COMMUNICATION COMPLEXITY OF REMOTE STATE PREPARATION WITH ENTANGLEMENT

Rahul Jain *†

Computer Science, University of California, Berkeley, California, 94720, USA

We consider the problem of *remote state preparation* recently studied in several papers. We study the *communication complexity* of this problem, in the presence of entanglement and in the scenario of single use of the channel.

1 Introduction

The remote state preparation problem has been studied in in several papers in recent times, see for example, [1], [2], [3], [4], [5]. We define the problem below. Let X be a set. Let $\mathcal{S}(\mathcal{K})$ be the set of quantum states in the Hilbert space $\mathcal{K}$. Let an *encoding* $E : X \mapsto \mathcal{S}(\mathcal{K})$ be a function from X to $\mathcal{S}(\mathcal{K})$. The remote state preparation, $RSP(X, E, \epsilon)$ problem is as follows:

Definition 1 (Remote state preparation) *Let Alice, who knows the function E, get an input $x \in X$. Alice and Bob are required to communicate and at the end of the communication Bob should have a quantum state ρ_x such that $F(\rho_x, E(x)) \geq 1 - \epsilon$, for some $0 \leq \epsilon < 1$. Alice and Bob may start with some prior entanglement between them.*

In several papers in the remote state preparation problem, Alice instead of x is given a *description* of the state ρ_x. We assume in this work that the description is given in the form of the element x of X. In [2], Bennett, Hayden, Leung, Shor and Winter studied the trade-off between the *rate* of communication and the rate of entanglement used. In some other papers like [3, 4, 1] the rate of communication required for this problem was studied with free use of the entanglement. In most of these earlier works the problem was studied in the *asymptotic setting* where multiple uses of the communication channel between Alice and Bob were considered. We study the communication complexity (i.e. the best possible communication with which a given problem $RSP(X, E, \epsilon)$ can be solved) of this problem in the scenario of single use of the channel. By $Q^{pub}(RSP(X, E, \epsilon))$ we denote the communication complexity, with prior entanglement, of $RSP(X, E, \epsilon)$. Please note that we are concerned with the total communication and not the rate as in the earlier papers. Also in this work we are not concerned with the amount of entanglement used.

We consider a notion of *maximum possible information* $T(E)$ in an encoding E and show that, in the presence of entanglement, the communication required for $RSP(X, E, 0)$, is at least $T(E)/2$ and $RSP(X, E, \epsilon)$ can be solved with communication at most $\frac{8}{\epsilon^2}(4T(E) + 7)$. Thus $T(E)$ almost tightly characterizes the communication complexity of the remote state preparation problem. It was pointed to us by an anonymous referee that in one of the main results in [BHL+05], the authors have also emphasized the role of T(E) for remote state preparation: there it is shown that the communication cost of preparing tensor products of $n \to \infty$ many pure states from the family E of pure states (that would be the family $E^{\otimes n}$) with an allowable constant fidelity loss is $\frac{n}{2}T(E) + o(n)$, so that the lower bound is indeed tight in this asymptotic setting.

There is an interesting point of note here. In earlier works since the problem was that of determining the rate of communication and rate of entanglement etc. in the asymptotic setting, the exact multiplicative constant in the rate was also important. Since we are concerned with the total communication in single use of the channel, the problem of identifying the best communication for a given $RSP(X, E, \epsilon)$ even up to constants is non-trivial. It is easy to see that in specific cases like when $T(E) = \log d$, where d is the dimension of $\mathcal{K}$, or

*rahulj@cs.berkeley.edu, 2020 Bancroft Way, Berkeley, CA, 94704.

†This work was supported by an Army Research Office (ARO), North California, grant number DAAD 19-03-1-00082.

when $T(E) = 0$, that $RSP(X, E, \epsilon)$ can be solved with communication which is like $T(E)$ up to constants. But for general values of $T(E)$ this problem is non-trivial.

2 Preliminaries

In this section we give a few definitions and state some facts that we will use later.

