Useful states and entanglement distillation

arXiv:1701.03081

Felix Leditzky

(JILA & CTQM, University of Colorado Boulder)

Joint work with Nilanjana Datta and Graeme Smith

Beyond IID, Singapore, 28 July 2017

Entanglement distillation

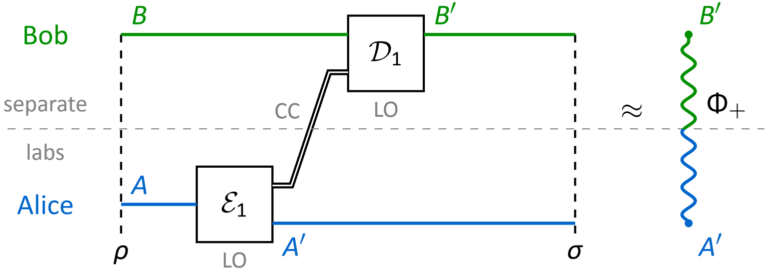
- Entanglement can be used as a resource in
  - teleporation;
  - dense coding;
  - entanglement-assisted classical/private communication;
  - ...
- Above tasks are usually defined (and easier to perform) with **clean entanglement** in the form of **ebits** $|\Phi_+\rangle \sim |00\rangle + |11\rangle$.
- However, entanglement resource is usually **noisy**, i.e., some mixed bipartite state ρ_{AB}.
- **Entanglement distillation:** Convert noisy entanglement into clean entanglement using local operations (LO) and classical communication (CC).

Outline of the talk

1. Operational setting and coding theorems
2. Useful and useless states for entanglement distillation
3. Bounding the distillable entanglement
4. Exploiting symmetries
5. Conclusion and open question

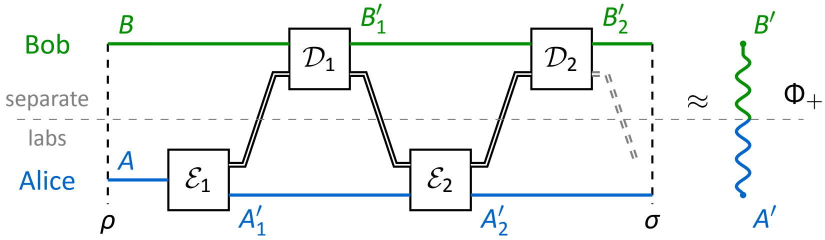
Table of Contents

Entanglement distillation using 1-LOCC



- **1-LOCC**: LO and *one-way* (or *forward*) CC.
- CC can always be bundled into a single round.
- Relevant scenario because of **relation to quantum data transmission** and quantum capacity (more later).

Entanglement distillation using 2-LOCC



- **2-LOCC**: LO and *two-way* CC.
- r rounds of communication between Alice and Bob ($r = 2$ in the above diagram).
- Strictly more powerful than one-way scenario.

Distillable entanglement: Operational definition

- Alice and Bob share n i.i.d. copies of a bipartite state ρ_{AB}.
- **Goal:** Distill m_n copies of an ebit $|\Phi_+\rangle \sim |00\rangle + |11\rangle$.
- **Final state:** $\sigma^n_{A'B'} = \Lambda(\rho_{AB}^{\otimes n})$, where $\Lambda\colon AB \to A'B'$ 1-LOCC or 2-LOCC.
- Rate $\lim\limits_{n\to\infty} \frac{m_n}{n}$ is **achievable**, if $\|\sigma^n_{A'B'} - \Phi_+^{\otimes m_n}\|_1 \xrightarrow{n\to\infty} 0$.
- **Distillable entanglement**:

$$D_{\to}(\rho_{AB}) = \sup\{R\colon R \text{ is achievable under 1-LOCC}\}$$
$$D_{\leftrightarrow}(\rho_{AB}) = \sup\{R\colon R \text{ is achievable under 2-LOCC}\}$$

Distillable entanglement: Hashing and coding theorem

- **Hashing bound** [Devetak and Winter 2005]:

$$D_{\leftrightarrow}(\rho_{AB}) \geq D_{\rightarrow}(\rho_{AB}) \geq I(A\rangle B)_\rho,$$

  where $I(A\rangle B)_\rho = S(B)_\rho - S(AB)_\rho$ is the coherent information.

