2022 IEEE International Symposium on Information Theory (ISIT) | 978-1-6654-2159-1/22/$31.00 ©2022 IEEE | DOI: 10.1109/ISIT50566.2022.9834596

Multi-Party Quantum Purity Distillation with Bounded Classical Communication

Touheed Anwar Atif
University of Michigan, USA
Email: touheed@umich.edu

S. Sandeep Pradhan
University of Michigan, USA
Email: pradhanv@umich.edu

***Abstract*—We consider the task of distilling local purity from a noisy quantum state ρ^{ABC}, wherein we provide a protocol for three parties, Alice, Bob and Charlie, to distill local purity (at a rate P) from many independent copies of a given quantum state ρ^{ABC}. The three parties have access to their respective subsystems of ρ^{ABC}, and are only allowed to use local unitary operations. In addition, Alice and Bob can communicate with Charlie using a one-way multiple-access dephasing channel of link rates R_1 and R_2, respectively. The objective of the protocol is to minimize the usage of the dephasing channel (in terms of rates R_1 and R_2) while maximizing the asymptotic purity that can be jointly distilled from ρ^{ABC}. To achieve this, we employ ideas from distributed measurement compression protocols, and in turn, characterize a set of sufficient conditions on (P, R_1, R_2) in terms of quantum information theoretic quantities such that P amount of purity can be distilled using rates R_1 and R_2.**

I. Introduction

A primary task in quantum information theory is to quantify the amount of local and non-local information present within a quantum information source. For instance, the task of entanglement distillation aims at capturing the non-local correlations to transform a noisy shared state ρ^{AB} into pure bell states (in particular, the ebit $|\Phi^+\rangle$), in an aymptotic sense. A complementary notion to this task is the paradigm of local purity distillation, where pure ancilla qubits are distilled from a distributed state ρ^{AB} using local unitary operations.

Although it may seem unusual, local pure states cannot be considered as a free resource. One may argue that pure states can be obtained from a mixed state by performing a measurement, but this is only true after a measurement apparatus is initialized in a pure state. For this reason, the second law of thermodynamics recognizes purity as indeed a resource [1], [2]. In this regard, the idea of distilling of local purity was first introduced in [3], [4] where the aim was to manipulate the qubits and concentrate the existing diluted form of purity. Two version of this problem have been introduced, (i) a single-party variant and (ii) a distributed version. In the former single-party scenario, also called as *local purity concentration*, many copies of a noisy state ρ^A are provided to Alice, and she aims at concentrating or extracting purity using only unitary operations. The authors in [5] characterized the asymptotic performance limit of this protocol ($\kappa(\rho^A)$) as the difference between the number of qubits describing the system and the von Neumann entropy of the state ρ^A. For the latter case of distilling purity from a non-local distributed state, commonly termed as *local purity distillation*, two parties, Alice and Bob, share many copies of the noisy state ρ^{AB} and aim at jointly distilling pure ancilla qubits. Again, they are allowed to perform only local unitaries and but can communicate classically (LOCC), possibly through the use of a dephasing channel [3]. Further, the protocols for both the variants require isolation (Closed-LOCC) from the environment which eliminated the possibility of unlimited consumption of the pure ancilla qubits. The authors in [4] provided bounds for this problem in the one-way and the two-way classical communication scenarios.

Later, Devetak in [6] considered a new paradigm called 1-CLOCC$'$, which was defined as an extension of Closed-LOCC, with (i) the allowance of using additional catalytic pure ancilla as long as these are returned back to the system, and (ii) the unlimited bidirectional classical communication replaced by unlimited one-way communication from Alice to Bob. Devetak obtained an information theoretic characterization of the distillable purity and also highlighted its connection to the earlier known one-way distillable common randomness measure [7]. Building upon this, the authors in [8] extended the result to a setting with bounded one-way classical communication. They improved upon the classical communication rate by using the Winter's approximate measurement [9], instead of an n-letter product measurement, and extracted purity for the states obtained thereby.

In this work, we revisit the task of distilling purity and consider a three-party setup. We ask the question of how many ancilla qubits can be distilled from a noisy state ρ^{ABC}, shared among three parties, Alice, Bob and Charlie. Similar to earlier problem formulation, we only allow local unitary operations at each party in a closed setting but permit the use of additional catalytic ancillas with the promise of returning them at the end of the protocol. In addition, similar to [8], we only allow limited classical communication, which we model using a one-way multiple-access dephasing channel, with Alice and Bob as the senders and Charlie as the centralized receiver.

The contributions of our work can be summarized as follows. We first formulate a three-party purity distillation problem, and develop a 1-CLOCC$'$ multi-party purity distillation protocol for this problem capable of extracting purity from n copies of the noisy shared state $\rho_{ABC}^{\otimes n}$, using only local unitary operations and a one-way multiple-access dephasing channel. Further, for $\rho_{ABC}^{\otimes n}$, we define the asymptotic performance limit of the problem as the set of all triples (P, R_1, R_2), where P

This work was supported by NSF grant CCF-2007878.

denotes the amount of purity that can be distilled from ρ^{ABC}, using R_1 and R_2 bits of classical communication. Then we characterize a quantum-information theoretic inner bound to the achievable rate region in terms of computable single-letter information quantities (see Theorem 1).

