in \widehat{\mathbb{F}_{q^{t-1}}^*}\}$ where $(\mu \otimes \chi)(\bar{x}, Y) = \mu(\bar{x})\chi(Y)$ for all $(\bar{x}, Y) \in G$. According to Lemma 2, we have

$$\lambda\left(T\Gamma_{q,u,t,H^+}^+\right) = \max \left\{ \left| \sum_{(\bar{x}, Y) \in D} (\mu \otimes \chi)(\bar{x}, Y) \right| : \mu \in \widehat{\mathbb{F}_q^+/H^+}, \chi \in \widehat{\mathbb{F}_{q^{t-1}}^*}, \mu \otimes \chi \neq \mu_0 \otimes \chi_0 \right\}.$$

By the assumption of D ,

$$\begin{aligned} \sum_{(\bar{x}, Y) \in D} (\mu \otimes \chi)(\bar{x}, Y) &= \sum_{(\bar{x}, Y) \in D} \mu(\bar{x})\chi(Y) \\ &= \sum_{\substack{Y \in \mathbb{F}_{q^{t-1}}^* \\ y = \text{Tr}_{q^{t-1}/q}(Y)}} \mu(\bar{y})\chi(Y) \\ &= \sum_{Y \in \mathbb{F}_{q^{t-1}}^*} \mu(\overline{\text{Tr}_{q^{t-1}/q}(Y)})\chi(Y). \end{aligned}$$

Defining an additive character ψ' of \mathbb{F}_q by letting $\psi'(x) = \mu(\bar{x})$ we have

$$\begin{aligned} \sum_{Y \in \mathbb{F}_{q^{t-1}}^*} \mu(\overline{\text{Tr}_{q^{t-1}/q}(Y)})\chi(Y) &= \sum_{Y \in \mathbb{F}_{q^{t-1}}^*} \psi'(\text{Tr}_{q^{t-1}/q}(Y))\chi(Y) \\ &= \sum_{Y \in \mathbb{F}_{q^{t-1}}^*} (\psi' \circ \text{Tr}_{q^{t-1}/q})(Y)\chi(Y) \end{aligned}$$

which is a Gaussian sum $\mathcal{G}_{q^{t-1}}(\psi' \circ \text{Tr}_{q^{t-1}/q}, \chi)$ since $\psi' \circ \text{Tr}_{q^{t-1}/q}$ is in fact an additive character of $\mathbb{F}_{q^{t-1}}$. Notice that the character $\psi' \circ \text{Tr}_{q^{t-1}/q}$ is principal if and only if ψ' is principal. By the definition of ψ' , the additive character $\psi' \circ \text{Tr}_{q^{t-1}/q}$ is non-principal if and only if μ is non-principal. Thus by Lemma 1, we have $\lambda(T\Gamma_{q,u,t,H^+}^+) = \max\{0, 1, q^{\frac{t-1}{2}}\} = q^{\frac{t-1}{2}}$, as required. □

As in Corollary 2 we can determine the whole spectrum of $T\Gamma_{q,u,t,H^+}^+$.

Corollary 3 *Let q be an odd prime power. Then the graph $T\Gamma_{q,u,t,H^+}^+$ has eigenvalues $q^{t-1} - 1$ (with multiplicity 1), $\pm q^{\frac{t-1}{2}}$ (with multiplicity $\frac{1}{2}(q^{t-1} - 2)(\frac{q}{u} - 1)$, respectively), 0 (with multiplicity $q^{t-1} - 2$) and ± 1 (with multiplicity $\frac{1}{2}(\frac{q}{u} - 1)$, respectively).*

The following propositions determine the diameter and estimate the Cheeger constant of $T\Gamma_{q,u,t,H^+}^+$.

Proposition 5 *The diameter of $T\Gamma_{q,u,t,H^+}^+$ is 2.*

Proof Since $T\Gamma_{q,u,t,H^+}^+$ is a $(q^{t-1} - 1)$ -regular graph with $(q^{t-1} - 1)(q/u)$ vertices and $\lambda(T\Gamma_{q,u,t,H^+}^+) = q^{\frac{t-1}{2}}$, the diameter is at most

$$\frac{t - \log(u)}{\frac{t-1}{2} + o(1)} = 2 \cdot \frac{t - \log(u)}{t - 1 + o(1)} < 3.$$

Notice that a graph G has diameter 1 if and only if G is a complete graph, and hence the diameter of $T\Gamma_{q,u,t,H^+}^+$ is 2 since it is not a complete graph. □

According to the Cheeger inequality (1), we have

Proposition 6 *For the Cheeger constant we have*

$$h\left(T\Gamma_{q,u,t,H^+}^+\right) \geq \frac{q^{t-1} - q^{\frac{t-1}{2}} - 1}{2}.$$

5 A connection between codebooks and Cayley sum graphs

In this section, we recall the basics of codebooks and establish a connection between codebooks and Cayley sum graphs.