- **Coding theorem** [Devetak and Winter 2005]:

  For $* \in \{\rightarrow, \leftrightarrow\}$,

$$D_*(\rho_{AB}) = \lim_{n\rightarrow\infty} \frac{1}{n} D_*^{(1)}(\rho_{AB}^{\otimes n}),$$

  where $D_*^{(1)}(\rho_{AB}) := \sup_{\Lambda:\ AB\rightarrow A'B'} I(A'\rangle B')_{\Lambda(\rho)}$ and Λ is 1-LOCC or 2-LOCC.

- **Regularization is necessary** in general.

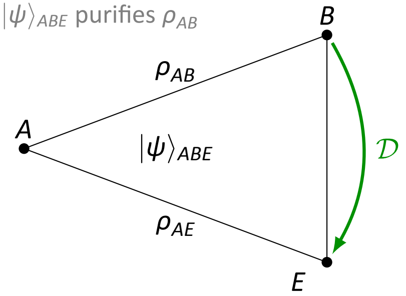
- **Computation** of $D_*(\cdot)$ **infeasible** in most cases.

Table of Contents

Useful and useless states for 1-LOCC

- **Hashing bound**: $D_{\rightarrow}(\rho_{AB}) \geq I(A\rangle B)$.
- Are there states for which this is optimal?

  $\longrightarrow$ **degradable states** [Devetak and Shor 2005; Smith et al. 2008]
- Motivation from classical IT (degraded broadcast channels).



degradable:

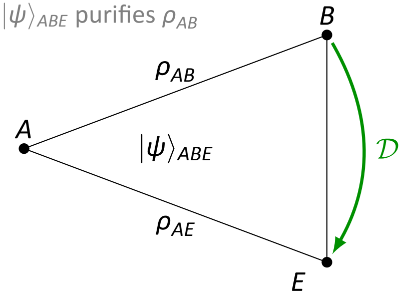
$\exists \mathcal{D}: B \rightarrow E$ s.t.

$\rho_{AE} = (\mathrm{id}_A \otimes \mathcal{D})(\rho_{AB})$

Useful and useless states for 1-LOCC

- Degradable states: $D_{\rightarrow}^{(1)}(\rho_{AB}) = \sup_{\Lambda \text{ 1-LOCC}} I(A'\rangle B')_{\Lambda(\rho)} = I(A\rangle B)_\rho$
- Coherent information is additive: $D_{\rightarrow}^{(1)}(\rho_{AB}^{\otimes n}) = n\, I(A\rangle B)_\rho$.
- **Single-letter formula** for one-way distillable entanglement:

$$D_{\rightarrow}(\rho_{AB}) = \lim_{n\to\infty} \frac{1}{n} D_{\rightarrow}^{(1)}(\rho_{AB}^{\otimes n}) = I(A\rangle B)_\rho.$$



degradable:

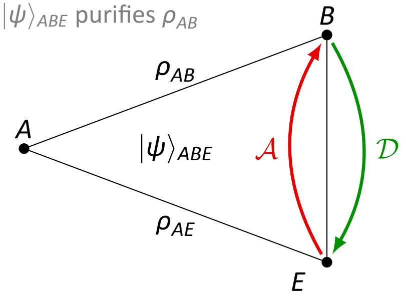
$\exists \mathcal{D}: B \rightarrow E$ s.t.

$\rho_{AE} = (\mathrm{id}_A \otimes \mathcal{D})(\rho_{AB})$

Useful and useless states for 1-LOCC

- Which states are useless? $\longrightarrow$ **antidegradable states**
- These states always have $I(A\rangle B)_\rho \leq 0$ and $D^{(1)}_{\to}(\rho_{AB}) \leq 0$.
- Antidegradable states are **undistillable:** $D_{\to}(\rho_{AB}) = 0$.
- A state is antidegradable iff it is **2-extendible**.

  ($\exists \rho_{ABB'}$ with $B' \cong B$ and $\rho_{AB'} = \rho_{AB}$.) [Myhr 2010]



degradable:

$\exists \mathcal{D}: B \to E$ s.t.

$\rho_{AE} = (\mathrm{id}_A \otimes \mathcal{D})(\rho_{AB})$

antidegradable:

$\exists \mathcal{A}: E \to B$ s.t.

$\rho_{AB} = (\mathrm{id}_A \otimes \mathcal{A})(\rho_{AE})$

Useful and useless states for 2-LOCC

- **Hashing bound** (using only **forward CC**):

$$D_{\leftrightarrow}(\rho_{AB}) \geq D_{\rightarrow}(\rho_{AB}) \geq I(A\rangle B).$$

- Are there states for which this is optimal even under 2-LOCC?

