An Exponential Lower Bound on the Highest Fidelity Achievable by Quantum Error-Correcting Codes

Mitsuru HAMADA

Quantum Computation and Information Project, ERATO
Japan Science and Technology Corporation
201 Daini Hongo White Bldg.
5-28-3, Hongo, Bunkyo-ku, Tokyo 113-0033, Japan
E-mail: `mitsuru@ieee.org`

This work presents an exponential lower bound on the highest fidelity achievable by quantum error-correcting codes used on a quantum channel. This immediately yields a lower bound on the quantum capacity of the channel, which coincides with the known one for the depolarizing channel but seems new for general channels. This work can be viewed as a refinement of the recent result of Matsumoto and Uyematsu [1].

Given a Hilbert space H of finite dimension, let $\mathsf{B}(\mathsf{H})$ denote the set of operators on H. In general, every completely positive (CP) linear map $\mathcal{L} : \mathsf{B}(\mathsf{H}) \to \mathsf{B}(\mathsf{H})$ has a operator-sum representation $\mathcal{L}(\rho) = \sum_{i\in\mathcal{I}} L_i \rho L_i^*$, where $L_i \in \mathsf{B}(\mathsf{H})$, $i \in \mathcal{I}$. When $\mathcal{L}$ is specified by a set of operators $\{L_i\}_{i\in\mathcal{I}}$ in this way, we write $\mathcal{L} \sim \{L_i\}_{i\in\mathcal{I}}$.

Hereafter, H is an arbitrarily fixed Hilbert space whose dimension d is a prime number. A quantum channel is a sequence $\{\mathcal{A}_n\}$ of TPCP (trace-preserving completely positive) linear maps on $\mathsf{B}(\mathsf{H}^{\otimes n})$. When $\mathcal{A}_n = \mathcal{A}^{\otimes n}$ for some $\mathcal{A} : \mathsf{B}(\mathsf{H}) \to \mathsf{B}(\mathsf{H})$, it is called memoryless channel $\mathcal{A}$. We want some large subspaces $H = H_n \subset \mathsf{H}^{\otimes n}$ every vector (state) in which remains almost unchanged after the effect of the channel followed by the action of some suitable recovery process. The recovery process is again a TPCP map

$$\mathcal{R}_n : \mathsf{B}(\mathsf{H}^{\otimes n}) \to \mathsf{B}(\mathsf{H}^{\otimes n}).$$

Such pair $(H_n, \mathcal{R}_n)$ is called a code and its performance is evaluated in terms of fidelity

$$F(H, \mathcal{R}_n\mathcal{A}_n) = \min_{|\varphi\rangle\in H} \langle\psi|\mathcal{R}_n\mathcal{A}_n(|\psi\rangle\langle\psi|)|\psi\rangle.$$

Let $F^*_{n,k}(\mathcal{A}_n)$ denote the supremum of $F(H, \mathcal{R}_n\mathcal{A}_n)$ such that a code $(H, \mathcal{R}_n)$ exists with $\log_d \dim H \geq k$. Now fix an orthonormal basis $\{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}$ of H arbitrarily. Let unitary operators $X, Z \in \mathsf{B}(\mathsf{H})$ be defined by

$$X|a\rangle = X|(a-1) \bmod d\rangle, \quad Z|a\rangle = \omega^a|a\rangle \qquad (1)$$

with ω being a primitive d-th root of one. Note that $\{X^iZ^j \mid i,j = 0,1,\ldots,d-1\}$ is a basis of $\mathsf{B}(\mathsf{H})$.

Theorem 1 *Let integers n, k and a real number R satisfy $0 \leq k \leq Rn$ and $0 \leq R < 1$; a typical choice is $k = \lfloor Rn \rfloor$ for an arbitrarily fixed rate R. Then, for a memoryless channel $\mathcal{A} : \mathsf{B}(\mathsf{H}) \to \mathsf{B}(\mathsf{H})$, we have*

$$F^*_{n,k}(\mathcal{A}^{\otimes n}) \geq 1 - (n+1)^{2d^2} d^{-nE(R,P)}$$

where

$$E(R,P) = \min_Q \{D(Q||P) + |1 - H(Q) - R|^+\}.$$

Here, $|x|^+ = \max\{x, 0\}$, $D(P||Q) = \sum_{x\in\mathcal{X}} P(x) \log_d \frac{P(x)}{Q(x)}$ (the classical Kullback-Leibler divergence or relative entropy), $H(Q) = -\sum_{x\in\mathcal{X}} Q(x) \log_d Q(x)$ (classical entropy), the minimization with respect to Q is over all probability distributions on $\mathcal{X} = \{0,1,\ldots,d-1\}^2$, and P is the probability distribution on $\mathcal{X}$ determined from the channel $\mathcal{A}$ in the following manner. Let $\{E_{(i,j)} = X^iZ^j\}_{(i,j)\in\mathcal{X}}$ be the basis of $\mathsf{B}(\mathsf{H})$ specified above in (1), $\mathcal{A} \sim \{A_i\}_{i\in\mathcal{X}}$, and $A_u = \sum_{v\in\mathcal{X}} a_{uv}E_v$, $u \in \mathcal{X}$. Then,

$$P(v) = \sum_{u\in\mathcal{X}} a_{uv}a^*_{uv}, \quad v \in \mathcal{X}.$$

A direct consequence of the theorem is that the capacity of the channel $\mathcal{A}$ is lower bounded by $1 - H(P)$. It is possible to extend the result to the case where d is a power of a prime as well as to the case where the probability distributions associated with channels are Markovian.

References

[1] R. Matsumoto and T. Uyematsu, "Lower bound for the quantum capacity of a discrete memoryless quantum channel," e-Print quant-ph/0105151, 2001.