REMOTE STATE PREPARATION FOR MULTIPLE PARTIES

Wenhan Dai, Tianyi Peng, and Moe Z. Win

Laboratory for Information and Decision Systems,
Massachusetts Institute of Technology

(Invited Paper)

ABSTRACT

Remote state preparation (RSP) is a technique to transmit quantum states with classical communication and previously shared entanglement. In this paper, we consider RSP in a multiparty setting. A simple yet nontrivial case is studied, where there is one sender and two receivers. We put forth a broadcasting method for developing multiparty RSP protocols. We show that this method can remotely prepare arbitrary states by consuming classical and quantum resources. For preparing highly entangled states, the proposed method achieves the lower bound for the amount of consumed resources asymptotically.

***Index Terms*—** Entanglement, Haar measure, quantum communication, remote state preparation, teleportation

1. INTRODUCTION

Transmission of quantum states with classical communication and previously shared entanglement among senders and receivers is a major topic in quantum information science. The results in this topic reveal the fundamental tradeoff between different types of resources such as quantum bits (qubits), bits of entanglement (ebits), and classical bits (cbits). In the celebrated teleportation technique [1], a qubit can be transmitted faithfully (i.e., exactly and deterministically) by using 2 cbits and 1 ebit with no knowledge of the qubit to be sent. Another important type of protocols is remote state preparation (RSP) [2–7]. Compared with teleportation, the sender is allowed to have the knowledge of the qubit to be sent. Such additional information makes it possible to transmit quantum states with fewer resources. For example, the protocol developed in [7] consumes 1 cbit and 1 ebit asymptotically per qubit.

In practical applications, it is common to encounter scenarios where there are multiple senders or receivers. Therefore, it is natural to ask how one can generalize the results of two-party RSP to multiple parties. In contrast to the fruitful results in the two-party scenario, little is known about multiparty RSP protocols that can transmit generic pure quantum states with a high success probability and a high fidelity [8,9].

If the pure quantum state to be transmit is separable among receivers, then one can directly generalize the point-to-point RSP to multiparty RSP. However, the task of multiparty RSP is challenging if the state is entangled among receivers. The major difficulty lies in the constraint that the operations for nodes in different locations have to be separable [10]. Moreover, a meaningful multiparty RSP protocol needs to be more resource-efficient than teleportation as more knowledge about the state to be transmitted is available to the sender, adding another layer of difficulty. The fundamental questions related to multiparty RSP are

- how to overcome the constraint of separable operations for nodes in different locations and
- how to exploit the knowledge of the quantum state to design more efficient protocols than teleportation?

The answers to these questions enable the design of efficient multiparty RSP protocols.

The goal of this paper is to develop multiparty RSP protocols for generic quantum states with high success probability and high fidelity. A simple yet nontrivial case is studied, where there is one sender and two receivers. We put forth a broadcasting method for developing multiparty RSP protocols. This method uses the invariant property of the Haar measure. To analyze the amount of resources used in the developed protocol, a key step is to determine the convergence rate of a sequence of random matrices. We observe the connection between the Haar measure and symmetric groups and show that using the results in symmetric groups can provide a tight upper bound for the aforementioned convergence rate.

This paper is among the first attempts to design and analyze multiparty RSP protocols for transmiting generic quantum states. The key contributions of this paper are three folds. First, we develop a framework for the remote preparation of three-party states and introduce a new type of resources, broadcast cbits, for evaluating multiparty RSP protocols. Second, we put forth a broadcasting method for developing multiparty

This research was supported, in part, by the MIT Institute for Soldier Nanotechnologies.

RSP protocols. Third, we characterize the used resources in terms of broadcast cbits and ebits for preparing arbitrary states and highly entangled states. We also show that for preparing highly entangled states, the proposed method achieves the lower bound for the number of consumed broadcast cbits and ebits, asymptotically.

Notation: Random variables are displayed in sans serif, upright fonts; their realizations in serif, italic fonts. Vectors and matrices are denoted by bold lowercase and uppercase letters, respectively. The m-by-m identity matrix is denoted by $\boldsymbol{I}_m$: the subscript is removed when the dimension of the matrix is clear from the context. † denotes the Hermitian adjoint, $^\mathsf{T}$ denotes the transpose, and * denotes the complex conjugate with basis $|0\rangle$ and $|1\rangle$. exp and log are to basis 2.