  $\longrightarrow$ **maximally correlated states** [Rains 1999; Rains 2001]

- **Operational definition:** Any measurement performed by either Alice or Bob yields identical outcomes.

- For some basis $\{|i\rangle_{A,B}\}$ and a matrix R with $R \geq 0$, $\operatorname{Tr} R = 1$,

$$\rho_{AB} = \textstyle\sum_{i,j} R_{ij} |i\rangle\langle j|_A \otimes |i\rangle\langle j|_B.$$

- Hashing protocol is optimal for maximally correlated states:

$$D_{\leftrightarrow}(\rho_{AB}) = I(A\rangle B)_\rho = I(B\rangle A)_\rho.$$

Useful and useless states for 2-LOCC

- Finally, which states are useless even under 2-LOCC?
  $\longrightarrow$ **states with positive partial transpose** (PPT)
- Partial transpose Γ_B is defined as
  $$(X_A \otimes Y_B)^{\Gamma_B} := X_A \otimes Y_B^T \quad (+\text{ linear extension}).$$
- A state ρ_{AB} is PPT if $\rho_{AB}^{\Gamma_B} \geq 0$.
- PPT states have $I(A\rangle B)_\rho \leq 0$. [Rains 1999; Rains 2001]
- They are **undistillable under 2-LOCC**: $D_\leftrightarrow(\rho_{AB}) = 0$.
  [Horodecki et al. 1998]
- Every separable state is PPT, but if $|A||B| > 6$, there are entangled PPT states called **bound-entangled states**.
  [Horodecki 1997]

Useful and useless states for entanglement distillation

	useful	useless
1-LOCC	DEG	ADG
2-LOCC	MC	PPT

DEG . . . degradable, ADG . . . antidegradable, MC . . . maximally correlated

- Picture is not completely symmetric.
- We have MC $\subseteq$ DEG.
- However, there are bound-entangled PPT states with distillable private key.
- Hence, PPT $\not\subseteq$ ADG.

Table of Contents

Bounding the distillable entanglement

- **Crucial observation**:

  Regularized quantities such as $D_*(\cdot)$ are **convex on mixtures** of states with **additive** $D_*(\cdot)$. [Wolf and Pérez-García 2007]

- Candidates:
  - Useful states: $D_*(\omega_{AB}) = I(A\rangle B)_\omega \longrightarrow$ additive ✓
  - Useless states: $D_*(\tau_{AB}) = 0 \longrightarrow$ additive ✓
  - For ”cross terms” $\omega^{\otimes m_1} \otimes \tau^{\otimes m_2}$ we can ignore useless part.

Main result

Let $\rho_{AB} = \sum_i p_i \omega_i + \sum_i q_i \tau_i$, where the ω_i are **useful** and the τ_i are **useless**. Then,

$$D_*(\rho_{AB}) \leq \sum_i p_i I(A\rangle B)_{\omega_i}.$$

Finding good decompositions

- **Caution:** Do such decompositions always exist? $\longrightarrow$ **Yes!**
- **Pure states** are ...
  - maximally correlated (by Schmidt decomposition);
  - degradable (environment is always product).
- Hence, every **pure-state decomposition** of ρ_{AB} is a **feasible point** for upper bound $D_*(\rho_{AB}) \leq \sum_i p_i\, I(A\rangle B)_{\omega_i}$.
- Optimum for these: **entanglement of formation**

$$E_F(\rho_{AB}) := \inf_{\{p_x, |\psi^x\rangle_{AB}\}} \sum_x p_x\, S(\mathrm{Tr}_B\, \psi^x_{AB}),$$

where infimum is over $\{p_x, |\psi^x\rangle_{AB}\}$ s.t. $\rho_{AB} = \sum_x p_x \psi^x_{AB}$.

- Hence, $D_*(\rho_{AB}) \leq \sum_i p_i\, I(A\rangle B)_{\omega_i} \leq E_F(\rho_{AB})$.