5.1 Codebooks

An (N, K) codebook $\mathcal{C} = \{\mathbf{c}_1, \dots, \mathbf{c}_N\} \subseteq \mathbb{C}^K$ consists of N complex vectors of length K over an alphabet such that $\|\mathbf{c}_i\|_2 = 1$ for all $1 \leq i \leq N$, which is also termed as a *signal set* or a *frame*. The *alphabet size* of \mathcal{C} refers to the number of elements in the alphabet. Define the *maximum cross-correlation amplitude* $I_{max}(\mathcal{C})$ of an (N, K) codebook \mathcal{C} as

$$I_{max}(\mathcal{C}) := \max_{1 \leq i < j \leq N} |\langle \mathbf{c}_i, \mathbf{c}_j \rangle|, \tag{6}$$

where $\langle \mathbf{c}_i, \mathbf{c}_j \rangle$ denotes the inner product of the complex vectors \mathbf{c}_i and \mathbf{c}_j . For a given K , it is desirable to construct an (N, K) codebook \mathcal{C} with as large N and small $I_{max}(\mathcal{C})$ as possible due to the practical applications in a variety of areas such as code-division multiple-access communication systems [20, 36]; quantum computing [39]; compressed sensing [8, 17, 30–32, 42, 44, 53]; coding theory [7, 13]; and many more. In the literature, a lower bound on $I_{max}(\mathcal{C})$ with respect to N and K was proved in [50], known as the *Welch bound*.

Theorem 1 ([50], Welch bound) *For any (N, K) -codebook \mathcal{C} with $N \geq K$, we have*

$$I_{max}(\mathcal{C}) \geq I_{wei}(N, K) := \sqrt{\frac{N - K}{(N - 1)K}}, \tag{7}$$

where the equality holds if and only if $|\mathbf{c}_i \mathbf{c}_j^H| = \sqrt{\frac{N-K}{(N-1)K}}$ for all $1 \leq i \neq j \leq N$.

A codebook achieving the Welch bound is usually called a *maximum-Welch-bound-equality (MWBE) codebook* [52]. It is also known as the *equiangular tight frame* [9] in frame theory and equivalent to the line packing in Grassmannian spaces [11]. In the literature, certain families of MWBE codebooks were deterministically constructed via discrete Fourier transform matrices [40, 52]; extended codes from any ideal two-level auto-correlation sequences [20, 52, 54];

conference matrices [11, 47]; difference sets in groups [14, 15, 25, 52]; Steiner systems [18], and so on.

As pointed out by Sarwate in [40], it is very hard to explicitly construct MWBE codebooks in general. Hence there have been a number of attempts to construct codebooks nearly meeting the Welch bound, that is, the maximum cross-correlation amplitude $I_{max}(C)$ is slightly higher than the corresponding Welch bound, but asymptotically achieves it when N is large enough. In this paper, we say an infinite family of (N, K_N) -codebooks $\{C_N\}_{N \geq 1}$ is *asymptotically optimal* with respect to the Welch bound if $\lim_{N \rightarrow \infty} I_{max}(C)/I_{wel}(N, K) = 1$. In the literature, asymptotically optimal codebooks have been constructed by using codes and signal sets [40]; almost difference sets [14–16, 56, 57]; binary sequences [54]; multivariate polynomials over finite fields [41]; and so forth.

In [47], it was proved that if $N > K^2$, no complex (N, K) -codebook could achieve the Welch bound $I_{wel}(N, K)$ in (7). Regarding this case, an improved lower bound on $I_{max}(C)$ was provided in [28], which is termed as the *Levenshtein bound* in the literature.

Theorem 2 ([28], Levenshtein bound) *For a complex (N, K) -codebook C with $N > K^2$,*

$$I_{max}(C) \geq I_{lev}(N, K) := \sqrt{\frac{2N - K^2 - 2K}{(N - 1)(K + 1)}}. \tag{8}$$

We say an infinite family of (N, K_N) codebooks $\{C_N\}_{N \geq 1}$ is *asymptotically optimal* with respect to the Levenshtein bound if $\lim_{N \rightarrow \infty} I_{max}(C)/I_{lev}(N, K) = 1$. In the literature, there are known constructions of optimal or asymptotically optimal codebooks with respect to the Levenshtein bound, see [23, 35, 38, 41, 49, 51, 58, 59] for example.

5.2 A generic construction of codebooks from abelian groups

In this subsection we briefly review a constructing method for codebooks proposed by Ding and Feng in [15] and widely adopted such as in [16, 25, 52, 56, 57]. Define a set of n vectors in \mathbb{C}^K by virtue of an abelian group and its K -element subset described as follows.

Definition 6 ([15]) Suppose that G is an abelian group of order n and $\widehat{G} = \{\chi_0, \chi_1, \dots, \chi_{n-1}\}$ is its character group, where χ_0 is the principal character. Let $D = \{d_1, d_2, \dots, d_K\} \subseteq G$. Then define the set of n vectors in \mathbb{C}^K as

$$C(G, D) := \{c_0, c_1, \dots, c_{n-1}\} \tag{9}$$

where

$$c_i := \frac{1}{\sqrt{K}}(\chi_i(d_1), \chi_i(d_2), \dots, \chi_i(d_K))^T, \quad \forall 0 \leq i \leq n - 1. \tag{10}$$

It was proved in [15] that $I_{max}(C(G, D))$ can be calculated by character sums.

