One-way Quantum Communication Complexity with Inner Product Gadget

Srijita Kundu

December 12, 2017

Abstract

This note is prepared based on the article titled “One-way Communication and Non-adaptive Decision Tree” (TR17-152) by Swagato Sanyal. We show that the technique developed in the aforementioned paper to lower bound one-way randomized communication complexity can be extended to prove one-way quantum communication complexity with shared entanglement of any total query function $f : \{0,1\}^n \rightarrow \{0,1\}$ that depends on all its input bits, composed with the inner product gadget $IP_m$ of size $m \geq 2$, is $\Omega(nm)$.

1 Preliminaries

1.1 Communication Complexity

In a one-way quantum communication protocol without entanglement, Alice sends a quantum state to Bob depending on her input $x$. Bob performs a measurement two-outcome $M_y$ depending on his input $y$ and his output is simply the result of the measurement. More generally, when Alice and Bob have access to a shared entangled state $|\Phi\rangle_{AB}$ (which we can assume to be pure, and of which Alice holds the register $A$ and Bob holds register $B$), Alice performs a unitary on her part of the entangled state depending on her input and sends her register to Bob, who now performs a joint measurement $M_y$ on both registers $A$ and $B$ to give his output. This is schematically represented in Figure 1.

The one-way communication complexity of the protocol in both cases is the number of qubits Alice communicates to Bob, that is, $\log |A|$. The $\varepsilon$-error one-way quantum communication complexity of a function $F$, denoted by $Q_1^\varepsilon(F)$ or $Q_\ast^\varepsilon(F)$ respectively, depending on whether Alice and Bob share entanglement, is the minimum number of qubits communicated by Alice in the worst case (over inputs) in a protocol that successfully computes $F$ with probability at least $1 - \varepsilon$.

![Figure 1: A one-way quantum communication protocol $\mathcal{P}$ between Alice and Bob](image-url)
1.2 Information Theory

The measure of information content of a quantum state $\rho$ is given by its von Neumann entropy $S(\rho) = -\text{Tr}(\rho \log \rho)$. We shall also use $S(A) = S(\rho)$ to denote the von Neumann entropy of a quantum register $A$ described by state $\rho$. For states across two (or more) registers, we shall use $S(AB)$ to denote the joint entropy of both registers according to $\rho$ and $S(A), S(B)$ to denote the von Neumann entropies of individual registers due to the marginals of $\rho$. It is well-known that $S(A)$ takes its minimum value 0 for a pure state and takes maximum value $\log |A|$ for a maximally mixed state.

**Fact 1** (Subadditivity of von Neumann entropy). $S(AB) \leq S(A) + S(B)$.

The conditional von Neumann entropy of register $A$ given register $B$ is defined as $S(A|B) = S(AB) - S(B)$. Due to subadditivity, this is upper bounded by $S(A)$. However, unlike conditional Shannon entropy, it is well-known that conditional von Neumann entropy can be negative, when $\rho$ is entangled across $A$ and $B$. We can upper and lower bound the positive and negative values of $S(A|B)$ as follows.

**Lemma 2.** $- \log |A| \leq S(A|B) \leq \log |A|$.

**Proof.** By subadditivity, $S(A|B) = S(AB) - S(B) \leq S(A) + S(B) - S(B) \leq \log |A|$. For the lower bound, consider a purification $\sigma$ of $\rho$ which is in registers $A, B, C$. Since $\sigma$ is a pure state, $S(ABC) = 0$. Moreover, $S(AB) = S(C)$ and $S(B) = S(AC)$, which can be seen by considering a Schmidt decomposition of $\sigma$. Subtracting the second equation from the first we get, $S(A|B) = -S(A|C)$. Now since we already proved, $S(A|C) \leq \log |A|$, we get the required lower bound.

The quantum mutual information between two registers is defined as $I(A : B) = S(A) + S(B) - S(AB) = S(A) - S(A|B)$. $I(A : B)$ takes its minimum value zero for a product state between $A$ and $B$. Conditional mutual information of $A$ and $B$ conditioned on $C$ is defined with analogously with the corresponding conditional entropies.

**Fact 3** (Chain rule of mutual information). $I(AC : B) = I(C : B) + I(A : B|C)$.

For classical random variables $X, Y$ we shall also use $I(X, Y)$ for their classical mutual information. Though this is the same as that for quantum mutual information, it will be clear from context which one we mean.

**Fact 4** (Holevo’s Theorem). For a random variable $X$ with distribution $\text{Pr}[X = x] = p_x$ which has a quantum encoding $x \mapsto \sigma_x$. Then if, $\sigma = \sum_x p_x\sigma_x$ and $Y$ is the random variable obtained by performing a measurement on the encoding, it holds that

$$I(X : Y) \leq S(\sigma) - \sum_x p_x S(\sigma_x).$$

The following lemma is a simple consequence of Holevo’s Theorem, which was proved in [Nay99]. We reproduce the proof here for completeness.

