EQIS 2002, Tokyo, Japan, Sep. 5 – Sep. 8, 2002

Information Rates Achievable with Algebraic Codes on Quantum Discrete Memoryless Channels

Mitsuru Hamada
Quantum Computation and Information Project (ERATO)
Japan Science and Technology Corporation
5-28-3, Hongo, Bunkyo-ku, Tokyo 113-0033, Japan
E-mail: mitsuru@ieee.org

Abstract — **The highest information rate at which quantum error-correction schemes work reliably on a channel, which is called the quantum capacity, is proven to be lower bounded by the limit of the quantity termed coherent information maximized over the set of input density operators which are proportional to the projections onto the code spaces of stabilizer codes. Quantum channels to be considered are those subject to independent errors and modeled as tensor products of copies of a completely positive linear map on a Hilbert space of finite dimension, and the codes that are proven to be have the desired performance are stabilizer codes. On the depolarizing channel, this work's bound is actually the highest possible rate at which stabilizer codes work reliably. The details of this work can be found in [1].**

I. Introduction

The problem of determining the capacity of quantum channels was posed by Shor in the first paper on quantum error-correcting codes (quantum codes, or codes, hereafter). He discussed it in the context of preservation of quantum states, which are to be used for quantum computation in the presence of quantum noise. There is a known upper bound on the quantum capacity based on the quantity called coherent information, and some authors conjecture that this bound is tight. On the other hand, known lower bounds appear to have left much room for improvement. For example, on the capacity of the depolarizing channel, which suffers uniform depolarization and can be specified by Kraus operators $\sqrt{1-p}I$, $\sqrt{p/3}X$, $\sqrt{p/3}Y$, $\sqrt{p/3}Z$ with I and X, Y, Z being the identity and Pauli operators, respectively, the highest lower bound known is $1 - h(p) - p\log_2 3$ for a wide range of p, where h is the binary entropy function. Shor and Smolin argued this bound is not tight showing the existence of concatenated quantum codes that slightly go beyond it for a limited range of p, which revealed a remarkable feature of the quantity called coherent information appearing in their improved bound. While their work and the subsequent analysis of DiVincenzo and these authors [2] abounded with suggestions, their code construction was apparently restricted, and explorations into the general nature behind their code construction and further analysis were awaited [2].

The aim of this work is to give a more general lower bound which partially closes the gap between the upper and lower bounds, at least qualitatively. The bound to be presented is expressed as the limit of coherent information maximized over the set of input density operators which are proportional to the projections onto the code spaces of standard algebraic quantum codes. This limit closely resembles the known upper bound on the capacity, which is the one defined in the same way but with the restriction on input density operators removed.

Concatenated quantum codes form a subclass of the class of standard algebraic quantum codes, which are called stabilizer, additive or symplectic stabilizer codes in the literature. A symplectic stabilizer code is a simultaneous eigenspace of a set of commuting operators, which is called a stabilizer. A stabilizer is obtained by constructing a code over a finite field which is self-orthogonal with respect to a symplectic bilinear form and then transforming it into operators on a Hilbert space through a one-to-one correspondence (a projective representation). A stabilizer of a concatenated quantum code, which will simply be called a concatenated code in what follows, is obtained by concatenating two such self-orthogonal codes and putting it through the representation. We refer to these two codes, or the corresponding quantum codes, an inner code and an outer one. Shor and Smolin's concatenated code uses an inner code with restricted parameters. Namely, their inner code is an $[[n, k = 1]]$ code, where an $[[n, k]]$ code is a 2^k-dimensional subspace of the tensor product of n copies of a two-dimensional Hilbert space. This paper develops DiVincenzo, Shor and Smolin's analysis [2] to include that of concatenated codes with general inner $[[n, k]]$ codes with $1 \le k \le n$.

II. Capacity and New Lower Bound

As usual, all quantum channels and decoding (state-recovery) operations in coding systems are described in terms of *trace-preserving completely positive* (TPCP) linear maps. Given a Hilbert space H of finite dimension, let $\mathsf{L}(\mathsf{H})$ denote the set of linear operators on H. In general, every completely positive (CP) linear map $\mathcal{M} : \mathsf{L}(\mathsf{H}) \to \mathsf{L}(\mathsf{H})$ has an operator-sum representation $\mathcal{M}(\rho) = \sum_{i\in\mathcal{I}} M_i \rho M_i^\dagger$ with some $M_i \in \mathsf{L}(\mathsf{H})$, $i \in \mathcal{I}$. When $\mathcal{M}$ is specified by a set of operators $\{M_i\}_{i\in\mathcal{I}}$ in this way, we write $\mathcal{M} \sim \{M_i\}_{i\in\mathcal{I}}$.

