Leakage Chain Rule and Superdense Coding

Yi-Hsiu Chen*[1], Kai-Min Chung†[2], Ching-Yi Lai‡[2], and Xiaodi Wu§[3]

[1]Harvard John A. Paulson School Of Engineering And Applied Sciences, Harvard University, USA
[2]Institute of Information Science, Academia Sinica, Taipei, Taiwan
[3]Department of Computer Science, Institute for Advanced Computer Studies, and Joint Center for Quantum Information and Computer Science, University of Maryland, USA

September 8, 2017

Abstract

In this note, we reprove the communication lower bound of Holevo's problem, using the Leakage Chain Rule for quantum min-entropy.

1 Introduction

Superdense coding tells us that one can learn two bits of information by receiving only one qubit as long as the sender (Alice) and receiver (Bob) share an EPR pair previously. A more general task is *Holevo's problem* [Hol73]: Alice wants to convey the n bits of classical information X to Bob through multiple rounds of two-way quantum communication, and assume Alice and Bob share an arbitrary amount of entanglement. Nayak and Salzman [NS06] showed that Alice has to send at least $\frac{1}{2}(n - \log 1/p)$ qubits to Bob so that he can recover X with probability p, no matter how many qubits are sent back from Bob.

The technique in [NS06] is quite involved. Wu and Yuen [WY15] simplified it by considering non-signaling resources. Here we provide another simplified proof for directly for quantum messages based on quantum min-entropy and its leakage chain rule.

2 Preliminary

We will first define the relative min-entropy (a.k.a max-divergence) of two quantum states, which will be used to define the conditional quantum min-entropy [RW05]. Relative min-entropy can be seen as a distance between two quantum states. The distance measures, in logarithm, of how much more likely an event happens for one state than the other.

*yihsiuchen@g.harvard.edu.Supported by NSF grant CCF-1420938.

†kmchung@iis.sinica.edu.tw.

‡cylai0616@iis.sinica.edu.tw.

§xiaodiwu@cs.uoregon.edu.

Definition 2.1 (Quantum relative min-entropy). *Let ρ and σ be two density operators on a space $\mathcal{H}$. The relative min-entropy between two quantum states ρ and σ is defined as*

$$D_\infty(\rho\|\sigma) \overset{\text{def}}{=} \inf\{\lambda \in \mathbb{R} : \rho \leq 2^\lambda \sigma\}.$$

Definition 2.2 (Conditional quantum min-entropy). *Let $\rho = \rho_{XB} \in \mathrm{Dens}\,(\mathcal{X} \otimes \mathcal{B})$ be a density operator describing a bipartite quantum system (X, B). The min-entropy of system X conditioned on system B is defined as*

$$H_{\min}(X|B)_\rho \overset{\text{def}}{=} \log|\mathcal{X}| - \inf_{\sigma_B \in \mathrm{Dens}(\mathcal{B})} \left\{ D_\infty\left(\rho_{XB} \middle\| \frac{1}{|\mathcal{X}|}\mathsf{id}_X \otimes \sigma_B\right)\right\}.$$

Another way to define min entropy is to use guessing probability. Here we only consider the case that ρ_{XB} is a cq-state: $\rho_{XB} = \sum_x p_x |x\rangle\langle x| \otimes \rho_B^x$ for $\rho_B^x \in \mathrm{Dens}\,(\mathcal{B})$. The probability of guessing X correctly given B by a given quantum circuit C is

$$P_C^{\text{guess}}(X|B)_\rho = \sum_x \Pr[X = x]\, \langle \Pi_x, \rho_B^x \rangle\,,$$

where $\{\Pi_x\}_x$ is the effective POVM for C, demonstrating the guessing strategy. Accordingly, the probability of guessing X correctly given B is defined as

$$P^{\text{guess}}(X|B)_\rho = \max_C P_C^{\text{guess}}(X|B)_\rho, \tag{2.1}$$

where the maximization is taken over arbitrary quantum circuits C of unbounded size. As in the purely classical case [DORS08], the guessing probability captures the conditional min-entropy of X given B:

Lemma 2.3 ([KRS09]). *Suppose ρ_{XB} is a cq-state on the space $\mathcal{X} \otimes \mathcal{B}$. Then*

$$H_{\min}(X|B)_\rho = -\log(P^{\text{guess}}(X|B)).$$

3 Leakage Chain Rule

Winkler *et al.* [WTHR11] showed the leakage Chain Rule for quantum min-entropy[1]. We also provide a proof here for completeness and clearness.