Toward the development of the results, we encounter two main challenges. The first challenge is in the compression of the joint measurements. Since the classical communication allowed by the protocol is limited, the joint measurements, that Alice and Bob employ, are required to be compressed. Although a distributed measurement compression protocol for compressing a joint measurement have been developed earlier [10], one cannot directly use this protocol as a complete black box. The reason for this is that the measurement compression protocol also requires additional common randomness as a resource which the current purity distillation protocol does not allow. Apart from this, the measurement compression protocols provided in [9]–[11] shows the "faithfulness" of the post-measurement state of the reference along with the classical-quantum register storing the measurement outcome. These protocols remain unconcerned about the post-measurement state of the system on which the measurement is performed. However, in the current problem the closeness of the latter is needed. To overcome this, we identify appropriate purifications of the post-measurement reference states and argue an existence of a collection of unitary operations achieving the latter (see Lemma 2 for more details).

The second major challenge is that after the application of the compressed measurement, the states across the three parties are not necessary separable. This is because a compressed measurement is usually not a "sharp" rank-one measurement. In [6] rank-one measurements are employed which makes the states separable and hence eases the analysis. To handle this, we develop a technique (see Lemma 3) and employ it in our proof.

II. Distributed Purity Distillation

In the following we describe the problem statement. Let ρ^{ABC} be a density operator acting on $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$. Consider two measurements M_A and M_B on sub-systems A and B, respectively. Imagine that we have three parties, named Alice, Bob and Charlie, trying to distill local purity from the noisy joint state ρ^{ABC}. The resources available to these parties are (i) the classical communication links of specified rates between Alice and Charlie, and Bob and Charlie, modelled as a multiple-access dephasing channel, and (ii) an additional triple of pure catalytic quantum systems A_C, B_C and C_C available to Alice, Bob and Charlie, respectively. Given the distributed nature of the problem, no communication is possible between Alice and Bob. The problem is formally defined in the following.

Definition 1. For a given finite set $\mathcal{Z}$, and a Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$, a distributed purity distillation protocol with parameters $(n, \Theta_1, \Theta_2, \kappa_1, \kappa_2, \kappa_3, \iota_1, \iota_2, \iota_3)$ is characterized by

1) a unitary operation on Alice's system $U_A\colon \mathcal{H}_A^{\otimes n} \otimes \mathcal{H}_{A_C} \to \mathcal{H}_{A_p} \otimes \mathcal{H}_{X_1} \otimes \mathcal{H}_{A_g}$, with $\dim(\mathcal{H}_{A_p}) = \kappa_1$, $\dim(\mathcal{H}_{A_C}) = \iota_1$, and $\dim(\mathcal{H}_{X_1}) = \Theta_1$.
2) a unitary operation on Bob's system $U_B\colon \mathcal{H}_B^{\otimes n} \otimes \mathcal{H}_{B_C} \to \mathcal{H}_{B_p} \otimes \mathcal{H}_{X_2} \otimes \mathcal{H}_{B_g}$, with $\dim(\mathcal{H}_{B_p}) = \kappa_2$, $\dim(\mathcal{H}_{B_C}) = \iota_2$, and $\dim(\mathcal{H}_{X_2}) = \Theta_2$.
3) a multiple access dephasing channel $\mathcal{N}\colon \mathcal{H}_{X_1} \otimes \mathcal{H}_{X_2} \to \mathcal{H}_{X_1} \otimes \mathcal{H}_{X_2}$.
4) a unitary operation on Charlie's system $U_C\colon \mathcal{H}_B^{\otimes n} \otimes \mathcal{H}_{C_C} \otimes \mathcal{H}_{X_1} \otimes \mathcal{H}_{X_2} \to \mathcal{H}_{C_p} \otimes \mathcal{H}_{C_g}$, with $\dim(\mathcal{H}_{C_C}) = \iota_3$ and $\dim(\mathcal{H}_{C_p}) = \kappa_3$.

Definition 2. Given a quantum state $\rho^{ABC} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{C})$, a triple (P, R_1, R_2) is said to be achievable, if for all $\epsilon > 0$ and for all sufficiently large n, there exists a distributed purity distillation protocol with parameters $(n, \Theta_1, \Theta_2, \kappa_1, \kappa_2, \kappa_3, \iota_1, \iota_2, \iota_3)$ such that

$$G \triangleq \| \xi^{A_p B_p C_p} - |0\rangle\langle 0|^{A_p} \otimes |0\rangle\langle 0|^{B_p} \otimes |0\rangle\langle 0|^{C_p} \|_1 \leqslant \epsilon,$$
$$\frac{1}{n} \log_2 \Theta_i \leqslant R_i + \epsilon \colon i \in [2],$$
$$\frac{1}{n} \sum_{i \in [3]} (\log_2 \kappa_i - \log_2 \iota_i) \leqslant P + \epsilon,$$

where $|\xi\rangle \triangleq U_C \mathcal{N} U_B U_A |\Psi_\rho^{\otimes n}\rangle^{ABCR}$, and $|\Psi_\rho^{\otimes n}\rangle^{ABCR}$ is a purification of $(\rho^{ABC})^{\otimes n}$. The set of all achievable triples (P, R_1, R_2) is called the achievable rate region.

Given a POVM $M \triangleq \{\Lambda_x^A\}_{x \in \mathcal{X}}$ acting on ρ, the post-measurement state of the reference together with the classical outputs is represented by $(\mathrm{id} \otimes M)(\Psi_{RA}^\rho) \triangleq \sum_{x \in \mathcal{X}} |x\rangle\langle x| \otimes \mathrm{Tr}_A\{(I^R \otimes \Lambda_x^A)\Psi_{RA}^\rho\}$.