Given a joint quantum system AB, the mutual information between them is defined as $I(A : B) = S(A) + S(B) - S(AB)$, where $S(A)$ is the von-Neumann entropy of the system A. Given two quantum states, ρ, σ the relative entropy between them is defined as $S(\rho||\sigma) \stackrel{\Delta}{=} \mathsf{Tr}\rho(\log\rho - \log\sigma)$. Let X be a finite set (below we always assume that X is a finite set) and let $E : x \in X \mapsto \rho_x$ be an encoding over X. For a probability distribution $\mu = \{p_x\}$ over X let $X_\mu(E)$ be the bipartite state $\mathbb{E}_\mu[|x\rangle\langle x| \otimes \rho_x] \stackrel{\Delta}{=} \sum_{x\in X} p_x|x\rangle\langle x| \otimes \rho_x$. Below $\mathbb{E}_\mu[.]$ always stands for probability average (expectation) under distribution μ of the corresponding quantity. Please note the difference in the font with the notation for an encoding, which is represented by an $'E'$. Let $I^X_\mu(E)$ be the mutual information between the two systems in $X_\mu(E)$. When the underlying set X is clear we omit the superscript. Let $\rho_\mu \stackrel{\Delta}{=} \mathbb{E}_\mu[\rho_x]$. We note that in this case from definitions $I^X_\mu(E) = \mathbb{E}_\mu[S(\rho_x||\rho_\mu)]$.

Definition 2 *(Maximum possible information)* Maximum possible information *in an encoding $E : X \mapsto \mathcal{S}(\mathcal{K})$ is defined as $T_X(E) \stackrel{\Delta}{=} \max_\mu I^X_\mu(E)$. When the underlying set X is clear we omit the subscript. It is easily seen that if d is the dimension of $\mathcal{K}$ then $T(E) \leq \log d$.*

We use the following information-theoretic result called the *substate theorem* due to Jain, Radhakrishnan, and Sen [6].

Fact 2.1 (Substate theorem, [6]) *Let $\mathcal{H}, \mathcal{K}$ be two finite dimensional Hilbert spaces and $\dim(\mathcal{K}) \geq \dim(\mathcal{H})$. Let $\mathbb{C}^2$ denote the two dimensional complex Hilbert space. Let ρ, σ be density matrices in $\mathcal{H}$ such that $S(\rho\|\sigma) < \infty$. Let $|\overline{\rho}\rangle$ be a purification of ρ in $\mathcal{H} \otimes \mathcal{K}$. Then, for $r > 1$, there exist pure states $|\phi\rangle, |\theta\rangle \in \mathcal{H} \otimes \mathcal{K}$ and $|\overline{\sigma}\rangle \in \mathcal{H} \otimes \mathcal{K} \otimes \mathbb{C}^2$, depending on r, such that $|\overline{\sigma}\rangle$ is a purification of σ and $F(|\overline{\rho}\rangle\langle\overline{\rho}|, |\phi\rangle\langle\phi|) \geq 1 - \frac{1}{\sqrt{r}}$, where*

$$|\overline{\sigma}\rangle \stackrel{\Delta}{=} \sqrt{\frac{r-1}{r2^{rk}}}\,|\phi\rangle|1\rangle + \sqrt{1 - \frac{r-1}{r2^{rk}}}\,|\theta\rangle|0\rangle$$

and $k \stackrel{\Delta}{=} 8S(\rho\|\sigma) + 14$.

The following fact can be found in Cleve et al [7].

Fact 2.2 *Let Alice have a classical random variable Z. Suppose Alice and Bob share a prior entanglement independent of Z. Initially Bob's qubits have no information about Z. Now let Alice and Bob run a quantum communication protocol, at the end of which Bob's qubits possess m bits of information about Z. Then, Alice has to send at least $m/2$ qubits to Bob.*

We will require the following minimax theorem from game theory(see [8]).

Fact 2.3 *Let A_1, A_2 be non-empty, either finite or convex and compact subsets of $\mathbb{R}^n$. Let $u : A_1 \times A_2 \mapsto \mathbb{R}$ be a continuous function. Let μ_1, μ_2 be distributions on A_1 and A_2 respectively. Then,*

$$\min_{\mu_1} \max_{a_2 \in A_2} \mathbb{E}_{\mu_1}[u(a_1, a_2)] = \max_{\mu_2} \min_{a_1 \in A_1} \mathbb{E}_{\mu_2}[u(a_1, a_2)]$$

We will also require the following Local transition theorem [9, 10, 11].

