Quantum Information and Computation, Vol. 17, No. 5&6 (2017) 0380–0398

ON THE ONE-SHOT ZERO-ERROR CLASSICAL CAPACITY OF CLASSICAL-QUANTUM CHANNELS ASSISTED BY QUANTUM NON-SIGNALLING CORRELATIONS

CHING-YI LAI[a] RUNYAO DUAN

Centre for Quantum Software and Information, Faculty of Engineering and Information Technology
University of Technology Sydney, NSW, 2007, Australia

Received August 18, 2016
Revised March 8, 2017

Duan and Winter studied the one-shot zero-error classical capacity of a quantum channel assisted by quantum non-signalling correlations, and formulated this problem as a semidefinite program depending only on the Kraus operator space of the channel. For the class of classical-quantum channels, they showed that the *asymptotic* zero-error classical capacity assisted by quantum non-signalling correlations, minimized over all classical-quantum channels with a confusability graph G, is exactly $\log \vartheta(G)$, where $\vartheta(G)$ is the celebrated Lovász theta function. In this paper, we show that the *one-shot* capacity for a classical-quantum channel, induced from a *circulant graph* G defined by *equal-sized cyclotomic cosets*, is $\log\lfloor\vartheta(G)\rfloor$, which further implies that its *asymptotic* capacity is $\log \vartheta(G)$. This type of graphs include the cycle graphs of odd length, the Paley graphs of prime vertices, and the cubit residue graphs of prime vertices. Examples of other graphs are also discussed. This gives Lovász ϑ function another operational meaning in zero-error classical-quantum communication.

Keywords: zero-error capacity, Lovász ϑ function, non-signalling correlation

Communicated by: R Cleve & M Mosca

1 Introduction

Shannon discussed the communication problem in the setting of zero errors and connected this problem to the graph theory [1]. Let $N : V \to W$ be a channel with discrete alphabets V and W. We want to determine the maximum messages that can be sent through the channel N without confusion. Two distinct messages can be confused if their channel outputs are equal with a nonzero probability. It turns out that the maximum distinguishable messages is equal to the largest number of independent vertices $\alpha(G)$ of its *confusability graph* G. The confusability graph G of channel N has a vertex set V, which is the channel input alphabet, and an edge set E so that two vertices v and w are connected (say, $vw \in E$) if their channel outputs are likely to be confused. Using the channel N twice in parallel corresponds to a confusability graph $G \boxtimes G$, where $\boxtimes$ is the graph *strong product*. (For two graphs G_1, G_2 with vertex sets V_1, V_2, and edge sets E_1, E_2, respectively, their strong product $G_1 \boxtimes G_2$ has a vertex set $V_1 \times V_2$, and two vertices (v_1, v_2) and $(w_1, w_2) \in V_1 \times V_2$ are connected if $v_1w_1 \in E_1$ and $v_2w_2 \in E_2$; or $v_1w_1 \in E_1$ and $v_2 = w_2$; or $v_1 = w_1$ and $v_2w_2 \in E_2$.) The *Shannon*

[a]email: cylai0616@gmail.com

capacity of a graph G is defined as

$$\Theta(G) = \sup_n \sqrt[n]{\alpha(G^{\boxtimes n})} = \lim_{n\to\infty} \sqrt[n]{\alpha(G^{\boxtimes n})}. \quad (1)$$

The quantity $\Theta(G)$ is difficult to determine, even for simple graphs, such as cycle graphs $\mathcal{C}_n$ of odd length. In [2], Lovász proposed an upper bound $\vartheta(G)$ (to be defined in Sec. 2) on $\Theta(G)$, and it is tight in some cases. For example, $\Theta(\mathcal{C}_5) = \vartheta(\mathcal{C}_5)$. Although $\Theta(\mathcal{C}_n)$ for odd $n \geq 7$ are still unknown, it seems close to $\vartheta(\mathcal{C}_n)$. However, Haemers showed that it is possible that there is a gap between $\vartheta(G)$ and $\Theta(G)$ for some graphs [3,4]. It is desired to find operational meanings for $\vartheta(G)$, apart from an upper bound for $\Theta(G)$.

Recently the problem of zero-error communication has been studied in quantum information theory [5,6]. Some unexpected phenomena were observed in the quantum case. For example, very noisy channels can be super-activated [7–10]. It is also likely that entanglement can increase the zero-error capacity of classical channels [11,12]. Again, entanglement-assisted zero-error capacity is upper-bounded by the Lovász ϑ function [13]. It is possible that a gap exists between the entanglement-assisted zero-error capacity and the corresponding Lovász ϑ function for some quantum channels [14]. For a classical channel, it is suspected that its entanglement-assisted zero-error capacity is exactly the Lovász ϑ function [6].

Non-signalling correlations have been studied in relativistic causality of quantum operations [19–23]. In [24], Cubitt *et al.* considered non-signalling correlations in the zero-error classical communications. Duan and Winter further introduced quantum non-signalling correlations (QNSCs) in the zero-error communication problem [25]. QNSCs are completely positive and trace-preserving linear maps shared between two parties so that they cannot send any information to each other by using these linear maps. Resources, such as shared randomness, entanglement, and classical non-signalling correlations, can be considered as special types of QNSCs. (QNSCs are also studied in [26].) The one-shot zero-error classical capacity of a quantum channel $\mathcal{N}$ assisted by a QNSC Π is the *logarithm* of the largest integer m so that a noiseless classical channel that can send m messages can be simulated by the composition of $\mathcal{N}$ and Π. Duan and Winter formulated this problem as a semidefinite program (SDP) [28]. For the class of classical-quantum (CQ) channels, the *one-shot* zero-error classical capacity assisted by QNSCs is $\log\lfloor\Upsilon(\mathcal{N})\rfloor$, where $\Upsilon(\mathcal{N})$ is the value of an SDP (see Eq. (4) below) [25]. Moreover, they proved that the *asymptotic* zero-error classical capacity assisted by QNSCs, minimized over all CQ channels with a confusability graph G, is exactly $\log\vartheta(G)$. This provides an operational meaning of the Lovász ϑ function. (The definition of a confusability graph can be generalized to quantum channels. For CQ channels, see Sec. 3.) In [27], they showed that $\vartheta(G)$ is also the one-shot QNSC-assisted zero error capacity activated by additional forward noiseless classical channels, minimized over all CQ channels with a confusability graph G.

Quantum capacity is usually defined as a regularized information quantity that requires an infinite uses of the channel. It is natural to consider the scenario of finite uses (e.g., [15–18]), which is more close to the real situations. In this article we focus on the same problem of zero-error classical capacity assisted by QNSCs in the *one-shot* setting. We consider the type of CQ channel $\mathcal{N} : |k\rangle\langle k| \mapsto |u_k\rangle\langle u_k|$, where $\{|u_k\rangle\}$ is an *orthonormal representation* of a graph G in some Hilbert space $\mathcal{B}$. We will provide a class of *circulant graphs*, defined by *equal-sized cyclotomic cosets*, and their orthonormal represntations so that the one-shot QNSC-assisted zero-error classical capacity of a CQ channel $\mathcal{N}$ induced from these orthonormal representations is

$$\log\lfloor\Upsilon(\mathcal{N})\rfloor = \log\lfloor\vartheta(G)\rfloor.$$

Moreover, the asymptotic QNSC-assisted zero-error classical capacity of $\mathcal{N}$ is

$$C_{0,\mathrm{NS}}(\mathcal{N}) = \lim_{m\to\infty}\frac{1}{m}\log\Upsilon(\mathcal{N}^{\otimes m}) = \log\vartheta(G),$$

since Υ is super-multiplicative and $C_{0,\mathrm{NS}}(\mathcal{N})$ is upper bounded by $\log\vartheta(G)$ (see Eq. (8)). This provides a more straightforward operational meaning for the Lovász ϑ function. In particular, our results apply to the cycles $\mathcal{C}_n$ of odd length. There are some works trying to connect the Shannon capacity $\Theta(\mathcal{C}_n)$ and independence number $\alpha(\mathcal{C}_n^{\boxtimes m})$ to $\vartheta(\mathcal{C}_n)$ [29–32]. Now we know that with the assistance of quantum non-signalling correlations, $\Upsilon(\mathcal{N}) = \vartheta(\mathcal{C}_n)$. This may explain why it is difficult to build equality between $\Theta(\mathcal{C}_n)$ and $\log\vartheta(\mathcal{C}_n)$.

This paper is organized as follows. We first give definitions of graphs, orthonormal representations, and the Lovász ϑ function in the next section. QNSC-assisted zero-error communication is introduced in Sec. 3. In Sec. 4, we provide an orthonormal representation for any circulant graph. Then we explicitly construct an optimal feasible solution to the SDP for the one-shot QNSC-assisted zero-error classical capacity of a CQ channel, whose confusability graph is a circulant graph defined by equal-sized cyclotomic cosets. These circulant graphs are characterized in Sec. 5, and they include three families of graphs: the cycle graphs $\mathcal{C}_n$ of odd length, the Paley graphs $\mathcal{QR}_p$, where p is a prime congruent to 1 modulo 4, and the cubic residue graphs $\mathcal{CR}_p$, where p is a prime congruent to 1 modulo 3. Finally we conclude with a discussion on other graphs with $\Upsilon(\mathcal{N}) = \vartheta(G)$ in Sec. 6.