Definition 3. Consider a quantum state $\rho^{ABC} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C)$, and a POVM $M_{AB} = \bar{M}_A \otimes \bar{M}_B$ acting on $\mathcal{H}_A \otimes \mathcal{H}_B$ where $\bar{M}_A = \{\bar{\Lambda}_s^A\}_{s \in \mathcal{S}}$ and $\bar{M}_B = \{\bar{\Lambda}_t^B\}_{t \in \mathcal{T}}$. Define the auxiliary states

$$\sigma_1^{RBCS} \triangleq (id_R \otimes \bar{M}_A \otimes id_{BC})(\Psi_\rho^{RABC}),$$
$$\sigma_2^{RACT} \triangleq (id_R \otimes id_{AC} \otimes \bar{M}_B)(\Psi_\rho^{RABC}), \quad \text{and}$$
$$\sigma_3^{RST} \triangleq \sum_{s,t} \sqrt{\rho^{AB}} \left(\bar{\Lambda}_s^A \otimes \bar{\Lambda}_t^B\right) \sqrt{\rho^{AB}} \otimes |s\rangle\langle s| \otimes |t\rangle\langle t|,$$

for some orthonormal sets $\{|s\rangle\}_{s \in \mathcal{S}}$ and $\{|t\rangle\}_{t \in \mathcal{T}}$, where Ψ_ρ^{RABC} is a purification of ρ^{ABC}. Let $\mathcal{R}_b(\rho^{ABC}, M_{AB})$ be defined as the set of all pairs (R_1, R_2) such that there exists finite sets $\mathcal{U}$ and $\mathcal{V}$ and a pair of mappings $f_S : \mathcal{S} \to \mathcal{U}$ and $f_T : \mathcal{T} \to \mathcal{V}$, yielding $U = f_S(S)$, $V = f_T(T)$, and $W = (U, V)$, and the following inequalities are satisfied:

$$R_1 \geqslant I(U; RBC)_{\sigma_1} - I_b(U; V)_{\sigma_3},$$
$$R_2 \geqslant I(V; RAC)_{\sigma_2} - I_b(U; V)_{\sigma_3},$$
$$R_1 + R_2 \geqslant I(U; RBC)_{\sigma_1} + I(V; RAC)_{\sigma_2} - I_b(U; V)_{\sigma_3},$$

where $I_b(\cdot)_\sigma = b \times I(\cdot)_\sigma$

Theorem 1. *Given a quantum state $\rho^{ABC} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C)$, a triple (R_1, R_2, P) is achievable if there exists a POVM $M_{AB} = \bar{M}_A \otimes \bar{M}_B$ acting on $\mathcal{H}_A \otimes \mathcal{H}_B$ with POVMs $\bar{M}_A =$*

$\{\Lambda_s^A\}_{s\in\mathcal{S}}$ and $\bar{M}_B = \{\Lambda_t^B\}_{t\in\mathcal{T}}$ $\mathcal{H}_A \otimes \mathcal{H}_B$ and a real number $b \in [0,1]$ such that the following holds:

$$P \leqslant \kappa(\rho_A) + \kappa(\rho_B) + \kappa(\rho_C) + I(C;U,V)_\sigma - I_b(U;V)_{\sigma_3},$$

and $(R_1, R_2) \in \mathcal{R}_b(\rho^{ABC}, M_{AB})$, where

$$\sigma^{RCST} \triangleq (\mathrm{id}_R \otimes \mathrm{id}_C \otimes \bar{M}_A \otimes \bar{M}_B)(\Psi_\rho^{RABC}).$$

Proof. The proof is provided in Section III. □

Definition 4. Given a quantum state $\rho^{ABC} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C)$, and a dephasing channel with communication links of rates R_1 and R_2 define 1-way distillable distributed local purity $\kappa_{\to}(\rho^{ABC}, R_1, R_2)$ as the supremum of the sum of all the locally distillable purity.

Corollary 1. *Given a quantum state $\rho^{ABC} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C)$, let*

$$\kappa_{\to}^I(\rho^{ABC}, R_1, R_2) \triangleq \kappa(\rho^A) + \kappa(\rho^B) + \kappa(\rho^C) + P_{\to}^D(\rho^{ABC}, R_1, R_2),$$

$$P_{\to}^D(\rho^{ABC}, R_1, R_2) \triangleq \frac{1}{n} \lim_{n\to\infty} \bar{P}_{\to}^D((\rho^{ABC})^{\otimes n}, nR_1, nR_2),$$

$$\bar{P}_{\to}^D(\rho^{ABC}, R_1, R_2) \triangleq \max_{M_{AB}, b\in[0,1]} \{I(C;U,V)_\sigma - I_b(U;V)_\sigma : (R_1, R_2) \in \mathcal{R}_b(\rho^{ABC}, M_{AB})\}.$$

With the above definitions, we have $\kappa_{\to}^I(\rho^{ABC}, R_1, R_2) \leqslant \kappa_{\to}(\rho^{ABC}, R_1, R_2)$. In other words, for any communication rates (R_1, R_2), $\kappa_{\to}^I(\rho^{ABC}, R_1, R_2)$ amount of purity can be jointly distilled from the three parties using the protocol defined in Def. 1.