Theorem 3 ([15])

$$I_{max}(C(G, D)) = \max_{0 \leq i \neq j \leq n-1} \frac{|(\chi_i \bar{\chi}_j)(D)|}{K} = \max_{\chi \in \widehat{G} \setminus \{\chi_0\}} \frac{|\chi(D)|}{K} \tag{11}$$

where for a character χ of G , $\chi(D) := \sum_{d \in D} \chi(d)$.

A slight modification of the construction in Definition 6 was also appeared in the literature such as [23, 34, 35, 41, 49, 58]. Here we provide a general expression and analysis of it. Let $\mathbf{e}_i = (0, \dots, 0, 1, 0, \dots, 0) \in \{0, 1\}^K$ denote a unit-norm vector such that the i th coordinate of \mathbf{e}_i is 1 and all the other coordinates are 0. Denote $\mathcal{E}_K := \{\mathbf{e}_i : 1 \leq i \leq K\}$, which forms a standard basis of the K -dimensional Hilbert space.

Lemma 3 *The set $\mathcal{C}(G, D) \cup \mathcal{E}_K$ is an $(n + K, K)$ -codebook such that*

$$I_{\max}(\mathcal{C}(G, D) \cup \mathcal{E}_K) = \max \left\{ \frac{1}{\sqrt{K}}, \max_{\chi \in \widehat{G} \setminus \{\chi_0\}} \frac{|\chi(D)|}{K} \right\}. \tag{12}$$

Proof Let \mathbf{a} and \mathbf{b} be two distinct vectors in $\mathcal{C}(G, D) \cup \mathcal{E}_K$. In terms of $|\langle \mathbf{a}, \mathbf{b} \rangle|$, there are three possible cases as follows.

- (1) If $\mathbf{a}, \mathbf{b} \in \mathcal{C}(G, D)$, then according to Theorem 3, we have $|\langle \mathbf{a}, \mathbf{b} \rangle| \leq \frac{1}{K} \max_{\chi \in \widehat{G} \setminus \{\chi_0\}} |\chi(D)|$.
- (2) If $\mathbf{a}, \mathbf{b} \in \mathcal{E}_K$, it is easy to see that $|\langle \mathbf{a}, \mathbf{b} \rangle| = 0$.
- (3) If $\mathbf{a} \in \mathcal{C}(G, D)$ and $\mathbf{b} \in \mathcal{E}_K$, without loss of generality, we may assume that

$$\mathbf{a} = \mathbf{c}_i = (\chi_i(d_1), \chi_i(d_2), \dots, \chi_i(d_K))^T / \sqrt{K}$$

and $\mathbf{b} = \mathbf{e}_j$, where $0 \leq i \leq N - 1$ and $1 \leq j \leq K$. Since χ is a character, we have $|\chi_i(d_j)| = 1$ and hence $|\langle \mathbf{a}, \mathbf{b} \rangle| = |\mathbf{c}_i \mathbf{e}_j^T| = |\chi_i(d_j) / \sqrt{K}| = 1 / \sqrt{K}$.

Thus the lemma follows. □

In terms of this framework, it is required to find appropriate abelian groups G and the corresponding subsets D such that the value $I_{\max}(\mathcal{C}(G, D))$ or $I_{\max}(\mathcal{C}(G, D) \cup \mathcal{E}_K)$ is small enough to meet the Welch bound or Levenshtein bound. However it is in general not an easy task. In the next subsection we provide a feasible way to find such pairs (G, D) from a graph theoretic perspective.

5.3 A connection between codebooks and Cayley sum graphs

In this subsection we establish a connection between complex codebooks and Cayley sum graphs in terms of eigenvalues.

According to each Cayley sum graph $\text{CayS}(G, D)$ we could exploit the pair G and D to construct a set $\mathcal{C}(G, D)$ of n vectors in \mathbb{C}^K by using Definition 6. From Lemma 2 and Theorem 3 we could see that evaluating the maximum cross-correlation amplitude $I_{\max}(\mathcal{C}(G, D))$ of the codebook $\mathcal{C}(G, D)$ is in fact equivalent to estimating the eigenvalue $\lambda(\text{CayS}(G, D))$ of the Cayley sum graph $\text{CayS}(G, D)$. Specifically we have

Corollary 4 *Let G be an abelian group and D be a K -element subset of G . Then the codebook $\mathcal{C}(G, D) \cup \mathcal{E}_K$ satisfies that*

$$I_{\max}(\mathcal{C}(G, D) \cup \mathcal{E}_K) = \max \left\{ \frac{1}{\sqrt{K}}, \frac{\lambda(\text{CayS}(G, D))}{K} \right\}.$$

Here we would like to remark that Corollary 4 could also be obtained from Cayley (directed) graph $\text{Cay}(G, D)$, which is a directed graph with vertex set G and edge set $\{(x, y) : x \ominus y \in D\}$, by using a similar argument of that every eigenvalue of $\text{Cay}(G, D)$ could be expressed by the form of $\chi(D)$ for $\chi \in \widehat{G}$.

