4. Entanglement conversion & quantification

a) Introduction & Setup

Entanglement $\equiv$ what cannot be changed by local operations & classical communication (LOCC)

Q: When can we convert ent. states into each other w/ LOCC?

Relevance:

- Different protocols might required different ("cheaper"/ "more expensive") entangled states.
- Use to quantify entanglement in terms of some reference state; How many "e-bits" $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ are contained in a state?

Known: same Schmidt coefficients $\Leftrightarrow$ related by local unitary $\Leftrightarrow$ same entanglement

What if Schmidt coeffs different?

Example: $|\chi\rangle = \sqrt{\frac{2}{3}}|00\rangle + \sqrt{\frac{1}{3}}|11\rangle$; $|\phi^+\rangle = \sqrt{\frac{1}{2}}|00\rangle + \sqrt{\frac{1}{2}}|11\rangle$

1. Can we convert $|\phi^+\rangle \longrightarrow |\chi\rangle$?

A does POVM $\{\Pi_0, \Pi_1\}$; $\Pi_0 = \begin{pmatrix} \sqrt{2/3} & \\ & \sqrt{1/3} \end{pmatrix}$; $\Pi_1 = \begin{pmatrix} \sqrt{1/3} & \\ & \sqrt{2/3} \end{pmatrix}$.

$\Rightarrow$ post-meas. states $|\tilde{\psi}_k\rangle = \Pi_k |\phi^+\rangle$:

$|\tilde{\psi}_0\rangle = \frac{1}{\sqrt{2}}\left(\sqrt{\frac{2}{3}}|00\rangle + \sqrt{\frac{1}{3}}|11\rangle\right)$; $|\tilde{\psi}_1\rangle = \frac{1}{\sqrt{2}}\left(\sqrt{\frac{1}{3}}|00\rangle + \sqrt{\frac{2}{3}}|11\rangle\right)$

$\Rightarrow$ $p_0 = \frac{1}{2}$: $|\psi_0\rangle = \sqrt{\frac{2}{3}}|00\rangle + \sqrt{\frac{1}{3}}|11\rangle = |\chi\rangle$: <u>OK!</u> ✓

$p_1 = \frac{1}{2}$: $|\psi_1\rangle = \sqrt{\frac{1}{3}}|00\rangle + \sqrt{\frac{2}{3}}|11\rangle$:

A & B need to apply $X \otimes X$.

<u>Protocol</u>: A does POVM, sends result to B, if result is 1, both apply X.

<u>Success probability</u> $\underline{\underline{p = p_0 + p_1 = 1}}$

<u>Best possible</u>: We cannot get >1 copies, as POVM cannot increase Schmidt rank!

2. <u>Can we do the converse: $|\chi\rangle \longrightarrow |\phi^+\rangle$?</u>

A does POVM $\{\Pi_0, \Pi_1\}$; $\Pi_0 = \begin{pmatrix} \sqrt{\frac{1}{2}} & \\ & 1 \end{pmatrix}$; $\Pi_1 = \begin{pmatrix} \sqrt{\frac{1}{2}} & \\ & 0 \end{pmatrix}$.

$\rightarrow |\tilde{\psi}_0\rangle = \sqrt{\frac{1}{3}}|00\rangle + \sqrt{\frac{1}{3}}|11\rangle$; $|\tilde{\psi}_1\rangle = \sqrt{\frac{1}{3}}|00\rangle$.

$p = \frac{2}{3}$: $|\psi_0\rangle = |\chi\rangle$

$p = \frac{1}{3}$: $|\psi_1\rangle = |00\rangle \longrightarrow$ no entanglement left!

$\Rightarrow$ $|\chi\rangle \longrightarrow |\phi^+\rangle$ w/ prob. $p = 2/3$.

(will see: best possible!)

$\Rightarrow$ Conversion not reversible! (cannot be used to quantify entanglement)

What is the best protocol?

