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

Ching-Yi Lai\textsuperscript{1,\ast} and Runyao Duan\textsuperscript{1,2,†}

\textsuperscript{1}Centre for Quantum Computation & Intelligent Systems, Faculty of Engineering and Information Technology, University of Technology, Sydney, NSW, 2007, Australia
\textsuperscript{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 $G$: $\Theta(G) = \sup_m \sqrt{\alpha(G^\otimes m)}$, where $\alpha(G)$ is the independence number of $G$ and $G^\otimes m$ 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 $C_n$ 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, $\Theta(C_5) = \vartheta(C_5)$. Although $\Theta(C_n)$ for $n \geq 7$ are still unknown, it is close to $\vartheta(C_n)$. 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 $\vartheta$ 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 $\vartheta$ function [13]. For classical channels, it is suspected that entanglement-assisted zero-error capacity is exactly the Lovász $\vartheta$ function [6].

In [14], Cubitt \textit{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 $\Pi : \mathcal{L}(A_i) \otimes \mathcal{L}(B_i) \to \mathcal{L}(A_o) \otimes \mathcal{L}(B_o)$ so that the two parties $A$ and $B$ cannot send any information to each other by using $\Pi$. 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 $\Pi$ 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 $\Pi$. In [15], Duan and Winter showed that the \textit{one-shot} QNSC-assisted zero-error classical capacity is the integral part of

\*chingyi.lai@uts.edu.au
\†runyao.duan@uts.edu.au
Moreover, since cyclotomic cosets α these C-Q channels are the integral part of Z

\[ \{ \text{minimum value over all representations and a representation with value } \} \]

This provides a more straightforward operational meaning for the Lovász \( \vartheta(G) \) function.

In this article we consider the type of C-Q channel \( \mathcal{N} : |k\rangle\langle k| \rightarrow |u_k\rangle\langle u_k| \), where \( \{u_0, \cdots, u_{n-1}\} \) 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 \( u \), 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 \( \vartheta \) is multiplicative, the asymptotic QNSC-assisted zero-error classical capacity of these C-Q channels are

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

This provides a more straightforward operational meaning for the Lovász \( \vartheta \) 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 \( \lambda_k = \sum_{j \in C} e^{2\pi ijk/n} \). Let

\[ u_0 = \frac{1}{\sqrt{\vartheta(G)}} \left( 1, \sqrt{\frac{\lambda_1 - \lambda_{\min}}{\lambda_{\max} - \lambda_{\min}}}, \cdots, \sqrt{\frac{\lambda_{n-1} - \lambda_{\min}}{\lambda_{\max} - \lambda_{\min}}} \right) \]

and \( u_k = U^k u_0 \), for \( k = 0, \cdots, n-1 \), where \( U = \text{diag}(1, e^{-2\pi i/n}, \cdots, e^{-2(n-1)\pi i/n}) \) is a unitary operator. Then \( \{u_k\} \) is an orthonormal representation of the circulant graph \( G \). If \( G \) is edge-transitive, then \( \{u_k\} \) 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

\[ C_s(q) = \{s, sq, sq^2, \cdots, sq^{r_s-1}\}, \]
where \( r_s \) is the smallest positive integer \( r \) so that \( sq^r \equiv s \pmod{n} \). The subscript \( s \) is called the coset representative of \( C(s) \). The cyclotomic cosets are well-defined: \( C(a) = C(b) \) if and only if \( \alpha = \beta q^r \pmod{n} \) 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: \( \mathbb{Z}_n = \bigcup_{j=0}^{p-1} C(\alpha_j) \), where \( \{\alpha_0 = 0, \alpha_1, \ldots, \alpha_{t}\} \) 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 \( N \) 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 \( \lambda_\beta = \lambda_{\text{min}} \) for some \( \beta \in \mathbb{Z}_p^\times \). Then the SDP (1) is solved with \( \Upsilon(N) = \vartheta(G) \). 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 \( d \mid n \) 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 \( C_n \). Suppose \( N \) is the C-Q channel induced by the OOR of the cycle graph \( C_n \). Then \( \Upsilon(N) = \vartheta(C_n) = \frac{n \cos \frac{\pi}{n}}{1 + \cos \frac{\pi}{n}} \).

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 \( \alpha \) 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 \( \mathbb{Z}_p^\times = \langle \alpha \rangle \). 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 \( Q\mathcal{R}_p \). A nonzero integer \( a \) is called a quadratic residue modulo \( n \) if \( a = b^2 \pmod{n} \) for some integer \( b \); otherwise, \( a \) is a quadratic nonresidue modulo \( n \). Let \( Q \) denote the set of quadratic residues modulo \( p \). Then \( Q\mathcal{R}_p = X(\mathbb{Z}_p, Q) \) [17]. The Paley graphs are self-complimentary and consequently \( \Theta(Q\mathcal{R}_p) = \vartheta(Q\mathcal{R}_p) = \sqrt{p} \) [2, Theorem 12]. Suppose \( N \) is the C-Q channel induced by the OOR of the Paley graph \( Q\mathcal{R}_p \). Then \( \Upsilon(N) = \vartheta(Q\mathcal{R}_p) = \sqrt{p} \).

When \( t = 3 \), the cosets lead to the cubic residue graphs \( C\mathcal{R}_p \) [19]. A nonzero integer \( a \) is called a cubic residue modulo \( p \) if \( a = b^3 \pmod{p} \) for some integer \( b \). The cyclotomic coset \( C(1) \) consists of cubic residues. \( C\mathcal{R}_p = X(\mathbb{Z}_p, C(1)) \) 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 \( a \equiv 1 \pmod{3} \) [20]. Currently the closed form for \( \vartheta(C\mathcal{R}_p) \) 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