It is worth noting that Corollary 4 shows an interesting relationship between the maximum cross-correlation amplitude of a complex codebook and the second largest eigenvalue of a Cayley sum graph. For a positive integer n , let G_n be an abelian group of order n and D_n be a K_n -element subset of G_n . It follows by the Welch bound and the Levenshtein bound that for an infinite family $\{(G_n, D_n)\}_{n \geq 1}$ such that $|D_n| = K_n = o(n)$ as $n \rightarrow \infty$, we have

$$I_{max}(\mathcal{C}(G_n, D_n) \cup \mathcal{E}_K) = \Omega\left(\frac{1}{\sqrt{K_n}}\right). \tag{13}$$

On the other hand, if $K_n = o(n)$, we could have the following bound (see e.g. [26, p. 217]):

$$\lambda(\text{CayS}(G_n, D_n)) = \Omega(\sqrt{K_n}). \tag{14}$$

By Corollary 4, we could see that in the regime of $K_n = o(n)$ the Cayley sum graph $\text{CayS}(G_n, D_n)$ achieves the optimal order of magnitude with respect to the bound (14) if and only if the codebook $\mathcal{C}(G_n, D_n)$ attains the optimal order of magnitude with respect to the bound (13). This implies that

$$\liminf_{n \rightarrow \infty} \frac{I_{max}(\mathcal{C}(G_n, D_n) \cup \mathcal{E}_K)}{I_{wel}(n + K_n, K_n)} = \kappa_1,$$

or

$$\liminf_{n \rightarrow \infty} \frac{I_{max}(\mathcal{C}(G_n, D_n) \cup \mathcal{E}_K)}{I_{lev}(n + K_n, K_n)} = \kappa_2,$$

where κ_1 and κ_2 are constants such that $\kappa_1 \geq 1$ and $\kappa_2 \geq 1$ according to Theorems 1 and 2 respectively. Recall that if $\kappa_1 = 1$ (resp. $\kappa_2 = 1$), the codebook $\mathcal{C}(G_n, D_n) \cup \mathcal{E}_K$ is said to be asymptotically optimal with respect to the Welch bound (resp. Levenshtein bound), which, however, is not easy to be deterministically constructed in general.

Remark 2 According to Ding and Feng [15], the codebook $\mathcal{C}(G, D)$ with a difference set D of G is optimal with respect to the Welch bound. Hence any Cayley sum graph $\text{CayS}(G, D)$ with difference set D of G gives rise to an optimal codebook. On the other hand there seems to be no known construction of optimal codebooks with respect to the Levenshtein bound via specific Cayley sum graphs, which would be an interesting open problem.

6 Explicit codebooks from Cayley sum graphs

In this section we derive asymptotically optimal codebooks based on the newly constructed Cayley sum graphs in Sects. 3 and 4 as well as the established relationship between Cayley sum graphs and codebooks in Sect. 5. The derived codebooks include some existing codebooks as special cases. Furthermore, a discussion on the derived codebooks is also provided based on a number-theoretic result.

6.1 Codebooks from norm-coset graphs

By means of norm-coset graphs, Proposition 1 and Corollary 4 bring forth the Construction 5 below.

Construction 5 Let $t \geq 2$ be an integer, q be a power of a prime p and v be a divisor of $q - 1$. Let H^\times be a subgroup of order v of the multiplicative group \mathbb{F}_q^* . Suppose that

Table 2 Codebooks from Construction 5 when $q = p$ is a prime, $t = 3$ and $v = 2$

| $q = p$ | N | K | I_{max} | I_{wel} | I_{wel}/I_{max} |
|---------|-------|------|-----------|-----------|-------------------|
| 7 | 195 | 48 | 0.145833 | 0.125643 | 0.86155 |
| 11 | 725 | 120 | 0.0916667 | 0.0834484 | 0.910346 |
| 13 | 1182 | 168 | 0.077381 | 0.071489 | 0.923858 |
| 17 | 2600 | 288 | 0.0590278 | 0.0555769 | 0.941539 |
| 19 | 3609 | 360 | 0.0527778 | 0.0500139 | 0.947631 |
| 23 | 6347 | 528 | 0.0435606 | 0.0416732 | 0.956672 |
| 29 | 12614 | 840 | 0.0345238 | 0.033336 | 0.965594 |
| 31 | 15375 | 960 | 0.0322917 | 0.031252 | 0.967805 |
| 37 | 26010 | 1368 | 0.0270468 | 0.0263168 | 0.97301 |
| 41 | 35300 | 1680 | 0.0244048 | 0.0238102 | 0.975637 |
| 43 | 40677 | 1848 | 0.0232684 | 0.0227278 | 0.976768 |
| 47 | 53015 | 2208 | 0.0212862 | 0.0208337 | 0.978742 |
| 53 | 75842 | 2808 | 0.0188746 | 0.0185188 | 0.981145 |

$G = (\mathbb{F}_q^*/H^\times) \times \mathbb{F}_{q^{t-1}}^+$ and $D = \{(\bar{x}, Y) \in (\mathbb{F}_q^*/H^\times) \times \mathbb{F}_{q^{t-1}}^+ : Nr_{q^{t-1}/q}(Y) \in \bar{x}\} \subseteq G$. Then, the codebook $\mathcal{C}(G, D) \cup \mathcal{E}_K$ is an $(n + K, K)$ -codebook such that $n = (q^t - q^{t-1})/v$, $K = q^{t-1} - 1$ and

$$I_{max}(\mathcal{C}(G, D) \cup \mathcal{E}_K) = \frac{q^{\frac{t-1}{2}}}{q^{t-1} - 1}.$$

The alphabet size of the codebook $\mathcal{C}(G, D) \cup \mathcal{E}_K$ is $p(q - 1)/v + 2$.