General LOCC protocol:

time ↓

A: POVM $\{A_i\}$ $\xrightarrow{\text{send result } i}$ B: $\{B^i_j\}$ POVM dep. on i

B $\xrightarrow{\text{send } j}$ A: POVM $\{C^{ij}_k\}$ dep on i,j

A $\xrightarrow{k}$ B: $\{D^{ijk}_\ell\}$

⋮

etc.: any # of rounds!

$$\rho \longmapsto \sum \left(\dots C^{ij}_k A_i\right) \otimes \left(\dots D^{ijk}_\ell B^i_j\right) \rho \left(\ \right)^\dagger \otimes \left(\ \right)^\dagger \ !$$

Very complicated structure!

But: For pure states, protocol can be replaced by

one-round protocol w/ one-way communication

$$\underset{\text{A}}{\text{POVM } \{M_k\}} \xrightarrow{k} \underset{\text{B}}{U_k}: \text{unitary},$$

i.e. $$|\psi\rangle \longrightarrow |\tilde{\psi}_k\rangle = \underset{\substack{\uparrow \\ \text{POVM}}}{M_k} \otimes \underset{\substack{\uparrow \\ \text{unitary}}}{U_k} |\psi\rangle$$

(Proof idea: A can "simulate" any meas. of B by a diff. meas. on her side, if state is known. $\longrightarrow$ Homework!)

General protocol for ent. conversion:

$$|\psi\rangle \rightarrow |\tilde{\psi}_k\rangle = M_k \otimes U_k |\psi\rangle; \quad p_k = \| |\tilde{\psi}_k\rangle \|^2$$

For entanglement: $|\psi\rangle$, $|\psi_k\rangle = \frac{|\tilde{\psi}_k\rangle}{\||\tilde{\psi}_k\rangle\|}$ fully char.

by Schmidt coefficients; and U_k irrelevant

$\Rightarrow$ study instead possible conversions

$$\rho_A \longrightarrow \{p_k, \rho_{A,k}\}:$$

Under which conds. $\exists$ POVM M_k s.th. $p_k \rho_{A,k} = M_k \rho M_k^\dagger$?

(Note: Several $\rho_{A,k}$ might be equal.)

6) Single-copy protocols: majorization

<u>Def.</u>: For $\lambda \in \mathbb{R}^d_{\geq 0}$, let $\lambda^\downarrow = (\lambda^\downarrow_1, \dots, \lambda^\downarrow_d)$, $\lambda^\downarrow_1 \geq \lambda^\downarrow_2 \geq \dots \geq 0$ denote the <u>ordered version</u> of λ.

<u>Definition (Majorization)</u>: We say that <u>λ is majorized by μ</u> (or <u>μ majorizes λ</u>),

$$\lambda \prec \mu,$$

iff $\displaystyle\sum_{i=1}^{k} \lambda_i^\downarrow \leq \sum_{i=1}^{k} \mu_i^\downarrow$ $\forall k = 1, \dots, d$, w/ equality for $k=d$.

<u>Theorem</u>: The following are equivalent:

(i) $\lambda \prec \mu$

(ii) there exist permutations P_i & probabilities q_i s.th.

$$\lambda = \sum q_i P_i \mu$$

(iii) there exists a doubly stochastic Q (i.e. $Q_{ij} \geq 0$, $\sum_i Q_{ij} = \sum_j Q_{ij} = 1$: rand. process w/ fpt. $(\frac{1}{d}, \dots, \frac{1}{d})$) s.th. $\lambda = Q\mu$.

((ii) $\Leftrightarrow$ (iii) follows from Birkhoff's thm: every $Q = \sum q_i P_i$)

<u>Intuition:</u> $\lambda \prec \mu \Leftrightarrow \lambda$ can be obtained by rand. permutation of μ: it is "more random" (e.g. as a prob. distr.); "largest": $(1,0,\dots,0)$; "smallest": $(\frac{1}{d},\dots,\frac{1}{d})$.