Theorem 3.1 ([WTHR11, Lemma 13] Leakage Chain Rule for quantum min-entropy). *Let $\rho = \rho_{XZB}$ be a state on the space $\mathcal{X} \otimes \mathcal{Z} \otimes \mathcal{B}$. Let $d = \min\{\dim(\mathcal{X} \otimes \mathcal{Z}), \dim(\mathcal{B})\}$ and $\ell = \log\dim(\mathcal{B})$. Then*

$$H_{\min}(X|ZB)_\rho \geq H_{\min}(X|Z)_\rho - 2\ell.$$

The factor 2 is crucial for the application in superdense coding as one can see in Section 3.

Proof. We first establish the following matrix inequality.

[1] They proved the chain rule for a more general notion *quantum smooth min-entropy*

Claim 1. *Suppose ρ_{AB} is a density operator of the joint system of A and B, which are of finite dimensions. Let $\rho_A = \mathrm{Tr}_{\mathcal{B}}(\rho_{AB})$ be the reduced density operator of system A. Then*

$$d \cdot \rho_A \otimes \mathsf{id}_B - \rho_{AB} \geq 0, \tag{3.1}$$

where id_B is the identity on system B and $d = \min\{\dim(\mathcal{A}), \dim(\mathcal{B})\}$.

proof of Claim. It suffices to consider a pure state $\rho_{AB} = |\psi\rangle\langle\psi|$, since a mixed state is a finite convex combination of pure states. Suppose $|\psi\rangle$ admits a Schmidt decomposition $|\psi\rangle = \sum_{j=1}^{s} \sqrt{\lambda_j}\, |j\rangle_A |j\rangle_B$, where $s \leq \min\{\dim(\mathcal{A}), \dim(\mathcal{B})\} = d$. Define the linear map on operators

$$f(\rho_{AB}) = d \cdot \rho_A \otimes \mathsf{id}_B - \rho_{AB}.$$

Then

$$f(|\psi\rangle\langle\psi|) = d \sum_j \lambda_j\, |j\rangle\langle j| \otimes \mathsf{id}_B - \sum_{j,k} \sqrt{\lambda_j \lambda_k}\, |j\rangle \langle k| \otimes |j\rangle \langle k| .$$

Let $X_A = \sum_j \frac{1}{\sqrt{\lambda_j}} |j\rangle\langle j|_A + \sum_{j'} |j'\rangle\langle j'|_A$ so that $\{|j\rangle_A\} \cup \{|j'\rangle_A\}$ form an orthonormal basis of states in A. Then X_A is an invertible operator. Define $f'(|\psi\rangle\langle\psi|) = (X_A \otimes \mathsf{id}_B)\,(f(|\psi\rangle\,\langle\psi|))\left(X_A^\dagger \otimes \mathsf{id}_B\right)$. Note that $f(|\psi\rangle\,\langle\psi|) \geq 0$ if and only if $f'(|\psi\rangle\langle\psi|) \geq 0$. Observe that

$$\begin{aligned} f'(|\psi\rangle\langle\psi|) =& d \sum_{j,k} |j\rangle\langle j| \otimes |k\rangle \langle k| - \sum_{j,k} |j\rangle \langle k| \otimes |j\rangle \langle k| \\ =& \sum_{j,k} (d\, |j\rangle\, |k\rangle)\, \langle j|\, \langle k| - \sum_{j,k} |j\rangle\, |j\rangle\, \langle k|\, \langle k| \\ =& \sum_k \left(d\, |k\rangle\, |k\rangle - \sum_j |j\rangle\, |j\rangle \right) \langle k|\, \langle k| + \sum_{j \neq k} d\, |j\rangle\, |k\rangle\, \langle j|\, \langle k| . \end{aligned}$$

Theorem 3.2 (Gershgorin circle theorem)**.** *Let M be a complex $n \times n$ matrix, with entries $m_{i,j}$. For $i \in \{1, \cdots, n\}$, let $R_i = \sum_{j \neq i} |m_{i,j}|$ be the sum of the absolute values of the non-diagonal entries in the i-th row. Let $D(m_{ii}, R_i)$ be the closed disk centered at $m_{i,i}$ with radius R_i. Then every eigenvalue of M lies within at least one of the Gershgorin disks $D(m_{ii}, R_i)$.*

From the above equation, a Gershgorin disk of $f(|\psi\rangle\langle\psi|)$ is centered at $(d-1)$ with radius $s-1$ or centered at d with radius 0. In either case, every eigenvalue is nonnegative. Therefore $f'(|\psi\rangle\langle\psi|) \geq 0$ and hence $f(|\psi\rangle\langle\psi|) \geq 0$.