Remark 3 Concerning $n + K = (q^t - q^{t-1})/v + q^{t-1} - 1$ and $K = q^{t-1} - 1$, the Welch bound in Theorem 1 gives

$$I_{wel}(n + K, K) = \sqrt{\frac{q^t - q^{t-1}}{(q^t + (v - 1)q^{t-1} - 2v)(q^{t-1} - 1)}}.$$

If $t \geq 3$ is fixed and $v = o(q)$ as $q \rightarrow \infty$, the complex codebooks from Construction 5 are asymptotically optimal in the sense that

$$\lim_{n \rightarrow \infty} \frac{I_{max}(\mathcal{C}(G, D) \cup \mathcal{E}_K)}{I_{wel}(n + K, K)} = \lim_{q \rightarrow \infty} \frac{\frac{q^{\frac{t-1}{2}}}{q^{t-1} - 1}}{\sqrt{\frac{q^t - q^{t-1}}{(q^t + (v - 1)q^{t-1} - 2v)(q^{t-1} - 1)}}} = 1.$$

Table 2 below shows numerical examples of codebooks from Construction 5.

We also remark that by virtue of sum-product graphs (i.e. norm-coset graphs with $t = 2$ and $v = 1$), the above Construction 5 can deduce codebooks as obtained in [49], which are asymptotically optimal with respect to the Levenshtein bound.

6.2 Codebooks from trace-coset graphs

Now we present our second construction for codebooks based on Proposition 4 and Corollary 4.

Table 3 Codebooks from Construction 6 when q is a square of a prime p and $t = 3, u = p$

| p | q | N | K | I_{max} | I_{wel} | I_{wel}/I_{max} |
|-----|------|-----------|---------|-------------|-------------|-------------------|
| 7 | 49 | 19200 | 2400 | 0.0204167 | 0.0191155 | 0.936269 |
| 11 | 121 | 175680 | 14640 | 0.00826503 | 0.00791539 | 0.957697 |
| 13 | 169 | 399840 | 28560 | 0.005901737 | 0.00570314 | 0.963796 |
| 17 | 289 | 1503360 | 83520 | 0.00346025 | 0.00336304 | 0.971908 |
| 19 | 361 | 2606400 | 130320 | 0.0027701 | 0.00270013 | 0.97474 |
| 23 | 529 | 6716160 | 279840 | 0.00189037 | 0.00185063 | 0.97898 |
| 29 | 841 | 21218400 | 707280 | 0.00118906 | 0.0011691 | 0.98321 |
| 31 | 961 | 29552640 | 923520 | 0.00104058 | 0.00102421 | 0.984266 |
| 37 | 1369 | 71218080 | 1874160 | 0.000730461 | 0.000720792 | 0.986763 |
| 41 | 1681 | 118681920 | 2825760 | 0.000594884 | 0.000587764 | 0.98803 |
| 43 | 1849 | 150427200 | 3418800 | 0.000540833 | 0.000534655 | 0.988577 |
| 47 | 2209 | 234224640 | 4879680 | 0.000452694 | 0.000447955 | 0.989533 |
| 53 | 3481 | 426085920 | 7890480 | 0.000355999 | 0.000352688 | 0.990701 |

Construction 6 Let $t \geq 2$ be an integer, q be a prime power and u be a divisor of q . Let H^+ be a subgroup of order u of the additive group \mathbb{F}_q^+ . Suppose that $G = (\mathbb{F}_q^+/H^+) \times \mathbb{F}_{q^{t-1}}^+$ and $D = \{(\bar{x}, Y) \in (\mathbb{F}_q^+/H^+) \times \mathbb{F}_{q^{t-1}}^* : \text{Tr}_{q^{t-1}/q}(Y) \in \bar{x}\} \subseteq G$. Then, the codebook $\mathcal{C}(G, D) \cup \mathcal{E}_K$ is an $(N + K, K)$ -codebook such that $N = (q^t - q)/u, K = q^{t-1} - 1$ and

$$I_{max}(\mathcal{C}(G, D) \cup \mathcal{E}_K) = \frac{q^{\frac{t-1}{2}}}{q^{t-1} - 1}.$$

The alphabet size of the codebook $\mathcal{C}(G, D) \cup \mathcal{E}_K$ is $p(q^{t-1} - 1) + 2$.

Remark 4 Concerning $n = (q^t - q)/u$ and $K = q^{t-1} - 1$, the Welch bound in Theorem 1 gives

$$I_{wel}(n + K, K) = \sqrt{\frac{q^t - q}{(q^t + uq^{t-1} - uq - 2u)(q^{t-1} - 1)}}.$$

If $t \geq 3$ is fixed and $u < q$ (equivalently, $u = o(q)$ as $q \rightarrow \infty$), the complex codebooks from Construction 6 are asymptotically optimal in the sense that

$$\lim_{n \rightarrow \infty} \frac{I_{max}(\mathcal{C}(G, D) \cup \mathcal{E}_K)}{I_{wel}(n + K, K)} = \lim_{q \rightarrow \infty} \frac{\frac{q^{\frac{t-1}{2}}}{q^{t-1} - 1}}{\sqrt{\frac{q^t - q}{(q^t + uq^{t-1} - uq - 2u)(q^{t-1} - 1)}}} = 1.$$

Table 3 below presents numerical examples of codebooks derived from Construction 6.