2. PREMILINARIES

This section introduces the system model and different notions that characterize the multiparty RSP protocols.

2.1. Multiparty RSP Protocols and Several Notions

Following the description of two-party RSP protocol [7], the multiparty RSP protocol discussed in this paper involves one sender T and two receivers R_1 and R_2: the sender is given a description of a pure state $|\psi\rangle$ from a subset $\mathcal{X}$ of the state set $\mathcal{S}(\mathcal{H}_{R_1} \otimes \mathcal{H}_{R_2})$, where $\mathcal{H}_{R_i}$ denotes the Hilbert space corresponding to the quantum systems at R_i, $i = 1, 2$. In this paper, we assume $\dim \mathcal{H}_{R_1} = \dim \mathcal{H}_{R_2} = D$, which is the asymptotic parameter (one should assume it is large). The protocol describes how to use quantum and classical resources to result in a state $\widetilde{\boldsymbol{\rho}}$ at R_1 and R_2. As mentioned above, the two receivers are not co-located and their operations need to be separable. An illustration of the multiparty RSP is shown in Fig. 1. Following the nomenclature in [7], a protocol is *probabilistic exact with error* ϵ if the protocol is successful with probability at least $1 - \epsilon$ and when the protocol is successful, $\widetilde{\boldsymbol{\rho}} = |\psi\rangle\langle\psi|$.[1]

2.2. Highly Entangled States

An RSP protocol is universal if the subset $\mathcal{X} = \mathcal{S}(\mathcal{H}_{R_1} \otimes \mathcal{H}_{R_2})$, i.e., the protocol can remotely prepare an *arbitrary* state from $\mathcal{S}(\mathcal{H}_{R_1} \otimes \mathcal{H}_{R_2})$. We also consider protocols that can remotely prepare highly entangled states:

Definition 1 (highly entangled states)**.** Given a constant C_1, a pure state $|\psi\rangle$ in $\mathcal{S}(\mathcal{H}_{R_1} \otimes \mathcal{H}_{R_2})$ is highly entangled if the maximum Schmidt coefficient is no greater than $\sqrt{C_1/D}$, i.e., $\alpha_i \leq \sqrt{C_1/D}$ for $i = 1, 2, \ldots, D$, where α_i are the Schmidt coefficients of in the following Schmidt decomposition $|\psi\rangle = \sum_{i=1}^{D} \alpha_i |u_i\rangle_{R_1} \otimes |v_i\rangle_{R_2}$.

[1]The indicator of "success" is required to be accessible to both the sender and receivers.

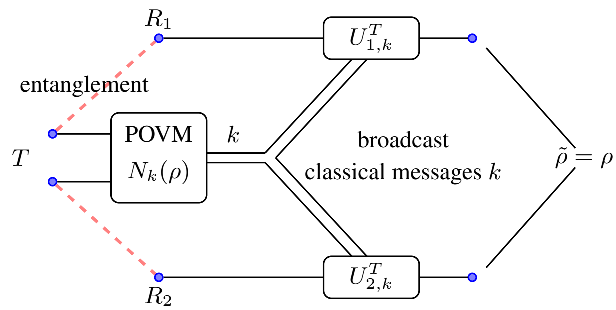

Fig. 1: Illustration of a three-party RSP: the sender performs a POVM $\boldsymbol{N}_k$, $k = 1, 2, \ldots$ and broadcasts the measurement outcome k to receivers R_1 and R_2.

Note that C_1 is irrelevant to the dimension of $\mathcal{H}_{R_1}$ and $\mathcal{H}_{R_2}$. We can find a fixed C_1 such that almost all the pure states are highly entangled states if $D \to \infty$. In fact, consider the set $\mathcal{K}_\mathrm{e} := \{|\phi\rangle \in \mathcal{S}(\mathcal{H}_{R_1} \otimes \mathcal{H}_{R_2}) : s(|\phi\rangle) \leq \sqrt{C_1/D}\}$ in which $s(|\phi\rangle)$ denotes the maximum Schmidt coefficient of $|\phi\rangle$ decomposing on $\mathcal{H}_{R_1} \otimes \mathcal{H}_{R_2}$. One can show that there exist constants $C_2, C_3 > 0$ such that for any D, $\nu(\mathcal{K}_\mathrm{e}) \geq 1 - C_2 \exp\{-C_3 D\}\}$, where $\nu(\cdot)$ is the uniform measure of unit vectors in $\mathcal{H}_{R_1} \otimes \mathcal{H}_{R_2}$.

