Title: Asymptotic performance of port-based teleportation

Date: May 04, 2018 11:00 AM

URL: http://pirsa.org/18050051

Abstract: <p>Port-based teleportation (PBT) is a variant of the well-known task of quantum teleportation in which Alice and Bob share multiple entangled states called "ports". While in the standard teleportation protocol using a single entangled state the receiver Bob has to apply a non-trivial correction unitary, in PBT he merely has to pick up the right quantum system at a port specified by the classical message he received from Alice. PBT has applications in instantaneous non-local computation and can be used to attack position-based quantum cryptography. Since perfect PBT protocols are impossible, there is a trade-off between error and entanglement consumption (or the number of ports), which can be analyzed using representation theory of the symmetric and unitary groups. In particular, without loss of generality the resource state can be assumed to have a â€œpurified" Schur-Weyl duality symmetry. I will give an introduction to the task of PBT and its symmetries, and show how the asymptotics of existing formulas for the optimal performance for a given number of ports can be derived using a connection between representation theory and the Gaussian unitary ensemble.</p>

<p>Joint work with M. Christandl, C. Majenz, G. Smith, F. Speelman & M. Walter</p>

Asymptotic performance of port-based teleportation

Felix Leditzky

(JILA & CTQM, University of Colorado Boulder)

Joint work with

M. Christandl, C. Majenz, G. Smith, F. Speelman, M. Walter

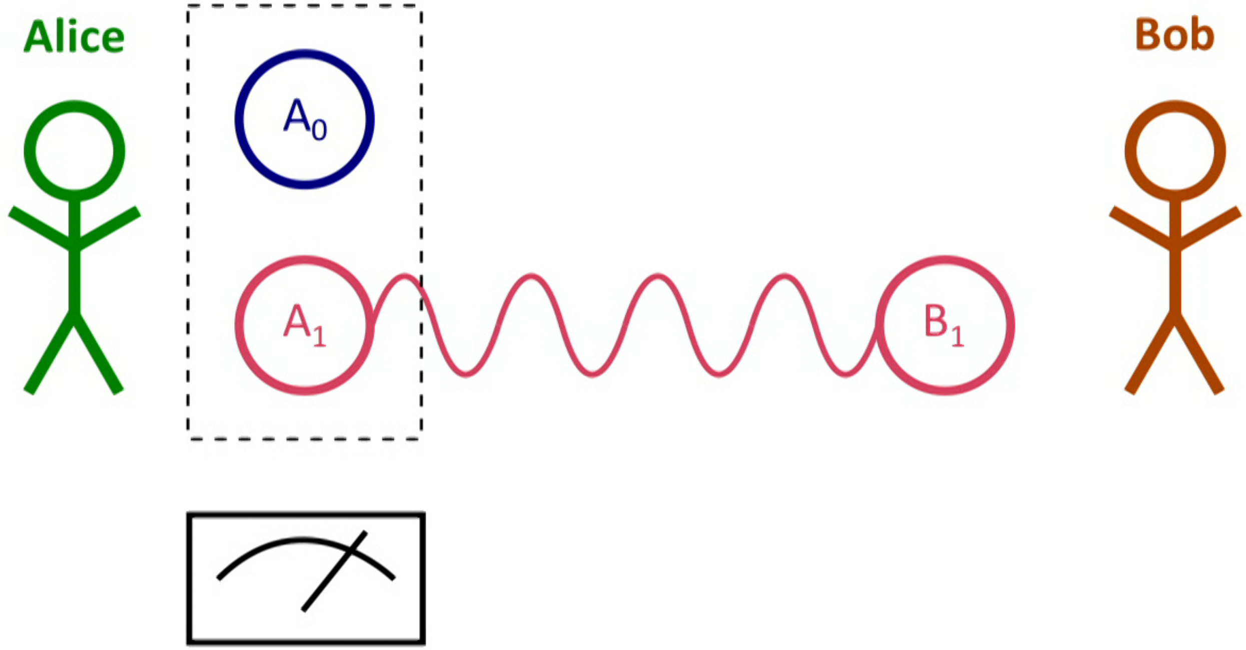
(to appear soon on arXiv)