As in the first construction, by virtue of sum-product graphs (i.e. trace-coset graphs with $t = 2$ and $u = 1$), the above Construction 6 can produce asymptotically optimal codebooks with respect to the Levenshtein bound as in [49].

6.3 A further discussion

In this section, we shall further discuss the parameters of asymptotically optimal codebooks derived from Cayley sum graphs (Constructions 5 and 6) with the aid of a number-theoretic result. Specifically, we have the following result.

Theorem 7 *Let p_i denote the i th prime (where $p_1 = 2, p_2 = 3, p_3 = 5, \dots$) and $t \geq 3$ be a fixed integer. Suppose that $p_i - p_{i-1} = o((p_{i-1})^l)$ ($i \rightarrow \infty$) for some real number $0 < l < 1/2$. Then for sufficiently large i and every K with $(p_{i-1})^{t-1} - 1 < K \leq (p_i)^{t-1} - 1$, we have a $((p_i)^t - 1, K)$ codebook which is asymptotically optimal with respect to the Welch bound.*

By the following theorem on prime gaps, we see that Theorem 7 provides asymptotically optimal codebooks for almost all possible length K .

Lemma 4 [12] *For each real number $0 < l \leq 1/2$ and sufficiently large $x > 0$, the number of primes $p_i \leq x$ such that $p_i - p_{i-1} < (p_{i-1})^l$ is at least $x/(\log x) - O(x^{1-(3/2)l+\varepsilon})$ where $\varepsilon > 0$ is an arbitrarily small real number.*

To prove Theorem 7, we need the following lemma which is a direct consequence of Lemma 3.

Lemma 5 *Let G be an abelian group of order n and $D \subseteq G$. Let $1 \leq k \leq K$ and $D' \subseteq D$ with $|D'| = k$. Then $\mathcal{C}(G, D \setminus D') \cup \mathcal{E}_{K-k}$ is an $(n + K - k, K - k)$ -codebook such that*

$$I_{\max}(\mathcal{C}(G, D \setminus D') \cup \mathcal{E}_{K-k}) \leq \max \left\{ \frac{1}{\sqrt{K - k}}, \max_{\chi \in \hat{G} \setminus \{\chi_0\}} \frac{|\chi(D)| + k}{K - k} \right\}.$$

Proof of Theorem 7 For simplicity, we shall focus on Construction 5 for the case that $v = 1$. According to this construction, there exist asymptotically optimal $(n_i + K_i, K_i)$ codebooks with

$$n_i = (p_i)^t - (p_i)^{t-1}, \quad K_i = (p_i)^{t-1} - 1.$$

Let $G_i = \mathbb{F}_{p_i}^* \times \mathbb{F}_{(p_i)^{t-1}}^+$ and $D_i = \{(x, Y) \in (\mathbb{F}_{p_i}^* \times \mathbb{F}_{(p_i)^{t-1}}^+ : \text{Nr}_{(p_i)^{t-1}/p_i}(Y) = x)\}$. Let k be any integer with $1 \leq k < (p_i)^{t-1} - (p_{i-1})^{t-1}$ and $D' \subset D_i$ with $|D'| = k$. By the assumption of p_i , we have $k = o((p_i)^{\frac{t-1}{2}})$. It suffices to prove that the $(n_i + K_i - k, K_i - k)$ codebook $\mathcal{C}(G_i, D_i \setminus D') \cup \mathcal{E}_{K_i-k}$ is asymptotically optimal with respect to the Welch bound. In fact, it follows from Lemma 5 that

$$I_{\max}(\mathcal{C}(G_i, D_i \setminus D') \cup \mathcal{E}_{K_i-k}) \leq \frac{(p_i)^{\frac{t-1}{2}} + o((p_i)^{\frac{t-1}{2}})}{(p_i)^{t-1} - o((p_i)^{\frac{t-1}{2}})},$$

where the right-hand side is asymptotically equal to $1/(p_i)^{\frac{t-1}{2}}$ as $i \rightarrow \infty$. Thus a simple calculation shows that

$$\limsup_{i \rightarrow \infty} \frac{I_{\max}(\mathcal{C}(G_i, D_i \setminus D') \cup \mathcal{E}_{K_i-k})}{I_{\text{Wel}}(n_i + K_i - k, K_i - k)} = 1,$$

proving the theorem. □

We remark that similarly to the above argument, the desired codebooks in Theorem 7 can be derived from Construction 6 and many existing constructions as well.

7 Conclusion

In this paper we constructed two families of Cayley sum graphs and estimated their second largest eigenvalues based on Gaussian sums. Next we established a connection between complex codebooks and Cayley sum graphs. Accordingly, infinite families of complex codebooks were derived, which have flexible new parameters, small alphabet size, and are asymptotically optimal with respect to the Welch bound or the Levenshtein bound. It would be of interest to explore more on the established relationship between Cayley sum graphs and codebooks, such as to consider explicitly constructing good Cayley sum graphs in the spirit of complex codebooks.