2.3. Resources for Quantum State Transmission

The sender and receivers have access to various resources in the RSP protocols. In this paper, the resources of entanglement and forward classical communication will be considered. We consider the following entanglement shared between the sender T and the receivers R_1 and R_2:

$$|\Phi_{D^2}\rangle = \frac{1}{D} \sum_{j=1}^{D^2} |j\rangle_T |j\rangle_{R_1 R_2}$$

where $|j\rangle$ are orthogonal states, and the subscript $_T$ and $_{R_i}$ denote the corresponding quantum systems.

Note that in a multi-party system, a sender can either adopts "point-to-point communication" (sequentially sending classical information to each receiver) or "broadcasting" (sending identical information to all of the receivers simultaneously). In the setting of broadcasting, a new type of resources, namely, broadcast classical bits, is needed to evaluate the amount of communication resources. Specifically, we refer to a broadcast cbit as the sender's ability to send 1 cbit of identical information to all the receivers.

3. BROADCASTING METHOD

In this section, we present a broadcast-based RSP protocol and characterize the resources used by this protocol.

3.1. RSP of Arbitrary Pure States

We consider the system model described in Section 2.1, i.e., the sender T would like to remotely prepare an arbitrary state $|\psi\rangle$ at two different receivers using the shared entanglement $|\Phi_{D^2}\rangle$. The broadcast method relies on the following observation: for any $\boldsymbol{\rho} = |\psi\rangle\langle\psi|$,

$$\int \boldsymbol{U}_{R_1} \otimes \boldsymbol{U}_{R_2}\, \boldsymbol{\rho}^* \boldsymbol{U}_{R_1}^\dagger \otimes \boldsymbol{U}_{R_2}^\dagger d\mu(\boldsymbol{U}_{R_1}) d\mu(\boldsymbol{U}_{R_2}) = \frac{\boldsymbol{I}}{D^2} \tag{1}$$

where $\mu(\boldsymbol{U}_{R_1})$ and $\mu(\boldsymbol{U}_{R_2})$ are two independent Haar measures. The equation (1) implies that for sufficiently large K, we can find two sets of unitary matrices $\{\boldsymbol{U}_{1,k}\}_{k=1}^K$ and $\{\boldsymbol{U}_{2,k}\}_{k=1}^K$ such that for any $\epsilon > 0$,

$$\frac{1}{K}\sum_{k=1}^K \boldsymbol{U}_{1,k} \otimes \boldsymbol{U}_{2,k}\, \boldsymbol{\rho}^* \boldsymbol{U}_{1,k}^\dagger \otimes \boldsymbol{U}_{2,k}^\dagger \in \Big[\frac{1-\epsilon}{D^2}\boldsymbol{I}, \frac{1+\epsilon}{D^2}\boldsymbol{I}\Big].$$

The equation above leads to the protocol below.

Protocol I:

1) The sender T performs the POVM $(\boldsymbol{N}_k)$ on its part of the entangled state $|\Phi_{D^2}\rangle$ and sends the outcome to two receivers by consuming broadcast cbits.
2) If the message received is k, receiver R_1 applies the unitary $\boldsymbol{U}_{1,k}^{\mathrm{T}}$ and receiver R_2 applies the unitary $\boldsymbol{U}_{2,k}^{\mathrm{T}}$ to their parts of the state $|\Phi_{D^2}\rangle$.

In the protocol above, the POVM $\boldsymbol{N}_k$ is

$$\boldsymbol{N}_k = \frac{D^2}{K(1+\epsilon)}\boldsymbol{U}_{1,k} \otimes \boldsymbol{U}_{2,k}\, \boldsymbol{\rho}^* \boldsymbol{U}_{1,k}^\dagger \otimes \boldsymbol{U}_{2,k}^\dagger, \quad k = 1, 2, \cdots, K$$

$$\boldsymbol{N}_{\text{failure}} = \boldsymbol{I} - \sum_{k=1}^K \boldsymbol{N}_k$$