**Lemma 5.** Let $\sigma^0$ and $\sigma^1$ be two density matrices such that a measurement $\mathcal{M}$ distinguishes between them with probability at least $1 - \varepsilon$. Then, $\sigma = \frac{1}{2}(\sigma^0 + \sigma^1)$ satisfies

$$S(\sigma) \geq \frac{1}{2}(S(\sigma^0) + S(\sigma^1)) + (1 - h(\varepsilon)),$$

where $h(\cdot)$ is the binary entropy function.

**Proof.** Let $X$ be the random variable representing $x$ in $x \mapsto \sigma_x$, and $Y$ be the random variable representing the outcome. By Fano’s inequality, $I(X : Y) \geq 1 - h(\varepsilon)$. Now applying Holevo’s theorem with $p_0 = p_1 = \frac{1}{2}$ gives the required result.

\[\square\]
2 Main Result

Theorem 6. Let \( f : \{0, 1\}^n \to \{0, 1\} \) be a total Boolean function that depends on all its input bits and let \( \text{IP}_m \) be the \( 2m \)-bit inner product function. Then for \( \varepsilon \in (0,1/2) \), the one-way entanglement-assisted quantum communication complexity with \( \varepsilon \) error is lower bounded as

\[
Q^{\varepsilon,1}_e(f \circ \text{IP}_m) \geq \frac{1}{2}(1 - h(\varepsilon)) \cdot n(m - 1)
\]

where \( h(\cdot) \) is the binary entropy.

We note that for such functions \( f \), it is known that the non-adaptive quantum query complexity is known to be \( \Theta(n) \) [Mon10]. So this theorem connects the non-adaptive quantum query complexity of \( f \) to the one-way communication complexity of \( f \circ \text{IP}_m \).

Proof. Consider a uniform distribution over inputs \( x \) to Alice where first bit of every \( m \)-length block is 1. The joint state of the registers \( X, A, B \) in a protocol \( P \) for \( f \circ \text{IP}_m \) before Alice performs the unitary (see Figure 1) is then

\[
\frac{1}{2^{n(m-1)}} \sum_{x \in \{0,1\}^{n(m-1)}} |x\rangle \langle x|_X \otimes |\Phi\rangle \langle \Phi|_{AB}.
\]

The joint state after the unitary, which we shall call \( \rho \) can be expressed as

\[
\rho = \frac{1}{2^{n(m-1)}} \sum_{x \in \{0,1\}^{n(m-1)}} |x\rangle \langle x|_X \otimes (U_A^x \otimes 1_B) |\Phi\rangle \langle \Phi|_{AB} U_A^{x†} \otimes 1_B.
\]

Claim 7. \( I(AB : X) \geq (1 - h(\varepsilon)) \cdot n(m - 1) \) under \( \rho \).

We prove the theorem assuming this claim and prove the claim later. By the chain rule,

\[
I(AB : X) = I(B : X) + I(A : X|B).
\]

We claim that \( I(B : X) = 0 \). To see this, consider a Schmidt decomposition \( \sum_i |i_A i_B\rangle \) of \( |\Phi\rangle_{AB} \).

The reduced state on registers \( B, X \) is given by

\[
\frac{1}{2^{n(m-1)}} \sum_{x \in \{0,1\}^{n(m-1)}} |x\rangle \langle x|_X \otimes \text{Tr}_A(U_A^x \otimes 1_B) |\Phi\rangle \langle \Phi|_{AB} U_A^{x†} \otimes 1_B.
\]

Now suppose \( U_A^x \) takes \( |i\rangle_A \) to \( |\psi^x_i\rangle_A \). Then,

\[
\text{Tr}_A(U_A^x \otimes 1_B) |\Phi\rangle \langle \Phi|_{AB} U_A^{x†} \otimes 1_B = \text{Tr}_A \left( \sum_{i,j} |\psi^x_i\rangle \langle \psi^x_j|_A \otimes |i\rangle_B \langle j|_B \right) = \sum_{i} |i\rangle \langle i|_B
\]

since \( |\psi^x_i\rangle_A \) and \( |\psi^x_j\rangle_A \) for \( i \neq j \) have to be orthogonal by unitarity of \( U^x \). This means that the reduced state on \( B, X \) is a product state, which makes \( I(B : X) = 0 \).