Proof. The proof follows from Theorem 1 and regularization. □

III. Proof of Theorem 1

The proof is mainly composed of two parts. In the first part, we construct a protocol by developing all the actions of the three parties, and describe them as unitary evolution (as these are the only actions allowed by the protocol, Def. 1). Simultaneously, we also provide necessary lemmas needed for the next part. The second part deals with characterizing the action of the developed unitary operators on the shared quantum state ρ^{ABC} and then bounding the error between the final state and the desired pure state. Since our result is derived for a bounded communication channel, we start by approximating the measurements to achieve a decreased outcome set, while preserving the statistics of the measurement.

A. Approximation of the measurement $M_A \otimes M_B$

We start by generating the canonical ensembles corresponding to M_A and M_B, defined as

$$\lambda_u^A \triangleq \mathrm{Tr}\{\Lambda_u^A \rho^A\}, \quad \lambda_v^B \triangleq \mathrm{Tr}\{\Lambda_v^B \rho^B\},$$
$$\lambda_{uv}^{AB} \triangleq \mathrm{Tr}\{(\Lambda_u^A \otimes \bar{\Lambda}_v^B)\rho^{AB}\}, \quad \text{and}$$
$$\hat{\rho}_u^A \triangleq \frac{1}{\lambda_u^A}\sqrt{\rho^A}\Lambda_u^A\sqrt{\rho^A}, \quad \hat{\rho}_v^B \triangleq \frac{1}{\lambda_v^B}\sqrt{\rho^B}\Lambda_v^B\sqrt{\rho^B},$$
$$\hat{\rho}_{uv}^{AB} \triangleq \frac{1}{\lambda_{uv}^{AB}}\sqrt{\rho^{AB}}(\Lambda_u^A \otimes \Lambda_v^B)\sqrt{\rho^{AB}}. \tag{2}$$

Let Π_{ρ^A} and Π_{ρ^B} denote the δ-typical projectors (as in [12, Def. 15.1.3]) for marginal density operators ρ^A and ρ^B, respectively. Also, for any $u^n \in \mathcal{U}^n$ and $v^n \in \mathcal{V}^n$, let $\Pi_{u^n}^A$ and $\Pi_{v^n}^B$ denote the strong conditional typical projectors (as in [12, Def. 15.2.4]) for the canonical ensembles $\{\lambda_u^A, \hat{\rho}_u^A\}$ and $\{\lambda_v^B, \hat{\rho}_v^B\}$, respectively. For each $u^n \in \mathcal{T}_\delta^{(n)}(U)$ and $v^n \in \mathcal{T}_\delta^{(n)}(V)$ define

$$\tilde{\rho}_{u^n}^{A'} \triangleq \Pi_{\rho^A}\Pi_{u^n}^A\hat{\rho}_{u^n}^A\Pi_{u^n}^A\Pi_{\rho^A}, \quad \tilde{\rho}_{v^n}^{B'} \triangleq \Pi_{\rho^B}\Pi_{v^n}^B\hat{\rho}_{v^n}^B\Pi_{v^n}^B\Pi_{\rho^B},$$

and $\tilde{\rho}_{u^n}^A = 0$, and $\tilde{\rho}_{v^n}^B = 0$ for $u^n \notin \mathcal{T}_\delta^{(n)}(U)$ and $v^n \notin \mathcal{T}_\delta^{(n)}(V)$, respectively, with $\hat{\rho}_{u^n}^A \triangleq \bigotimes_i \hat{\rho}_{u_i}^A$ and $\hat{\rho}_{v^n}^B \triangleq \bigotimes_i \hat{\rho}_{v_i}^B$.

Randomly and independently select $2^{n\tilde{R}_1}$ and $2^{n\tilde{R}_2}$ sequences $(U^n(l), V^n(k))$ according to the pruned distributions, i.e.,

$$\mathbb{P}\left((U^{n,(\bar{\mu}_1)}(l), V^{n,(\bar{\mu}_2)}(k)) = (u^n, v^n)\right) = \begin{cases} \dfrac{\lambda_{u^n}^A}{(1-\varepsilon)}\dfrac{\lambda_{v^n}^B}{(1-\varepsilon')} & \text{for} \quad u^n \in \mathcal{T}_\delta^{(n)}(U), v^n \in \mathcal{T}_\delta^{(n)}(V) \\ 0 & \text{otherwise} \end{cases}, \tag{3}$$

where $\varepsilon = \sum_{u^n\in\mathcal{T}_\delta^{(n)}(U)} \lambda_{u^n}^A$ and $\varepsilon' = \sum_{v^n\in\mathcal{T}_\delta^{(n)}(V)} \lambda_{v^n}^B$. Let $\mathcal{C}$ denote the codebook containing all pairs of codewords $(U^n(l), V^n(k))$.

Further, define $\sigma^{A'}$ and $\sigma^{B'}$ as

$$\sigma^{A'} \triangleq \sum_{u^n\in\mathcal{T}_\delta^{(n)}(U)} \frac{\lambda_{u^n}^A}{(1-\varepsilon)}\tilde{\rho}_{u^n}^{A'}, \quad \sigma^{B'} \triangleq \sum_{v^n\in\mathcal{T}_\delta^{(n)}(V)} \frac{\lambda_{v^n}^B}{(1-\varepsilon')}\tilde{\rho}_{v^n}^{B'}, \tag{4}$$