Perimeter Institute, Waterloo

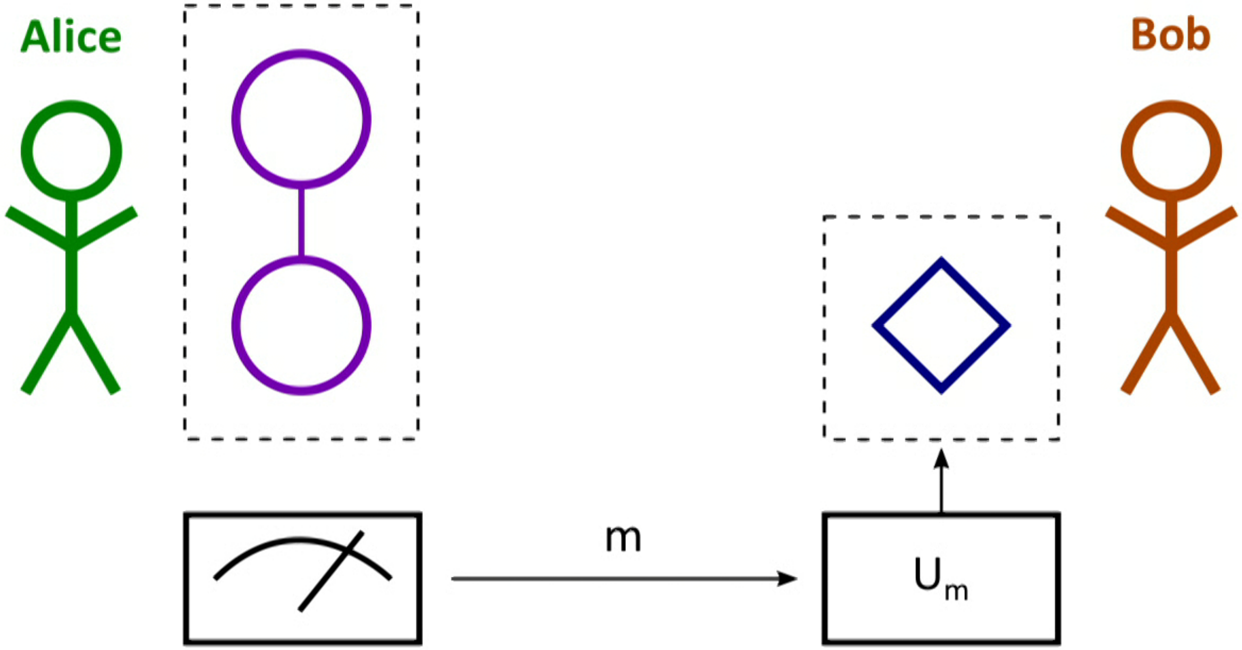
4 May 2018

Standard teleportation protocol

Standard teleportation protocol

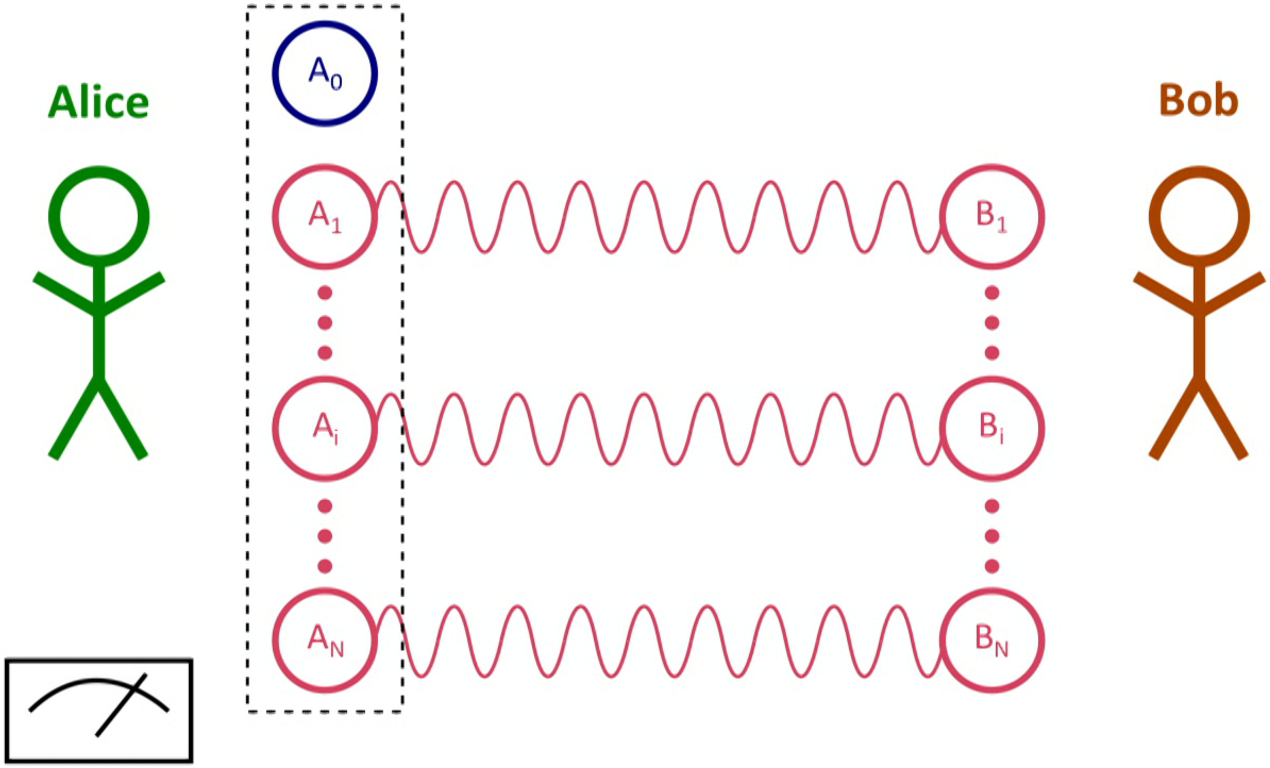


Standard teleportation protocol

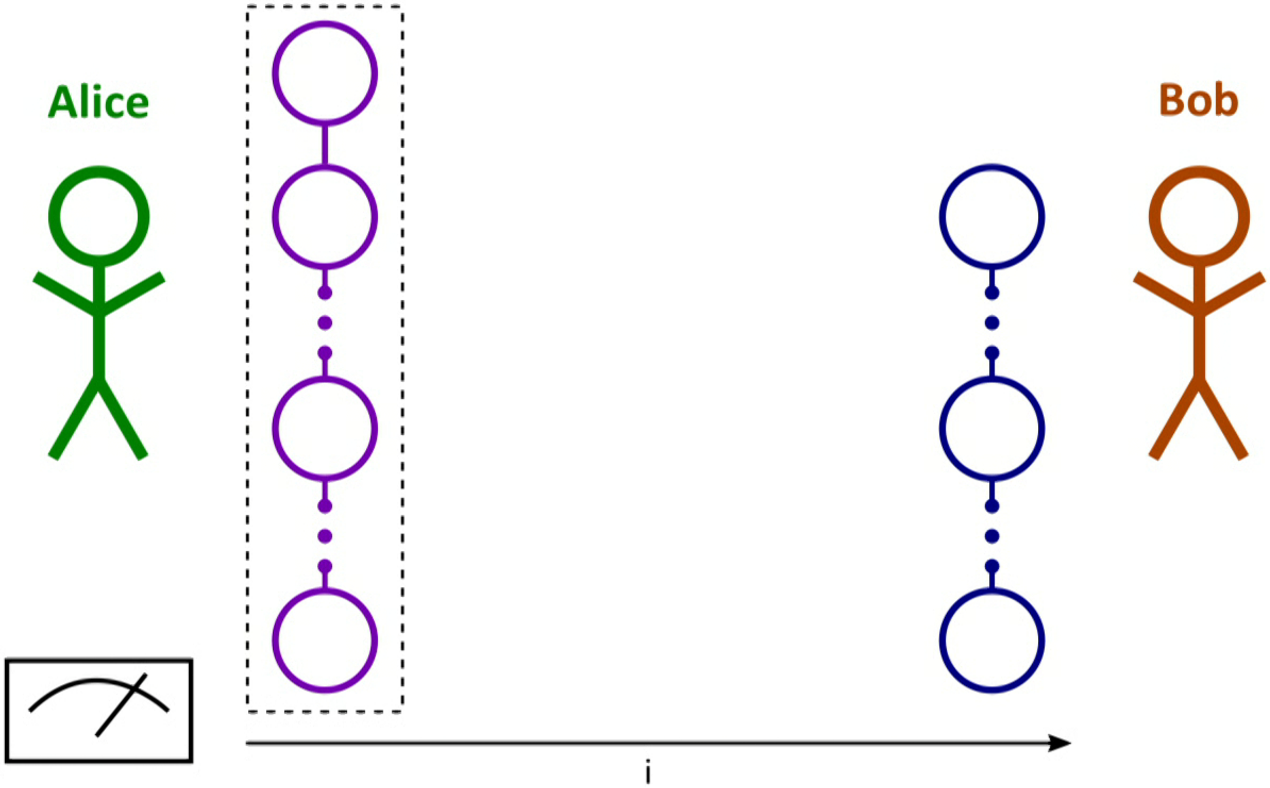


2 / 35

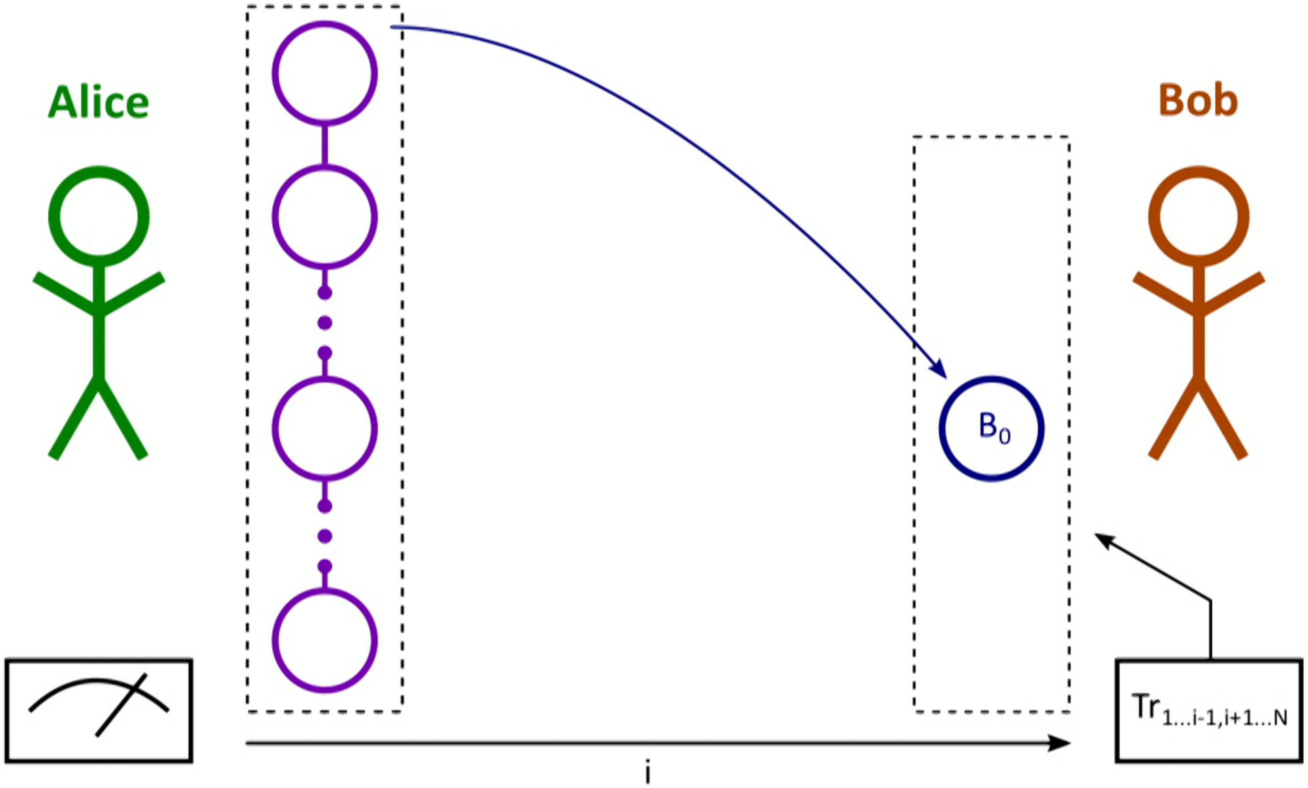
Port-based teleportation



Port-based teleportation



Port-based teleportation



Why is PBT interesting?

- Since partial trace commutes with $U^{\otimes N}$, PBT is **unitarily covariant** (details later).
- PBT enables instantaneous non-local quantum computation (INQC). [Beigi and König 2011]
- INQC can be used to break position-based cryptography. [Buhrman et al. 2014]

Caveat

Unitary covariance leads to the fact that
perfect PBT is impossible with finite resources.

[Ishizaka and Hiroshima 2008]

Variants of PBT

- Hence, need to allow for error in protocol, leading to deterministic and probabilistic PBT.
- **Deterministic PBT**: Protocol always yields final state that approximates target state.
- **Probabilistic PBT:** Protocol yields exact target state with certain success probability.
- **Goal of this talk:** Understand symmetries of PBT and determine asymptotic performance of standard protocols.

Outline

1. Operational setting & bounds on protocols
2. Symmetries & representation theory
3. Main results: Asymptotics of standard PBT protocols
4. Proof methods
5. Concluding remarks

Operational setting

- **Protocol:** Alice implements a collective measurement on $A_0 A_1 \dots A_N$ using a POVM $E = \{E^{(i)}\}_{i=1}^{N}$.
- Alice sends measurement outcome to Bob.
- Bob selects the right port that holds an (approximate) copy of target state and discards the rest.
- Selecting B_i corresponds to the quantum operation $\mathrm{Tr}_{B_i^c}$.
- The pair $(|\varphi\rangle, E)$ determines the PBT protocol.