Finding good decompositions

- **Challenge**: Find good decompositions into **mixed states**, and make useless part as large as possible.
- **1-LOCC:**
  - Useful = degradable, useless = antidegradable
  - Easy for **2-qubit states:** Every 2-qubit state of rank 2 is either degradable or antidegradable. [Wolf and Pérez-García 2007]
- **2-LOCC:**
  - Useful = maximally correlated, useless = PPT
  - For states block-diagonal in **generalized Bell basis**: Algebraic condition whether state is MC. [Wiegmann 1948; Gibson 1974; Hiroshima and Hayashi 2004]

Table of Contents

Convex roof extensions and symmetries

- Let f be a function defined on a subset M of all bipartite states K (e.g. entanglement entropy $S(\mathrm{Tr}_B \cdot)$ on pure states).
- If conv $M = K$, extend f to all of K by minimizing over average of f on convex decompositions in M:

$$\tilde{f}(k) := \inf \{\textstyle\sum_i p_i f(m_i) \colon K \ni k = \sum_i p_i m_i, m_i \in M\}$$

- For entanglement entropy: **entanglement of formation**

$$E_F(\rho_{AB}) := \inf_{\{p_x, |\psi^x\rangle_{AB}\}} \textstyle\sum_x p_x S(\mathrm{Tr}_B \psi^x_{AB}).$$

- If ρ is **invariant** under some symmetry group G: $\tilde{f}$ can be computed on those $\sigma \in M$ that **"twirl"** to ρ, i.e., $\rho = \int_G d\mu(g)\, U_g \sigma U_g^\dagger$. [Vollbrecht and Werner 2001]

Symmetric states

- Our bound can be phrased as a convex roof extension.
- For entanglement distillation we are interested in **local symmetry groups** such as $G = \{U \otimes \bar{U} \colon U \text{ unitary}\}$.
- **Isotropic states:** invariant under G, parametrized by $f \in [0,1]$ as

$$I_d(f) := f\,\Phi_+ + \tfrac{1-f}{d^2-1}(\mathbb{1}_{d^2} - \Phi_+).$$

- Isotropic state $I_d(f)$ is the Choi state of the **depolarizing channel**

$$\mathcal{D}_p(\rho) = (1-p)\rho + \frac{p}{3}(X\rho X + Y\rho Y + Z\rho Z),$$

  where $p \in [0,1]$ and X, Y, Z are the Pauli operators ($p = 1 - f$).
- **Quantum capacity** $Q(\mathcal{D}_p)$ is **unknown**.

  ($Q(\mathcal{N}) :=$ max. rate at which entanglement can be generated through $\mathcal{N}$)

Bounding quantum capacity of depolarizing channel

- $\mathcal{D}_p$ is **teleportation-simulable** [Bennett et al. 1996], and hence

$$Q(\mathcal{D}_p) = D_{\rightarrow}(\mathcal{J}(\mathcal{D}_p)).$$

- If $p \geq \frac{1}{4}$, then $\mathcal{J}(\mathcal{D}_p)$ is antidegradable, and

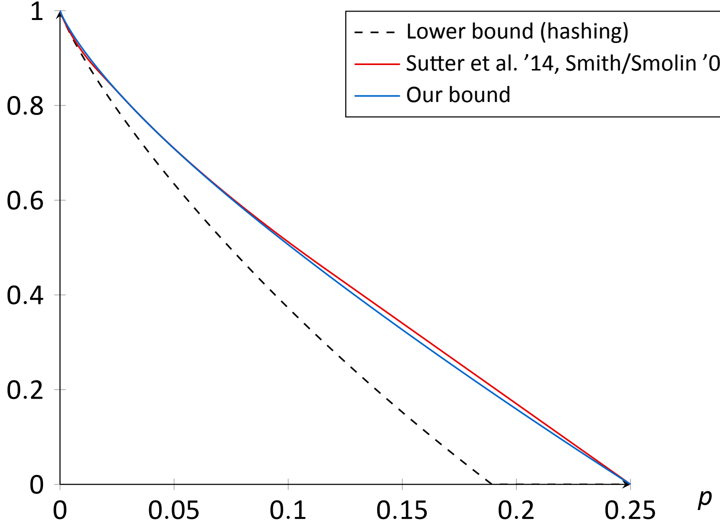
$$D_{\rightarrow}(\mathcal{J}(\mathcal{D}_p)) = Q(\mathcal{D}_p) = 0.$$

Application: Upper bound on $Q(\mathcal{D}_p)$ for $p \in [0, 1/4]$

$$Q(\mathcal{D}_p) \leq \min \left\{ I(A\rangle B)_\rho : \rho_{AB} \in \mathrm{DEG}, \langle \Phi_+ | \rho_{AB} | \Phi_+ \rangle = 1 - p \right\}$$

- **Bad news:** Non-convex optimization problem, since **set of degradable states is not convex**.
- **Good news:** Still solvable numerically for $d = 2, 3, \ldots$.

