Useful states and entanglement distillation

arXiv:1701.03081

Felix Leditzky

(JILA & CTQM, University of Colorado Boulder)

Joint work with Nilanjana Datta and Graeme Smith

IQI seminar, Caltech, 18 July 2017

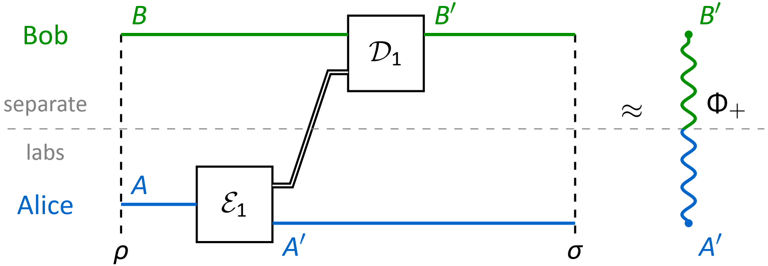
Outline

Table of Contents

Entanglement distillation

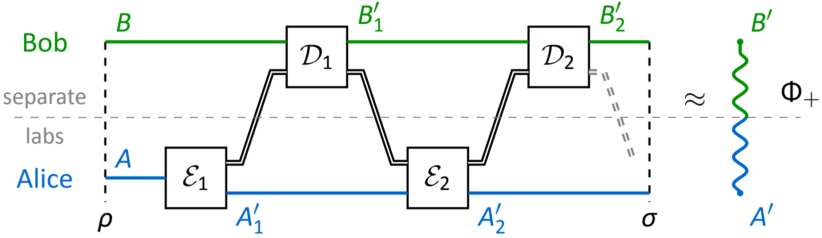
- Entanglement can be used as a resource in
  - teleporation;
  - dense coding;
  - entanglement-assisted classical or private communication;
  - ...
- Imagine Alice and Bob are separated and share **noisy entanglement**, i.e., some mixed bipartite state ρ_{AB}.
- Above tasks are easier to perform with **clean entanglement** in the form of **ebits**.
- **Entanglement distillation:** Convert noisy entanglement into clean entanglement using local operations (LO) and classical communication (CC).

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 copies of a bipartite (mixed) 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 $\Lambda \colon AB \to A'B'$ is a 1-LOCC or 2-LOCC operation.
- Rate $\lim\limits_{n\to\infty} \dfrac{m_n}{n}$ is **achievable**, if $\|\sigma^n_{A'B'} - \Phi_+^{\otimes m_n}\|_1 \xrightarrow{n\to\infty} 0$.
- **Distillable entanglement**:

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

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.

- Define the following single-letter quantities:

$$D_{*}^{(1)}(\rho_{AB}) := \sup_{\Lambda:\, AB \to A'B'} I(A'\rangle B')_{\Lambda(\rho)},$$

where $* \in \{\rightarrow, \leftrightarrow\}$, and Λ is 1-LOCC or 2-LOCC.

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

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

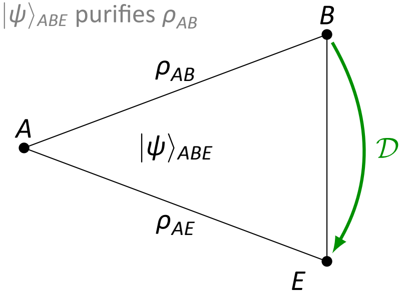
- Regularization renders **computation** of distillable entanglement **infeasible** in most cases!

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]



degradable:

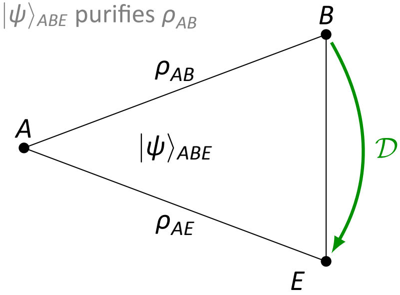
$\exists \mathcal{D} : B \rightarrow E$ s.t.