<u>Remarks:</u>

- Majorization defines <u>partial order</u> on prob. distributions
- $\lambda \prec \mu$: λ more disordered than μ (in part: more entropy)

  (Made rigorous by "Schur concavity/convexity": for a concave/convex $f(x)$, $F(\lambda) = \sum f(\lambda_i)$ fulfils
  $\lambda \prec \mu \Leftrightarrow F(\lambda) \gtreqless F(\mu)$)

<u>Generalization to operators:</u>

A hermitian matrix: $\lambda^\downarrow(A)$ = ordered eigenvalues of A.

<u>Lemma:</u> $\lambda^\downarrow(A+B) \prec \lambda^\downarrow(A) + \lambda^\downarrow(B)$

(Intuition: Eigenvals of $A+B$ most ordered if in same basis.)

(<u>Proof</u>: Using <u>Ky-Fan maximum principle</u>:

$$\sum_{j=1}^{k} \lambda_j^\downarrow(A) = \max_P \mathrm{tr}(AP); \quad P \text{ all proj's of rank } P = k.$$

Then,

$$\sum_{j=1}^{k} \lambda_j^\downarrow(A+B) = \max_P \mathrm{tr}((A+B)P) \leq$$

$$\leq \max_P \mathrm{tr}(AP) + \max_P \mathrm{tr}(BP) = \sum_{j=1}^{k} \lambda_j^\downarrow(A) + \sum_{j=1}^{k} \lambda_j^\downarrow(B).$$

Theorem (single-copy entanglement conversion):

We can convert $|\psi\rangle \longrightarrow \{p_k, |\psi_k\rangle\}_{k=1}^{K}$ by LOCC if & only if
$\lambda^\downarrow(\rho) \prec \sum_{k=1}^{K} p_k \lambda^\downarrow(\rho_k)$, where $\rho = \mathrm{tr}_A |\psi\rangle\langle\psi|$, $\rho_k = \mathrm{tr}_A |\psi_k\rangle\langle\psi_k|$.

Proof: "$\Rightarrow$": Protocol: A does POVM $\{\Pi_k\}$; wlog Bob's unitary $U_k = \mathbb{1}$ (only Schmidt coeffs matter!).

Then, $$\sum_{k=1}^{K} p_k \lambda^\downarrow(\rho_k) = \sum_{k=1}^{K} \lambda^\downarrow(p_k \rho_k) =$$

$$= \sum_{k=1}^{K} \lambda^\downarrow\left(\mathrm{tr}_A\left[(\Pi_k \otimes \mathbb{1}) |\psi\rangle\langle\psi| (\Pi_k^\dagger \otimes \mathbb{1}) \right]\right)$$

$$\overset{\text{Lemma}}{\succ} \lambda^\downarrow\Big(\mathrm{tr}_A\Big[\underbrace{\sum_k \Pi_k^\dagger \Pi_k \otimes \mathbb{1}}_{=\mathbb{1}} |\psi\rangle\langle\psi| \Big]\Big) = \lambda^\downarrow(\rho) \quad \checkmark$$

"$\Leftarrow$": $\lambda^\downarrow(\rho) \prec \sum p_k \lambda^\downarrow(\rho_k) \Rightarrow \exists P_j, q_j$ s.th. $\lambda^\downarrow(\rho) = \sum p_k q_j P_j \lambda^\downarrow(\rho_k)$

Wlog: ρ, ρ_i diagonal $\rightarrow$ otherwise, add unitaries!

Def. E_{kj} via $E_{kj}\sqrt{\rho} = \sqrt{p_k q_j}\,\sqrt{\rho_k}\, P_j^\dagger$. Then,

$$\sqrt{\rho}\Big(\sum_{kj} E_{kj}^\dagger E_{kj}\Big)\sqrt{\rho} = \sum_{kj} p_k q_j P_j \rho_k P_j^\dagger \overset{\rho,\,\rho_k \text{ diag.}}{=} \rho$$

$\Longrightarrow \sum_{kj} E_{kj}^\dagger E_{kj} = \mathbb{1}$ (if ρ invertible; otherwise any E_{kj} on $\ker\rho$ will do)

And $E_{kj}\rho E_{kj}^\dagger = p_k q_j \rho_k \Rightarrow \sum_j E_{kj}\rho E_{kj}^\dagger = p_k \rho_k$ (65)

$\Rightarrow$ POVM for $\rho \longmapsto \{p_k, \rho_k\}$, i.e., $|\psi\rangle = \{p_k, |\psi_k\rangle\}$.

