On the One-Shot Zero-Error Classical Capacity of Classical-Quantum Channels Assisted by Quantum Non-signalling Correlations

Ching-Yi Lai[1,*] and Runyao Duan[1,2,†]

[1]Centre for Quantum Computation & Intelligent Systems,

Faculty of Engineering and Information Technology, University of Technology, Sydney, NSW, 2007, Australia

[2]UTS-AMSS Joint Research Laboratory of Quantum Computation and Quantum Information Processing,

Academy of Mathematics and Systems Science, Chinese Academy of Science, Beijing 100190, China

(Dated: September 12, 2014)

Shannon discussed the communication problem in the setting of zero errors and connected this problem to the graph theory [1]. It turns out that the zero-error capacity of a channel only depends on its induced confusability graph G and it suffices to discuss the Shannon capacity of a graph G: $\Theta(G) = \sup_m \sqrt[m]{\alpha(G^{\boxtimes m})}$, where $\alpha(G)$ is the independence number of G and $G^{\boxtimes m}$ is the m-fold strong product of G with itself. However, $\Theta(G)$ is difficult to determine, even for a simple graph, such as cycle graphs $\mathcal{C}_n$ of odd length. Lovász proposed an upper bound $\vartheta(G)$ on the Shannon capacity of a graph G [2], and it is tight in some cases. For example, $\Theta(\mathcal{C}_5) = \vartheta(\mathcal{C}_5)$. Although $\Theta(\mathcal{C}_n)$ for $n \geq 7$ are still unknown, it is 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 additional operational meanings for the Lovász ϑ function.

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, 8, 9, 10]. In general, 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]. For classical channels, it is suspected that entanglement-assisted zero-error capacity is exactly the Lovász ϑ function [6].

In [14], 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 information theory [15]. QNSCs are completely positive and trace-preserving linear maps $\Pi : \mathcal{L}(\mathcal{A}_i) \otimes \mathcal{L}(\mathcal{B}_i) \to \mathcal{L}(\mathcal{A}_o) \otimes \mathcal{L}(\mathcal{B}_o)$ so that the two parties A and B cannot send any information to each other by using Π. Resources, such as shared randomness, entanglement, and classical non-signalling correlations, can be considered as special types of QNSCs.

Suppose $\mathcal{N} : |k\rangle\langle k| \to \rho_k$ is a classical-quantum (C-Q) channel that maps a set of classical states $|k\rangle\langle k|$ into a set of quantum states $\rho_k \in \mathcal{L}(\mathcal{B})$. The one-shot zero-error capacity of the C-Q channel $\mathcal{N}$ assisted by a QNSC Π is equivalent to 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. In [15], Duan and Winter showed that the *one-shot* QNSC-assisted zero-error classical capacity is the integral part of

*chingyi.lai@uts.edu.au

†runyao.duan@uts.edu.au

the solution $\Upsilon(\mathcal{N})$ to the following SDP with variables $s_k \in \mathbb{R}$ and $R_k \in \mathcal{L}(\mathcal{B})$:

$$\begin{aligned} \Upsilon(\mathcal{N}) = &\max \sum_k s_k \\ \text{subject to: } & s_k \geq 0, \\ & 0 \leq R_k \leq s_k(\mathbb{I} - P_k), \\ & \sum_k (s_k P_k + R_k) = \mathbb{I}, \end{aligned} \tag{1}$$

where P_k be the projector onto the support of ρ_k and $\mathbb{I}$ is the identity operator. Moreover, they proved that the *asymptotic* zero-error classical capacity of a QNSC-assisted C-Q channel is exactly $\log \vartheta(G)$ when ρ_k are induced from an *optimal orthonormal representation* (OOR) of a graph G. An orthonormal representation of a graph G of n vertices is a set of n unit vectors $\{\mathbf{u}_0, \cdots, \mathbf{u}_{n-1}\} \in \mathbb{C}^d$ for some d so that their inner product $\langle \mathbf{u}_i, \mathbf{u}_j \rangle = \mathbf{u}_i^\dagger \mathbf{u}_j = 0$ if vertices i and j are not neighbors. Its *value* is defined as $\theta(\{\mathbf{u}_j\}) = \min_{\mathbf{c}:||\mathbf{c}||=1} \max_j \frac{1}{|\mathbf{c}^\dagger \mathbf{u}_j|^2}$. The Lovász function $\vartheta(G)$ is defined as the minimum value over all representations and a representation with value $\vartheta(G)$ is called optimal.

