One-shot Multiparty Purity Distillation

SuSTech-Nagoya workshop on Quantum Science

Aditya Nema
Jointly with: Sayantan Chakraborty (CQT-NUS) and Francesco Buscemi (Nagoya University)

2^{nd} June, 2022

A very high level problem description:

→ Single party:
Given a quantum mixed state ρ^A how much purity can Alice distill by application of only local unitaries ? (Devetak, 2004)

→ Two parties:
Given a mixed quantum state ρ^{AB} where state on system A is with Alice and that on B is with Bob, what is the amount of **TOTAL** purity that can Alice and Bob can distill using only local unitaries ?

→ Multi-party generalization
Given a multipartite density matrix $\rho^{A_1,A_2,\ldots,A_n}$,where n parties $A_1, \ldots, A_n$ are given the marginal states each, how much **TOTAL** purity can they distill by application of only local unitaries ?

A detailed description of the problem:

Given a density matrix (say to Alice) ρ^A on an $|A|$ dimensional Hilbert space :

- Distill purity $\Leftrightarrow$ Extract pure states, specifically $|0\rangle^{A_p}$ where $|A_p| \leq |A|$.
  Trivial checks: $|A_p| = |A| \Rightarrow \rho^A = |0\rangle^A \langle 0|$; $|A_p| = 0 \Rightarrow \rho^A = \frac{I^A}{|A|}$.
- Allowed operations to Alice: Only a unitary operator on A;
  If Alice wish to use ancilla, then she can do so *only catalytically*, i.e., with a promise to return it at the end of the protocol.
- **Pure state**$\Leftrightarrow$ $|0\rangle$; since, any other pure state can be created by applying another local unitary.
  Aliter: Not charged for local unitary operations.
- Multi-party case: Allow unidirectional classical communication.
  (Reason to be described shortly!)

Single Party Case: (aka Local Protocol)

Aim: Find maximum $\log|A_p|$ s.t. for a small $\epsilon > 0$:

$$\| U^A \rho^A (U^\dagger)^A - |0\rangle\langle 0|^{A_p} \otimes \rho'^{A/A_p} \|_1 \le \epsilon \quad (1)$$

Definition: A rate $R := \log|A_p|$ is said to be ϵ-achievable for one-shot purity distillation protocol $\iff$ $\exists$ a unitary U^A that satisfies Eq (1).

Theorem

Given a state ρ^A and $\epsilon > 0$, there exists a unitary on the system $A \to A_p \otimes A_q$ such that: $\| U \rho U^\dagger - (\Pi \rho \Pi)^{A_q} \otimes |0\rangle\langle 0|^{A_p} \|_1 \le \epsilon$ and

$$\boxed{R = \log|A_p| = \log|A| - \widetilde{H}^{\epsilon}_{\max}(A)_\rho}, \textit{ where}$$

$$\boxed{\widetilde{H}^{\epsilon}_{\max}(A)_\rho := \log \operatorname{supp}(\rho'^A)}$$

ρ'^A is the matrix obtained by zeroing out the smallest eigen vectors of ρ that sum up to $\le \epsilon$.

Proof of local protocol

$$A \cong A_p \otimes A_q : A_q = \text{eigen space}(\rho') \text{ (thm. above)}.$$

- Thus, $|A_q| = 2^{\widetilde{H}^{\epsilon}_{\max}(A)_\rho}$.
- Π projector onto $A_q \rightarrow (1-\epsilon)$ probability eigen space(ρ) :

$$\mathbf{Tr}(\mathbf{\Pi}) = |\mathbf{A_q}|;\ \mathrm{Tr}\left[\mathbf{\Pi}\rho\right] \geq \mathbf{1} - \epsilon.$$

- $\because [\Pi, \rho] = 0 \Rightarrow A_q \cong$ eig. space$(\Pi\rho\Pi)$.
  Hence, eigen vectors $\{|i\rangle^{A_q}\}$ of $\Pi\rho\Pi \in \mathit{Basis}(A_q)$.
- Let $\{|i'\rangle^{A}\}_{i' \in A}$ = eigen vectors(ρ^A).
  $\because [\Pi, \rho] = 0 \Rightarrow \exists$ embedding from $\mathrm{span}\ \{|i\rangle^{A_q}\}$ into $\mathrm{span}\ \{|i'\rangle^{A}\}$ as:

Proof of local protocol

$$\boxed{U : A \to A_p \otimes A_q : |i'\rangle^A \mapsto |i\rangle^{A_q} |0\rangle^{A_p} ; U(\Pi\rho\Pi)^A U^\dagger = (\Pi\rho\Pi)^{A_q} \otimes |0\rangle\langle 0|^{A_p} .}$$

$$\|\rho^A - (\Pi\rho\Pi)^A\|_1 \le \epsilon \Rightarrow \|(U\rho U^\dagger)^A - (\Pi\rho\Pi)^{A_q} \otimes |0\rangle\langle 0|^{A_p}\|_1 \underset{inv.}{\overset{uni.}{\le}} 2\sqrt{\epsilon}$$