(Note: We bin several POVM ops j to same outcome!)

Example: Optimal rate for $(\frac{1}{2}, \frac{1}{2}) \longleftrightarrow (\frac{2}{3}, \frac{1}{3})$:

$$\left(\tfrac{1}{2}, \tfrac{1}{2}\right) \prec \left(\tfrac{2}{3}, \tfrac{1}{3}\right).$$

$$\left(\tfrac{2}{3}, \tfrac{1}{3}\right) \prec \underbrace{\tfrac{2}{3}}_{\text{max. value!}} \left(\tfrac{1}{2}, \tfrac{1}{2}\right) + \tfrac{1}{3}(1, 0) = \left(\tfrac{2}{3}, \tfrac{1}{3}\right)$$

c) Asymptotic protocols

single-copy protocol: not reversible, ent. is lost

(e.g. $\left(\frac{2}{3}, \frac{1}{3}\right)$: needs 1 ebit, gives "$\frac{2}{3}$ ebits").

Can we do better with more copies?

$$|\chi\rangle^{\otimes 2} \longrightarrow p_2 |\phi^+\rangle^{\otimes 2} + p_1 |\phi^+\rangle^{\otimes 2} \; ?$$

$$|\chi\rangle^{\otimes 3} \longrightarrow p_3 |\phi^+\rangle^{\otimes 3} + p_2 |\phi^+\rangle^{\otimes 2} + \ldots$$

Average yield of max. ent. states:

$$\bar{p} = \frac{p_1 + 2p_2 + 3p_3 + \ldots}{k \longleftarrow \#\text{ copies}}$$

Can we increase $\bar{p}$ by using more copies?

Yes! ($\rightarrow$ Homework)

Requirements for asymptotic protocols:

- convert $|\phi^+\rangle^{\otimes m} \longleftrightarrow |\chi\rangle^{\otimes n}$ with rate $\frac{n}{m} \to R > 0$

  for $n, m \to \infty$.

- success probability $p \to 1$ for $n \to \infty$.

- conversion can be imperfect, as long as error $\to 0$

  as $n \to \infty$.

Error measure: $\delta = 1 - F$; $F = |\langle\psi|\phi\rangle|^2$: "fidelity"

Good measure: Bounds distance for any observable!

What is form of $|\chi\rangle^{\otimes N}$, $|\chi\rangle = \sum \sqrt{p(x)}\, |x\rangle_A |x\rangle_B$, $x = 1, \dots, d$?

$$|\chi\rangle^{\otimes N} = \sum_{x_1, \dots, x_N} \sqrt{p(x_1) \cdot \ldots \cdot p(x_N)}\; |x_1, \dots, x_N\rangle |x_1, \dots, x_N\rangle$$

$\Rightarrow$ prob. of $|x_1, \dots, x_N\rangle$: $p(x_1, \dots, x_N) = p(x_1) \cdot \ldots \cdot p(x_N)$:

i.i.d. (independently & identically distributed):

law of large numbers etc. applies!

(i.e., $\mathrm{prob}\left(\left|\frac{1}{n}\sum x_i - E(x_i)\right| \geq \varepsilon\right) \to 0 \;\forall \varepsilon$)

What is typical output of iid source (i.e., typ $|x_1, \dots, x_N\rangle$)? (68)

Most likely: Output x appears $\approx N \cdot p(x)$ times.

$$\Longrightarrow p(x_1, \dots, x_N) \approx p(x_1) \cdot \ldots \cdot p(x_N) \approx p(1)^{Np(1)} \cdot \ldots \cdot p(d)^{Np(d)}$$

$$\Longrightarrow -\log p(x_1, \dots, x_N) \approx N \underbrace{\left(- \sum_x p(x) \log p(x) \right)}_{=: H(p):\ \text{Shannon entropy of } p}$$

base 2

Asymptotically: prob. $= 1$ to be ε-close to this, more precisely:

$$\text{prob}\left(\left| -\tfrac{1}{N} \log p(x_1, \dots, x_N) - H(p) \right| \geq \varepsilon \right) \to 0$$

We call all such $(x_1, \dots, x_N)$ ε-typical sequences.