Deterministic PBT

- In deterministic PBT the protocol always yields a final state as an approximation to the target state.
- Hence, PBT protocol is supposed to **simulate perfect *d*-dimensional channel**.
- **Figure of merit:** entanglement fidelity of PBT protocol Λ to identity channel $\mathrm{id}\colon \mathbb{C}^d \to \mathbb{C}^d$:

$$F_d = F(\Lambda, \mathrm{id}) = \langle \Phi^+_{A'A} | (\mathrm{id} \otimes \Lambda)(\Phi^+_{A'A}) | \Phi^+_{A'A} \rangle .$$

$|\Phi^+\rangle_{A'A} = \frac{1}{\sqrt{d}} \sum_x |x\rangle|x\rangle$ is a max. entangled state.

- Alternative: diamond norm distance to identity channel.

Deterministic PBT and state discrimination

- Deterministic PBT $\Longleftrightarrow$

  state discrimination of the uniformly drawn states

  $\omega^{(i)}_{A^N B} = \mathrm{Tr}_{B_i^c}\, \varphi_{A^N B^N}$. [Ishizaka and Hiroshima 2009]

- Success probability q of discriminating between $\omega^{(i)}$:

$$q = \frac{d^2}{N} F_d.$$

- State discrimination: **pretty good measurement** as POVM.

- Further protocol simplification: N maximally entangled states $|\Phi^+\rangle_{A_i B_i} = \frac{1}{\sqrt{d}} \sum_x |x\rangle_{A_i} |x\rangle_{B_i}$ as ports.

Probabilistic PBT

- Probabilistic PBT yields the exact target state with **success probability** p_d and aborts otherwise.

- Extended POVM $E_{\text{prob}} = \{E^{(i)}\}_{i=0}^{N}$, where $E^{(0)}$ corresponds to abortion of the protocol.

- Probabilistic PBT is a **special case of deterministic PBT**.

- Again: consider special case where $|\varphi\rangle_{A^N B^N} = |\Phi^+\rangle_{AB}^{\otimes N}$.

Existing results: optimal performance of PBT

- Det. PBT with PGM as POVM and EPR pairs as ports:

$$F_d^{\text{PGM,EPR}} \geq 1 - \frac{d^2-1}{N}.$$

[Ishizaka and Hiroshima 2008; Beigi and König 2011]

- Converse bound for arbitrary POVM and resource state:

$$F_d^* \leq 1 - \frac{1}{4(d-1)N^2} + O(N^{-3}).$$

[Ishizaka 2015]

- Closed form for $d = 2$: [Ishizaka and Hiroshima 2009]

$$F_2^{\text{PGM}} = F_2^{\text{PGM,EPR}} = 1 - \frac{3}{4N} + o(N^{-1})$$

$$p_2^{\text{EPR}} \sim 1 - \left(\frac{8}{\pi N}\right)^{-1/2} + o(N^{-1/2}).$$

Existing results: optimal performance of PBT

- PBT has a lot of inherent **symmetries**

  $\longrightarrow$ use **representation theory** (RT)!

- [Studziński et al. 2017] and [Mozrzymas et al. 2017]:
  exact expressions for F_d and p_d in terms of RT quantities, hard to calculate.

- To state these: understand symmetries and RT of PBT.

- Our main results: Determine the asymptotics of these expressions for $F_d^{\mathrm{PGM,EPR}}$ and p_d^{EPR} to first order.

Symmetries

- **Permutation symmetry:**

  Every port B_i is equally good for teleportation

  $\longrightarrow S_N$-symmetry of $\rho_{B^N} = \mathrm{Tr}_{A^N}\,\varphi$.

- Similar symmetry for POVM elements

  $\longrightarrow S_N$-symmetry of $E^{(i)}$.

- **Unitary invariance:**

  The protocol works equally well for all input states

  $\longrightarrow U_d$-symmetry of ρ_{B^N}.

Symmetries

Proposition: Symmetries of PBT

Every PBT protocol can be symmetrized to one with entanglement fidelity no worse than the original one, and:

- Resource state is a purification of a symmetric Werner state, i.e., invariant under $U^{\otimes N} \otimes \overline{U}^{\otimes N}$ and S_N.
- POVM elements form an orbit under the S_N-action, and are each invariant under $\overline{U}_{A_0} \otimes U_A^{\otimes N}$.
- Effective channel $\mathbb{C}^d \to \mathbb{C}^d$ is covariant w.r.t. the unitary group.

"Folklore" results, proofs in our paper and C. Majenz's PhD thesis.

Schur-Weyl duality

- Resource state invariant under both U_d- and S_N-action

  $\longrightarrow$ structure determined by **Schur-Weyl duality**.

