The Idenfication Capacity of a Descrete Memoryless Classical-Quantum Channel

Stephen Diadamo

November 25, 2017

Defintion. (DMCQC) For finite alphabet $\mathcal{X}$ and finite dimentional Hilbert space $\mathcal{H}$, let $W : \mathcal{X} \to \mathcal{S}(\mathcal{H})$ be a CQ channel. The discrete memoryless CQ channel (DMCQC) generated by W is given by the family $\{W^{\otimes n} : \mathcal{X}^n \to \mathcal{S}(\mathcal{H}^{\otimes n})\}_{n\in\mathbb{N}}$, where

$$W^{\otimes n}(x^n) = \bigotimes_{i=1}^{n} W(x_i).$$

Defintion. ((n, M)-code) For a finite alphabet $\mathcal{X}$ and finite dimentional Hilbert space $\mathcal{H}$, an (n, M)-code for classical message transmission over DMCQC generated by CQ channel $W : \mathcal{X} \to \mathcal{S}(\mathcal{H})$ is a family $\mathcal{C} \coloneqq (x_m, E_m)_{m=1}^{M}$, where $x_1, ..., x_M \in \mathcal{X}^n$ and $\{E_m\}_{m=1}^{M} \subset \mathcal{L}(\mathcal{H}^{\otimes n})$ forms a POVM on $\mathcal{H}^{\otimes n}$.

For (n, M)-code $\mathcal{C}$ we define maximum error $e(\mathcal{C}, W^{\otimes n})$ and $N(W, n, \lambda)$ such that

$$\begin{aligned} e(\mathcal{C}, W^{\otimes n}) &\coloneqq \max_{m\in[M]} \operatorname{tr}\big[(\mathbf{1} - E_m)W^{\otimes n}(x_m)\big] \\ N(W, n, \lambda) &\coloneqq \max\{M \in \mathbb{N} \mid \exists (n, M) - \text{code } \mathcal{C} \text{ with } e(\mathcal{C}, W^{\otimes n}) \le \lambda\} \end{aligned}$$

Defintion. (Holevo quantity) For a finite alphabet $\mathcal{X}$ and finite dimentional Hilbert space $\mathcal{H}$, let $W : \mathcal{X} \to \mathcal{S}(\mathcal{H})$ be a CQ channel and $p \in \mathcal{P}(\mathcal{X})$ a probability distribution on $\mathcal{X}$. The function

$$\chi(p, W) \coloneqq S(\overline{W}_p) - \sum_{x\in\mathcal{X}} p(x)S(W(x))$$

with $\overline{W}_p \coloneqq \sum_{x\in\mathcal{X}} p(x)W(x)$, is called the Holevo quantity of the tuple (p, W).

Defintion. (Classical Capacity over CQ Channel) For a finite alphabet $\mathcal{X}$ and finite dimentional Hilbert space $\mathcal{H}$, let $W : \mathcal{X} \to \mathcal{S}(\mathcal{H})$ be a CQ channel. We define the capcity of W as,

$$C_0 \coloneqq \sup_{p\in\mathcal{P}(\mathcal{X})} \chi(p, W)$$

Defintion. ((n, M)-ID-code) For a finite alphabet $\mathcal{X}$ and finite dimentional Hilbert space $\mathcal{H}$, let $W : \mathcal{X} \to \mathcal{S}(\mathcal{H})$ be a CQ channel. An (n, M)-ID-code is a family $\mathcal{C}_{\text{id}} \coloneqq (Q_m, D_m)_{m=1}^{M}$, where $Q_1, ..., Q_M \in \mathcal{P}(\mathcal{X}^n)$ are probability distributions and for each $m \in [M]$, $D_m \in \mathcal{L}(\mathcal{H}^{\otimes n})$, $0 \le D_m \le \mathbf{1}_{\mathcal{H}^{\otimes n}}$.

For an (n, M)-ID-code $\mathcal{C}_{\text{id}}$ we define two types of errors,

$$\begin{aligned} e_1(\mathcal{C}_{\text{id}}, W^{\otimes n}) &\coloneqq \max_{m\in[M]} \sum_{x^n\in\mathcal{X}^n} Q_m(x^n) \operatorname{tr}\left[(\mathbf{1} - D_m)W^{\otimes n}(x^n)\right] \\ e_2(\mathcal{C}_{\text{id}}, W^{\otimes n}) &\coloneqq \max_{\substack{m,m'\in[M] \\ m\neq m'}} \sum_{x^n\in\mathcal{X}^n} Q_{m'}(x^n) \operatorname{tr}\big[D_m W^{\otimes n}(x^n)\big] \\ N_{\text{id}}(W, n, \lambda_1, \lambda_2) &\coloneqq \max\{M \in \mathbb{N} \mid \exists (n, M)\text{-ID-code } \mathcal{C}_{\text{id}} \text{ with } e_1(\mathcal{C}_{\text{id}}, W^{\otimes n}) \le \lambda_1 \text{ and } e_2(\mathcal{C}_{\text{id}}, W^{\otimes n}) \le \lambda_2\} \end{aligned}$$