2 Lovász ϑ function and Graphs

In this article the vertex set V of a graph G under consideration is the ring of integers modulo n for $n = |V|$. That is, $V = \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n = \{0, 1, \dots, n-1\}$. Let E be the edge set of G and let vw denote an edge connecting vertices v with w. Let $[M]_{i,j}$ denote the (i, j) entry of a matrix M. The adjacency matrix A_G of G has entries

$$[A_G]_{i,j} = \begin{cases} 1, & \text{if } ij \in E; \\ 0, & \text{otherwise.} \end{cases}$$

The eigenvalues and eigenvectors of a graph G are the eigenvalues and eigenvectors of its adjacency matrix A_G. An *automorphism* on a graph G is a permutation on its vertex set V that preserves the adjacency. Consequently, the adjacency matrix A_G is invariant under the conjugation of an automorphism. A graph is called *asymmetric* if it has no nonidentity automorphism. If for any two edges of G, there exists an automorphism mapping one edge to the other, then G is *edge-transitive*.

In order to estimate $\Theta(G)$, Lovász proposed an upper bound $\vartheta(G)$ on the Shannon capacity of a graph G [2], which is the minimum *value* of an *orthonormal representation* of the graph. We use a more general definition of an orthonormal representation as follows.

Definition 1 *Suppose $\{P_k\} \in \mathbb{C}^{d\times d}$ is a set of n orthogonal projectors so that*

$$Tr(P_i P_j) = 0$$

if $ij \notin E$. Then $\{P_k\}$ is an orthonormal representation of G. The value of $\{P_k\}$ is defined as

$$\eta(\{P_k\}) = \min_{\substack{\sigma\geq 0:\\ Tr(\sigma)=1}} \max_k \frac{1}{Tr\,(P_k\sigma)}.$$

(This definition of η is different from that in [25].) The trace-one, positive semidefinite operator $\sigma \in \mathbb{C}^{d\times d}$ that yields the minimum value is called the handle *of the representation. Then $\vartheta(G)$ is defined as*

$$\vartheta(G) = \min_{\{P_k\}} \eta(\{P_k\}).$$

We also say that $\vartheta(G)$ is the *Lovász number* of G. An *optimal* orthonormal representation (OOR) of G is a representation with value $\vartheta(G)$. If P_k and σ are restricted to rank-one matrices, this is exactly the definition in [2]. When $P_k = |u_k\rangle\langle u_k|$ and $\sigma = |c\rangle\langle c|$, we also say that $\{|u_k\rangle\}$ is an orthonormal representation of G with handle $|c\rangle$, without ambiguity. Following [25, 33], one can show that the definition is well-defined even allowing P_k and σ to have rank greater than one.

In [2], it is shown that $\alpha(G) \leq \vartheta(G)$. Furthermore, $\vartheta(G)$ is multiplicative:

$$\vartheta(G \boxtimes H) = \vartheta(G)\vartheta(H) \tag{2}$$

for two graphs G and H. Therefore, it is easy to see that $\Theta(G) \leq \vartheta(G)$.

Finally, in [2, Theorem 3], Lovász showed that $\vartheta(G)$ is the minimum of the largest eigenvalue of any symmetric matrix A such that

$$[A]_{i,j} = 1 \text{ if } i = j \text{ or } ij \notin E. \tag{3}$$

Thus $\vartheta(G)$ can be determined by solving an SDP, and it serves as a practical upper bound on $\Theta(G)$.

3 Zero-Error Communication Assisted with Quantum Non-Signalling Correlations

Let $\mathcal{L}(\mathcal{H})$ denote the space of linear operators on Hilbert space $\mathcal{H}$. Quantum non-signalling correlations are completely positive and trace-preserving linear maps $\Pi : \mathcal{L}(\mathcal{A}_i) \otimes \mathcal{L}(\mathcal{B}_i) \to \mathcal{L}(\mathcal{A}_o) \otimes \mathcal{L}(\mathcal{B}_o)$ shared between two parties Alice and Bob (with Hilbert spaces $\mathcal{A}$ and $\mathcal{B}$, respectively, and the subscripts i and o stand for input and output, repectively) such that they cannot send classical information to each other by using Π. Let the Choi matrix of Π be

$$\Omega_{\mathcal{A}_i'\mathcal{A}_o\mathcal{B}_i'\mathcal{B}_o} = (\mathrm{id}_{\mathcal{A}_i'} \otimes \mathrm{id}_{\mathcal{B}_i'} \otimes \Pi)(\Phi_{\mathcal{A}_i\mathcal{A}_i'} \otimes \Phi_{\mathcal{B}_i\mathcal{B}_i'}),$$

where $\mathrm{id}_{\mathcal{A}} \in \mathcal{L}(\mathcal{A})$ denotes the identity operator on the Hilbert space $\mathcal{A}$, $\Phi_{\mathcal{A}_i\mathcal{A}_i'} = |\Phi_{\mathcal{A}_i\mathcal{A}_i'}\rangle\langle\Phi_{\mathcal{A}_i\mathcal{A}_i'}|$, $\Phi_{\mathcal{B}_i\mathcal{B}_i'} = |\Phi_{\mathcal{B}_i\mathcal{B}_i'}\rangle\langle\Phi_{\mathcal{B}_i\mathcal{B}_i'}|$,and $|\Phi_{\mathcal{A}_i\mathcal{A}_i'}\rangle = \sum_k |k_{\mathcal{A}_i}\rangle|k_{\mathcal{A}_i'}\rangle$ and $|\Phi_{\mathcal{B}_i\mathcal{B}_i'}\rangle = \sum_k |k_{\mathcal{B}_i}\rangle|k_{\mathcal{B}_i'}\rangle$ are the unnormalized maximally-entangled states. For Π to be a QNSC, Duan and Winter derived the following constraints [25]:

$$\begin{aligned}
\Omega_{\mathcal{A}_i'\mathcal{A}_o\mathcal{B}_i'\mathcal{B}_o} &\geq 0,\\
\mathrm{Tr}_{\mathcal{A}_o\mathcal{B}_o}\left(\Omega_{\mathcal{A}_i'\mathcal{A}_o\mathcal{B}_i'\mathcal{B}_o}\right) &= \mathbb{I}_{\mathcal{A}_i'\mathcal{B}_i'},\\
\mathrm{Tr}_{\mathcal{A}_o\mathcal{A}_i'}\left(\Omega_{\mathcal{A}_i'\mathcal{A}_o\mathcal{B}_i'\mathcal{B}_o} X_{\mathcal{A}_i'}^T\right) &= 0, \forall \mathrm{Tr}\,(X) = 0,\\
\mathrm{Tr}_{\mathcal{B}_o\mathcal{B}_i'}\left(\Omega_{\mathcal{A}_i'\mathcal{A}_o\mathcal{B}_i'\mathcal{B}_o} Y_{\mathcal{B}_i'}^T\right) &= 0, \forall \mathrm{Tr}\,(Y) = 0,
\end{aligned}$$

where $\mathbb{I}$ is the identity matrix of appropriate dimension, X and Y are Hermitian operators, and X^T is the transpose of X. The first and second constraints require Π to be completely positive and trace-preserving; the third and fourth constraints mean that Π is non-signalling from both Alice to Bob and Bob to Alice.

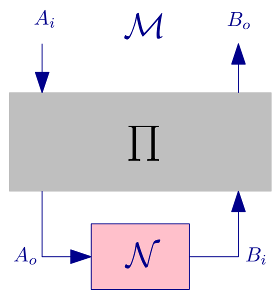

Fig. 1. A general simulation network: implementing a channel $\mathcal{M}$ using another channel $\mathcal{N}$ once, and the QNSC Π between Alice and Bob.

Suppose $\mathcal{N} : |k\rangle\langle k| \to \rho_k \in \mathcal{L}(\mathcal{B})$ is a CQ channel that maps a set of classical states $|k\rangle\langle k|$ for $k = 0, \ldots, n-1$ into some quantum states $\rho_k \in \mathcal{L}(\mathcal{B})$. Suppose that P_k are the orthogonal projectors onto the support of ρ_k, respectively. Then $\{P_k\}$ defines a confusability graph G with vertex set $\mathbb{Z}_n$ and two vertices i and j are connected if and only if $\operatorname{Tr}(P_i P_j) \neq 0$.