- S_N-action: $|\psi_1\rangle \otimes \ldots \otimes |\psi_N\rangle \xrightarrow{\pi} |\psi_{\pi^{-1}(1)}\rangle \otimes \ldots \otimes |\psi_{\pi^{-1}(N)}\rangle$

- U_d-action: $|\psi_1\rangle \otimes \ldots \otimes |\psi_N\rangle \xrightarrow{U} U|\psi_1\rangle \otimes \ldots \otimes U|\psi_N\rangle$

- **Schur-Weyl decomposition:**

$$(\mathbb{C}^d)^{\otimes N} \cong \bigoplus_{\lambda \vdash_d N} [\lambda] \otimes V_\lambda$$

- **Irreducible representations:**
  - $[\lambda]$ is an irrep of S_N with $\dim[\lambda] = d_\lambda$.
  - V_λ is an irrep of U_d with $\dim V_\lambda = m_\lambda$.

Exact expressions for F_d and p_d using RT

Exact expressions for deterministic and probabilistic PBT

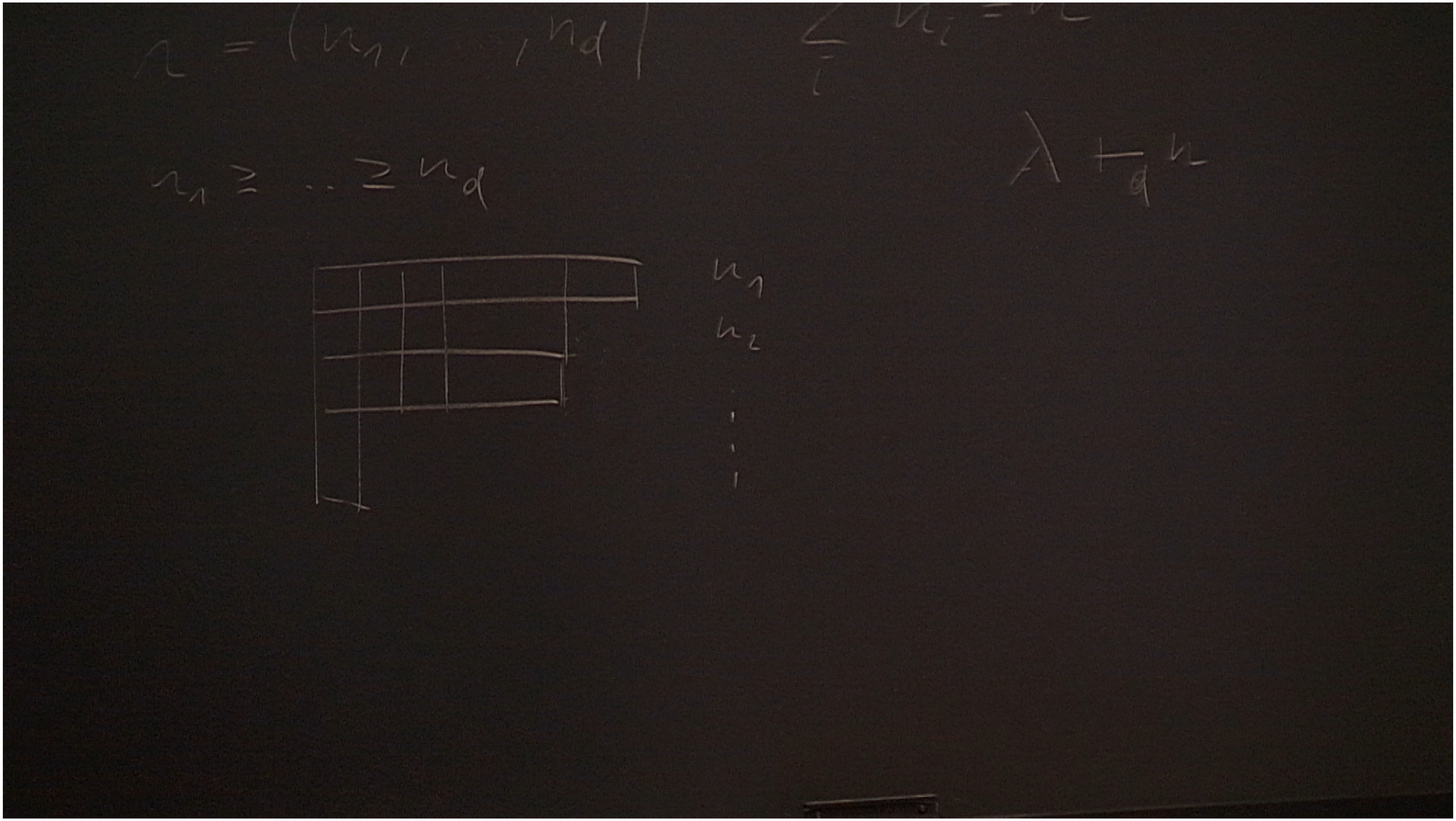
[Studziński et al. 2017; Mozrzymas et al. 2017]

- $$F_d^{\mathrm{PGM,EPR}} = \frac{1}{d^{N-2}} \sum_{\alpha \vdash_d N-1} \left(\sum_{\mu = \alpha + \square} \sqrt{d_\mu m_\mu} \right)^2,$$

  where $\mu = \alpha + \square$ denotes a Young diagram $\mu \vdash_d N$ obtained from $\alpha \vdash_d N-1$ by adding a single box (!).