Upper and lower bounds on $Q(\mathcal{D}_p)$



Isotropic states and 2-LOCC

- In 2-LOCC setting, our bound is only as good as the **PPT-relative entropy of entanglement** $D(\rho\|\sigma) = \mathrm{Tr}(\rho(\log\rho - \log\sigma))$

$$E_R^{\mathrm{PPT}}(\rho_{AB}) := \min_{\sigma\in\mathrm{PPT}} D(\rho_{AB}\|\sigma_{AB}).$$

- For isotropic states: [Rains 1999]

$$D_{\leftrightarrow}(I_d(f)) \leq E_R^{\mathrm{PPT}}(I_d(f)) = \log d - (1-f)\log(d-1) - h(f),$$

Application: Alternative formula for $E_R^{\mathrm{PPT}}(I_d(f))$

With the Vollbrecht/Werner reduction,

$$E_R^{\mathrm{PPT}}(I_d(f)) = \min\{I(A\rangle B)_\rho : \rho_{AB}\in\mathrm{MC}, \langle\Phi_+|\rho_{AB}|\Phi_+\rangle = f\}.$$

- Similar result for Werner states (with $U\otimes U$ symmetry).

Table of Contents

Conclusion

- One-way and two-way **distillable entanglement** $D_{\rightarrow}(\cdot)$ resp. $D_{\leftrightarrow}(\cdot)$ are **hard to compute** in most cases.
- **Main result:** upper bound on $D_{*}(\cdot)$ in terms of decomposition of a state into useful and useless states.
- Easy to compute in low dimensions and for states with symmetries.
- **Application to depolarizing channel**: strong upper bound on quantum capacity in high-noise regime.
- 1-LOCC and 2-LOCC setting are not really on same footing.
- **Is there an analogue of Rains' PPT theory for 1-LOCC?**

References

Bennett, C. H. et al. (1996). *Physical Review A* 54.5, pp. 3824–3851. arXiv: quant-ph/9604024.

Devetak, I. and P. W. Shor (2005). *Communications in Mathematical Physics* 256.2, pp. 287–303. arXiv: quant-ph/0311131 [quant-ph].

Devetak, I. and A. Winter (2005). *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Science* 461.2053, pp. 207–235. arXiv: quant-ph/0306078.

Gibson, P. (1974). *Linear Algebra and its Applications* 9, pp. 45–53.

Hiroshima, T. and M. Hayashi (2004). *Physical Review A* 70 (3), p. 030302. arXiv: quant-ph/0405107.

Horodecki, M. et al. (1998). *Physical Review Letters* 80.24, pp. 5239–5242. quant-ph: quant-ph/9801069.

Horodecki, P. (1997). *Physics Letters A* 232.5, pp. 333 –339. arXiv: quant-ph/9703004.

Leditzky, F. et al. (2017). *arXiv preprint*. arXiv: 1701.03081 [quant-ph].

Myhr, G. O. (2010). PhD thesis. Friedrich-Alexander-Universität Erlangen-Nürnberg. arXiv: 1103.0766 [quant-ph].

Rains, E. M. (1999). *Physical Review A* 60.1, pp. 179–184. arXiv: quant-ph/9809082.

Rains, E. M. (2001). *IEEE Transactions on Information Theory* 47.7, pp. 2921–2933. arXiv: quant-ph/0008047.

Smith, G. and J. A. Smolin (2008). *2008 IEEE Information Theory Workshop (ITW)*. IEEE, pp. 368–372. arXiv: 0712.2471 [quant-ph].

Smith, G. et al. (2008). *IEEE Transactions on Information Theory* 54.9, pp. 4208–4217. arXiv: quant-ph/0607039.

Sutter, D. et al. (2015). *arXiv preprint*. arXiv: 1412.0980 [quant-ph].

Vollbrecht, K. G. H. and R. F. Werner (2001). *Physical Review A* 64.6, p. 062307. arXiv: quant-ph/0010095.

Wiegmann, N. A. (1948). *Bulletin of the American Mathematical Society* 54.10, pp. 905–908.

Wolf, M. M. and D. Pérez-García (2007). *Physical Review A* 75.1, p. 012303. arXiv: quant-ph/0607070.

Thank you very much for your attention!