Let $\mathcal{M}$ be the composition channel of $\mathcal{N}$ and a QNSC Π as illustrated in Fig. 1. The input quantum system A_i is preprocessed by Π and the output A_o is sent through the channel $\mathcal{N}$. Then the channel output B_i will be postprocessed by Π and the final output is B_o. The *one-shot* zero-error classical capacity of $\mathcal{N}$ assisted by Π is the logarithm of the largest integer m so that $\mathcal{M}$ can simulate a noiseless classical channel that can send m messages. In [25], Duan and Winter showed that this one-shot capacity is $\log\lfloor \Upsilon(\mathcal{N}) \rfloor$, where $\Upsilon(\mathcal{N})$ is the value of the following SDP with variables $s_k \in \mathbb{R}$ and $R_k \in \mathcal{L}(\mathcal{B})$:

$$\begin{aligned} \Upsilon(\mathcal{N}) = \max & \sum_k s_k \\ \text{subject to: } & s_k \geq 0, \\ & 0 \leq R_k \leq s_k(\mathbb{I} - P_k), \\ & \sum_k (s_k P_k + R_k) = \mathbb{I}. \end{aligned} \tag{4}$$

It is not difficult to see that Υ is super-multiplicative [25]:

$$\Upsilon(\mathcal{N}_1 \otimes \mathcal{N}_2) \geq \Upsilon(\mathcal{N}_1)\Upsilon(\mathcal{N}_2). \tag{5}$$

For an arbitrary graph G, Duan and Winter considered the case of asymptotically many channel uses and showed that

$$\min_{\mathcal{N}} \lim_{m \to \infty} \frac{1}{m} \log \Upsilon(\mathcal{N}^{\otimes m}) = \log \vartheta(G),$$

where the minimization is over all CQ channels $\mathcal{N}$ with confusability graph G.

Herein we try to determine $\Upsilon(\mathcal{N})$. Apparently $\Upsilon(\mathcal{N}) \geq \alpha(G)$, the independence number of G. This lower bound can be achieved as follows. We choose a maximum independent set $\mathcal{I}$ of size $\alpha(G)$ and set $s_k = 1$ if $k \in \mathcal{I}$ and $s_k = 0$, otherwise. For some $s_{k^*} = 1$, let $R_{k^*} = \mathbb{I} - \sum_{k\in\mathcal{I}} P_k$ and $R_k = 0$ for $k \neq k^*$. Then the constraints of (4) are satisfied and $\Upsilon(\mathcal{N}) \geq \sum_k s_k = \alpha(G)$.

To find an upper bound on $\Upsilon(\mathcal{N})$, we consider the dual problem of (4):

$$\begin{aligned} \hat{\Upsilon}(\mathcal{N}) = &\min \operatorname{Tr}(T) \\ \text{subject to: } &\operatorname{Tr}(P_k T) - \operatorname{Tr}((\mathbb{I} - P_k)Q_k) \geq 1, \\ &Q_k + T \geq 0, \\ &Q_k \geq 0, \end{aligned} \tag{6}$$

where $T \in \mathcal{L}(\mathcal{B})$ is Hermitian. It can be verified that

$$\operatorname{Tr}(T) - \sum_k \operatorname{Tr}(R_k(T + Q_k)) \geq \sum_k s_k$$

and the duality gap is zero when $\operatorname{Tr}(R_k(T + Q_k)) = 0$ for $s_k \neq 0$. By choosing $Q_k = 0$ for all k and $T = \eta(\{P_k\})\sigma$, where σ is the handle of $\{P_k\}$, we have

$$\hat{\Upsilon}(\mathcal{N}) \leq \eta(\{P_k\}).$$

When $\{P_k\}$ is an OOR of G, we have

$$\hat{\Upsilon}(\mathcal{N}) \leq \vartheta(G). \tag{7}$$

Note that (7) is also implied by Lemma 13 and the proof of Theorem 5 in [25]. The asymptotic QNSC-assisted zero-error classical capacity of $\mathcal{N}$ is upper bounded by $\log \vartheta(G)$:

$$C_{0,\mathrm{NS}}(\mathcal{N}) = \lim_{m\to\infty} \frac{1}{m} \log \Upsilon(\mathcal{N}^{\otimes m}) \leq \lim_{m\to\infty} \frac{1}{m} \log \vartheta(G^{\boxtimes m}) = \log \vartheta(G), \tag{8}$$

where the inequality follows from (7) and $G^{\boxtimes m}$ is the confusability corresponding to $\mathcal{N}^{\otimes m}$; the last equality is because that ϑ is multiplicative (2).

It is suspected that equality may hold in (8) for graphs with nontrivial automorphisms. In the rest of this article, we will directly solve the SDP (4) for the CQ channel $\mathcal{N} : |k\rangle\langle k| \to |u_k\rangle\langle u_k|$, where $\{|u_k\rangle\}$ is an OOR for some circulant graph G, defined by equal-sized cyclotomic cosets.

4 Circulant Graphs

In this section we first discuss the definition of a circulant graph and its properties, and then derive an orthonormal representation $\{|u_k\rangle\}$ with $|u_k\rangle = U^k|u_0\rangle$, where U is a unitary operator. Then we show that a circulant graph G, defined by equal-sized cyclotomic cosets modulo n, will induce a CQ channel $\mathcal{N}$ so that $\Upsilon(\mathcal{N}) = \vartheta(G)$. This is done by explicitly constructing s_k and R_k, which lead to a feasible solution to the above SDP with object function $\sum_k s_k = \vartheta(G)$.

4.1 Orthonormal Representation of Circulant Graphs

Let C be a subset of $\mathbb{Z}_n \setminus \{0\}$ so that $-C = C$. A circulant graph $G = X(Z_n, C)$, defined by the connection set C, has an edge set $\{ij : i - j \in C\}$. Consequently its adjacency matrix A_G has entries $[A_G]_{i,j} = 1$ if and only if $i - j \in C$. (For example, a cycle graph $\mathcal{C}_n$ is defined by the connection set $C = \{1, n-1\}$.) Define a unitary matrix

$$U = \mathrm{diag}\left(1, e^{-2\pi i/n}, \ldots, e^{-2(n-1)\pi i/n}\right). \tag{9}$$

Let $|\mathbf{1}\rangle = (1\ 1 \cdots 1)$ be the vector whose entries are all ones of appropriate dimension. It can be easily verified that the eigenvectors of A_G are $|v_k\rangle = U^{-k}|\mathbf{1}\rangle$ with corresponding eigenvalues

$$\lambda_k = \sum_{j \in C} e^{2\pi i jk/n} \tag{10}$$

for $k = 0, \ldots, n-1$. Let $\lambda_{\max}$ and $\lambda_{\min}$ be the largest and the smallest eigenvalues of A_G, respectively. It is easy to see that $\lambda_{\max} = \lambda_0 = |C|$. For a circulant graph G that is edge-transitive, its Lovász number is $\vartheta(G) = \frac{-n\lambda_{\min}}{\lambda_{\max}-\lambda_{\min}}$ [2]. Note that $\lambda_{\min} < 0$ since $\mathrm{Tr} A_G = 0$. Below we provide an orthonormal representation for an arbitrary circulant graph.

Theorem 1 *Consider a circulant graph $G = X(\mathbb{Z}_n, C)$. Let $\eta = \frac{-n\lambda_{\min}}{\lambda_{\max}-\lambda_{\min}}$. Define*

$$|u_0\rangle = \frac{1}{\sqrt{\eta}}\left(1, \sqrt{\frac{\lambda_1 - \lambda_{\min}}{\lambda_{\max} - \lambda_{\min}}}, \ldots, \sqrt{\frac{\lambda_{n-1} - \lambda_{\min}}{\lambda_{\max} - \lambda_{\min}}}\right)$$

and

$$|u_k\rangle = U^k|u_0\rangle, \qquad k = 0, \ldots, n-1, \tag{11}$$

where U is the unitary operator defined in (9). Then $\{|u_k\rangle\}$ is an orthonormal representation of the circulant graph G. Moreover,

$$\langle u_k|u_{k+m}\rangle = \frac{[A_G]_{k+m,k}}{-\lambda_{\min}} + \delta_{m,0}$$

for any k, where $\delta_{m,j}$ is the Kronecker delta function. If G is edge-transitive, then $\{|u_k\rangle\}$ is an OOR with value $\eta = \vartheta(G)$ and handle $|c\rangle = (1, 0, \ldots, 0)$.

□

Proof. It is straightforward to verify that $\{|u_k\rangle\}$ is an orthonormal representation:

$$\begin{aligned}\langle u_k|u_{k+m}\rangle =&\frac{1}{\vartheta(G)}\sum_{j=0}^{n-1}\frac{\lambda_j-\lambda_{\min}}{\lambda_{\max}-\lambda_{\min}}e^{-2\pi ijm/n}\\ =&-\frac{1}{n\lambda_{\min}}\sum_{j=0}^{n-1}\lambda_j e^{-2\pi ijm/n}+\frac{1}{n}\sum_{j=0}^{n-1}e^{-2\pi ijm/n}\\ =&\frac{1}{-\lambda_{\min}}\sum_{j=0}^{n-1}\sum_{l\in C}\frac{e^{2\pi ij(l-m)/n}}{n}+\delta_{m,0}\\ =&\frac{1}{-\lambda_{\min}}\sum_{l\in C}\sum_{j=0}^{n-1}\frac{e^{2\pi ij(l-m)/n}}{n}+\delta_{m,0}\\ =&\frac{[A_G]_{k,k+m}}{-\lambda_{\min}}+\delta_{m,0}.\end{aligned}$$

If G is edge-transitive, $\vartheta(G)=\eta$ [2], $\{|u_k\rangle\}$ is an OOR of G and $|c\rangle=(1,0,\dots,0)$ is the handle:

$$\frac{1}{|\langle c|u_k\rangle|^2}=\vartheta(G),\qquad k=0,\dots,n-1.$$

□.