where $\varepsilon = \sum_{u^n\in\mathcal{T}_\delta^{(n)}(U)} \lambda_{u^n}^A$ and $\varepsilon' = \sum_{v^n\in\mathcal{T}_\delta^{(n)}(V)} \lambda_{v^n}^B$. Note that $\sigma^{A'}$ and $\sigma^{B'}$ defined above are expectations with respect to the pruned distribution [12]. Let $\hat{\Pi}^A$ and $\hat{\Pi}^B$ be the projectors onto the subspaces spanned by the eigenstates of $\sigma^{A'}$ and $\sigma^{B'}$ corresponding to eigenvalues that are larger than $\varepsilon 2^{-n(S(\rho_A)+\delta_1)}$ and $\varepsilon' 2^{-n(S(\rho_B)+\delta_1)}$, where $\delta_1 > 0$ is such that $\mathrm{Tr}(\Pi_{\rho_A}) \leqslant 2^{n(S(\rho_A)+\delta_1)}$, and $\mathrm{Tr}(\Pi_{\rho_B}) \leqslant 2^{n(S(\rho_B)+\delta_1)}$, and $\delta_1 \searrow 0$ as $\delta \searrow 0$. Lastly, define

$$\tilde{\rho}_{u^n}^A \triangleq \hat{\Pi}^A\tilde{\rho}_{u^n}^{A'}\hat{\Pi}^A, \quad \text{and} \quad \tilde{\rho}_{v^n}^B \triangleq \hat{\Pi}^B\tilde{\rho}_{v^n}^{B'}\hat{\Pi}^B.$$

Note that using the Average Gentle Measurement Lemma [12, Lemma 9.4.3], for any given $\epsilon \in (0,1)$, and sufficiently large n and sufficiently small δ, we have

$$\sum_{u^n\in\mathcal{U}^n} \lambda_{u^n}^A \|\hat{\rho}_{u^n}^A - \tilde{\rho}_{u^n}^A\|_1 \leqslant \epsilon, \quad \sum_{v^n\in\mathcal{V}^n} \lambda_{v^n}^B \|\hat{\rho}_{v^n}^B - \tilde{\rho}_{v^n}^B\|_1 \leqslant \epsilon,$$

for all $u^n \in \mathcal{T}_\delta(U)$ and $v^n \in \mathcal{T}_\delta(V)$. (A detailed proof of the statement can be found in [11, Eq. 35].)

Using this, construct operators

$$A_{u^n} \triangleq \gamma_{u^n}\left(\sqrt{\rho_A}^{-1}\tilde{\rho}_{u^n}^A\sqrt{\rho_A}^{-1}\right) \quad \text{and}$$
$$B_{v^n} \triangleq \zeta_{v^n}\left(\sqrt{\rho_B}^{-1}\tilde{\rho}_{v^n}^B\sqrt{\rho_B}^{-1}\right), \tag{5}$$

where

$$\gamma_{u^n} \triangleq \frac{1-\varepsilon}{1+\eta} 2^{-n\tilde{R}_1} |\{l : U^n(l) = u^n\}| \quad \text{and}$$
$$\zeta_{v^n} \triangleq \frac{1-\varepsilon'}{1+\eta} 2^{-n\tilde{R}_2} |\{k : V^n(k) = v^n\}|, \tag{6}$$

where $\eta \in (0,1)$ is a parameter that determines the probability of not obtaining sub-POVMs. Then construct $M_1^{(n)}$ and $M_2^{(n)}$ as in the following

$$M_1^{(n)} \triangleq \{A_{u^n} : u^n \in \mathcal{T}_\delta^{(n)}(U)\},$$
$$M_2^{(n)} \triangleq \{B_{v^n} : v^n \in \mathcal{T}_\delta^{(n)}(V)\}. \tag{7}$$

We show later that $M_1^{(n)}$ and $M_2^{(n)}$ form sub-POVMs, with high probability, These collections $M_1^{(n)}$ and $M_2^{(n)}$ are completed using the operators $I - \sum_{u^n \in \mathcal{T}_\delta^{(n)}(U)} A_{u^n}$ and $I - \sum_{v^n \in \mathcal{T}_\delta^{(n)}(V)} B_{v^n}$, and these operators are associated with sequences u_0^n and v_0^n, which are chosen arbitrarily from $\mathcal{U}^n \backslash \mathcal{T}_\delta^{(n)}(U)$ and $\mathcal{V}^n \backslash \mathcal{T}_\delta^{(n)}(V)$, respectively. Let $\mathbb{1}_{\{\text{sP-i}\}}$ denote the indicator random variable corresponding to the event that $M_i^{(n)}$ form sub-POVM for $i = 1, 2$. We use the trivial POVM $\{I\}$ in the case of the complementary event and associate it with u_0^n and v_0^n as the case maybe. In summary, the POVMs are given by $\{\mathbb{1}_{\{\text{sP-1}\}} A_{u^n} + (1 - \mathbb{1}_{\{\text{sP-1}\}}) \mathbb{1}_{\{u^n = u_0^n\}} I\}_{u^n \in \mathcal{U}^n}$, and $\{\mathbb{1}_{\{\text{sP-2}\}} B_{v^n} + (1 - \mathbb{1}_{\{\text{sP-2}\}}) \mathbb{1}_{\{v^n = v_0^n\}} I\}_{v^n \in \mathcal{V}^n}$.

Now, we intend to use the completions $[M_1^{(n,\bar{\mu}_1)}]$ and $[M_2^{(n,\bar{\mu}_2)}]$ in constructing the unitaries U_A and U_B, as described in the protocol (Def. 1), for Alice and Bob, respectively. Note that the above constructed POVMs are different from Winter's POVMs, in that they do not have the cut-off operators. Before concluding the discussion on the POVMs, we provide two lemmas which would be useful in the sequel. The first lemma deals with bounding from below the probability that the constructed collection of operators indeed form a sub-POVM, and is as follows.