and $\boldsymbol{U}_{i,k}$ ($i = 1, 2,\ k = 1, 2, \cdots, K$) are unitary matrices on $\mathcal{H}_{R_i}$. To make Protocol I valid, we need to show that there exist unitary matrices $\boldsymbol{U}_{1,k}$ and $\boldsymbol{U}_{2,k}$, $k = 1, 2, \ldots, K$, such that $\boldsymbol{N}_{\text{failure}} \succeq 0$ for every state $\boldsymbol{\rho} = |\varphi\rangle\langle\varphi| \in \mathcal{X} \subseteq \mathcal{S}(\mathcal{H}_{R_1} \otimes \mathcal{H}_{R_2})$. Moreover, note that the measurement outcome sent by T is from an alphabet with cardinality K, meaning that the protocol consumes $\log K$ broadcast cbits. Therefore, a small K is desirable.

Theorem 1. For $\mathcal{X} = \mathcal{S}(\mathcal{H}_{R_1} \otimes \mathcal{H}_{R_2})$ and $\epsilon \in (0, 1)$, there exist

$$K \leq \left\lceil \left(1 + 4D^2 \log \frac{20D^2}{\epsilon}\right) \cdot \frac{8(\ln 2)(D+1)e^4}{\pi\epsilon^2} \right\rceil$$

pairs of unitary matrices $\boldsymbol{U}_{1,k}$, $\boldsymbol{U}_{2,k}$, $k = 1, 2, \ldots, K$, such that for every pure state $\boldsymbol{\rho}_\varphi = |\varphi\rangle\langle\varphi| \in \mathcal{X}$,

$$\frac{1}{K}\sum_{k=1}^K \boldsymbol{U}_{1,k} \otimes \boldsymbol{U}_{2,k}\, \boldsymbol{\rho}_\varphi^* \boldsymbol{U}_{1,k}^\dagger \otimes \boldsymbol{U}_{2,k}^\dagger \in \Big[\frac{1-\epsilon}{D^2}\boldsymbol{I}, \frac{1+\epsilon}{D^2}\boldsymbol{I}\Big]. \tag{2}$$

Theorem 1 shows that Protocol I can remotely prepare an arbitrary state in $\mathcal{H}_{R_1} \otimes \mathcal{H}_{R_2}$ by consuming 3 broadcast cbits and 2 ebits per pairs of qubits, asymptotically. Comparatively, teleportation consumes 4 cbits (2 to R_1 and 2 to R_2) and 2 ebits per pairs of qubits.

Proof. The condition (2) is equivalent to the condition that for all pure states $|\varphi\rangle$ and $|\widetilde{\varphi}\rangle$,

$$\left|\frac{1}{K}\sum_{k=1}^K \operatorname{tr}\Big(\boldsymbol{U}_{1,k} \otimes \boldsymbol{U}_{2,k} \boldsymbol{\rho}_\varphi^* \boldsymbol{U}_{1,k}^\dagger \otimes \boldsymbol{U}_{2,k}^\dagger |\widetilde{\varphi}\rangle\langle\widetilde{\varphi}|\Big) - \frac{1}{D^2}\right| \leq \frac{\epsilon}{D^2}.$$

To achieve so, select matrices $\boldsymbol{U}_{1,k}$ and $\boldsymbol{U}_{2,k}$ independently from the Haar measure. We need to evaluate the Cramér function $\Lambda(z) = \sup_{y\in\mathbb{R}}[yz - \ln \mathbb{E}_{\mathsf{x}}\{e^{y\mathsf{x}}\}]$ corresponding to

$$\mathsf{x} = \operatorname{tr}\Big(\mathbf{U}_1 \otimes \mathbf{U}_2 \boldsymbol{\rho}_\varphi^* \mathbf{U}_1^\dagger \otimes \mathbf{U}_2^\dagger |\widetilde{\varphi}\rangle\langle\widetilde{\varphi}|\Big) \tag{3}$$

where $\mathbf{U}_1$ and $\mathbf{U}_2$ are $D \times D$ independent random matrices and both of them are distributed according to Haar measure. For $\epsilon \in (0, 1)$,