Defintion. An (n, M)-ID-code $(Q_m, D_m)_{m=1}^{M}$ is called simultanious if for $K \in \mathbb{N}$ there is a POVM $(E_i)_{i=1}^{K}$ and subsets $A_1, ..., A_M \subseteq [K]$ such that for each $m \in [M]$, $D_m = \sum_{j\in A_m} E_j$. We define for CQ channel $W : \mathcal{X} \to \mathcal{S}(\mathcal{H})$,

$$N_{\text{id}}^{\text{sim}}(W, n, \lambda_1, \lambda_2) \coloneqq \max\{M \in \mathbb{N} \mid \exists \text{ sim. } (n, M)\text{-ID-code } \mathcal{C}_{\text{id}}^{\text{sim}} \text{ with } e_1(\mathcal{C}_{\text{id}}^{\text{sim}}, W^{\otimes n}) \le \lambda_1 \text{ and } e_2(\mathcal{C}_{\text{id}}^{\text{sim}}, W^{\otimes n}) \le \lambda_2\}$$

It is clear that $N_{\text{id}} \ge N_{\text{id}}^{\text{sim}}$.

Theorem. *Let $\lambda_1, \lambda_2 > 0$. Then,*

$$\liminf_{n\to\infty} \frac{1}{n} \log\log N_{id}^{sim}(W, n, \lambda_1, \lambda_2) \geq C_0$$

Lemma. Let $M \in \mathbb{N}$ be a fintite number and $\lambda \in (0,1)$. Let $\epsilon > 0$ be such that $\lambda \log\big(\frac{1}{\epsilon} - 1\big) > 2$. Then, there are at least $N \geq \frac{1}{M} 2^{\lfloor \epsilon M \rfloor}$ subsets $\mathcal{A}_1, ..., \mathcal{A}_N \subset [M]$ such that each A_i has cardinality $\lfloor \epsilon M \rfloor$. Further, the cardinalities of the pairwise intersetions satisfy

$$|\mathcal{A}_i \cap \mathcal{A}_j| \leq \lambda \lfloor \epsilon M \rfloor, \qquad (\forall\, i, j \in [N], i \neq j).$$

Proposition. *Let $\lambda_1, \lambda_2, \delta > 0$. Let $\lambda := \min(\lambda_1, \frac{\lambda_2}{2})$. Let $\epsilon > 0$, such that $\lambda \log\big(\frac{1}{\epsilon} - 1\big) > 2$. Then there exists an $n_0 \in \mathbb{N}$ such that for any $n \geq n_0$, there exists a simultanious (n, M)-ID-code, $\mathcal{C}_{id}^{sim}$, with $e_1(\mathcal{C}_{id}^{sim}, W^{\otimes n}) \leq \lambda_1$ and $e_2(\mathcal{C}_{id}^{sim}, W^{\otimes n}) \leq \lambda_2$ with $M \geq 2^{\lfloor \epsilon 2^{(C-\delta)n} \rfloor - n}$.*

Proof. By the Holevo-Schumacher-Wesmoreland theorem, for $\lambda \in (0,1)$, there is a large enough $n \in \mathbb{N}$ such that $M := N(W, n, \lambda) \geq 2^{n(C_0 - \delta)}$. Therefore there exists an (n, M)-code $\mathcal{C} := (x_m, E_m)_{m=1}^M$ such that $e(\mathcal{C}, W^{\otimes n}) \leq \lambda$. From the above lemma, we have that there exists $N \geq \frac{1}{M} 2^{\lfloor \epsilon M \rfloor}$ subsets $\mathcal{A}_1, ..., \mathcal{A}_N \subset [M]$ such that for each $i, j \in [N], |\mathcal{A}_i| = \lfloor \epsilon M \rfloor$ and for $i \neq j$, $|\mathcal{A}_i \cap \mathcal{A}_j| \leq \lambda \lfloor \epsilon M \rfloor$. We have that for large n,

$$N \geq \frac{1}{M} 2^{\lfloor \epsilon M \rfloor} \geq 2^{\lfloor \epsilon 2^{n(C_0 - \delta)} \rfloor - n}.$$