Lemma 1. *For any $\epsilon \in (0,1)$, any $\eta \in (0,1)$, any $\delta \in (0,1)$ sufficiently small, and any n sufficiently large, we have*

$$\frac{1}{\tilde{N}_1 \tilde{N}_2} \sum_{\tilde{\mu}_1, \tilde{\mu}_2} 2\Big(1 - \mathbb{E}\Big[\mathbb{1}_{\{sP\text{-}1\}} \mathbb{1}_{\{sP\text{-}2\}}\Big]\Big) < 2\epsilon,$$

if $\tilde{R}_1 > I(U;RB)_{\sigma_1}$ and $\tilde{R}_2 > I(V;RA)_{\sigma_2}$, where σ_1, σ_2 are defined as in the statement of the theorem.

Proof. The proof is provided in [13]. □

The second lemma provides a unitary to show closeness of the post-measurement states obtained from approximating measurements and the actual measurements. Note that the faithful simulation results [9]–[11] show the closeness of states in the reference system, but the current result proves the closeness of the post-measurement states. The main elements of the proof is in identifying appropriate purifications and using the Uhlmann's Theorem [12]. The lemma is as follows.

Lemma 2. *Using the above definitions, for all $(u^n, v^n) \in \mathcal{C}$ let*

$$|\hat{\sigma}_{u^n}\rangle^{AE} \triangleq \frac{(I^E \otimes \sqrt{\Lambda_{u^n}^A})\,|\Psi_{\rho^{\otimes n}}\rangle^{ABCR}}{\sqrt{\lambda_{u^n}^A}},$$
$$|\tilde{\sigma}_{u^n}\rangle^{AE} \triangleq \frac{(I^E \otimes \sqrt{A_{u^n}})\,|\Psi_{\rho^{\otimes n}}\rangle^{ABCR}}{\sqrt{\gamma_{u^n}}},$$

($|\hat{\sigma}_{v^n}\rangle^{BF}$ and $|\tilde{\sigma}_{v^n}\rangle^{BF}$ defined analogously) where E and F denotes the system BCR and ACR, respectively, then for each $l \in [2^{n\tilde{R}_1}]$ and $k \in [2^{n\tilde{R}_2}]$ there exists a pair of unitaries $U_r^A(l)$ and $U_r^B(k)$, such that

$$F(|\hat{\sigma}_{u^n}\rangle^{AE}, (I^E \otimes U_r^A(l))|\tilde{\sigma}_{u^n}\rangle^{AE}) \geqslant \Big(1 - \frac{1}{2}\|\hat{\rho}_{u^n}^A - \tilde{\rho}_{u^n}^A\|_1\Big)^2,$$
$$F(|\hat{\sigma}_{v^n}\rangle^{BF}, (I^F \otimes U_r^B(k))|\tilde{\sigma}_{v^n}\rangle^{BF}) \geqslant \Big(1 - \frac{1}{2}\|\hat{\rho}_{v^n}^B - \tilde{\rho}_{v^n}^B\|_1\Big)^2.$$

Proof. The proof is provided in the detailed version [13]. □

We now move on to characterizing the unitaries U_A and U_B.

B. Action of Alice and Bob

Using the approximating POVMs constructed above, as a first unitary Alice and Bob implements the coherent version of the approximating POVM defined as

$$U_M^A \triangleq \sum_{l \in [2^{n\tilde{R}_1}]} \sqrt{A_{U^n(l)}} \otimes |l\rangle, \quad U_M^B \triangleq \sum_{k \in [2^{n\tilde{R}_2}]} \sqrt{B_{V^n(k)}} \otimes |k\rangle.$$

Although the operators defined above are isometry operators, but with the help of additional catalyst qubits, these can be implemented as unitary operators. Now, to extract purity from the states obtained after performing the measurements we employ the approach of [8]. More formally, we define the collection of unitaries $\{U_p^A(l)\}_{l \in [2^{n\tilde{R}_1}]}$ and $\{U_p^B(k)\}_{k \in [2^{n\tilde{R}_2}]}$ as the unitaries that can extract purity for the collection of states $\{\hat{\sigma}_l^A\}_{l \in [2^{n\tilde{R}_1}]}$ and $\{\hat{\sigma}_k^B\}_{k \in [2^{n\tilde{R}_2}]}$, respectively. Note that since $\hat{\sigma}_l^A$ and $\hat{\sigma}_k^B$ and product states, the approach of [8] can be followed in a straight-forward manner in designing the unitaries $U_p^A(l)$ and $U_p^B(k)$, respectively. However, note that since the approximating measurements are not rank-one operators, $U_p^A(l)$ and $U_p^B(k)$ will act on not necessarily separable states. Therefore, we provide the following lemma which ensures that the state of the remaining sub-systems is only slightly disturbed after distilling purity from a given sub-system.

Lemma 3. *Consider the above defined joint state ρ^{ABC}. Let $\mathcal{N}$ be any CPTP map capable of concentrating local purity out of the n-letter state $(\rho^A)^{\otimes n}$, while using additional catalytic ancilla, returned at the end of the protocol, i.e., $\|\mathcal{N}(\rho_A^{\otimes n}) - |0\rangle\langle 0|_{A_p}\|_1 \leqslant \epsilon$ for any ϵ, some sub-system $\mathcal{H}_{A_p}$ and sufficiently large n, then*

$$\|(\mathcal{N} \otimes I^{BCR})\Psi_{\rho^{\otimes n}}^{ABCR} - \rho_{BCR}^{\otimes n} \otimes |0\rangle\langle 0|_{A_p}\| \leqslant 2\epsilon, \tag{8}$$

where Ψ_ρ^{ABCR} is the canonical purification of ρ^{ABC}, $\rho_A \triangleq \mathrm{Tr}_{BCR}\{\rho^{ABCR}\}$, and $\rho_{BCR} \triangleq \mathrm{Tr}_A\{\rho^{ABCR}\}$.