Acknowledgements The authors are very grateful to the anonymous reviewers and associated editor for their insightful and constructive comments and suggestions. The authors would like to thank Professor Ofer Shayevitz and Professor Rami Zamir for helpful discussions. S. Satake has been supported by Grant-in-Aid for JSPS Fellows 18J11282 and 20J00469 of the Japan Society for the Promotion of Science and ACT-X JPMJAX2109 of the Japan Science and Technology Agency. Y. Gu has been supported by Grant-in-Aid for Early-Career Scientists 21K13830 of the Japan Society for the Promotion of Science. Parts of this work were presented at [43].

References

1. Alon N.: Large sets in finite fields are sumsets. *J. Number Theory* **126**, 110–118 (2007).
2. Alon N., Rödl V.: Sharp bounds for some multicolor Ramsey numbers. *Combinatorica* **25**, 125–141 (2005).
3. Alon N., Rónyai L., Szabó T.: Norm-graphs: variations and applications. *J. Comb. Theory Ser. B* **76**, 280–290 (1999).
4. Artin M.: *Algebra*. Prentice Hall Inc, New Jersey (1991).
5. Bien F.: Constructions of telephone networks by group representations. *Notices Am. Math. Soc.* **36**, 5–22 (1989).
6. Brouwer A.E., Haemers W.H.: *Spectra of Graphs*. Springer, New York (2012).
7. Calderbank A.R., Cameron P.J., Kantor W.M., Seidel J.J.: \mathbb{Z}_4 -kerdock codes, orthogonal spreads, and extremal Euclidean linesets. *Proc. Lond. Math. Soc.* **75**, 436–480 (1997).
8. Candès E.J., Wakin M.B.: An introduction to compressive sampling. *IEEE Signal Process. Mag.* **25**, 21–30 (2008).
9. Christensen O.: *An Introduction to Frames and Riesz Bases*. Birkhäuser, Boston (2003).
10. Chung F.R.K.: Diameters and eigenvalues. *J. Am. Math. Soc.* **2**, 187–196 (1989).
11. Conwoy J.H., Harding R.H., Sloane N.J.A.: Packing lines, planes, etc.: packings in Grassmannian spaces. *Exp. Math.* **5**, 139–159 (1996).
12. Crámer H.: On the distribution of primes. *Proc. Cam. Philos. Soc.* **20**, 272–280 (1921).
13. Delsarte P., Goethals J.M., Seidel J.J.: Spherical codes and designs. *Geometriae Dedicata* **67**, 363–388 (1977).
14. Ding C.: Complex codebooks from combinatorial designs. *IEEE Trans. Inf. Theory* **52**, 4229–4235 (2006).
15. Ding C., Feng T.: A generic construction of complex codebooks meeting the Welch bound. *IEEE Trans. Inf. Theory* **53**, 4245–4250 (2007).
16. Ding C., Feng T.: Codebooks from almost difference sets. *Des. Codes Cryptogr.* **46**, 113–126 (2008).
17. Donoho D.L., Elad M.: Optimally sparse representation in general (nonorthogonal) dictionaries via ℓ_1 minimization. *Proc. Natl. Acad. Sci. USA* **100**, 2197–2202 (2003).
18. Fickus M., Mixon D.G., Tremain J.C.: Steiner equiangular tight frames. *Linear Algebra Appl.* **436**, 1014–1027 (2012).
19. Garaev M.Z.: An explicit sum-product estimate in \mathbb{F}_q . *Int. Math. Res. Not.* **2007**, 1–11 (2007).
20. Golomb S.W., Gong G.: *Signal Design for Good Correlation: For Wireless Communication, Cryptography and Radar*. Cambridge University Press, Cambridge (2005).
21. Grynkiewicz D., Lev V.F., Serra O.: The connectivity of addition Cayley graphs. *Electron. Notes Discret. Math.* **29**, 135–139 (2007).
22. He X., Wigderson Y.: Multicolor Ramsey numbers via pseudorandom graphs. *Electron. J. Comb.* **27**, 32 (2020).