Hereafter, H denotes an arbitrarily fixed Hilbert space of dimension d, which is a prime number. A quantum memoryless channel is a TPCP linear map $\mathcal{A} : \mathsf{L}(\mathsf{H}) \to \mathsf{L}(\mathsf{H})$. A memoryless channel $\mathcal{A}$ is supposed to act on a state or a density operator ρ in $\mathsf{L}(\mathsf{H}^{\otimes n})$ as $\mathcal{A}^{\otimes n}(\rho)$. A pair $(\mathcal{C}_n, \mathcal{R}_n)$ consisting of a subspace $\mathcal{C}_n \subseteq \mathsf{H}^{\otimes n}$ and a TPCP linear map $\mathcal{R}_n : \mathsf{L}(\mathsf{H}^{\otimes n}) \to \mathsf{L}(\mathsf{H}^{\otimes n})$, which is supposed to serve as a recovery operator, is called a *(quantum) code*, its *information rate* (or simply rate) is defined to be $n^{-1} \log_d \dim \mathcal{C}_n$, and its performance is evaluated in terms of *minimum fidelity*

$$F(\mathcal{C}_n, \mathcal{R}_n \mathcal{A}^{\otimes n}) = \min_{|\psi\rangle \in \mathcal{C}_n} \langle \psi | \mathcal{R}_n \mathcal{A}^{\otimes n}(|\psi\rangle\langle\psi|) | \psi \rangle, \qquad (1)$$

where $\mathcal{R}_n \mathcal{A}^{\otimes n}$ denotes the composition of $\mathcal{A}^{\otimes n}$ and $\mathcal{R}_n$. A subspace $\mathcal{C}_n$ alone is also called a code assuming implicitly some recovery operator.

For simplicity, we will work on a special class of channels that are specified as follows though the lower bound to be presented is applicable to general channels. Fix an orthonormal basis $\{|0\rangle, \ldots, |d-1\rangle\}$ of H. Put $\mathcal{X} = \{0, \ldots, d-1\}^2$ and

$$N_{(i,j)} = X^i Z^j, \quad (i,j) \in \mathcal{X}, \qquad (2)$$

where $X, Z \in \mathsf{L}(\mathsf{H})$ are Weyl's unitary operators defined by $X|j\rangle = |(j-1) \bmod d\rangle$, $Z|j\rangle = \omega^j |j\rangle$ with ω being a primitive d-th root of unity. The set $\mathsf{N} = \{N_u\}_{u \in \mathcal{X}}$ is a basis of $\mathsf{L}(\mathsf{H})$ and could be viewed as a generalization of the Pauli operators (including the identity). We will treat channels that can be written as $\mathcal{A} \sim \{\sqrt{P(u)} N_u\}_{u \in \mathcal{X}}$, which will be called Pauli channels or N-channels, where P is a probability distribution on $\mathcal{X}$. From the basis $\{N_{(i,j)}\}$ of $\mathsf{L}(\mathsf{H})$, we obtain a basis $\mathsf{N}_n = \{N_x\}_{x \in \mathcal{X}^n}$ of $\mathsf{L}(\mathsf{H}^{\otimes n})$, where $N_x = N_{x_1} \otimes \ldots \otimes N_{x_n}$ for $x = (x_1, \ldots, x_n) \in \mathcal{X}^n$.

Definition 1 *Let $F^\star_{n,k}(\mathcal{A}^{\otimes n})$ denote the supremum of $F(\mathcal{C}, \mathcal{R}\mathcal{A}^{\otimes n})$ such that there exists a code $(\mathcal{C} \subseteq \mathsf{H}^{\otimes n}, \mathcal{R})$ with $\log_d \dim \mathcal{C} \geq k$, where $n > 0$ is an integer and k, $0 \leq k \leq n$, is a real number. The supremum of nonnegative numbers R satisfying*

$$\limsup_{n \to \infty} F^\star_{n, Rn}(\mathcal{A}^{\otimes n}) = 1$$

is called the quantum capacity *of $\mathcal{A}$ and denoted by $\mathsf{C}(\mathcal{A})$.*

For a density operator $\rho \in \mathsf{L}(\mathsf{H}')$ and a TPCP map $\mathcal{A}' : \mathsf{L}(\mathsf{H}') \to \mathsf{L}(\mathsf{H}')$, the coherent information $I_{\mathrm{c}}(\rho, \mathcal{A}')$ is defined by

$$I_{\mathrm{c}}(\rho, \mathcal{A}') = S\big(\mathcal{A}'(\rho)\big) - S\big([\mathrm{I} \otimes \mathcal{A}'](|\Psi\rangle\langle\Psi|)\big),$$

where $S(\sigma)$ denotes the von Neumann entropy of σ, I is the identity map on $\mathsf{L}(\mathsf{H}')$, and $|\Psi\rangle \in \mathsf{H}'' \otimes \mathsf{H}'$ is a purification of ρ. This work's main result is the next one.