In this article we consider the type of C-Q channel $\mathcal{N} : |k\rangle\langle k| \to |u_k\rangle\langle u_k|$, where $\{\mathbf{u}_0, \cdots, \mathbf{u}_{n-1}\}$ is an OOR of a graph G in some Hilbert space $\mathcal{B}$. (For convenience, we use the Dirac notation $|u\rangle$ to denote the quantum state corresponding to the vector $\mathbf{u}$, and vice versa.) It is easy to see that $\alpha(G) \leq \Upsilon(\mathcal{N}) \leq \vartheta(G)$. We will provide a class of *circulant graphs*, defined by *equal-sized cyclotomic cosets*, so that the one-shot QNSC-assisted zero-error classical capacity of their induced C-Q channels are the integral part of

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

Moreover, since ϑ is multiplicative, the asymptotic QNSC-assisted zero-error classical capacity of these C-Q channels are

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

This provides a more straightforward operational meaning for the Lovász ϑ function.

We first provide an orthonormal representation for any circulant graphs. A circulant graph $G = X(\mathbb{Z}_n, C)$ has an edge set $\{(i,j) : i - j \in C\}$, where C is a subset of $\mathbb{Z}_n \setminus \{0\}$, called the connection set, and $-C = C$. The eigenvalues of the adjacency matrix of G are $\lambda_k = \sum_{j\in C} e^{2\pi i jk/n}$. Let

$$\mathbf{u}_0 = \frac{1}{\sqrt{\vartheta(G)}} \left(1, \sqrt{\frac{\lambda_1 - \lambda_{\min}}{\lambda_{\max} - \lambda_{\min}}}, \cdots, \sqrt{\frac{\lambda_{n-1} - \lambda_{\min}}{\lambda_{\max} - \lambda_{\min}}}\right)^T$$

and $\mathbf{u}_k = U^k \mathbf{u}_0$, for $k = 0, \cdots, n-1$, where $U = \text{diag}\left(1, e^{-2\pi i/n}, \cdots, e^{-2(n-1)\pi i/n}\right)$ is a unitary operator. Then $\{\mathbf{u}_k\}$ is an orthonormal representation of the circulant graph G. If G is edge-transitive, then $\{\mathbf{u}_k\}$ is an OOR.

Cyclotomic cosets usually appear in the application of coding theory to determine minimal polynomials over finite fields or integer rings [16]. 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

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

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 $C_{(s)}$. The cyclotomic cosets are well-defined: $C_{(\alpha)} = C_{(\beta)}$ if and only if $\alpha = \beta q^c \mod n$ for some $c \in \mathbb{Z}$. Hence any element in a coset can be the coset representative. As a consequence, the integers modulo n are partitioned into disjointed cyclotomic cosets: $\mathbb{Z}_n = \bigcup_{j=0}^{t} C_{(\alpha_j)}$, where $\{\alpha_0 = 0, \alpha_1, \cdots, \alpha_t\}$ is a set of (disjointed) coset representatives. If $C_{(1)} = C_{(-1)}$, then we can generate the circulant graph $G = X(\mathbb{Z}_n, C_{(1)})$. 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 has some interesting properties that are key to the proof of our main theorem: the nontrivial eigenvalues are indexed by the cyclotomic coset representatives and have equal multiplicity.

Next we explicitly construct feasible solutions to the SDP (1) when the C-Q channel $\mathcal{N}$ is induced by these circulant graphs. Let $s_k = \frac{\vartheta(G)}{n}$, $R_k = U^k R_0 U^{-k}$, and

$$R_0 = \frac{1}{n}\left(\mathbb{I} - \sum_{j=0}^{n-1} x_j P_j\right),$$

where $x_j = \frac{\lambda_{j\beta} - \lambda_\beta}{\lambda_0 - \lambda_\beta}$, given $\lambda_\beta = \lambda_{\min}$ for some $\beta \in \mathbb{Z}_n^\times$. Then the SDP (1) is solved with $\Upsilon(\mathcal{N}) = \vartheta(G)$. A central part of the proof is using the Perron-Frobenius theorem to show that R_0 is positive semi-definite.