- $$p_d^{\mathrm{EPR}} = \frac{1}{d^N} \sum_{\alpha \vdash_d N-1} m_\alpha^2 \frac{d_{\mu^*}}{m_{\mu^*}},$$

  where μ^* is the Young diagram obtained from $\alpha \vdash_d N-1$ by adding a single box such that $N\frac{m_\mu d_\alpha}{m_\alpha d_\mu}$ is maximal.


n = (n_1, ..., n_d)
Σ_i n_i = n
λ ⊢_d n
n_1 ≥ ... ≥ n_d
n_1
n_2

Exact expressions for F_d and p_d using RT

Exact expressions for deterministic and probabilistic PBT

[Studziński et al. 2017; Mozrzymas et al. 2017]

- $$F_d^{\mathrm{PGM,EPR}} = \frac{1}{d^{N-2}} \sum_{\alpha \vdash_d N-1} \left(\sum_{\mu=\alpha+\square} \sqrt{d_\mu m_\mu} \right)^2,$$

  where $\mu = \alpha + \square$ denotes a Young diagram $\mu \vdash_d N$ obtained from $\alpha \vdash_d N-1$ by adding a single box (!).

- $$p_d^{\mathrm{EPR}} = \frac{1}{d^N} \sum_{\alpha \vdash_d N-1} m_\alpha^2 \frac{d_{\mu^*}}{m_{\mu^*}},$$

  where μ^* is the Young diagram obtained from $\alpha \vdash_d N-1$ by adding a single box such that $N \frac{m_\mu d_\alpha}{m_\alpha d_\mu}$ is maximal.

Main result 1: deterministic PBT

For deterministic PBT using PGM and EPR, we prove:

$$F_d^{\mathrm{PGM,EPR}} = 1 - \frac{d^2 - 1}{4N} + o(N^{-1}).$$

- Recovers qubit result $F_2^{\mathrm{PGM,EPR}} = 1 - \frac{3}{4N} + o(N^{-1})$.
- Shows that $F_d^{\mathrm{PGM,EPR}} \geq 1 - \frac{d^2-1}{N}$ is not tight. (previously known from numerics)

Main result 2: probabilistic PBT

For probabilistic PBT using EPR, we prove:

$$p_d^{\mathrm{EPR}} = 1 - \sqrt{\frac{d}{N-1}}\mathbb{E}[\lambda_{\max}(\mathbf{G})] + o(N^{-1}),$$

where **G** is a Hermitian, traceless random $d \times d$ matrix with independent Gaussian RVs as entries.

- For qubits (i.e., **G** is a 2×2 matrix), one can prove
$$\mathbb{E}[\lambda_{\max}(\mathbf{G})] = 2\pi^{-1/2}.$$
- Hence, our result asymptotically recovers the qubit result
$$p_2^{\mathrm{EPR}} \sim 1 - \sqrt{\frac{8}{\pi N}} + o(N^{-1/2}).$$

Table of Contents

1 Operational setting & bounds on protocols

2 Symmetries & representation theory

3 Main results: Asymptotics of standard PBT protocols

4 Proof methods

5 Concluding remarks

Spectrum estimation & random matrix theory

- Recall the decomposition of $(\mathbb{C}^d)^{\otimes N}$ obtained from Schur-Weyl duality,

$$(\mathbb{C}^d)^{\otimes N} \cong \bigoplus_{\lambda \vdash_d N} [\lambda] \otimes V_\lambda.$$

- Consider the projective measurement $\{P_\lambda\}_{\lambda \vdash_d N}$, where P_λ projects onto $[\lambda] \otimes V_\lambda$.