Theorem 1 *Let ρ be a quantum state in $\mathcal{K}$. Let $|\phi_1\rangle$ and $|\phi_2\rangle$ be two purification of ρ in $\mathcal{H}\otimes\mathcal{K}$. Then there is a local unitary transformation U acting on $\mathcal{H}$ such that $(U\otimes I)|\phi_1\rangle = |\phi_2\rangle$.*

3 Communication bounds

The following lemma states the communication lower bound.

Lemma 1 *Let $E : x \mapsto \rho_x$ be an encoding, then $Q^{pub}(RSP(X, E, 0)) \geq T(E)/2$.*

Proof. Let $T(E) = c$. Let μ be the distribution on X such that $I_\mu(E) = c$. Consider the random variable Z taking values in X with distribution μ. Let Alice be given inputs according to μ. We know that after the remote state preparation protocol mutual information between Z and the qubits of Bob, where the state is created, is c. Hence by fact 2.2 at least $c/2$ qubits must be communicated by Alice to Bob. $\square$.

Remark: As suggested by an anonymous referee we out point here that the above lemma is not robust for positive ϵ. This is because after allowing for a small error $T(E')$ may be smaller than $T(E)$ by up to order $\epsilon \log d + \epsilon \log \epsilon$, where E' is the new encoding obtained by allowing the positive error ϵ. This follows from Fannes inequality [12].

On the other hand we show the following upper bound on the communication required to solve the problem.

Theorem 2 *Let $E : x \mapsto \rho_x$ be an encoding and $0 < \epsilon < 1$ be a constant, then $Q^{pub}(RSP(X, E, \epsilon)) \leq \frac{8}{\epsilon^2}(4T(E) + 7)$.*

Proof. We first show the following key lemma.

Lemma 2 *Let $E : x \mapsto \rho_x$ be an encoding. There exists a distribution μ such that*

$$\forall x \in X, S(\rho_x || \rho_\mu) \leq T(E)$$

Proof. Let A_1 be the set of all distribution on the set X. Let A_2 be the set X itself. The function $u : A_1 \times A_2 \mapsto \mathbb{R}$ be such that $u(\mu, x) = S(\rho_x || \rho_\mu)$. The conditions of Fact 2.3 are satisfied and therefore we have:

$$\begin{aligned}
\min_\mu \max_x S(\rho_x || \rho_\mu) &\leq \min_{\mu*:\text{distribution over distributions } \mu} \max_x \mathbb{E}_{\mu*}[S(\rho_x || \rho_\mu)] && (1)\\
&= \max_{\lambda:\text{distribution over } X} \min_\mu \mathbb{E}_\lambda[S(\rho_x || \rho_\mu)] && (2)\\
&\leq \max_\lambda \mathbb{E}_\lambda[S(\rho_x || \rho_\lambda)] && (3)\\
&= \max_\lambda I_\lambda(E) = T(E) && (4)
\end{aligned}$$

Inequality (1) follows since relative entropy is jointly convex in its arguments. Equality (2) is from Fact 2.3. $\square$.

Let $T(E) = c$, then from lemma 2 we get a distribution μ on X such that $\forall x, S(\rho_x || \rho_\mu) \leq c$. Let Alice and Bob start with 2^{rk} $(r = 4/\epsilon^2, k = 8c + 14)$ copies of some purification $|\psi\rangle$ of ρ_μ with the purification part being with Alice and ρ_μ with Bob in each of the copies of $|\psi\rangle$. Let us invoke Fact 2.1 with $\rho \stackrel{\Delta}{=} \rho_x, \sigma \stackrel{\Delta}{=} \rho_\mu$ and $|\overline{\rho}\rangle$ being any purification of ρ_x. Let $|\psi_x\rangle$ be the purification of ρ_μ obtained from Fact 2.1 corresponding to $|\overline{\sigma}\rangle$. Since the reduced quantum state on Bob's part in both $|\psi_x\rangle$ and $|\psi\rangle$ is the same, from local transition theorem, there exists a transformation acting only in Alice's side which takes $|\psi\rangle$ to $|\psi_x\rangle$. Alice on input x, transforms each $|\psi\rangle$ to $|\psi_x\rangle$ and measures the first bit. If she obtains 1 in any copy of $|\psi_x\rangle$ she communicates the number of that copy to Bob. It is easily seen that the communication from Alice is at most $rk = \frac{8}{\epsilon^2}(4c + 7)$. Also since $\Pr(\text{Alice observes } 1) = \frac{r-1}{r2^{rk}}$, and Alice makes 2^{rk} tries she succeeds with probability at least $1 - 1/r$. In case she succeeds, let the state with Bob in which Alice succeeds be ρ'_x. From Fact 2.1, $F(\rho'_x, \rho_x) \geq 1 - 1/\sqrt{r}$. So for the final state $\tilde{\rho_x}$ produced with Bob, it follows from concavity of fidelity that $F(\tilde{\rho_x}, \rho_x) \geq 1 - 2/\sqrt{r} = 1 - \epsilon$. $\square$.