Now from equation 1, \( I(AB : X) = I(A : X|B) = S(A|B) - S(A|BX) \). Applying the upper bound and lower bound of Lemma 2 on \( S(A|B) \) and \( S(A|BX) \) respectively, we get

\[
2 \log |A| \geq I(AB : X) \geq (1 - h(\varepsilon)) \cdot n(m - 1)
\]

which proves the theorem.
Proof of Claim 7. Expanding $I(AB : X) = S(AB) + S(X) - S(ABX)$. Since $\rho$ is a classical-quantum state $\frac{1}{2^{n(m-1)}} \sum |x⟩⟨x|_X \otimes \rho_{AB}^x$ where each $\rho_{AB}^x$ is pure, $S(ABX)$ is simply equal to $S(X)$. So $I(AB : X) = S(AB)$. Now we lower bound $S(AB)$ which is the von Neumann entropy of the reduced state 

$$\frac{1}{2^{n(m-1)}} \sum_{x \in \{0,1\}^{n(m-1)}} \rho_{AB}^x$$

in a manner similar to [Nay99].

Let us label the bits of $x$ by $k = (i, j) \equiv mi + j$, where $i \in [n]$ and $j \in [m]$. For a substring $s \in \{0,1\}^k$ which satisfies the constraint that the first bit of each $m$-length block is 1, let us define

$$\sigma^s = \frac{1}{2^{n(m-1)-k}} \sum_{x' \in \{0,1\}^{n(m-1)-k}} \rho_{AB}^{sx'}$$

where $sx'$ denotes the concatenation of $s$ and $x'$ and the summation over $x'$ is also over substrings that respect the constraint that the first bit of each block is 1. We shall prove that for $s \in \{0,1\}^k$

$$S(\sigma^s) \geq \begin{cases} (1 - h(\varepsilon)) \cdot (n(m-1) - k - 1) & \text{if } k \neq (i,0) \\ (1 - h(\varepsilon)) \cdot (n(m-1) - k) & \text{otherwise.} \end{cases}$$

so that taking $s$ to be the empty string proves the main claim.

The proof is by backwards induction on $k$ – it holds for $k = (n, m)$ simply by the positivity of von Neumann entropy. Now, assuming it holds for $k + 1$, we show it holds for $k$. Note that for $s \in \{0,1\}^k$,

$$\sigma^s = \begin{cases} \sigma^{x_1} & \text{if } k = (i,0) \\ \frac{1}{2}(\sigma^{x_0} + \sigma^{x_1}) & \text{otherwise.} \end{cases}$$

So the lower bound holds for $k = (i,0)$ trivially from the induction hypothesis. For $k = (i, j)$ for $j > 0$, note that $\sigma^{x_0}$ and $\sigma^{x_1}$ are mixtures of states corresponding to inputs that differ in the $(mi + j + 1)$-th location. We shall demonstrate that there is a 2-outcome measurement that distinguishes between $\rho_{AB}^{sx_0'}$ and $\rho_{AB}^{sx_1}''$ for any substrings $x', x''$ within our constrained set of substrings. This means that the same measurement distinguishes between convex mixtures of $\rho_{AB}^{sx_0'}$ and $\rho_{AB}^{sx_1}''$, i.e., between $\sigma^{x_0}$ and $\sigma^{x_1}$.

Since $f$ is a total function, for every $i \in [n]$, there must exist $z^{(-i)} \in \{0,1\}^{n-1}$ such that $f(0z^{(-i)}) \neq f(1z^{(-i)})$, where $bz^{(-i)}$ is the concatenated string with $b$ in the $i$-th position. We define the following input for Bob such that the value of $f \circ \Pi^n_n$ on $(sbx', y)$ is equal to $b$ for any $x'$.

$$y(i', j') = \begin{cases} 1 & \text{if } i' = i, j' = j + 1 \\ 0 & \text{if } i' = i, j' \neq j + 1 \\ (z^{(-i)})_{i'} & \text{if } i' \neq i, j' = 1 \\ 0 & \text{if } i' \neq i, j' \neq 1. \end{cases}$$

For $P$ to be correct with probability $1 - \varepsilon$, Bob’s measurement $M_y$ must distinguish between $\rho_{AB}^{sx_0'}$ and $\rho_{AB}^{sx_1}''$, and hence $\sigma^{x_0}$ and $\sigma^{x_1}$ with probability at least $1 - \varepsilon$. Hence, applying Lemma 5,

$$S(\sigma^s) \geq \frac{1}{2}(S(\sigma^{x_0}) + S(\sigma^{x_1})) + (1 - h(\varepsilon)) \cdot (n(m-1) - k) \geq (1 - h(\varepsilon)) \cdot (n(m-1) - k)$$

where the last step follows from the induction hypothesis.
Remark 8. When Alice and Bob do not share entanglement, $|\Phi\rangle_{AB}$ is a product state, which means that $S(A|B) = 0$ and $I(AB : X) \leq \log |A|$. If we denote by $Q_1^1(\cdot)$ the one-way quantum communication complexity without entanglement, then for this we get the lower bound

$$Q_1^1(f \circ \text{IP}_m^n) \geq (1 - h(\varepsilon)) \cdot n(m - 1).$$

References