□

Let $\lambda = \log \dim(\mathcal{X}) - H_{\min}(X|Z)_\rho$. By Definition 2.2 there exists a density operator σ_Z such that

$$\rho_{XZ} \leq 2^\lambda \frac{\mathsf{id}_X}{\dim(\mathcal{X})} \otimes \sigma_Z.$$

By the claim,

$$\begin{aligned} \rho_{XZB} &\leq d \cdot \rho_{XZ} \otimes \mathsf{id}_B \leq d \dim(B) 2^\lambda \frac{\mathsf{id}_X}{\dim(\mathcal{X})} \otimes \sigma_Z \otimes \frac{\mathsf{id}_{\mathcal{B}}}{\dim(B)} \\ &= 2^{\lambda + \ell + \log d} \frac{\mathsf{id}_X}{\dim(\mathcal{X})} \otimes \sigma_Z \otimes \frac{1}{2^\ell} \mathsf{id}_{\mathcal{B}}. \end{aligned}$$

Thus by definition, we have

$$H_{\min}(X|ZB)_\rho \geq \log \dim(\mathcal{X}) - (\lambda + \ell + \log d) \geq H_{\min}(X|Z)_\rho - 2\ell.$$

□

We remark that Theorem 3.1 is tight. In the case that the dimensions of $\mathcal{X}$ and $\mathcal{B}$ are both 2^ℓ, X and B are maximally entangled, it is easy to verify that $H_{\min}(X|B)_\rho = -\ell$ and $H_{\min}(X) = \ell$. On the other hand, when there is no entanglement between Z, B, one has the following leakage chain rule.

Lemma 3.3 (Chain rule for quantum min-entropy of separable states)**.** *Let $\rho = \rho_{XZB}$ be a separable state on the space $(\mathcal{X} \otimes \mathcal{Z}) \otimes \mathcal{B}$. Namely, $\rho_{XZB} = \sum_k p_k \rho^k_{XZ} \otimes \rho^k_B$. Suppose B is an ℓ-qubit system. Then*

$$H_{\min}(X|ZB)_\rho \geq H_{\min}(X|Z)_\rho - \ell.$$

Proof. Let $\lambda = \log \dim(\mathcal{X}) - H_{\min}(X|Z)_\rho$. By Definition 2.2, there exists a density operator σ_Z such that

$$\rho_{XZ} \leq 2^\lambda \frac{\mathsf{id}_X}{\dim(\mathcal{X})} \otimes \sigma_Z.$$

Because $\rho^k_B \leq \mathsf{id}_\mathcal{B}$, we have

$$\begin{aligned}\rho_{XZB} =& \sum_k p_k \rho^k_{XZ} \otimes \rho^k_B \leq 2^{-\lambda} \frac{\mathsf{id}_X}{\dim(\mathcal{X})} \otimes \sigma_Z \otimes \mathsf{id}_\mathcal{B} \\ =& 2^{\lambda+\ell} \frac{\mathsf{id}_X}{\dim(\mathcal{X})} \otimes \sigma_Z \otimes \frac{1}{2^\ell} \mathsf{id}_\mathcal{B} \\ =& 2^{\lambda+\ell} \frac{\mathsf{id}_X}{\dim(\mathcal{X})} \otimes \sigma_{ZB},\end{aligned}$$

where $\sigma_{ZB} = \sigma_Z \otimes \frac{1}{2^\ell} \mathsf{id}_\mathcal{B}$. Thus by definition, we have

$$H_{\min}(X|ZB)_\rho \geq \log \dim(\mathcal{X}) - (\lambda + l) \geq H_{\min}(X|Z)_\rho - \ell.$$

□

4 Lower Bound of Superdense Coding

Theorem 4.1. *Suppose Alice wants to send a message of n classical bits to Bob by communicating over a quantum channel, and they may share an arbitrary amount of entanglement. For every $x \in \{0, 1\}^n$, Bob has to recover x with probability at least p, then the total number of qubits m that Alice has to send is at least $\frac{1}{2}(n - \log(1/p))$.*

Proof. Let X be the uniform distribution over $\{0, 1\}^n$ and Alice wants to convey a sample x from X to Bob. Let A_i be the system on Alice's side, B_i be the system on Bob's side, where i is an index indicating the round of communication. Let $\rho^{(i)}$ be the density operator of joint system at the end of round i. The initial state of the joint system is $\rho^{(0)}_{XA_0B_0}$ where A_0 and B_0 represent the shared entanglement between Alice and Bob. Since X is uniform, initially we have $H_{\min}(X|B_0)_{\rho^{(0)}} = n$.