Theorem 1 *Let the basis $\mathsf{N} = \{N_u\}_{u \in \mathcal{X}} = \{X^i Z^j\}_{(i,j) \in \mathcal{X}}$ be specified as above. For a memoryless channel $\mathcal{A} \sim \{\sqrt{P(u)} N_u\}_{u \in \mathcal{X}}$, where P is a probability distribution on $\mathcal{X}$, we have*

$$\mathsf{C}(\mathcal{A}) \geq \sup_{n \geq 1} \max_{\mathcal{C} \in \mathsf{S}_n(\mathsf{N})} \frac{I_{\mathrm{c}}\big((\dim \mathcal{C})^{-1} \Pi_{\mathcal{C}}, \mathcal{A}^{\otimes n}\big)}{n},$$

where $\Pi_{\mathcal{C}}$ is the projection onto $\mathcal{C}$ and $\mathsf{S}_n(\mathsf{N})$ is the set of all symplectic stabilizer codes designed with N_n.

To be precise, a symplectic stabilizer code designed with N_n is a simultaneous eigenspace of a set of commuting operators that belong to N_n (see, e.g., [3, Lemma 2 and its Remarks]). An upper bound on $\mathsf{C}(\mathcal{A})$ for a general CP map $\mathcal{A} : \mathsf{H} \to \mathsf{H}$ that trivially follows from a known result is

$$\sup_{n \geq 1} \max_{\mathcal{C}} \frac{I_{\mathrm{c}}\big((\dim \mathcal{C})^{-1} \Pi_{\mathcal{C}}, \mathcal{A}^{\otimes n}\big)}{n}$$

where the maximum is taken over all subspaces of $\mathsf{H}^{\otimes n}$. Observe that the difference between the upper bound and the lower one only resides in the ranges for the maximization. This author conjectures that for the memoryless channel $\mathcal{A} \sim \{\sqrt{P(u)} N_u\}_{u \in \mathcal{X}}$, the upper bound and the lower one are equal to each other.

This work also shows that the bound in the above theorem is actually the 'conditional' capacity of the depolarizing channel on symplectic stabilizer codes, which indicates the supremum of information rates at which symplectic stabilizer codes work reliably.

III. Remarks

We remark that this work's bound applies to general discrete memoryless channels (TPCP maps) as treated in [3]. Namely, if we associate the probability distribution $P = P_{\mathcal{A}}$ with a channel $\mathcal{A}$ [or $P = P_{\mathcal{U}\mathcal{A}}$ with some TPCP map $\mathcal{U}$ on $\mathsf{L}(\mathsf{H})$] as in [3, Section II], we have

$$\mathsf{C}(\mathcal{A}) \geq \sup_{n \geq 1} \max_{\mathcal{C} \in \mathsf{S}_n(\mathsf{N})} \frac{I_{\mathrm{c}}\big((\dim \mathcal{C})^{-1} \Pi_{\mathcal{C}}, \mathcal{A}'^{\otimes n}\big)}{n}$$

where $\mathcal{A}' \sim \{\sqrt{P(u)} N_u\}_{u \in \mathcal{X}}$. This generalization can be proved in a quite similar way to that in [3].

The details of this work can be found in [1].

Acknowledgments

The author is grateful to Hiroshi Imai and Keiji Matsumoto for support.

References

[1] M. Hamada, "Information rates achievable with algebraic codes on quantum discrete memoryless channels," e-Print quant-ph/0207113, LANL, 2002.

[2] D. P. DiVincenzo, P. W. Shor, and J. A. Smolin, "Quantum-channel capacity of very noisy channels," *Phys. Rev. A*, vol. 57, pp. 830–839, Feb. 1998. Correction: Phys. Rev. A, 59, p. 1717.

[3] M. Hamada, "Lower bounds on the quantum capacity and highest error exponent of general memoryless channels," *IEEE Trans. Information Theory*, 2002, in press. E-Print, quant-ph/0112103, LANL, 2001.