Finally we characterize the graphs defined by equal-sized cyclotomic cosets. A necessary condition is that $|C_{(1)}|$ is a common divisor of $\varphi(d)$ for all $d|n$ and $d > 1$. It remains to find conditions so that $C_{(1)} = C_{(-1)}$.

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 $n-1$, and it defines the cycle graph $\mathcal{C}_n$. Suppose $\mathcal{N}$ is the C-Q channel induced by the OOR of the cycle graph $\mathcal{C}_n$. Then $\Upsilon(\mathcal{N}) = \vartheta(\mathcal{C}_n) = \frac{n\cos\frac{\pi}{n}}{1+\cos\frac{\pi}{n}}$.

When $n = p^r$ is a prime power, $\mathbb{Z}_{p^r}^\times$ is cyclic. Let $\mathbb{Z}_{p^r}^\times = \langle\alpha\rangle$ for $\alpha \in \mathbb{Z}_p$, and α is of order $\varphi(p^r)$. Consequently, $-1 \equiv \alpha^{\varphi(p^r)/2}$. Therefore, $-1 \in C_{(1)} = \langle q\rangle$ if $q = \alpha^b$ for some $b \mid (\varphi(p^r)/2)$, and then $|C_{(1)}| = \frac{\varphi(p^r)}{b}$. Then the graph $X(\mathbb{Z}_{p^r}, \langle\alpha^{p^{r-1}}\rangle)$ is defined by equal-sized cyclotomic cosets.

The case is simpler when n is a prime. 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.

When $t = 2$, the cosets 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. Let Q denote the set of quadratic residues modulo p. Then $\mathcal{QR}_p = X(\mathbb{Z}_p, Q)$ [17]. The Paley graphs are self-complimentary and consequently $\Theta(\mathcal{QR}_p) = \vartheta(\mathcal{QR}_p) = \sqrt{p}$ [2, Theorem 12]. Suppose $\mathcal{N}$ is the C-Q channel induced by the OOR of the Paley graph $\mathcal{QR}_p$. Then $\Upsilon(\mathcal{N}) = \vartheta(\mathcal{QR}_p) = \sqrt{p}$.

When $t = 3$, the cosets lead to the cubic residue graphs $\mathcal{CR}_p$[19]. 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 $4p = a^2 + b^2$ and $a \equiv 1 \mod 3$ [20]. Currently the closed form for $\vartheta(\mathcal{CR}_p)$ is still unknown.

The type of circulant graphs defined by equal-sized cyclotomic cosets bear very a strong symmetry. It is interesting to see if there are other graphs that have this property. For example, we may consider (strongly) regular graphs.

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. [Online]. Available: arXiv:quantum-ph/0611042v2

[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. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.101.020501

[8] R. Duan, “Super-activation of zero-error capacity of noisy quantum channel.” [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. Cubitt, D. Leung, W. Matthews, and A. Winter, “Improving zero-error classical communication with entanglement,” *Phys. Rev. Lett.*, vol. 104, p. 230503, Jun 2010. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.104.230503

[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. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.82.010303

[14] 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.

[15] R. Duan and A. Winter, “Zero-error classical channel capacity and simulation cost assisted by quantum non-signalling correlations,” 2014. [Online]. Available: http://arxiv.org/abs/1409.3426

[16] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.

[17] C. Godsil and G. Royle, *Algebra Coding Theory*. New York: Springer-Verlag, 2001.

[18] 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.

[19] E. R. van Dam, “Graphs with few eigenvalues: An interplay between combinatorics and algebra,” Ph.D. dissertation, Tilburg University, Tilburg, Netherlands, 1996.

[20] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*. New York: Springer-VErlag, 1990.