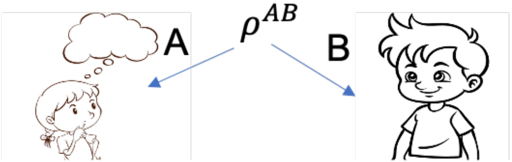
$$R = \log|A_p| = \log\frac{|A|}{|A_q|} = \log|A| - \widetilde{H}^{\epsilon}_{\max}(A)_\rho \quad [QED]$$

- Devetak (2004) showed that in asymptotic iid setting:

$$\max \mathbf{R} = \log|\mathbf{A}| - \mathbf{H}(\mathbf{A})_\rho, \text{ with a matching converse.}$$

- In either one-shot and asymptotic iid case, R=0, if $\rho = \frac{I}{|A|}$ (intuitively).

Purity distillation from a BIPARTITE state



Alice and Bob want to distill max # pure states from their respective halves of ρ^{AB}.

- Naively, if they apply the local (single party) protocol, they can distill a total purity of $\boxed{\log|A| - \widetilde{H}^{\epsilon}_{max}(A)_\rho + \log|B| - \widetilde{H}^{\epsilon}_{max}(B)_\rho}$.
- Can classical correlations help to increase the rate?
- e.g. let $|A| = |B| = 2, \epsilon < \frac{1}{2}$; $\rho^{AB} = \frac{|0\rangle\langle 0|^A \otimes |0\rangle\langle 0|^B}{2} + \frac{|1\rangle\langle 1|^A \otimes |1\rangle\langle 1|^B}{2}$, then $\widetilde{H}^{\epsilon}_{max}(A)_\rho = 1 = \widetilde{H}^{\epsilon}_{max}(B)_\rho$. $\Rightarrow R_{AB} = 0$ by local protocol!
- If classical communication is allowed from Alice $\rightarrow$ Bob, then Alice can simply send her A system to Bob and the Bob can apply the controlled unitary CNOT on A(rx. from Alice),B. Then, Alice distills 0 purity but Bob distills 1 bit of purity and $R_{AB} = 1$!!

Purity distillation from a BIPARTITE state

- Can do better by utilizing classical correlations in ρ^{AB}.
- A way to create such a classical correlated state is via measurement!
- Thus, further allowed: catalytic use of ancilla for Alice; Alice $\xrightarrow[\text{communication}]{\text{1-way classical}}$ Bob; Alice can perform measurements, leading to:

Theorem

Given $\rho^{AB} \xrightarrow{\text{purification}} |\rho\rangle^{RAB}$. A one-shot achievable total rate for distilling purity under the above conditions is:

$$R_{AB} = \log|A||B| - I^{\epsilon}_{\max}(X:RB) - \widetilde{H}^{\epsilon}_{\max}(B) + I^{\epsilon_0/2}_{H}(X:B) + 0(\epsilon,\epsilon_0) - O(1)$$

for a given $\epsilon > 0$ and $\epsilon_0 = O(\epsilon)$ and the above entropic quantities are evaluated wrt the $\rho^{XRB} = (I^{RB} \otimes \Lambda^{A})|\rho\rangle^{RAB}$, where Λ^A are rank one measurement operators on A. The maximum achievable rate can be obtained by optimizing over the Λ^A.

Purity distillation from a BIPARTITE state

- Asymptotic iid rate (with a matching converse, Devetak, 2004)

$$= \log|A| - H(A) + \log|B| - H(B) + \lim_{n\to\infty} \frac{\max_{\text{rank 1-POVM: } \Lambda^A} I(X^n;B^n)_{(I^B\otimes\Lambda^A)^{\otimes n}(\rho^{AB})^{\otimes n}}}{n}$$

Protocol for one-shot achievability:

Step 1: Alice applies normalized rank 1-POVM $\Lambda^A = \{|\psi_x\rangle\langle\psi_x|\}_{\{x\in\mathcal{X}\}}$ on her system A "coherently" by borrowing $\log|\mathcal{X}|$ ancilla $\to$ applies unitary: $U_1^{AX} : |0\rangle^X |\rho\rangle^{ABR} (\stackrel{\text{Schmidt}}{=} \sum_i \lambda_i |i\rangle^A |\varphi_i\rangle^{BR}) \mapsto$
$\sum_{x,i} |x\rangle^X (|\psi_x\rangle\langle\psi_x| |a_i\rangle)^A |\tilde{\varphi}_i\rangle^{RB} = \sum_x |x\rangle^X |\psi_x\rangle^A |\tilde{\varphi}_x\rangle^{RB}$.