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

Useful and useless states for 1-LOCC

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

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



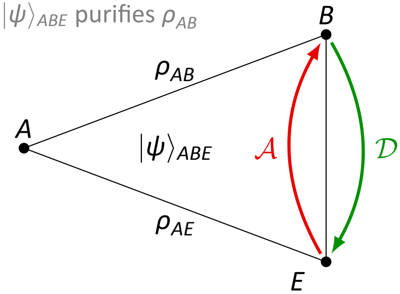
degradable:

$\exists \mathcal{D} : B \rightarrow E$ 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 $D^{(1)}_{\rightarrow}(\rho_{AB}) \leq 0$.
- Antidegradable states are **undistillable:** $D_{\rightarrow}(\rho_{AB}) = 0$.
- A state is antidegradable iff it is **2-extendible**. [Myhr 2010]



degradable:

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

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

antidegradable:

$\exists \mathcal{A}: E \rightarrow B$ 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 $R \geq 0$, $\operatorname{Tr} R = 1$,

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

- 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 pos. 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 $I(A\rangle B)_\rho \leq 0$.
- 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

- We have MC $\subseteq$ DEG, but PPT $\not\subseteq$ ADG.
  (take any bound-entangled PPT state with distillable private key)
- Note that SEP $\subseteq$ ADG (and SEP $\subseteq$ PPT).
- $\rho_{AB} \in \text{DEG} \iff \rho_{AE} \in \text{ADG}$.
- $\rho_{AB} \in \text{MC} \Rightarrow \rho_{AE} \in \text{SEP} \subseteq \text{PPT}$ (in fact, ρ_{AE} is cq).
- $\rho_{AB} \in \text{PPT} \overset{?}{\Rightarrow} \rho_{AE} \in \text{MC}$.

Table of Contents

Bounding the distillable entanglement

- **Crucial observation** [Wolf and Pérez-García 2007]:

  Regularized quantities such as $D_*(\cdot)$ are **convex on mixtures** of states with **additive** $D_*(\cdot)$.

- Candidates:
  - Useful states: $D_*(\omega_{AB}) = I(A\rangle B)_\omega \longrightarrow$ additive.
  - Useless states: $D_*(\tau_{AB}) = 0 \longrightarrow$ additive.

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?
- Pure state $|\psi\rangle_{AB} = \sum_i \lambda_i |i\rangle_A \otimes |i\rangle_B$:

$$|\psi\rangle\langle\psi|_{AB} = \sum_{i,j} \lambda_i \lambda_j \, |ii\rangle\langle jj|_{AB} \in \mathrm{MC} \subseteq \mathrm{DEG}$$

- Hence, every **pure-state decomposition** of ρ_{AB} is a **feasible point** for upper bound.
- Optimum for these: **entanglement of formation**

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

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

- Hence, $D_*(\rho_{AB}) \leq \sum_i p_i \, I(A\rangle B)_{\omega_i} \leq E_F(\rho_{AB})$.
- **Challenge**: Find good decompositions into **mixed states**.

Finding good decompositions

- **1-LOCC:** degradable and antidegradable states.
- Easy for **2-qubit states:**
  Every 2-qubit state of rank 2 is either degradable or antidegradable. [Wolf and Pérez-García 2007]
- **Recipe:** $(\psi_i \equiv |\psi_i\rangle\langle\psi_i|)$
  - $\rho_{AB} = p_1\,\psi_1 + p_2\,\psi_2 + p_3\,\psi_3 + p_4\,\psi_4$
  - $\omega_1 := \frac{p_1}{p_1+p_2}\psi_1 + \frac{p_2}{p_1+p_2}\psi_2$ and $\omega_2 := \frac{p_3}{p_3+p_4}\psi_3 + \frac{p_4}{p_3+p_4}\psi_4$
  - Then, $\operatorname{rank}\omega_i = 2$ and $\rho_{AB} = (p_1+p_2)\omega_1 + (p_3+p_4)\omega_2$.
  - Apply our main result to this decomposition.