$$\begin{aligned}
&\mathbb{P}\left\{\left|\frac{1}{K}\sum_{k=1}^K \operatorname{tr}\left(\mathbf{U}_{1,k} \otimes \mathbf{U}_{2,k} \boldsymbol{\rho}_\varphi^* \mathbf{U}_{1,k}^\dagger \otimes \mathbf{U}_{2,k}^\dagger |\widetilde{\varphi}\rangle\langle\widetilde{\varphi}|\right) - \frac{1}{D^2}\right| \geq \frac{\epsilon}{D^2}\right\} \\
&\leq \exp\left\{-\frac{K}{\ln 2}\inf_{x\geq 1+\epsilon}\Lambda(x)\right\} + \exp\left\{-\frac{K}{\ln 2}\inf_{x\leq 1-\epsilon}\Lambda(x)\right\} \\
&\leq 2\exp\left\{-\frac{\pi\epsilon^2 K}{2\ln 2(D+1)e^4}\right\}
\end{aligned} \tag{4}$$

where the first inequality is because of Cramér's theorem [11], and the second inequality is because of Lemma 2 shown later.

We consider a $\frac{\epsilon}{4D^2}$-net $\mathcal{M}$ for the Hilbert space $\mathcal{H}_{R_1} \otimes \mathcal{H}_{R_2}$ according to Lemma 1 shown later. Replacing ϵ with $\epsilon/2$ in the inequality (4), together with the union bound, gives

$$\begin{aligned}
&\mathbb{P}\left\{\exists |\varphi\rangle, |\widetilde{\varphi}\rangle \in \mathcal{M}, \left|\frac{1}{K}\sum_{k=1}^K \operatorname{tr}(\mathbf{U}_{1,k} \otimes \mathbf{U}_{2,k} \boldsymbol{\rho}_\varphi^* \mathbf{U}_{1,k}^\dagger \otimes \mathbf{U}_{2,k}^\dagger |\widetilde{\varphi}\rangle\langle\widetilde{\varphi}|) - \frac{1}{D^2}\right| > \frac{\epsilon}{2D^2}\right\} \\
&\leq 2\left(\frac{20D^2}{\epsilon}\right)^{4D^2} \exp\left\{-\frac{K\pi\epsilon^2}{8(\ln 2)(D+1)e^4}\right\}.
\end{aligned}$$

With the triangle inequality for the trace norm, we get

$$\begin{aligned}
&\mathbb{P}\left\{\exists |\varphi\rangle, |\widetilde{\varphi}\rangle \in \mathcal{H}_{R_1} \otimes \mathcal{H}_{R_2}\left|\frac{1}{K}\sum_{k=1}^K \operatorname{tr}(\mathbf{U}_{1,k} \otimes \mathbf{U}_{2,k} \boldsymbol{\rho}_\varphi^* \mathbf{U}_{1,k}^\dagger \otimes \mathbf{U}_{2,k}^\dagger |\widetilde{\varphi}\rangle\langle\widetilde{\varphi}|) - \frac{1}{D^2}\right| > \frac{\epsilon}{D^2}\right\} \\
&\leq 2\left(\frac{20D^2}{\epsilon}\right)^{4D^2} \exp\left\{-\frac{K\pi\epsilon^2}{8(\ln 2)(D+1)e^4}\right\}.
\end{aligned}$$

Hence, if K is as large as stated in the theorem, there exist unitary matrices $\boldsymbol{U}_{1,k}$ and $\boldsymbol{U}_{2,k}$ such that (2) is true. $\square$

Lemma 1. [7] Let $\mathcal{H}$ be a Hilbert space of dimension S. Then there exists, for every $\delta > 0$, a set $\mathcal{M}$ of pure state vectors in $\mathcal{H}$ of cardinality $|\mathcal{M}| \leq \left(\frac{5}{\delta}\right)^{2S}$ such that for every state vector $|\varphi\rangle \in \mathcal{H}$, there exists a state vector $|\widetilde{\varphi}\rangle \in \mathcal{M}$ such that $\|\varphi - \widetilde{\varphi}\|_1 \leq \delta$. Such a set $\mathcal{M}$ is referred to as δ-net.

Lemma 2. The Cramér function corresponding to x defined in (3) can be lower bounded by

$$\Lambda(1+\delta) \geq \max\left\{\frac{\pi\delta^2}{4e^4D^2\big(s(|\varphi\rangle)\big)^4}, \frac{\pi\delta^2}{4e^4D^2\big(s(|\widetilde{\varphi}\rangle)\big)^4}, \frac{\pi\delta^2}{2(D+1)e^4}\right\}$$

for $\delta \in (-1, 1)$.