Proof. The proof is provided in [13]. □

Now we characterize the complete action at Alice and Bob as

$$U_A \triangleq U_P^A U_R^A U_M^A \quad \text{and} \quad U_B \triangleq U_P^B U_R^B U_M^B, \tag{9}$$

where U_P^A and U_R^A are controlled unitaries defined as

$$U_P^A \triangleq \sum_{l\in[2^{n\tilde{R}_1}]} U_p^A(l)\otimes |l\rangle\langle l|\,, \quad U_R^A \triangleq \sum_{l\in[2^{n\tilde{R}_1}]} U_r^A(l)\otimes |l\rangle\langle l|\,,$$

and similar is true for U_P^B and U_R^B. This gives

$$U_A = \sum_{l\in[2^{n\tilde{R}_1}]} U_p^A(l)U_r^A(l)\sqrt{A_{U^n(l)}}\otimes|l\rangle$$

$$U_B = \sum_{k\in[2^{n\tilde{R}_2}]} U_p^B(k)U_r^B(k)\sqrt{B_{V^n(k)}}\otimes|k\rangle$$

Finally, let

$$|\Psi_1\rangle^{ABCRLK} \triangleq (I^{CR}\otimes U_A\otimes U_B)\,|\Psi_{\rho^{\otimes n}}\rangle^{ABCR}$$

C. Transmission over the Dephasing Channel $\mathcal{N}$

Before we proceed to employ the dephasing channel, observe that the classical registers created by the coherent measurement contains correlations across Alice and Bob. These correlations could be exploited which can further reduce the communication needed over the dephasing channel. For this, we employ the traditional binning operation. Begin by fixing the binning rates (R_1, R_2), with $R_1 \leqslant \tilde{R}_1$ and $R_2 \leqslant \tilde{R}_2$. For each sequence $u^n \in \mathcal{T}_\delta^{(n)}(U)$ assign an index from $[1, 2^{nR_1}]$ randomly and uniformly, such that the assignments for different sequences are done independently. Perform a similar random and independent assignment for all $v^n \in \mathcal{T}_\delta^{(n)}(V)$ with indices chosen from $[1, 2^{nR_2}]$. For each $i \in [1, 2^{nR_1}]$ and $j \in [1, 2^{nR_2}]$, let $\mathcal{B}_1(i)$ and $\mathcal{B}_2(j)$ denote the i^{th} and the j^{th} bins, respectively. More precisely, $\mathcal{B}_1(i)$ is the set of all u^n sequences with assigned index equal to i, and similar is $\mathcal{B}_2(j)$. Also, note that the effect of the binning is in reducing the communication rates from $(\tilde{R}_1, \tilde{R}_2)$ to (R_1, R_2). Moreover, let $\iota_1 : \mathcal{T}_\delta^{(n)}(U) \to [1, 2^{nR_1}]$, and $\iota_2 : \mathcal{T}_\delta^{(n)}(V) \to [1, 2^{nR_2}]$, denote the corresponding random binning functions. With this, we can denote $|l\rangle$ for $l \in [2^{n\tilde{R}_1}]$ as $|l\rangle_L = |\iota_1(l)\rangle_{L_1}|\beta_U(l)\rangle_{L_2}$ and similarly, $|k\rangle$ for $k \in [2^{n\tilde{R}_2}]$ as $|k\rangle_K = |\iota_2(k)\rangle_{K_1}|\beta_V(k)\rangle_{K_2}$[1], where the functions β_U and β_V describe the remaining $\tilde{R}_1 - R_1$ and $\tilde{R}_2 - R_2$ qubits, respectively. Now the qubits in the state $|\iota_1(\cdot)\rangle$ and $|\iota_2(\cdot)\rangle$ are sent over the multiple-access dephasing channel $\mathcal{N}$, each requiring rates of R_1 and R_2 qubits, respectively. Let

$$\sigma^{ABCRLK} \triangleq \mathcal{N}({\Psi_1}^{ABCRLK}).$$

With this, we move on to describing the action Charlie.

[1]Note that $\iota_1(l) = \iota_1(U^n(l))$, and similar holds for the functions $\iota_2, \beta_U, \beta_V$.

D. Action of Charlie

Charlie begins by undoing the binning operation. For this, let

$$D_{i,j} \triangleq \{(u^n, v^n) \in \mathcal{C} : (u^n, v^n) \in \mathcal{T}_\delta^{(n)}(UV) \text{ and } (u^n, v^n) \in \mathcal{B}_1(i)\times\mathcal{B}_2(j)\}.$$