Finding good decompositions

- **2-LOCC:** maximally correlated and PPT states.
- Easy for states block-diagonal in **generalized Bell basis** $\{\Phi_{i,j}\}_{0\leq i,j\leq d-1}$, defined by

$$|\Phi_{i,j}\rangle := X^j Z^i |\Phi_+\rangle,$$

  where X and Z are the shift and clock operators (generalized Paulis in d dimensions).
- A state $\rho_{AB} \in \operatorname{span}\{|\Phi_{i_\alpha,j_\alpha}\rangle\}_{\alpha=1,\ldots,l}$ with $l \leq d$ is maximally correlated iff for all $\alpha, \beta, \gamma \in \{1,\ldots,l\}$

$$j_\alpha(i_\gamma - i_\beta) - i_\gamma j_\beta = i_\alpha(j_\gamma - j_\beta) - j_\gamma i_\beta \mod d.$$

[Wiegmann 1948; Gibson 1974; Hiroshima and Hayashi 2004]

Table of Contents

Convex roof extensions

- Suppose we have a set K and know how to evaluate a real-valued function f on a subset $M \subseteq K$.
- Example to keep in mind: Entanglement entropy $S(\mathrm{Tr}_B\, \psi_{AB})$ evaluated on pure states $|\psi\rangle_{AB}$.
- If $\mathrm{conv}\, M = K$, then we can extend f to K as follows:

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

- The function $\tilde{f}$ is called the **convex roof extension** of f on K.
- For $f = S(\mathrm{Tr}_B(\cdot))$: Convex roof extension of entanglement entropy is the entanglement of formation E_F.

Convex roof extensions

- Convex roof extensions are much easier to compute in the presence of symmetry.
- Suppose we have a symmetry group G with a measure $d\mu(g)$ on K and an action $g \cdot k$ on elements $k \in K$.
- Define the **twirling operation**

$$\mathcal{T}_G(k) := \int_G d\mu(g)\, g \cdot k,$$

  and the set of invariant elements $\mathcal{T}_G(K) := \{k \in K \colon \mathcal{T}_G(k) = k\}$.
- [Vollbrecht and Werner 2001]: The convex roof $\tilde{f}$ of an invariant element $k \in \mathcal{T}_G(K)$ can be computed on elements $m \in M$ that "twirl" to k via $\mathcal{T}_G$:

$$\tilde{f}(k) = \inf \{f(m) \colon m \in M, \mathcal{T}_G(m) = k\}.$$

Our upper bound as convex roof extensions

- Set $F = \{\text{useful states}\}$ and $L = \{\text{useless states}\}$.
- The choices

$$K = \text{set of bipartite states}$$
$$M = F \cup L$$
$$f = \max\{I(A\rangle B), 0\}$$

  yield our upper bound.
- Written out: For $\rho_{AB} = \sum_i p_i \omega_i + \sum_i q_i \tau_i$ with $\omega_i \in F$, $\tau_i \in L$,

$$\begin{aligned} D_*(\rho_{AB}) &\leq \sum_i p_i f(\omega_i) + \sum_i q_i f(\tau_i) \\ &= \sum_i p_i I(A\rangle B)_{\omega_i} \end{aligned}$$

- Use the Vollbrecht/Werner reduction in the presence of symmetry!

Symmetric states

- For entanglement distillation we are interested in **local symmetry groups**.
- Let $G = \{U \otimes U \colon U \text{ unitary}\}$, then the states invariant under G are the **Werner states**:

$$W_d(p) := \frac{1-p}{d^2+d}(\mathbb{1}_{d^2} + \mathbb{F}_d) + \frac{p}{d^2-d}(\mathbb{1}_{d^2} - \mathbb{F}_d),$$

  where $p \in [0,1]$ and $\mathbb{F}_d$ is the swap operator on $\mathbb{C}^d \otimes \mathbb{C}^d$.
- Let $G = \{U \otimes \bar{U} \colon U \text{ unitary}\}$, then the states invariant under G are the **isotropic states**:

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

  where $f \in [0,1]$.

Isotropic states and depolarizing channel

- 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 ($p = 1 - f$).

- Despite its simplicity, **quantum capacity** $Q(\mathcal{D}_p)$ is **unknown**.