23. Heng Z., Ding C., Yue Q.: New constructions of asymptotically optimal codebooks with multiplicative characters. *IEEE Trans. Inf. Theory* **63**, 6179–6187 (2017).
24. Hoory S., Linnal N., Wigderson A.: Expander graphs and their applications. *Bull. Am. Math. Soc. (N.S.)* **43**, 439–561 (2006).
25. Hu H., Wu J.: New constructions of codebooks nearly meeting the Welch bound with equality. *IEEE Trans. Inf. Theory* **60**, 1348–1355 (2014).
26. Krivelevich M., Sudakov B.: Pseudo-random graphs. In: Györi E., Katona G.O.H., Lovász L., Fleiner T. (eds.) *More Sets, Graphs and Numbers*. Bolyai Society Mathematical Studies, vol. 15. Springer, Berlin (2006).
27. Lenz J., Mubayi D.: Multicolor Ramsey numbers for complete bipartite versus complete graphs. *J. Graph Theory* **77**, 19–38 (2014).
28. Levenshtein V.I.: Bounds for packing of metric spaces and some of their applications. *Probl. Cybern.* **40**, 43–110 (1983).
29. Li W.-C.W., Feng K.Q.: Character sums and abelian Ramanujan graphs. *J. Number Theory* **41**, 199–217 (1992).
30. Li S., Ge G.: Deterministic sensing matrices arising from near orthogonal systems. *IEEE Trans. Inf. Theory* **60**, 2291–2302 (2014).
31. Li S., Ge G.: Deterministic construction of sparse sensing matrices via finite geometry. *IEEE Trans. Signal Process.* **62**, 2850–2859 (2014).
32. Li S., Gao F., Ge G., Zhang S.: Deterministic construction of compressed sensing matrices via algebraic curves. *IEEE Trans. Inf. Theory* **58**, 5035–5041 (2012).
33. Lidl R., Niederreiter H.: *Finite Fields*. Cambridge University Press, Cambridge (1984).
34. Lu W., Wu X., Cao X., Chen M.: Six constructions of asymptotically optimal codebooks via the character sums. *Des. Codes Cryptogr.* **88**, 1139–1158 (2020).
35. Luo G., Cao X.: Two constructions of asymptotically optimal codebooks via the hyper Eisenstein sum. *IEEE Trans. Inf. Theory* **64**, 6498–6505 (2018).
36. Massey J.L., Mittelholzer T.: Welch bound and sequence sets for code-division multiple-access systems. In: Capocelli R., De Santis A., Vaccaro U. (eds.) *Sequences II*. Springer, New York (1993).
37. Mubayi D., Verstraëte J.: A note on pseudorandom Ramsey graphs. [arXiv:1909.01461](https://arxiv.org/abs/1909.01461)
38. Qi Y., Mesnager S., Tang C.: Codebooks from generalized bent \mathbb{Z}_4 -valued quadratic forms. *Discret. Math.* **343**, 111736 (2020).
39. Renes J.M., Blume-Kohout R., Scot A., Caves C.: Symmetric informationally complete quantum measurements. *J. Math. Phys.* **45**, 2171–2180 (2004).
40. Sarwate D.V.: Meeting the Welch bound with equality. In: Ding C., Helleseht T., Niederreiter H. (eds.) *Sequences and their Applications*. Discrete Mathematics and Theoretical Computer Science. Springer, London (1999).
41. Satake S.: Certain codebooks and the generalized Erdős–Falconer distance problem (extended abstract). In: *Sequences and their Applications* (2020).
42. Satake S.: On the restricted isometry property of the Paley matrix. *Linear Algebra Appl.* **631**, 35–47 (2021).
43. Satake S., Gu Y.: Constructions of complex codebooks asymptotically meeting the Welch bound: A graph theoretic approach. In: *2020 IEEE International Symposium on Information Theory* (pp. 48–53) (2020).
44. Satake S., Gu Y.: On compressed sensing matrices breaking the square-root bottleneck. In: *2020 IEEE Information Theory Workshop* (pp. 1–5) (2020).
45. Sipser M., Spielman D.: Expander codes. *IEEE Trans. Inf. Theory* **42**, 1710–1722 (1996).
46. Solymosi J.: Incidences and the spectra of graphs. In: *Combinatorial Number Theory and Additive Group Theory*. Advanced Courses in Mathematics - CRM Barcelona. Birkhäuser Basel (2009).
47. Strohmer T., Heath R.: Grassmannian frames with applications to coding and communication. *Appl. Comput. Harmon. Anal.* **14**, 257–275 (2003).
48. Szabó T.: On the spectrum of projective norm-graphs. *Inform. Process. Lett.* **86**, 71–74 (2003).
49. Tan P., Zhou Z., Zhang D.: A construction of codebooks nearly achieving the Levenstein bound. *IEEE Signal Process. Lett.* **23**, 1306–1309 (2016).
50. Welch L.: Lower bounds on the maximum cross correlation of signals. *IEEE Trans. Inf. Theory* **20**, 397–399 (1974).
51. Wootters W., Fields B.: Optimal state-determination by mutually unbiased measurements. *Ann. Phys.* **191**, 363–381 (1989).
52. Xia P., Zhou S., Giannakis G.B.: Achieving the Welch bound with difference sets. *IEEE Trans. Inf. Theory* **51**, 1900–1907 (2005).
53. Xu G., Xu Z.: Compressed sensing matrices from Fourier matrices. *IEEE Trans. Inf. Theory* **61**, 469–478 (2015).

54. Yu N.Y.: A construction of codebooks associated with binary sequences. *IEEE Trans. Inf. Theory* **58**, 5522–5533 (2012).
55. Zémor G.: Hash functions and Cayley graphs. *Des. Codes Cryptogr.* **4**, 381–394 (1994).
56. Zhang A., Feng K.: Two classes of codebooks nearly meeting the Welch bound. *IEEE Trans. Inf. Theory* **58**, 2507–2511 (2012).
57. Zhang A., Feng K.: Construction of cyclotomic codebooks nearly meeting the Welch bound. *Des. Codes Cryptogr.* **63**, 209–224 (2012).
58. Zhou Z., Tang X.: New nearly optimal codebooks from relative difference sets. *Adv. Math. Commun.* **5**, 521–527 (2011).
59. Zhou Z., Ding C., Li N.: New families of codebooks achieving the Levenshtein bound. *IEEE Trans. Inf. Theory* **60**, 7382–7387 (2014).

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.