Remark: If $\lambda_{\min}$ is of multiplicity μ, then μ entries of $|u_k\rangle$ are zeros. Also, it is straightforward to see that a graph with an orthonormal representation in the form of (11) must be circulant.

4.2 Circulant Graphs defined by Cyclotomic Cosets Modulo n

In the following we will define circulant graphs by cyclotomic cosets modulo n. Cyclotomic cosets usually appear in the application of coding theory for minimal polynomials over finite fields or integer rings [34]. We use a more general concept here.

Let $\mathbb{Z}_n^\times=(\mathbb{Z}/n\mathbb{Z})^\times$ denote the multiplicative group of $\mathbb{Z}_n$, which consists of the units in $\mathbb{Z}_n$ and its size is determined by the Euler's totient function: $|\mathbb{Z}_n^\times|=\varphi(n)$. Suppose $q\in\mathbb{Z}_n^\times$. The cyclotomic coset modulo n over q which contains $s\in\mathbb{Z}_n$ is

$$C_{(s)}=\{s,sq,sq^2,\dots,sq^{r_s-1}\},$$

where r_s is the smallest positive integer r so that $sq^r\equiv s \mod n$. The subscript s is called the coset representative of $C_{(s)}$. Since q and n are relatively prime, we have $q^{\varphi(n)}\equiv 1 \mod n$ by Fermat-Euler theorem. Thus r_s exists for any s and the cyclotomic cosets are well-defined: $C_{(\alpha)}=C_{(\beta)}$ if and only if $\alpha=\beta q^c \mod n$ for some $c\in\mathbb{Z}$. Any element in a coset can be the coset representative, though it is usually the smallest number in the coset. As a consequence, the integers modulo n are partitioned into disjointed cyclotomic cosets:

$$\mathbb{Z}_n=\bigcup_{j=0}^{t}C_{(\alpha_j)},$$

where $\{\alpha_0=0,\alpha_1,\dots,\alpha_t\}$ is a set of (disjointed) coset representatives. We consider $t>1$, while the case $t=1$ is trivial. Since q is relatively prime to n, we always have $C_{(0)}=\{0\}$. It suffices to consider partitions of $\mathbb{Z}_n^*=\mathbb{Z}_n\setminus\{0\}$.

If $-1 \in C_{(1)}$, we can define a circulant graph $X(\mathbb{Z}_n, C_{(\alpha)})$ for any $\alpha \neq 0$. Assume further that these cyclotomic cosets are *equal-sized*, except $C_{(0)} = \{0\}$. That is, $|C_{(\alpha)}| = |C_{(1)}|$ for any $\alpha \neq 0$, and $n = t|C_{(1)}| + 1$. A circulant graph defined by these cyclotomic cosets have some interesting properties that are critical to the proof of our main theorem. First, by (10), the eigenvalues of $X(\mathbb{Z}_n, C_{(\alpha_j)})$ are

$$\lambda_k^{(\alpha_j)} = \sum_{l \in C_{(k\alpha_j)}} e^{2\pi i l/n},$$

which depends only on its cyclotomic coset. Each $\lambda_k^{(\alpha_j)}$ is of multiplicity $|C_{(1)}|$, except for λ_0, which is of multiplicity one. It can be seen that these graphs $X(\mathbb{Z}_n, C_{(\alpha_j)})$ are equivalent and it suffices to consider $G = X(\mathbb{Z}_n, C_{(1)})$.

On the other hand, suppose $\beta \in \mathbb{Z}_n^\times \setminus C_{(1)}$. Let $\tau_\beta(C_{(\alpha)}) = C_{(\alpha\beta)}$. It can be checked that τ_β is a permutation on the cyclotomic cosets of order at most t. One can delve into more about the structure of τ_β, but we only need the following equation in the proof of our main theorem:

$$\mathbb{Z}_n = \bigcup_{j=0}^{t} C_{(\alpha_j)} = \bigcup_{j=0}^{t} C_{(\alpha_j\beta)}. \tag{12}$$

(Note that the indices are under modulo n and we will always omit "mod n" as it is clear from the context.)

Example 1 For $\mathbb{Z}_{17}^\times = \langle 3 \rangle$, $-1 \equiv 3^8$ and $13 \equiv 3^4$. Let $C_{(1)} = \langle 13 \rangle$ and we have

$$\begin{aligned} C_{(0)} =& \{0\}, \\ C_{(1)} =& \{1, 13, 16, 4\}, \\ C_{(2)} =& \{2, 9, 15, 8\}, \\ C_{(3)} =& \{3, 5, 14, 12\}, \\ C_{(6)} =& \{6, 10, 11, 7\}. \end{aligned}$$

The circulant graph $X(\mathbb{Z}_{17}, C_{(1)})$ is shown in Fig. 2.

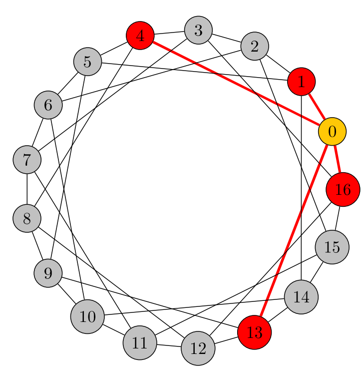

Fig. 2. The circulant graph $X(\mathbb{Z}_{17}, \{1, 13, 16, 4\}))$.

□

Now we are ready to derive our main theorem. Characterization of equal-sized cyclotomic cosets is left to the next section.

Theorem 2 *Suppose* $\mathbb{Z}_n^* = \bigcup_{j=1}^t C_{(\alpha_j)}$*, where* $\{C_{(\alpha_j)}\}$ *are cyclotomic cosets modulo* n *over* q *of equal size for some* q *relatively prime to* n *and* $C_{(1)} = C_{(-1)}$*. Let* $\mathcal{N}$ *be the CQ channel induced by the orthonormal representation* $\{|u_k\rangle\}$ *of* $G = X(\mathbb{Z}_n, C_{(1)})$ *in Theorem 1. Assume further that* G *is edge-transitive. Then*

$$\Upsilon(\mathcal{N}) = \vartheta(G)$$

and

$$C_{0,NS}(\mathcal{N}) = \log \vartheta(G).$$

Moreover, an optimal solution to the SDP (4) is

$$s_k = \frac{1}{n}\vartheta(G),\ R_k = U^k R_0 U^{-k},\ R_0 = \frac{1}{n}\left(\mathbb{I} - \sum_{j=0}^{n-1} x_j P_j\right), \tag{13}$$

where U *is defined in (9) and* $x_j = \frac{\lambda_{j\beta}-\lambda_\beta}{\lambda_0-\lambda_\beta}$*, given* $\lambda_\beta = \lambda_{\min}$ *for some* $\beta \in \mathbb{Z}_n^\times$*. (In particular,* $x_0 = 1$ *and* $x_j = 0$ *for* $j \in C_{(1)}$*.)*

□

Proof. Apparently, $\Upsilon(\mathcal{N}) = \sum_k s_k = \vartheta(G)$. Also,

$$\begin{aligned}\sum_k (s_k P_k + R_k) &= \frac{1}{n}\sum_k \left(\vartheta(G))P_k - \sum_{j=0}^{n-1} x_j U^k P_j U^{-k}\right) + \mathbb{I}\\ &= \frac{1}{n}\left(\vartheta(G) - \sum_{j=0}^{n-1} x_j\right)\sum_k P_k + \mathbb{I}\\ &= \frac{1}{n}\left(-\sum_{j=0}^{n-1}\frac{\lambda_{j\beta}}{\lambda_0-\lambda_\beta}\right)\sum_k P_k + \mathbb{I}\\ &= \mathbb{I},\end{aligned}$$

where the last equality is because $\sum_{j=0}^{n-1}\lambda_{j\beta} = \sum_{j=0}^{n-1}\lambda_j = 0$. It remains to verify $0 \le R_0 \le s_0(\mathbb{I} - P_0)$.