A general communication strategy proceeds as follows. In each round, Alice or Bob prepare a message (a quantum system) to another alternatively. Precisely, at the i-th round for odd i, according to x and the state of A_{i-1}, Alice prepares a quantum system M_i with density operator σ_{M_i} and send it to Bob. Then we have $\rho^{(i)}_{B_i} = \rho^{(i)}_{B_{i-1}M_i} = \rho^{(i-1)}_{B_{i-1}} \otimes \sigma_{M_i}$ and $\rho^{(i)}_{XA_iB_{i-1}M_i} = \rho^{(i)}_{XA_iB_i}$. Similarly, at the i-th round for even i, Bob prepares N_i with density operator σ_{N_i} and send it to Alice, in which case, $\rho^{(i)}_{A_i} = \rho^{(i)}_{A_{i-1}N_i} = \rho^{(i-1)}_{A_{i-1}} \otimes \sigma_{N_i}$ and $\rho^{(i)}_{XA_{i-1}N_iB_i} = \rho^{(i)}_{XA_iB_i}$.

Observe that for odd i, $\rho^{(i)}_{XB_{i-1}} = \rho^{(i-1)}_{XB_{i-1}}$ since Alice and only locally operates on her side preparing their messages. Therefore, $H_{\min}(X|B_{i-1})_{\rho^{(i-1)}} = H_{\min}(X|B_{i-1})_{\rho^{(i)}}$. Then by Lemma 3.1, we have

$$\begin{aligned} H_{\min}(X|B_i)_{\rho^{(i)}} &= H_{\min}(X|M_i, B_{i-1})_{\rho^{(i)}} \\ &\geq H_{\min}(X|B_{i-1})_{\rho^{(i)}} - 2\log\dim(M_i) \\ &= H_{\min}(X|B_{i-1})_{\rho^{(i-1)}} - 2\log\dim(M_i) \end{aligned}$$

At the i-th round for even i, since Alice does nothing, the local operation of Bob does not lower the entropy of X from his view. Thus

$$H_{\min}(X|B_i)_{\rho^{(i)}} \geq H_{\min}(X|B_{i-1})_{\rho^{(i-1)}}.$$

In sum up, if there are a total of k rounds in the protocol, then we have

$$H_{\min}(X|B_k)_{\rho^{(k)}} \geq H_{\min}(X|B_0)_{\rho^{(0)}} - 2\sum_{i:\text{ odd}} \log\dim(M_i) = n - 2m,$$

where $m = \sum_{i:\text{ odd}} \log\dim(M_i)$.

If Bob can recover all $x \in \{0,1\}^n$ correctly with probability at least p, then $P^{\text{guess}}(X|B_k)_{\rho^{(k)}} \geq p$. By Lemma 2.3, $H_{\min}(X|B_k)_{\rho^k} \leq -\log(p)$. Combining with the above inequality, we get $m \geq \frac{1}{2}(n - \log(1/p))$, which exactly reproduce the result of Nayak and Salzman [NS06].

□

References

[DORS08] Yevgeniy Dodis, Rafail Ostrovsky, Leonid Reyzin, and Adam D. Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. *SIAM J. Comput.*, 38(1):97–139, 2008.

[Hol73] Alexander Semenovich Holevo. Bounds for the quantity of information transmitted by a quantum communication channel. *Problemy Peredachi Informatsii*, 9(3):3–11, 1973.

[KRS09] Robert König, Renato Renner, and Christian Schaffner. The operational meaning of min- and max-entropy. *IEEE Trans. Information Theory*, 55(9):4337–4347, 2009.

[NS06] Ashwin Nayak and Julia Salzman. Limits on the ability of quantum states to convey classical messages. *Journal of the ACM (JACM)*, 53(1):184–206, 2006.

[RW05] Renato Renner and Stefan Wolf. *Simple and Tight Bounds for Information Reconciliation and Privacy Amplification*, pages 199–216. Springer Berlin Heidelberg, Berlin, Heidelberg, 2005.

[WTHR11] Severin Winkler, Marco Tomamichel, Stefan Hengl, and Renato Renner. Impossibility of growing quantum bit commitments. *Physical review letters*, 107(9):090502, 2011.

[WY15] Xiaodi Wu and Henry Yuen. On the limits of communication with non-local resources. manuscript, 2015.