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

- What we do know: $\mathcal{D}_p$ is **teleportation-simulable**, i.e.,

entanglement generation through $\mathcal{D}_p$

$\Longleftrightarrow$ [Bennett et al. 1996]

one-way entanglement distillation from Choi state $\mathcal{J}(\mathcal{D}_p)$

- In other words: $Q(\mathcal{D}_p) = D_{\rightarrow}(\mathcal{J}(\mathcal{D}_p))$

Bounding quantum capacity of depolarizing channel

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

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

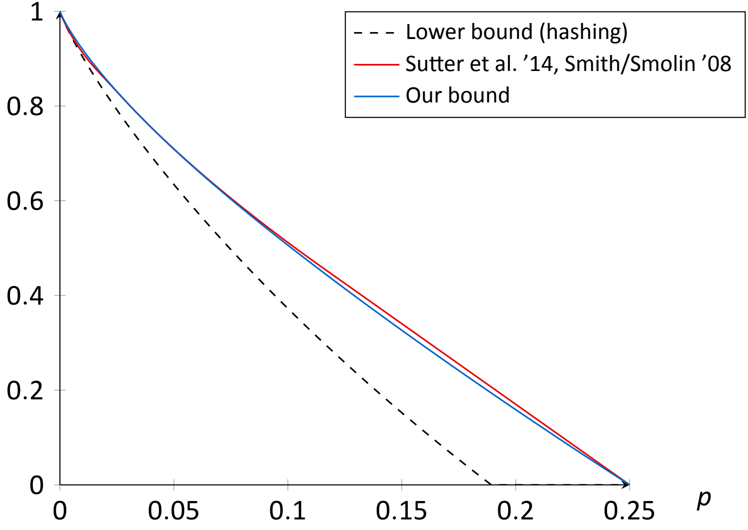
- For $0 \leq p \leq \frac{1}{4}$ we have the following

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

$$\begin{aligned} Q(\mathcal{D}_p) &= D_{\rightarrow}(\mathcal{J}(\mathcal{D}_p)) \\ &\leq \min\{I(A\rangle B)_\rho : \rho_{AB} \in \mathrm{DEG}, \langle \Phi_+ | \rho_{AB} | \Phi_+ \rangle = 1 - p\} \end{aligned}$$

- **Bad news:** Non-convex optimization problem, since **set of degradable states is not convex**.
- **Good news:** In low dimensions ($d = 2, 3$) we can still solve this numerically.

Bounding quantum capacity of depolarizing channel



Isotropic states and 2-LOCC

- In 2-LOCC setting, our bound is only as good as the **PPT-relative entropy of entanglement**

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

where $D(\rho\|\sigma) = \mathrm{Tr}(\rho(\log\rho - \log\sigma))$ is the relative entropy.

- For isotropic states:

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

where $h(f) = -f\log f - (1-f)\log(1-f)$ is the binary entropy.

- Our bound using Vollbrecht/Werner-simplification:

$$D_{\leftrightarrow}(I_d(f)) \leq \min\left\{I(A\rangle B)_\rho : \rho_{AB} \in \mathrm{MC}, \langle\Phi_+|\rho_{AB}|\Phi_+\rangle = f\right\}.$$

Isotropic states and 2-LOCC

- Consider the following state:

$$\rho_{AB} = f\,\Phi_{0,0} + \frac{1-f}{d-1}\sum_{i=1}^{d-1}\Phi_{0,i},$$

where $\{\Phi_{i,j} : 0 \le i,j \le d-1\}$ is the Bell basis ($\Phi_{0,0} = \Phi_+$).

- This state satisfies $\langle\Phi_+|\rho_{AB}|\Phi_+\rangle = f$.

- ρ_{AB} is **maximally correlated** (can be shown using the algebraic relation mentioned before), and

$$I(A\rangle B)_\rho = E_R^{\mathrm{PPT}}(I_d(f)) = \log d - (1-f)\log(d-1) - h(f).$$

- Hence,

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

Table of Contents

Conclusion

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

- 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.

Open questions

	useful	useless
1-LOCC	DEG	? $\supseteq$ ADG
2-LOCC	MC	PPT $\supseteq$ SEP

- Rains' work showed that analyzing PPT states is a powerful tool in characterizing two-way distillable entanglement.
- Useless states: PPT $\supseteq$ SEP.
- For 2-LOCC our bound is essentially a reformulation of the PPT-relative entropy of entanglement.
- By analogy, can we find a superset ? $\supseteq$ ADG giving an analogue of the PPT-relative entropy bound 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!