Step 2: Alice now applies controlled unitary
$\sum_x |x\rangle\langle x|^X \otimes U_x^A : |x\rangle^X |\psi_x\rangle^A \mapsto |x\rangle^X |0\rangle^A$, thus distilling
$\log|A| - \log|\mathcal{X}|$ purity. (**Note:** $\log|\mathcal{X}|$ catalyst is be returned.)
Remark: Now the state is $\sum_x |x\rangle^A |\tilde{\varphi}_x\rangle^{RB} \Rightarrow I(X;RB) = H(A)_\rho$.

Step 3: Alice $\xrightarrow[\text{measure}]{\{|x\rangle\}} \tau^{XB} = \sum_x p_X(x) |x\rangle\langle x|^X \otimes \rho_x^B$.
Note: $\tau^B = \sum_x p_X(x)\rho_x^B = \rho^B$ (unaltered).

Purity distillation from a BIPARTITE state

• Alice $\xrightarrow[\text{on X}]{\text{local protocol}} \tau^{XB}$ & further distill: $\log|\mathcal{X}| - \widetilde{H}^{\epsilon}_{\max}(X)_{p_X}$ purity.

Alice's $\xrightarrow[\text{purity}]{\text{overall}} \log|A| - \log|\mathcal{X}| + \log|\mathcal{X}| - \tilde{H}^{\epsilon}_{max}(X) = \log|A| - \tilde{H}^{\epsilon}_{max}(X)$.

• Resultant state ($\mathcal{S} = (1-\epsilon)$ prob. subset of $x's$ under p_X):

$\sigma^{X_1B} = \frac{\sum_{x\in\mathcal{S}} P_X(x)|x\rangle\langle x|^{X_1}\otimes\rho^B_x}{\mathrm{Tr}[\Pi_{\mathcal{S}}\tau]}$; $\Pi_{\mathcal{S}}$: proj.($\mathcal{S}$). Alice now aims at transferring these correlations to Bob for him to be able to distill some purity from these classical correlations.

Naively: Alice sends X_1 to Bob and Bob tries to distill purity from X_1!

Won't work naively: $\mathcal{S}$ is a high prob. set, with almost no redundancies.

What else can Bob do to distill purity from classical correlations?

New idea: One shot classical data compression with quantum side information.

Tool: One-shot classical data-compression with quantum side information

Lemma (Chakraborty et al., 2022)

Given $\rho^{XB} = \sum_x P_X(x) \left|x\right\rangle \left\langle x\right|^X \otimes \rho_x^B \ \exists$ *bijection* $\sigma : \mathcal{X} \to [M] \times [N]$, *s.t.*

1. *for* $\epsilon > 0$, $\log |N| \leq I_H^\epsilon(X : B) + 2 \log \epsilon$;
2. $\rho^{XB} \xrightarrow{\sigma} \sum_{m,n} P_{MN}(m,n) \left|m,n\right\rangle \left\langle m,n\right|^{MN} \otimes \rho_{mn}^B$; *then* $\forall m \in [M] \ \exists$ *a POVM* $\Theta_n(m)$ *s.t. for* $\epsilon_0 := O(\epsilon^{1/4})$

$$\sum_{m,n} P_{MN}(m,n) \|\rho_{mn}^B - \sqrt{\Theta_n(m)}\rho_{mn}^B\sqrt{\Theta_n(m)}\|_1 \leq \epsilon_0.$$

Proof: Binning at the encoder; one-shot cq packing lemma at the decoder.

Corollary

For $\rho^{MNB} \ \exists$ *a unitary* W^{MNB}: $\|\mathrm{Tr}_{BM}\left(W^{MNB} \cdot \sigma^{MNB}\right) - \left|0\right\rangle\left\langle 0\right|^N\|_1 \leq 2\epsilon_0$

Purity distillation from a BIPARTITE state, contd..

Step 4: $\tau^{X_1 B} \xrightarrow[\text{bij.}\sigma]{\text{Alice}} \sigma^{MNB} = \sum_{m,n} P_{MN}(m,n) \left|m,n\right\rangle \left\langle m,n\right|^{MN} \otimes \rho^B_{mn}$

s.t. $\log|N| \leq I_H^{\sqrt{\epsilon_0}}(X_1 : B) + \log \epsilon_0$; $\xrightarrow{MN}$ Bob using $\tilde{H}^{\epsilon}_{\max}(X)$ bits.