Using the concept of *net* to show the existence of desired unitary operators follows from [7]. The key novelty in our work is Lemma 2. Due to space constraints, the detailed proof of Lemma 2 is omitted, but a key intermediate result used to prove Lemma 2 is presented below.

Lemma 3. Suppose $\boldsymbol{M} \in \mathbb{C}^{D\times D}$ is a deterministic matrix and $\mathbf{U} \in \mathbb{C}^{D\times D}$ is distributed according to Haar measure, then for an arbitrary $k \in \mathbb{Z}^*$,

$$\mathbb{E}\{|\operatorname{tr}(\mathbf{U}\boldsymbol{M})|^{2k}\} \leq k!\left(\frac{\sqrt{2\pi}}{e^2}\right)^{-k} D^{-k}\big(\operatorname{tr}\{\boldsymbol{M}\boldsymbol{M}^\dagger\}\big)^k.$$

The proof of Lemma 3 is based on the connection between the Haar measure and symmetric groups and the results in symmetric groups (e.g., Young tableau and Hook's formula) [12].

3.2. RSP of Highly Entangled States

Protocol I can remotely prepare any state in $\mathcal{K}_{\mathrm{e}}$ with fewer resources (i.e., smaller K), shown in the following theorem.

Theorem 2. For $\mathcal{X} = \mathcal{K}_{\mathrm{e}}$ and $\epsilon \in (0, 1)$, there exist

$$K \leq \left\lceil \left(1 + 4D^2 \log\frac{20D^2}{\epsilon}\right)\frac{4(\ln 2)C_1^2e^4}{\pi\epsilon^2} \right\rceil$$

pairs of unitary matrices $\boldsymbol{U}_{1,k}$, $\boldsymbol{U}_{2,k}$, $k = 1, 2, \ldots, K$, such that for every pure state $\boldsymbol{\rho}_\varphi = |\varphi\rangle\langle\varphi| \in \mathcal{X}$, the condition (2) holds.

Proof. We can follow the proof of Theorem 1 until (4). We next obtain a tighter bound for the convergence than (4)

$$\mathbb{P}\left\{\left|\frac{1}{K}\sum_{k=1}^{K}\operatorname{tr}\left(\mathbf{U}_{1,k}\otimes\mathbf{U}_{2,k}\boldsymbol{\rho}_\varphi^*\mathbf{U}_{1,k}^\dagger\otimes\mathbf{U}_{2,k}^\dagger|\widetilde{\varphi}\rangle\langle\widetilde{\varphi}|\right) - \frac{1}{D^2}\right| \geq \frac{\epsilon}{D^2}\right\} \leq 2\exp\left\{-\frac{K\pi\epsilon^2}{4(\ln 2)e^4C_1^2}\right\}$$

where the inequality is because of Lemma 2 and the fact that $s(|\varphi\rangle) \leq \sqrt{C_1/D}$. Then similarly to the proof of Theorem 1, one can verify that

$$\mathbb{P}\left\{\exists\,|\varphi\rangle, |\widetilde{\varphi}\rangle \in \mathcal{K}_{\mathrm{e}}, \left|\frac{1}{K}\sum_{k=1}^{K}\operatorname{tr}(\mathbf{U}_{1,k}\otimes\mathbf{U}_{2,k}\boldsymbol{\rho}_\varphi^* \mathbf{U}_{1,k}^\dagger\otimes\mathbf{U}_{2,k}^\dagger|\widetilde{\varphi}\rangle\langle\widetilde{\varphi}|) - \frac{1}{D^2}\right| > \frac{\epsilon}{D^2}\right\} \leq 2\left(\frac{20D^2}{\epsilon}\right)^{4D^2}\exp\left\{-\frac{K\pi\epsilon^2}{4(\ln 2)e^4C_1^2}\right\}$$

Hence, if K is as large as stated in the theorem, there exist unitary matrices $\boldsymbol{U}_{1,k}$ and $\boldsymbol{U}_{2,k}$ such that (2) is true. $\square$

Theorem 2 shows that Protocol I can remotely prepare an arbitrary state in $\mathcal{K}_{\mathrm{e}}$ by consuming 2 broadcast cbits and 2 ebits per pairs of qubits, asymptotically. The resources required are fewer compared with preparing an arbitrary pure state in $\mathcal{H}_{R_1}\otimes\mathcal{H}_{R_2}$. Moreover, we can show that the required resources are also necessary in the next proposition.