Let $D = \sum_{j=0}^{n-1} x_j P_j$. From Theorem 1, we have

$$[P_j]_{a,b} = \frac{1}{\vartheta(G)}\sqrt{\frac{(\lambda_a-\lambda_\beta)(\lambda_b-\lambda_\beta)}{(\lambda_0-\lambda_\beta)^2}}e^{-2\pi i j(a-b)/n}.$$

Thus for $a \neq b$,

$$\begin{aligned}[D]_{a,b} =& \frac{1}{\vartheta(G)}\sqrt{\frac{(\lambda_a-\lambda_\beta)(\lambda_b-\lambda_\beta)}{(\lambda_0-\lambda_\beta)^2}}\sum_{j=0}^{n-1}\frac{\lambda_{j\beta}-\lambda_\beta}{\lambda_0-\lambda_\beta}e^{-2\pi ij(a-b)/n}\\ =& \frac{1}{-n\lambda_\beta}\sqrt{\frac{(\lambda_a-\lambda_\beta)(\lambda_b-\lambda_\beta)}{(\lambda_0-\lambda_\beta)^2}}\sum_{j=0}^{n-1}\lambda_{j\beta}e^{-2\pi ij(a-b)/n}\\ =& \frac{1}{-n\lambda_\beta}\sqrt{\frac{(\lambda_a-\lambda_\beta)(\lambda_b-\lambda_\beta)}{(\lambda_0-\lambda_\beta)^2}}\sum_{j=0}^{n-1}\sum_{k\in C_{(\beta)}}e^{2\pi ij(k-(a-b))/n}\\ =& \begin{cases}\frac{1}{-\lambda_\beta}\sqrt{\frac{(\lambda_a-\lambda_\beta)(\lambda_b-\lambda_\beta)}{(\lambda_0-\lambda_\beta)^2}}, & \text{if } a-b\in C_{(\beta)};\\ 0, & \text{if } a-b\neq C_{(\beta)}.\end{cases}\end{aligned}$$

Similarly, we have

$$[D]_{a,a} = \sqrt{\frac{(\lambda_a-\lambda_\beta)(\lambda_a-\lambda_\beta)}{(\lambda_0-\lambda_\beta)^2}}$$

for $0 \leq a \leq n-1$. Therefore, D is a nonnegative matrix. Observe that $|u_0\rangle$ is a positive eigenvector of D with eigenvalue 1.

Claim: the largest eigenvalue of D is 1.

As a consequent, $R_0 = \frac{1}{n}(\mathbb{I}-D) \geq 0$. Also, $R_0 \leq s_0(\mathbb{I}-P_0)$ as long as $\vartheta(G) \geq 1$. Therefore,

$$C_{0,\mathrm{NS}}(\mathcal{N}) = \lim_{m\to\infty}\frac{1}{m}\log\Upsilon(\mathcal{N}^{\otimes m}) \geq \lim_{m\to\infty}\frac{1}{m}\log\Upsilon^m(\mathcal{N}) = \log\vartheta(G),$$

where the inequality is because Υ is super-multiplicative (5). Combining with (8), we have $C_{0,\mathrm{NS}}(\mathcal{N}) = \log\vartheta(G)$.

It remains to prove the claim. Let $|u_0\rangle = (a_0, a_1, \ldots, a_{n-1})$. Then define $V = \mathrm{diag}(a_0, a_1, \ldots, a_{n-1})$, which is an invertible matrix since $a_j \geq 0$. Define $B = V^{-1}DV$, which has the same eigenvalues as D. Also

$$B|\mathbf{1}\rangle = V^{-1}DV|1\rangle = V^{-1}D|u_0\rangle = V^{-1}|u_0\rangle = |\mathbf{1}\rangle.$$

Since D is nonnegative, B is also nonnegative, so every row sum of B is 1. As a corollary of Gershgorin's disk theorem, we know that the largest eigenvalue of a nonnegative matrix is upper bounded by its largest row sum. Thus the largest eigenvalue of B is exactly 1. □.

5 Characterization of Equal-sized Cyclotomic Cosets

In this section we characterize some properties of the equal-sized cyclotomic cosets. Then we provide three families of graphs that fit Theorem 2: the cycle graphs, the Paley graphs, and the cubic residue graphs.

Observe that the cyclotomic coset of 1 modulo n over q is $C_{(1)} = \langle q\rangle$, which is a cyclic subgroup of the multiplicative group $\mathbb{Z}_n^\times$. Thus $|C_{(1)}|$ divides $\varphi(n)$. Since $C_{(1)} = C_{(-1)}$, $|C_{(1)}|$ is even, which implies n is odd. Consequently, $|C_{(1)}|$ is a common divisor of $\varphi(n)$ and $n-1$. Let

$$\Gamma_d^n = \{a \in \mathbb{Z}_{n+1}^* : \gcd(a,n) = n/d\}$$

and then $|\Gamma_d^n| = \varphi(d)$. We have $\mathbb{Z}_n = \bigcup_{d:d|n} \Gamma_d^n$. For each $\alpha \neq 0$, $C_{(\alpha)} \subseteq \Gamma_{d_\alpha}^n$ for some $d_\alpha | n$. Therefore we have the following lemma.

Lemma 1 *If $\{C_{\alpha_1}, \ldots, C_{\alpha_t}\}$ is a set of equal-sized cyclotomic cosets modulo n, then $|C_{(1)}|$ must be a common divisor of $\varphi(d)$ for all $d|n$ and $d > 1$.* □

It remains to find conditions so that $C_{(1)} = C_{(-1)}$. In the following we provide several families of graphs.

Remark: Lemma 1 is a necessary condition that equal-sized cyclotomic cosets modulo n exist for a certain n. It is likely also a sufficient condition. However, we did not find composite n so that the nontrivial equal-sized cyclotomic cosets has $C_{(1)} = C_{(-1)}$.

5.1 Trivial Equal-sized Cyclotomic Cosets

For any odd $n \geq 3$, there exists a trivial connection set $C_{(1)} = \{1, n-1\}$, which is a cyclotomic coset modulo n over $n-1$.

Example 2 For $n = 7$ and $q = 6$, we have

$$\begin{aligned} C_{(0)} &= \{0\}, \\ C_{(1)} = C_{(6)} &= \{1, 6\}, \\ C_{(2)} = C_{(5)} &= \{2, 5\}, \\ C_{(3)} = C_{(4)} &= \{3, 4\}. \end{aligned}$$

Each of the coset, except $C_{(0)}$, defines a circulant graph equivalent to the cycle graph $\mathcal{C}_7$.

If $\mathcal{N}_1 : |k\rangle\langle k| \to \rho_k \in \mathcal{L}(\mathcal{B})$ is a CQ channel induced from the OOR of $\mathcal{C}_7$ as in Theorem 1, then ρ_k is a state in a 5-dimensional Hilbert space and we have $\Upsilon(\mathcal{N}_1) = \vartheta(\mathcal{C}_7) = 3.317$.

□

As shown in Example 2, $C_{(1)}$ defines the cycle graph $\mathcal{C}_n$ and we have $\mathbb{Z}_n = \bigcup_{j=0}^{\frac{n-1}{2}} C_{(j)}$. Each nontrivial eigenvalue has multiplicity 2, as can be seen from $|C_{(j)}| = 2$ for $j \neq 0$, and $\lambda_{\min} = \lambda_{\frac{n-1}{2}} = \lambda_{\frac{n+1}{2}} = -2\cos\frac{\pi}{n}$.

Corollary 1 *Suppose $\mathcal{N}$ is a CQ channel induced by the OOR of the cycle graph $\mathcal{C}_n$ as in Theorem 1. Then*

$$\Upsilon(\mathcal{N}) = \vartheta(\mathcal{C}_n) = \frac{n\cos\frac{\pi}{n}}{1 + \cos\frac{\pi}{n}}.$$

□

5.2 Nontrivial Equal-sized Cyclotomic Cosets

When n is a prime power, $\mathbb{Z}_n^\times$ is cyclic. Let $\mathbb{Z}_n^\times = \langle\alpha\rangle$, and α is of order $\varphi(n)$. Consequently, $-1 \equiv \alpha^{\varphi(n)/2}$. Therefore, $-1 \in C_{(1)} = \langle q\rangle$ if $q = \alpha^b$ for some $b \mid (\varphi(n)/2)$, and then $|C_{(1)}| = \frac{\varphi(n)}{b}$. It is clear that $\mathbb{Z}_n^\times$ is equally partitioned by $C_{(1)}$. Furthermore, if $\mathbb{Z}_n^* \setminus \mathbb{Z}_n^\times$ can also be equally partitioned by $C_{(1)}$, then $X(\mathbb{Z}_n, C_{(1)})$ is defined by equal-sized cyclotomic cosets.

We first consider the case when n is not a prime.

Theorem 3 *Let $n = p^r$ be a prime power. Suppose $\mathbb{Z}_n^\times = \langle\alpha\rangle$ for $\alpha \in \mathbb{Z}_p$. Then the graph $X(\mathbb{Z}_{p^r}, \langle\alpha^{p^{r-1}}\rangle)$ is defined by equal-sized cyclotomic cosets.*

□

Proof. We have $\varphi(n) = p^{r-1}(p-1)$ and then $\alpha^{p^{r-1}(p-1)} \equiv 1 \mod p$. Let $C^r_{(1)}$ be the cyclotomic coset modulo p^r over $\alpha^{p^{r-1}}$ that contains 1. Thus $|C^r_{(1)}| = p-1$, which divides $\varphi(p^a)$ for $a = 1, \ldots, r$. Also, $-1 \equiv (\alpha^{p^{r-1}})^{\frac{p-1}{2}} \in C^r_{(1)}$.