Remarks:

1. Given an encoding $E : x \mapsto \rho_x$, a small constant ϵ and states ρ'_x such that $F(\rho'_x, \rho_x) \geq 1 - \epsilon$, let a *perturbed encoding* E' be, $E' : x \mapsto \rho'_x$. It is quite possible that $T(E')$ is much less than $T(E)$ as allowed by Fannes bound. In such a case communication can be reduced a lot by running the above protocol for E' instead of E since we are ready to tolerate constant fidelity loss anyway.

2. One can consider the classical version of the remote state generation problem in which the encoding considered is a mapping from X to the set of classical distributions on some

set. On input $x \in X$ to Alice, they are required to communicate, at the end of which Bob is required to sample from a distribution close to $E(x)$. The same communication bounds apply for this problem as well.

4 Conclusions

The protocol for the upper bound, mentioned in this paper uses a large amount of entanglement. It will be interesting to see if it can be reduced or even eliminated if possible. Also it will be interesting to get entanglement-communication trade-offs for this problem as opposed to the trade-offs in the rates of entanglement and communication mentioned in some of the earlier works.

5 Acknowledgment

We thank Rohit Khandekar, Pranab Sen, Julia Kempe and Jaikumar Radhakrishnan for useful discussions and for pointing out useful references. We also thank anonymous referees for useful suggestions and comments.

References

1. H.-K. Lo (2000), *Classical communication cost in distributed quantum information processing - a generalization of quantum communication complexity*, Phys. Rev. A, 62.
2. C.H. Bennett, P. Hayden, W. Leung, P.W. Shor, and A. Winter (2005), *Remote preparation of quantum states*, IEEE transaction of information theory, 51, pp 56-74.
3. C.H. Bennett, D.P. DiVincenzo, P.W. Shor, J.A. Smolin, B.M. Terhal, and W.K. Wootters (2001), *Remote state preparation*, Phys. Rev. Lett, 87.
4. A.K. Pati (2001), *Minimum classical bit for remote preparation and measurement of a qubit*, Phys. Rev. A, 63.
5. B. Zeng and P. Zhang (2002), *Remote-state preparation in higher dimension and the parallelizable manifold* s^{n-1}, Phys. Rev. A, 65.
6. R. Jain, J. Radhakrishnan, and P. Sen (2002), *Privacy and interaction in quantum communication complexity and a theorem about the relative entropy of quantum states*, Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science, pp 429-438.
7. R. Cleve, Wim van Dam, M. Nielsen, and A. Tapp (1998), *Quantum entanglement and the communication complexity of the inner product function*, Proceedings of the 1st NASA International Conference on Quantum Computing and Quantum Communications, Lecture Notes in Computer Science, 1509, pp 61-74, Springer-Verlag, quant-ph/9708019.
8. M. Osborne and A. Rubinstein (1994), *A course in game theory*, MIT Press.
9. D. Mayers (1997), *Unconditionally secure quantum bit commitment is impossible*, Phys. Rev. Lett, 78, pp 3414-3417.
10. H.-K. Lo and H.F. Chau (1997), *Is quantum bit commitment really possible?*, Phys. Rev. Lett., 78.
11. H.-K. Lo and H.F. Chau (1998), *Why quantum bit commitment and ideal quantum coin tossing are impossible*, Physica D, 120.
12. M. Fannes (1973), *A continuity property of the entropy density of spin lattice systems*, Comm. Math. Phys., 31, pp 291-294.