For every $i \in [1, 2^{nR_1}]$ and $j \in [1, 2^{nR_2}]$ define the function $F(i,j) = (u^n, v^n)$ if (u^n, v^n) is the only element of $D_{i,j}$; otherwise $F(i,j) = (u_0^n, v_0^n)$ Further, $F(i,j) = (u_0^n, v_0^n)$ for $i = 0$ or $j = 0$. Using the qubits received from Alice and Bob, and the above definition of $F(i,j)$, Charlie aims at undoing the binning operations. This can be characterized as an isometric map $U_F^C : \mathcal{H}_{Y_1}\otimes\mathcal{H}_{Y_1} \to \mathcal{H}_{Y_1}\otimes\mathcal{H}_{Y_1}\otimes\mathcal{H}_F$ defined as

$$U_F^C \triangleq \sum_{i\in[2^{nR_1}]}\sum_{j\in[2^{nR_2}]} |i, j, F(i,j)\rangle\langle i, j|\,, \tag{10}$$

where $\dim(\mathcal{H}_F) = R_{tb} \triangleq \tilde{R}_1 - R_1 + \tilde{R}_2 - R_2$. Note that, since binning decreased the total number of qubits transmitted by R_{tb}, to implement the above isometry, Charlie would need R_{tb} number of additional catalytic qubits present in the pure state. As the protocol allows for the use of additional catalysts, as long as they are returned successfully, such an isometry can be implemented as a unitary.

Remark 1. As will be shown in the sequel, the error analysis gives an upper bound on R_{tb}. As this is only an upper bound, one can choose to not bin at the maximum rate and can save on the catalytic qubits needed. However, this would increase the communication rates by equivalent factors. This is modelled in the theorem statement using the real number $b \in [0,1]$. Therefore, we observe a continuous trade-off between the distillable purity and classical communication, which was not prominent in the two-party setup [8] (although, time-sharing between P at $R = 0$ and P at maximum allowable R could give one such trade-off).

After the complete identification of the measurement outcomes of Alice and Bob, Charlie now extracts the purity from her state, conditioned on these outcomes. For this, she develops an collection of unitaries $\{U_p^C(k,l)\}_{l\in[2^{n\tilde{R}_1}],k\in[2^{n\tilde{R}_2}]}$, analogous to the earlier ones, using the approach of [8]. Further, she constructs the controlled unitary U_P^C defined as

$$U_P^C \triangleq \sum_{l\in[2^{n\tilde{R}_1}]}\sum_{k\in[2^{n\tilde{R}_2}]} U_p^C(k,l)\otimes|l,k\rangle\langle l,k|\,. \tag{11}$$

This characterizes Charlie's unitary as $U_C = U_P^C U_F^C$, and gives

$$\xi^{ABCRLK} \triangleq (I\otimes U_P^C U_F^C)\sigma^{ABCRL_1K_1}(I\otimes U_P^C U_F^C)^\dagger.$$

At this point, we have the characterized the actions of all the three parties as unitary operations. The next step is to measure the distance between the obtained state and the desired pure state, and establish the G can be made arbitrary small. For the remainder of the proof, we direct the interested readers to detailed version of the manuscript [13] where the complete analysis is provided.

REFERENCES

[1] R. Alicki, M. Horodecki, P. Horodecki, and R. Horodecki, "Thermodynamics of quantum information systems—hamiltonian description," *Open Systems & Information Dynamics*, vol. 11, no. 3, pp. 205–217, 2004.

[2] M. Horodecki, P. Horodecki, R. Horodecki, J. Oppenheim, A. Sen, U. Sen, B. Synak-Radtke *et al.*, "Local versus nonlocal information in quantum-information theory: formalism and phenomena," *Physical Review A*, vol. 71, no. 6, p. 062307, 2005.

[3] J. Oppenheim, M. Horodecki, P. Horodecki, and R. Horodecki, "Thermodynamical approach to quantifying quantum correlations," *Physical review letters*, vol. 89, no. 18, p. 180402, 2002.

[4] M. Horodecki, K. Horodecki, P. Horodecki, R. Horodecki, J. Oppenheim, A. Sen, U. Sen *et al.*, "Local information as a resource in distributed quantum systems," *Physical review letters*, vol. 90, no. 10, p. 100402, 2003.

[5] M. Horodecki, P. Horodecki, and J. Oppenheim, "Reversible transformations from pure to mixed states and the unique measure of information," *Physical Review A*, vol. 67, no. 6, p. 062104, 2003.

[6] I. Devetak, "Distillation of local purity from quantum states," *Physical Review A*, vol. 71, no. 6, p. 062303, 2005.

[7] I. Devetak and A. Winter, "Distilling common randomness from bipartite quantum states," *IEEE Transactions on Information Theory*, vol. 50, no. 12, pp. 3183–3196, 2004.

[8] H. Krovi and I. Devetak, "Local purity distillation with bounded classical communication," *Physical Review A*, vol. 76, no. 1, p. 012321, 2007.

[9] A. Winter, ""Extrinsic" and "intrinsic" data in quantum measurements: asymptotic convex decomposition of positive operator valued measures," *Communication in Mathematical Physics*, vol. 244, no. 1, pp. 157–185, 2004.

[10] T. A. Atif, M. Heidari, and S. S. Pradhan, "Faithful simulation of distributed quantum measurements with applications in distributed rate-distortion theory," *IEEE Transactions on Information Theory*, 2021.

[11] M. M. Wilde, P. Hayden, F. Buscemi, and M.-H. Hsieh, "The information-theoretic costs of simulating quantum measurements," *Journal of Physics A: Mathematical and Theoretical*, vol. 45, no. 45, p. 453001, 2012.

[12] M. M. Wilde, "From classical to quantum shannon theory," *arXiv preprint arXiv:1106.1445*, 2011.

[13] T. A. Atif and S. S. Pradhan, "Multi-party quantum purity distillation with bounded classical communication," *arXiv preprint arXiv:2203.05511*, 2022.