Let $pC = \{p\alpha : \alpha \in C\}$ for a set $C \subseteq \mathbb{Z}_{p^r}$. First, we have $\mathbb{Z}^*_p = \Gamma^p_p = C^1_{(1)}$. Also $\mathbb{Z}^*_{p^2} = \Gamma^{p^2}_{p^2} \cup \Gamma^p_{p^2} = \Gamma^{p^2}_{p^2} \cup p\Gamma^p_{p^2}$. Since $\Gamma^{p^a}_{p^a} = \mathbb{Z}^\times_{p^a}$ can be equally partitioned by the cyclotomic coset $C^a_{(1)}$ for any a as in the proof of Theorem 4, $\mathbb{Z}_{p^2}$ can be partitioned into cosets of size $p-1$. Observe that

$$\begin{aligned}\mathbb{Z}^*_{p^r} =&\Gamma^{p^r}_{p^r} \cup \Gamma^{p^r}_{p^{r-1}} \cup \cdots \cup \Gamma^{p^r}_{p}\\ =&\Gamma^{p^r}_{p^r} \cup p\left\{\Gamma^{p^{r-1}}_{p^{r-1}} \cup \cdots \cup \Gamma^{p^{r-1}}_{p}\right\}\\ =&\Gamma^{p^r}_{p^r} \cup \left\{\bigcup_{j=1}^{r-1} p^j \Gamma^{p^{r-j}}_{p^{r-j}}\right\},\end{aligned} \tag{14}$$

where $\Gamma^{p^r}_{p^r} = \mathbb{Z}^\times_{p^r}$ can be equally partitioned by the cyclotomic coset $C^r_{(1)}$. Thus by induction, $\mathbb{Z}^*_{p^r}$ can be partitioned into cosets of size $p-1$.

Let $C^r_{(1)} \mod p^a = \{a \mod p^a : a \in C^r_{(1)}\}$. Since $\langle \alpha \mod p^r\rangle = \mathbb{Z}^\times_{p^r}$, $\langle \alpha \mod p^a\rangle = \mathbb{Z}^\times_{p^a}$ for any $a \leq r$. An interesting property is

$$C^r_{(1)} \mod p^a = C^a_{(1)}.$$

Therefore, these cosets are exactly the cyclotomic cosets modulo p^r over $\alpha^{p^{r-1}}$ of equal size. Suppose $\Gamma^{p^a}_{p^a}$ is partitioned into the cyclotomic cosets $\{C^a_{(\alpha_1)}, C^a_{(\alpha_2)}, \ldots, C^a_{(\alpha_{p^a-1})}\}$. Then by (14), the cyclotomic cosets of $\mathbb{Z}^*_{p^r}$ are $\{p^{r-a}C^a_{(\alpha_j)}\}$. □.

Example 3 For $\mathbb{Z}_{125} = \langle 2\rangle$, $-1 \equiv 2^{50}$ and $57 \equiv 2^{25}$. Let $C^3_{(1)} = \langle 57\rangle$ and we have

$$\begin{aligned}C^2_{(1)} =&\{1, 7, 24, 18\},\\ C^2_{(2)} =&\{2, 14, 23, 11\},\\ C^2_{(3)} =&\{3, 21, 22, 4\},\\ C^2_{(6)} =&\{6, 17, 19, 8\},\\ C^2_{(9)} =&\{9, 13, 16, 12\}\end{aligned}$$

and

$$C^2_{(5)} = \{5, 10, 20, 15\} = 5\{1, 2, 4, 3\} = 5\{C^1_{(1)}\}.$$

Consequently, $\mathbb{Z}^*_{125} \setminus \mathbb{Z}^\times_{125} = 5\{C^2_{(1)} \cup C^2_{(2)} \cup C^2_{(3)} \cup C^2_{(6)} \cup C^2_{(9)}\} \cup 25C^1_{(1)}$. □

It is simpler for the case that n is a prime.

Theorem 4 *Let $p = 2st + 1$ be a prime. Suppose $\mathbb{Z}^*_p = \langle\alpha\rangle$. Then the graph $X(\mathbb{Z}_p, \langle\alpha^t\rangle)$ is defined by equal-sized cyclotomic cosets.* □

Proof. In this case $\mathbb{Z}^*_n = \mathbb{Z}^\times_n$ and $\varphi(n) = n-1$. Since $\alpha^{2st} \equiv 1 \mod p$, the cyclotomic cosets modulo p over α^t are $C_{(1)}, C_{(\alpha)}, \ldots, C_{(\alpha^{t-1})}$. Also, $-1 \equiv (\alpha^t)^s \in C_{(1)}$. These cosets are equal-sized and $\mathbb{Z}^*_p = \bigcup_{j=1}^t C_{(\alpha^j)}$. If $|C_{(\beta)}| < |C_{(1)}|$ for some β, then $\beta\alpha^{t|C_{(\beta)}|} \equiv \beta$. Since β is a unit in $\mathbb{Z}^*_p$, we must have $\alpha^{t|C_{(\beta)}|} \equiv 1$, which is a contradiction to the order of α. Then the result is straightforward. □.

Example 4 Consider $\mathbb{Z}_{37} = \langle 2 \rangle$. The following graphs satisfy the conditions in Theorem 4: $\mathcal{C}_{37} = X(\mathbb{Z}_{37}, \{1, 36\})$, $X(\mathbb{Z}_{37}, \{1, 6, 36, 31\})$, $X(\mathbb{Z}_{37}, \langle 27 \rangle)$, $\mathcal{CR}_{37} = X(\mathbb{Z}_{37}, \langle 8 \rangle)$, $\mathcal{QR}_{37} = X(\mathbb{Z}_{37}, \langle 4 \rangle)$. □

5.3 Paley Graphs

When $t = 2$, the cosets in Theorem 4 lead to exactly the Paley graphs or the quadratic residue graphs $\mathcal{QR}_p$.

A nonzero integer a is called a quadratic residue modulo n if $a = b^2 \mod n$ for some integer b; otherwise, a is a quadratic nonresidue modulo n. Note that 0 is neither a quadratic residue, nor a nonresidue. Suppose p is a prime such that $p \equiv 1 \mod 4$. Let Q denote the set of quadratic residues modulo p and N the set of nonresidues. Since $p \equiv 1 \mod 4$, $-1 \in Q$. Then $\mathcal{QR}_p = X(\mathbb{Z}_p, Q)$ [35].

Suppose α is a primitive element of $\mathbb{Z}_p$. Then $Q = \{\alpha^c : c \text{ even}\}$ and $N = \{\alpha^c : c \text{ odd}\}$. It is clear that $|Q| = |N| = (p-1)/2$ and $\mathbb{Z}_p = Q \cup N \cup \{0\}$. By Eq. (10) and the formula for quadratic Gauss sum: $\sqrt{p} = \sum_{j=0}^{p-1} e^{2\pi i j^2/p}$, the eigenvalues of $\mathcal{QR}_p$ are

$$\lambda_j = \begin{cases} (-1+\sqrt{p})/2, & \text{if } j \in Q; \\ (-1-\sqrt{p})/2, & \text{if } j \in N; \\ (p-1)/2, & \text{if } j = 0, \end{cases}$$

The Paley graphs are self-complimentary and consequently $\Theta(\mathcal{QR}_p) = \vartheta(\mathcal{QR}_p) = \sqrt{p}$ [2, Theorem 12]. In fact, $\alpha(\mathcal{QR}_p^{\boxtimes 2}) = p$ [36]. Let $b \in N$ and then $\{(a, ab \mod p) : a \in \mathbb{F}_p\}$ is an independent set of size p in $\mathcal{QR}_p^{\boxtimes 2}$. For example, the smallest Paley graph is $\mathcal{QR}_5 = \mathcal{C}_5$, and $\{(0,0), (1,2), (2,4), (3,1), (4,3)\}$ is an independent set of size five in $\mathcal{C}_5^{\boxtimes 2}$. This shows that the capacity can be achieved by two uses of a channel corresponding to $\mathcal{QR}_p$.

Corollary 2 *Suppose $\mathcal{N}$ is a CQ channel induced by the OOR of the Paley graph $\mathcal{QR}_p$ as in Theorem 1. Then*

$$\Upsilon(\mathcal{N}) = \vartheta(\mathcal{QR}_p) = \sqrt{p}.$$

Proof. The proof for Paley graphs is easier than the general proof in Theorem 2 since there are only three cyclotomic cosets and two nontrivial eigenvalues. The SDP (4) can be achieved by

$$R_0 = \frac{1}{p}\left(\mathbb{I} - P_0 - \frac{2}{\sqrt{p}+1}\sum_{j\in N} P_j\right).$$

One can show that

$$p[R_0]_{a,b} = \begin{cases} 1, & \text{if } a = b \in N; \\ \frac{-1+\sqrt{p}}{1+\sqrt{p}}, & \text{if } a = b \in Q; \\ -\left(\frac{2}{1+\sqrt{p}}\right)^2, & \text{if } a, b \in Q \text{ and } a - b \in N; \\ 0, & \text{otherwise.} \end{cases}$$

A key observation here is that

$$\sum_{b: b\neq a} |p[R_0]_{a,b}| = \begin{cases} p[R_0]_{a,a}, & \text{if } a \in Q; \\ 0, & \text{if } a \in N. \end{cases}$$

Then by Gershgorin's disk theorem, the eigenvalues of pR_0 are either 1 or lie in the disks with center $p[R_0]_{a,a}$ and radius $p[R_0]_{a,a}$ for $a \in Q$. Also note that R_0 is Hermitian and it has real eigenvalues. As a consequence, the eigenvalues of R_0 are nonnegative and thus $R_0 \geq 0$.