Proposition 1. Any multiparty remote state preparation protocol that is exact probabilistic with error ϵ for states in $\mathcal{K}_{\mathrm{e}}$ requires the sender to transmit

$$\log K \geq 2\log D + \log(1-\epsilon)$$

cbits. Moreover, if the protocol uses an entanglement state of Schmidt rank less or equal than qD^2 with $q < 1-\epsilon$, then it requires classical communication of at least $\Omega(D)$ cbits.

Proof. (Sketch) We can find a set consisting of D^2 orthogonal maximumly entangled states [1]. The capability to remotely prepare an orthogonal basis exactly with probability at least $1-\epsilon$ permits the sender to transmit one out of D^2 classical messages with probability at least $1-\epsilon$ of correct decoding. Causality implies that the number of cbits required by the protocol is at least $2\log D + \log(1-\epsilon)$. The second part of proof can be proved similarly to Theorem 8 in [7]. $\square$

4. CONCLUSION

We developed an RSP protocol in a three-party scenario, where there is one sender and two receivers. We showed that this protocol can remotely prepare arbitrary states and highly entangled states by consuming 3 broadcast cbits and 2 broadcast cbits, respectively, in addition to 2 ebits, per pairs of qubits sent, asymptotically. For preparing highly entangled states, the proposed method achieves the lower bound of resources asymptotically. The study for this simple but nontrivial setting reveals some phenomena not observed in point-to-point RSP, e.g., the additional classical resource consumption brought by the different locations of receivers compared to the result in [7]. Our results can be extended to the scenario where the quantum systems at two receivers have different dimensions.

5. REFERENCES

[1] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," *Phys. Rev. Lett.*, vol. 70, no. 13, pp. 1895–1899, Mar. 1993.

[2] Hoi-Kwong Lo, "Classical-communication cost in distributed quantum-information processing: A generalization of quantum-communication complexity," *Phys. Rev. A*, vol. 62, pp. 012313, July 2000.

[3] Arun K. Pati, "Minimum classical bit for remote preparation and measurement of a qubit," *Phys. Rev. A*, vol. 63, pp. 014302, Dec. 2000.

[4] Igor Devetak and Toby Berger, "Low-entanglement remote state preparation," *Phys. Rev. Lett.*, vol. 87, pp. 197901, Nov. 2001.

[5] Dominic W. Berry and Barry C. Sanders, "Optimal remote state preparation," *Phys. Rev. Lett.*, vol. 90, pp. 057901, Feb. 2003.

[6] Charles H. Bennett, David P. DiVincenzo, Peter W. Shor, John A. Smolin, Barbara M. Terhal, and William K. Wootters, "Remote state preparation," *Phys. Rev. Lett.*, vol. 87, no. 7, pp. 077902, July 2001.

[7] Charles H. Bennett, Patrick Hayden, Debbie W. Leung, Peter W. Shor, and Andreas Winter, "Remote preparation of quantum states," *IEEE Trans. Inf. Theory*, vol. 51, no. 1, pp. 56–74, Jan. 2005.

[8] Ya-Fei Yu, Jian Feng, and Ming-Sheng Zhan, "Preparing remotely two instances of quantum state," *Physics Letters A*, vol. 310, pp. 329–332, Apr. 2003.

[9] Yan Xia, Jie Song, and He-Shan Song, "Multiparty remote state preparation," *Journal of Physics B: Atomic, Molecular and Optical Physics*, vol. 40, pp. 3719–3724, Sept. 2007.

[10] Runyao Duan, Yuan Feng, Yu Xin, and Mingsheng Ying, "Distinguishability of quantum states by separable operations," *IEEE Trans. Inf. Theory*, vol. 55, no. 3, pp. 1320–1330, Mar. 2009.

[11] A. Dembo and O. Zeitouni, *Large Deviations Techniques and Applications*, New York: Springer-Verlag., New York, NY, 1998.

[12] Jonathan Novak, "Truncations of random unitary matrices and young tableaux," *The Electronic Journal of Combinatorics*, vol. 14, pp. 1–12, 2007.