Step 5: Bob applies unitary W^{MNB} from Cor. [4] and extracts $\log|N| \approx I_H^{\sqrt{\epsilon_0}}(X_1 : B) + \log \epsilon_0$ purity. Further, by lemma [3] and cor. [4] and fact that $\mathcal{S}$ being a high prob. set implies: (non-trivial)

$$\|\sum_x p_X(x)\rho^B_x - \frac{1}{\mathrm{Tr}\,[\Pi_{\mathcal{S}}\tau]} \sum_{x\in\mathcal{S}} p_X(x)\rho^B_x\|_1 \leq O(\epsilon_0^{1/8}).$$

$\Rightarrow$ Bob's state $\approx \rho^B$; Distills $I_H^{\sqrt{\epsilon_0}}(X_1; B)$ purity.

> Lemma: $I_H^{\sqrt{\epsilon_0}}(X_1 : B)_{\sigma^{X_1 B}} \geq I_H^{\epsilon_0/2}(X : B)_{\rho^{XB}} - O(1) + O(\log(1-\epsilon_0))$

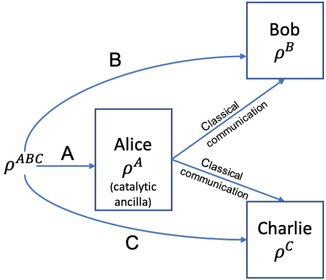
Step 6: Bob now applies the local protocol on approximate version of his local state and distill $\log|B| - \tilde{H}^{\epsilon}_{\max}(B)$ purity.

Thus, $\boxed{R_{AB} \overset{(\epsilon,\epsilon_0)}{\approx} \log|A| - \tilde{H}^{\epsilon}(X) + I_H^{\epsilon_0/2}(X : B) + \log|B| - \tilde{H}^{\epsilon}_{\max}(B)}$.

Bipartite purity distillation and further

- Can recover the aysmptotic iid rate $\because$ entropic quantities are smooth.
- The amount of classical communication $\log|supp(X_1)| = \tilde{H}^{\epsilon}_{\max}(X)_{p_X}$.
  Can we save on this?
  YES! By using a modification to a recent **one-shot measurement compression** (Chakraborty et al., 2022).
  Idea: Come up with a smaller outcome rank 1-measurement, $\{\widetilde{\Lambda_y}^A\}_{\{y\in\mathcal{Y}\}}$, $|\mathcal{Y}| \leq |\mathcal{X}|$ from Λ^A :
  $\boxed{I_H^{\sqrt{\epsilon_0}}(Y:B)_\sigma \geq I_H^{\epsilon_0/2}(X:B)_\rho - O(1) + O(\log(1-\epsilon_0))}$ and find a high prob. set (under p_Y obtained from $\widetilde{\Lambda}$) $\mathcal{S}_\mathcal{Y} : |\mathcal{S}_\mathcal{Y}| \leq 2^{I^{\epsilon}_{\max}(X:RB)_{\rho^{XRB}}}$.
- $\Rightarrow$ Catalytic ancilla $\downarrow$-classical communication $\downarrow$ and Alice's purity from correlations $\uparrow$ to $\log|\mathcal{Y}| - I^{\epsilon}_{\max}(X:RB)_{\rho^{XRB}}$.

Purity distillation from a BIPARTITE state



Alice, Bob and Charlie want to distill max # pure states from their respective parts of ρ^{ABC}.

- Need: A multiparty version of classical data compression with quantum side information at Bob and Charlie, respectively. Can modify a similar theorem from Chakraborty et al. (2022).
- Proposed rate is:

$$R_{ABC} \overset{\epsilon,\epsilon_0,\epsilon_1}{\approx} \log|A| - I^{\epsilon}_{\max}(X, Y : B, C)$$
$$+ \log|B| - \tilde{H}^{\epsilon}_{\max}(B) + I^{\epsilon_0}_{H}(X : B) + \log|C| - \tilde{H}^{\epsilon}_{\max}(C) + I^{\epsilon_1}_{H}(Y : C)$$

Conclusion and Future Prospects

- We have obtained the rate for one-shot purity distillation of pure states of form $|0\rangle\langle 0|$.
  - We have used a modified version of the recent one-shot measurement compression theorem.
  - We have used the strategy for classical data compression with quantum side information.
  - Using the insights from above two lemmas, we have shown inequalities between the entropic quantities that show up in the rate expression.
- **Ongoing Work:** To prove the suggested rate for the tripartite case and in general, for the multipartite case.
- **For future work:** Investigate if this protocol or some minor variant of it can serve as an operational meaning to the so-called Grünwald information gain. This is definfined as: $H(R)_\sigma - H(B|X)_\sigma$ for the state $\sigma^{RXB} := \sum_x \Lambda_x^{A\to B}(|\rho\rangle^{RA}) \otimes |x\rangle\langle x|^X$, where $\Lambda^{A\to BX}$ is a quantum instrument.

Thank you and Questions ??
(To be out on arXiv shortly!!)