The null space of R_0 are spanned by $\sum_{j:j\in N} |u_j\rangle$ and $|u_0\rangle$, which implies $(1, 0, \ldots, 0)$ is an eigenvector of R_0 with eigenvalue 0. □.

5.4 Cubic Residue Graphs

When $t = 3$, the cosets in Theorem 4 lead to the cubic residue graphs $\mathcal{CR}_p$ [37]. A nonzero integer a is called a cubic residue modulo p if $a = b^3 \mod p$ for some integer b. The cyclotomic coset $C_{(1)}$ consists of cubic residues.

$\mathcal{CR}_p = X(\mathbb{Z}_p, C_{(1)})$ has three nontrivial eigenvalues, which can be found by the formula for cubic Gauss sum. These three eigenvalues are the roots of $x^3 - 3px - ap = 0$, where $4p = a^2 + b^2$ for some integers $a \equiv 1 \mod 3$ and b [38]. Currently the closed form for $\vartheta(\mathcal{CR}_p)$ is still unknown, since it is related to the determination of Gauss sums [39, 40].

These discussions can be extended to $t \geq 4$.

6 Discussion

We have shown that $\Upsilon(\mathcal{N}) = \vartheta(G)$ for $\mathcal{N}$ induced by an OOR $\{|u_k\rangle\}$ of a class of edge-transitive circulant graphs that are defined by equal-sized cyclotomic cosets. These circulant graphs bear very strong symmetries. It is interesting to see if there are other graphs that have this property. For graphs with $\vartheta(G) = \alpha(G)$,[b] they naturally lead to CQ channels with $\Upsilon(\mathcal{N}) = \vartheta(G)$. Now we consider graphs with $\vartheta(G) > \alpha(G)$.

Recall from Definition 1, an orthonormal representation of a graph indicates that two vertices are not connected if the trace inner product of their representations is zero. We say a graph G' is a *degenerate* graph of G if an orthonormal representation of G is also an orthonormal representation of G', and hence their Lovász numbers are equal: $\vartheta(G) = \vartheta(G')$. Consequently, if an edge $E \notin G$, $E \notin G'$. We say a graph $\hat{G}$ is *essential* if it has no proper subgraph $H \subset \hat{G}$ with $\vartheta(H) = \vartheta(\hat{G})$. Suppose $\{P_k\}$ is an orthonormal representation of the essential graph $\hat{G}$. Then two vertices i and j are connected if and only if $\mathrm{Tr}\,(P_iP_j) \neq 0$. Apparently, for any graph G, it has an essential subgraph $\hat{G}$ that is a subgraph of all degenerate graphs of G by the definition of orthonormal representation.

Example 5 Consider Fig. 3, where G_1 is an asymmetric graph and G_2 is a degenerate graph of G_1. The Lovász numbers are $\vartheta(G_1) = \vartheta(G_2) = \sqrt{5} + 2$. Their essential graph is the union of $\mathcal{C}_5$ and two isolated points: removing any edge will increase the Lovász number of this graph. One can check that $\vartheta(G_1) = \vartheta(G_2) = \vartheta(\mathcal{C}_5) + 2 = \sqrt{5} + 2$.

As shown in Example 5, it is possible that an asymmetric graph has a degenerate graph with nonidentity automorphisms and $\vartheta(G) > \alpha(G)$.

Corollary 3 *Suppose a graph G leads to a CQ channel $\mathcal{N}$ with $\Upsilon(\mathcal{N}) = \vartheta(G)$. Then so do the degenerate graphs of G.*

Suppose a graph G has an essential graph $\hat{G}$ with $\Upsilon(\hat{\mathcal{N}}) = \vartheta(\hat{G})$. It is also possible that G leads to $\Upsilon(\mathcal{N}) = \vartheta(G)$ as shown in the following example.

[b] We tried computer search on random graphs and found that $\vartheta(G) = \alpha(G)$ for several asymmetric graphs. It is unknown whether most graphs would have $\vartheta(G) = \alpha(G)$ or $\vartheta(G) > \alpha(G)$.

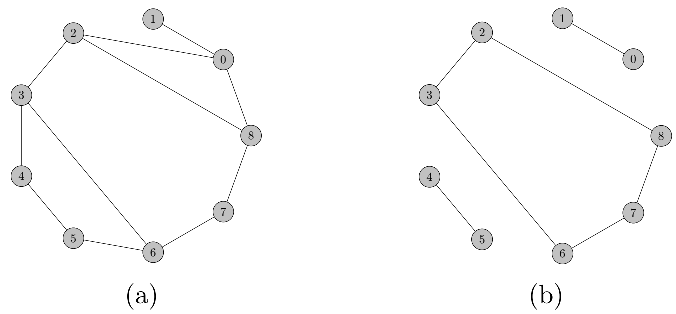

Fig. 3. (a) an asymmetric graph G_1; (b) a degenerate graph G_2 of G_1.

Example 6 Fig. 4 is a graph G whose essential graph is $\mathcal{C}_5$. An orthonormal representation of $\mathcal{C}_5$ can be easily extended to an orthonormal representation of G by choosing $|u_5\rangle = |u_0\rangle$.

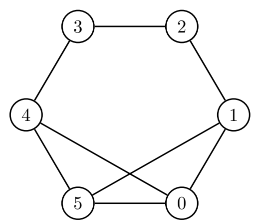

Fig. 4. A graph with essential graph $\mathcal{C}_5$.

However, generally it is nontrivial to construct an orthonormal representation of a graph from an orthonormal representation of its proper essential graph.

So far we have shown that circulant graphs defined by equal-sized cyclotomic cosets and their degenerate graphs would induce CQ channels with $\Upsilon(\mathcal{N}) = \vartheta(G)$. Now let us consider graphs other than these. First we show how to find an OOR for any graph G, following the proof of [2, Theorem 3]. After solving the SDP for $\vartheta(G)$ [2, Theorem 3], we end up with a symmetric matrix A satisfying (3) with the largest eigenvalue $\vartheta(G)$. Then there exist vectors $|x_1\rangle, \ldots, |x_n\rangle \in \mathbb{R}^{d+1}$, where $d = \operatorname{rank}(\vartheta(G)I - A)$, such that

$$\vartheta(G)\delta_{i,j} - [A]_{i,j} = \langle x_i | x_j \rangle$$

and the first entry of $|x_k\rangle$ is 0 for all k. Let $|c\rangle = (1, 0, \ldots, 0) \in \mathbb{R}^{d+1}$ and

$$|u_k\rangle = \frac{1}{\sqrt{\vartheta(G)}}(|c\rangle + |x_k\rangle). \tag{15}$$

Then $\{|u_k\rangle\}$ is an OOR of G with value

$$\vartheta(G) = \frac{1}{|\langle c|u_k\rangle|^2}, \ \forall k.$$

For a CQ channel induced by $\{|u_k\rangle\}$ to have $\Upsilon(\mathcal{N}) = \vartheta(G)$ in the SDP (4), we must have

$$\langle c|R_k|c\rangle = 0, \ \forall k. \tag{16}$$

That is, the first row and the first column of R_k are all zeros.

Example 7 Consider the Möbius ladder $M_8 = X(\mathbb{Z}_8, \{1,4\})$ as shown in Fig. 5, which is circulant but beyond the scope of Theorem 2. Clearly we may choose $s_k = \vartheta(G)/n$ for all k. Let

$$R_0 = \frac{s_0}{\vartheta(G)} \left(\mathbb{I} - P_0 - \sum_{k=1}^{7} x_k P_k \right)$$

and R_k can be defined by permuting the indices of P_k in R_0 appropriately. Since vertices $1, 8$, and 4 are neighbors of vertex 0, we may choose $x_1 = x_7 = x_4 = 0$. We define a map:

$$\Gamma : i \mapsto n - i.$$

Apparently, Γ is an automorphism of M_8. Assume $x_2 = x_6$ and $x_3 = x_5$. By solving the linear system from (16), we have $x_2 = x_6 = 0.5$ and $x_3 = x_5 = \frac{\vartheta(G)}{2} - 1$. Surprisingly, $\sum_k x_k = \vartheta(G)$, $0 \le R_k \le s_k(\mathbb{I} - P_k)$, and $\sum_k s_k P_k + R_k = \mathbb{I}$. Thus $\Upsilon(\mathcal{N}) = \vartheta(G)$ for $G = M_8$.

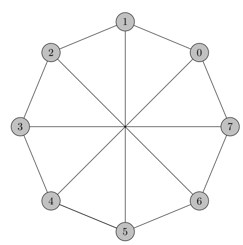

Fig. 5. Möbius ladder $M_8 = X(\mathbb{Z}_8, \{1,4\})$.