We can consider $[M]$ as an index set for the $(x_m)_{m=1}^M$ messages and therefore can define $\mathcal{X}_i := \{x_m \mid m \in \mathcal{A}_i\}$. With this, we can construct an (n, N)-ID-code. Let $Q_i \in \mathcal{P}(\mathcal{X}_i)$ be the uniform distribution on $\mathcal{X}_i$ such that $Q_i(x_m) = \frac{1}{|\mathcal{X}_i|} \mathbf{I}_{\mathcal{X}_i}(x_m)$ and define $D_i := \sum_{m \in \mathcal{A}_i} E_m$. We can now show that the two types of errors are bounded by λ_1 and λ_2 respectivly and can conclude that $N_{\mathrm{id}}^{\mathrm{sim}}(W, n, \lambda_1, \lambda_1) \geq N$. For $\mathcal{C}_{\mathrm{id}}^{\mathrm{sim}} := (Q_i, D_i)_{i=1}^N$, we have for a fixed $i \in [N]$,

$$\begin{aligned}
\sum_{m \in [M]} Q_i(x_m) \operatorname{tr}\big[(\mathbf{1} - D_i) W^{\otimes n}(x_m)\big] &= \frac{1}{\lfloor \epsilon M \rfloor} \sum_{m \in \mathcal{A}_i} \operatorname{tr}\big[(\mathbf{1} - D_i) W^{\otimes n}(x_m)\big] \\
&= \frac{1}{\lfloor \epsilon M \rfloor} \sum_{m \in \mathcal{A}_i} \operatorname{tr}\Big[(\mathbf{1} - \sum_{m' \in \mathcal{A}_i} E_{m'}) W^{\otimes n}(x_m)\Big] \\
&\leq \frac{1}{\lfloor \epsilon M \rfloor} \sum_{m \in \mathcal{A}_i} \underbrace{\operatorname{tr}\big[(\mathbf{1} - E_m) W^{\otimes n}(x_m)\big]}_{\leq \lambda} \\
&\leq \frac{1}{\lfloor \epsilon M \rfloor} \lambda \lfloor \epsilon M \rfloor \\
&= \lambda \leq \lambda_1.
\end{aligned}$$

Since i was chosen arbitrarily, it holds that $e_1(\mathcal{C}_{\mathrm{id}}, W^{\otimes n}) \leq \lambda_1$. For the second type of error, again fix an $i, j \in [N]$ such that $i \neq j$,

$$\begin{aligned}
\sum_{m \in [M]} Q_i(x_m) \operatorname{tr}\big[D_j W^{\otimes n}(x_m)\big] &= \frac{1}{\lfloor \epsilon M \rfloor} \sum_{m \in \mathcal{A}_i} \operatorname{tr}\big[D_j W^{\otimes n}(x_m)\big] \\
&= \frac{1}{\lfloor \epsilon M \rfloor} \sum_{m \in \mathcal{A}_i} \operatorname{tr}\left[\left(\sum_{k \in A_j} E_k\right) W^{\otimes n}(x_m)\right] \\
&= \frac{1}{\lfloor \epsilon M \rfloor} \sum_{k \in \mathcal{A}_j} \operatorname{tr}\left[\sum_{m \in \mathcal{A}_i \cap \mathcal{A}_j} E_k W^{\otimes n}(x_m) + \sum_{m \in \mathcal{A}_i \setminus \mathcal{A}_j} E_k W^{\otimes n}(x_m)\right] \\
&= \frac{1}{\lfloor \epsilon M \rfloor} \sum_{m \in \mathcal{A}_i \cap \mathcal{A}_j} \underbrace{\operatorname{tr}\left(\sum_{k \in \mathcal{A}_j} E_k W^{\otimes n}(x_m)\right)}_{\leq 1} + \frac{1}{\lfloor \epsilon M \rfloor} \sum_{m \in \mathcal{A}_i \setminus \mathcal{A}_j} \underbrace{\operatorname{tr}\left(\sum_{k \in \mathcal{A}_j} E_k W^{\otimes n}(x_m)\right)}_{\leq \lambda} \\
&\leq \frac{1}{\lfloor \epsilon M \rfloor} \lambda \lfloor \epsilon M \rfloor + \frac{1}{\lfloor \epsilon M \rfloor} \lambda \lfloor \epsilon M \rfloor \\
&= 2\lambda \leq \lambda_2
\end{aligned}$$

Since i, j are chosen arbitarily, it holds that $e_2(\mathcal{C}_{\mathrm{id}}, W^{\otimes n}) \leq \lambda_2$. $\square$