There are asymptotically $\approx 2^{NH(p)}$ typ. sequences.

Fix $\varepsilon > 0$. Define

$$|\vartheta_N\rangle := \sum_{x_1, \dots, x_N\ \varepsilon\text{-typ.}} \sqrt{p(x_1) \cdot \ldots \cdot p(x_N)}\, |x_1, \dots, x_N\rangle |x_1, \dots, x_N\rangle,$$

$$|\hat{\vartheta}_N\rangle = \frac{|\vartheta_N\rangle}{\| |\vartheta_N\rangle \|}.$$

We have

$$\langle \hat{\vartheta}_N | \chi^{\otimes N} \rangle = \frac{\sum_{\varepsilon\text{-typ}} p(x_1, \dots, x_N)}{\sqrt{\sum_{\varepsilon\text{-typ}} p(x_1, \dots, x_N)}} \xrightarrow{N \to \infty} 1$$

and # terms $\approx 2^{NH(p)}$ (and in fact $\leq 2^{N(H(p)+\varepsilon)}$).

<u>Protocol $|\phi^+\rangle^{\otimes M} \longrightarrow |\chi\rangle^{\otimes N}$:</u>

- Use $M = N(H(p)+\varepsilon)$ Bell pairs to prepare $|\vartheta_N\rangle$ (possible: $|\phi^+\rangle^{\otimes M}$ majorizes all distributions).
- $\frac{M}{N} \longrightarrow H(p) + \varepsilon \longrightarrow H(p)$, and $|\hat{\vartheta}_N\rangle \longrightarrow |\chi\rangle^{\otimes N}$

$\Rightarrow$ can prepare $|\chi\rangle$ asymptotically at a cost $H(p)$ per copy!

<u>Protocol $|\chi\rangle^{\otimes N} \longrightarrow |\phi^+\rangle^{\otimes M}$:</u>

- Use $|\hat{\vartheta}_N\rangle$ instead of $|\chi\rangle^{\otimes N}$, since fidelity $\longrightarrow 1$.
- Schmidt coeffs. approach <u>flat distribution</u> with $N(H(p)-\varepsilon)$ terms asymptotically

$\Rightarrow$ Can extract $\frac{M}{N} = H(p) - \varepsilon \longrightarrow H(p)$ e-bits per copy of $|\chi\rangle$.

Asymptotically: Can dilute ($|\phi^+\rangle^{\otimes \dots} \to |\chi\rangle^{\otimes \dots}$)

and distill ($|\chi\rangle^{\otimes \dots} \to |\phi^+\rangle^{\otimes \dots}$) at the same rate

$H(p)$, with $p = (p_1, \dots, p_d)$, $\sqrt{p_k}$ the Schmidt coeffs.

(Note: Same rate: necessarily optimal!)

Can be expressed in terms of the

$$\boxed{\text{"von Neumann entropy"} \quad S(\rho) := -\mathrm{tr}(\rho \log \rho)}$$

$$H(p) = S(\mathrm{tr}_A |\psi\rangle\langle\psi|) = S(\mathrm{tr}_B |\psi\rangle\langle\psi|)$$

Protocol allows to go reversibly between any two states

$|\psi\rangle^{\otimes K} \longleftrightarrow |\chi\rangle^{\otimes L}$ as long as $K S(\mathrm{tr}_B |\psi\rangle\langle\psi|) = L S(\mathrm{tr}_B |\chi\rangle\langle\chi|)$,

by going via $|\phi^+\rangle$.

Result: The entropy of entanglement

$$E(|\psi\rangle) := S(\mathrm{tr}_A |\psi\rangle\langle\psi|) = S(\mathrm{tr}_B |\psi\rangle\langle\psi|)$$

uniquely quantifies the amount of entanglement in a pure bipartite state.