To sum up, we have found many more graphs with $\Upsilon(\mathcal{N}) = \vartheta(G)$. If this holds for general graphs, it would imply that $\lfloor \vartheta(G) \rfloor$ can be achieved by a single channel use[c]In fact, the techniques used in Example 7 can be generalized to other graphs. However, we do not know how to prove $R_k \ge 0$. For example, we have $\Upsilon(\mathcal{N}) = \vartheta(G)$ for the graph $G = Z_7$ in Fig. 6 and its OOR constructed in (15). At the same time, the dual program (6) is satisfied with $T = \vartheta(G)|c\rangle\langle c|$ and $Q_k = 0$. Thus there should be a more unifying theory than Theorem 2 and this is our future research direction.

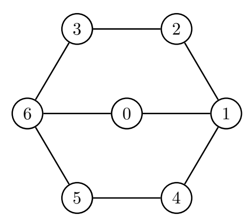

Fig. 6. A graph Z_7 that is not circulant, regular, or edge-transitive.

[c]More precisely, the one-shot capacity is given by $\log\lfloor \Upsilon(\mathcal{N}) \rfloor$ so the operational meaning of $\Upsilon(\mathcal{N}) = \vartheta(G)$ may not be clear since the fractional part of $\vartheta(G)$ will be lost in the one-shot capacity. However, we can always choose a noiseless m-bit channel $\mathcal{I}_m$ with $\Upsilon(\mathcal{I}_m) = m$ for $m = 10^d$ for some d. Then $\mathcal{N} \otimes \mathcal{I}_m$ is a channel with one-shot capacity $\log\lfloor \Upsilon(\mathcal{N} \otimes \mathcal{I}_m) \rfloor = \log\lfloor m\vartheta(G) \rfloor$, which is clearly different from $\log(m\lfloor \vartheta(G) \rfloor)$.

Acknowledgements

The authors would like to thank Min-Hsiu Hsieh, Cheng Guo, Xin Wang, and Andreas Winter for helpful discussion. CYL and RD were supported by the Australian Research Council (ARC) under Grant DP120103776. RD was also supported by the ARC Future Fellowship under Grant FT120100449 and the National Natural Science Foundation of China under Grant 61179030.

References

1. C. Shannon, "The zero error capacity of a noisy channel," *IRE Trans. Inf. Theory*, vol. 2, no. 3, pp. 8–19, September 1956.
2. L. Lovász, "On the Shannon capacity of a graph," *IEEE Trans. Inf. Theory*, vol. IT-25, no. 1, pp. 1–7, 1979.
3. W. Haemers, "On some problems of Lovász concerning the Shannon capacity of a graph," *IEEE Trans. Inf. Theory*, vol. IT-25, no. 2, pp. 231–232, 1979.
4. ——, "An upper bound for the Shannon capacity of a graph," *Coll. Math. Soc. János Bolyai*, vol. 25, pp. 267–272, 1978.
5. R. A. C. Medeiros, R. Alléaume, G. Cohen, and F. M. de Assis, "Quantum states characterization for the zero-error capacity," 2006.
6. R. Duan, S. Severini, and A. Winter, "Zero-error communication via quantum channels, noncommutative graphs, and a quantum Lovász number," *IEEE Trans. Inf. Theory*, vol. 59, no. 2, pp. 1164–1174, Feb 2013.
7. R. Duan and Y. Shi, "Entanglement between two uses of a noisy multipartite quantum channel enables perfect transmission of classical information," *Phys. Rev. Lett.*, vol. 101, p. 020501, Jul 2008.
8. R. Duan, "Super-activation of zero-error capacity of noisy quantum channel," 2009. [Online]. Available: http://arxiv.org/abs/quant-ph/0906.2527
9. T. Cubitt, J. Chen, and A. W. Harrow, "Superactivation of the asymptotic zero-error classical capacity of a quantum channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 12, pp. 8114–8126, December 2011.
10. T. Cubitt and G. Smith, "An extreme form of superactivation for quantum zero-error capacities," *IEEE Trans. Inf. Theory*, vol. 58, no. 3, pp. 1953–1961, March 2012.
11. T. S. Cubitt, D. Leung, W. Matthews, and A. Winter, "Improving zero-error classical communication with entanglement," *Phys. Rev. Lett.*, vol. 104, p. 230503, Jun 2010.
12. D. Leung, L. Mancinska, W. Matthews, M. Ozols, and A. Roy, "Entanglement can increase asymptotic rate of zero-error classical communication over classical channels," *Commun. Math. Phys.*, vol. 311, pp. 97–111, 2012.
13. S. Beigi, "Entanglement-assisted zero-error capacity is upper-bounded by the Lovász ϑ function," *Phys. Rev. A*, vol. 82, p. 010303, Jul 2010.
14. X. Wang and R. Duan, "Separation between quantum Lovász number and entanglement-assisted zero-error classical capacity," 2016. [Online]. Available: http://arxiv.org/abs/1608.04508
15. M. Mosonyi and N. Datta, "Generalized relative entropies and the capacity of classical-quantum channels," *J. Math. Phys.*, vol. 50, no. 7, p. 072104, 2009.
16. L. Wang and R. Renner, "One-shot classical-quantum capacity and hypothesis testing," *Phys. Rev. Lett.*, vol. 108, p. 200501, May 2012. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.108.200501
17. N. Datta and M. H. Hsieh, "One-shot entanglement-assisted quantum and classical communication," *IEEE Trans. Inf. Theory*, vol. 59, no. 3, pp. 1929–1939, March 2013.
18. W. Matthews and S. Wehner, "Finite blocklength converse bounds for quantum channels," *IEEE Trans. Inf. Theory*, vol. 60, no. 11, pp. 7317–7329, Nov 2014.
19. D. Beckman, D. Gottesman, M. A. Nielsen, and J. Preskill, "Causal and localizable quantum

operations," *Phys. Rev. A*, vol. 64, p. 052309, Oct 2001.
20. T. Eggeling, D. Schlingemann, and R. F. Werner, "Semicausal operations are semilocalizable," *Europhys. Lett*, vol. 57, no. 6, pp. 782–788, 2002.
21. M. Piani, M. Horodecki, P. Horodecki, and R. Horodecki, "Properties of quantum nonsignaling boxes," *Phys. Rev. A*, vol. 74, p. 012305, Jul 2006.
22. O. Oreshkov, F. Costa, and Č. Brukner, "Quantum correlations with no causal order," *Nature Comm.*, vol. 3, no. 10, p. 1092, 2012.
23. G. Chiribella, "Perfect discrimination of no-signalling channels via quantum superposition of causal structures," *Phys. Rev. A*, vol. 86, p. 040301, Oct 2012.
24. T. Cubitt, D. Leung, W. Matthews, and A. Winter, "Zero-error channel capacity and simulation assisted by non-local correlations," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 5509–5523, Aug 2011.
25. R. Duan and A. Winter, "No-signalling-assisted zero-error capacity of quantum channels and an information theoretic interpretation of the lovász number," *IEEE Trans. Inf. Theory*, vol. 62, no. 2, pp. 891–914, Feb 2016.
26. D. Leung and W. Matthews, "On the power of PPT-preserving and non-signalling codes," *IEEE Trans. Inf. Theory*, vol. 61, no. 8, pp. 4486–4499, Aug 2015.
27. R. Duan and X. Wang, "Activated zero-error classical capacity of quantum channels in the presence of quantum no-signalling correlations," 2015. [Online]. Available: http://arxiv.org/abs/1510.05437
28. S. B. L. Vandenberghe, "Semidefinite programming," *SIAM Rev.*, vol. 38, no. 1, 1996.
29. A. Vesel and J. Žerovnik, "Improved lower bound on the Shannon capacity of C_7," *Information Processing Letters*, vol. 81, no. 5, pp. 277 – 282, 2002.
30. B. Codenotti, I. Gerace, and G. Resta, "Some remarks on the Shannon capacity of odd cycles," 2003.
31. T. Bohman, "A limit theorem for the Shannon capacities of odd cycles I," *Proc. Amer. Math. Soc.*, vol. 131, no. 11, pp. 3559–3569, 2003.
32. ——, "A limit theorem for the Shannon capacities of odd cycles II," *Proc. Amer. Math. Soc.*, vol. 133, no. 2, pp. 537–543, 2005.
33. A. Cabello, S. Severini, and A. Winter, "Graph-theoretic approach to quantum correlations," *Phys. Rev. Lett.*, vol. 112, p. 040401, Jan 2014.
34. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes.* Amsterdam, The Netherlands: North-Holland, 1977.
35. C. Godsil and G. Royle, *Algebra Coding Theory.* New York: Springer-Verlag, 2001.
36. R. J. McEliece, E. R. Rodemich, and J. H. C. Rumsey, "The Lovász bound and some generalizations," *J. Combin. Inform. Syst. Sci.*, vol. 3, pp. 134–152, 1978.
37. E. R. van Dam, "Graphs with few eigenvalues: An interplay between combinatorics and algebra," Ph.D. dissertation, Tilburg University, Tilburg, Netherlands, 1996.
38. K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory.* New York: Springer-VErlag, 1990.
39. H. Ito, "An application of a product formula for the cubic Gauss sum," *Journal of Number Theory*, vol. 135, no. 0, pp. 139 – 150, 2014.
40. B. C. Berndt and R. J. Evans, "The determination of Gauss sums," *Bull. Amer. Math. Soc.*, vol. 5, no. 2, pp. 107–129, 1981.