Spectrum estimation [Keyl and Werner 2005]

Let $\mathbf{Y}_N$ denote the outcome of the measurement $\{P_\lambda\}_{\lambda \vdash_d N}$ applied to $\rho^{\otimes N}$ where ρ is a state. Then, as $N \to \infty$,

$$\frac{1}{N}\mathbf{Y}_N \xrightarrow{D} \mathrm{spec}(\rho).$$

Spectrum estimation & random matrix theory

- For $\rho = \frac{1}{d}\mathbb{1}$ the corresponding outcome probability distribution $p_{d,N}$ of the measurement $\{P_\lambda\}_{\lambda \vdash_d N}$ is called **Schur-Weyl distribution**:

$$p_{d,N} = d_\lambda m_\lambda / d^N.$$

- Spectrum estimation: $\frac{1}{N}\mathbf{Y}_N \xrightarrow{D} (1/d, \ldots, 1/d)$
- A "typical" Young diagram w.r.t. $p_{d,N}$ has

$$\lambda_1 \approx \frac{N}{d} + 2\sqrt{N} \qquad \lambda_d \approx \frac{N}{d} - 2\sqrt{N},$$

and the remaining λ_i's interpolate between these.

Spectrum estimation & random matrix theory

- To make this exact, define the centered and normalized RV

$$\mathbf{A}_N = \frac{\lambda_N - (N/d, \ldots, N/d)}{\sqrt{N/d}},$$

where $\lambda_N \sim p_{d,N}$ takes values in the set of Young diagrams.

- Let $\mathbf{M}$ be a Hermitian random matrix whose entries are independent Gaussian RVs

(df: $\exp(-\frac{1}{2}\operatorname{Tr}\mathbf{H}^2)$ where $\mathbf{H}$ is a Hermitian matrix-valued RV.)

- Define $\mathbf{M}_0 = \mathbf{M} - \frac{\operatorname{Tr}(\mathbf{M})}{d}\mathbb{1}$, called the **traceless Gaussian unitary ensemble** $\mathrm{GUE}_0(d)$.

Spectrum estimation & random matrix theory

Fluctuations of Schur-Weyl distribution [Johansson 2001]

For the centered and normalized RV $\mathbf{A}_N$,

$$\mathbf{A}_N \xrightarrow{D} \mathrm{spec}(\mathbf{G}),$$

where $\mathbf{G} \sim \mathrm{GUE}_0(d)$ is drawn from the traceless Gaussian unitary ensemble.

- A strengthening of Johansson's result allows us to determine asymptotics of the RT-formulae by [Studziński et al. 2017] and [Mozrzymas et al. 2017].

Proof idea: probabilistic PBT

- Recall formula: $p_d^{\mathrm{EPR}} = \frac{1}{d^N} \sum_{\alpha \vdash_d N-1} m_\alpha^2 \frac{d_{\mu^*}}{m_{\mu^*}}$,

  where μ^* is the Young diagram obtained from $\alpha \vdash_d N-1$ by adding a single box such that $N\frac{m_\mu d_\alpha}{m_\alpha d_\mu}$ is maximal.
- First step: Prove that

$$\frac{m_\mu d_\alpha}{m_\alpha d_\mu} = \frac{\alpha_i - i + d + 1}{N}$$

  $\longrightarrow$ maximized by choosing $i = 1$.
- Second step: Rewrite $p_d^{\mathrm{EPR}} = \frac{N}{d}\mathbb{E}_\alpha[(\alpha_1 + d)^{-1}]$.
- Show result by proving **uniform integrability** of A_i^k.

  (such that $\mathbb{E}_\alpha[A_1^k] \xrightarrow{N\to\infty} \mathbb{E}[\lambda_{\max}(\mathbf{G})^k]$)

Proof idea: deterministic PBT

- Recall: $F_d^{\text{PGM,EPR}} = \frac{1}{d^{N-2}} \sum_{\alpha \vdash_d N-1} \left(\sum_{\mu=\alpha+\square} \sqrt{d_\mu m_\mu} \right)^2$,

  where $\mu = \alpha + \square$ denotes a Young diagram $\mu \vdash_d N$ obtained from $\alpha \vdash_d N-1$ by adding a single box.

- Rewrite: $F_d^{\text{PGM,EPR}} \propto \mathbb{E}_\alpha \left[\left(\sum_{\mu=\alpha+\square} f(\alpha_i^{-1}, \mu_i^{-1}) \right)^2 \right]$.

- Remember: Typical Young diagrams have echelon form, where you can add a box to every row.

- Contribution of atypical YD is negligible in the expectation value $\mathbb{E}_\alpha[\cdot]$, and hence $\mu = \alpha + \square \longrightarrow \mu = \alpha + e_i$.

Summary

- We discussed port-based teleportation (PBT) and its two variants:
  - deterministic PBT with entanglement fidelity F_d;
  - probabilistic PBT with success probability p_d.
- PBT protocols have a number of inherent symmetries that give rise to closed representation-theoretic formulas for F_d and p_d.
- Using a connection between Young diagrams and Gaussian unitary ensembles, we were able to determine the asymptotics of some of these formulae.

Converse bound

- We also show the following general converse on PBT:

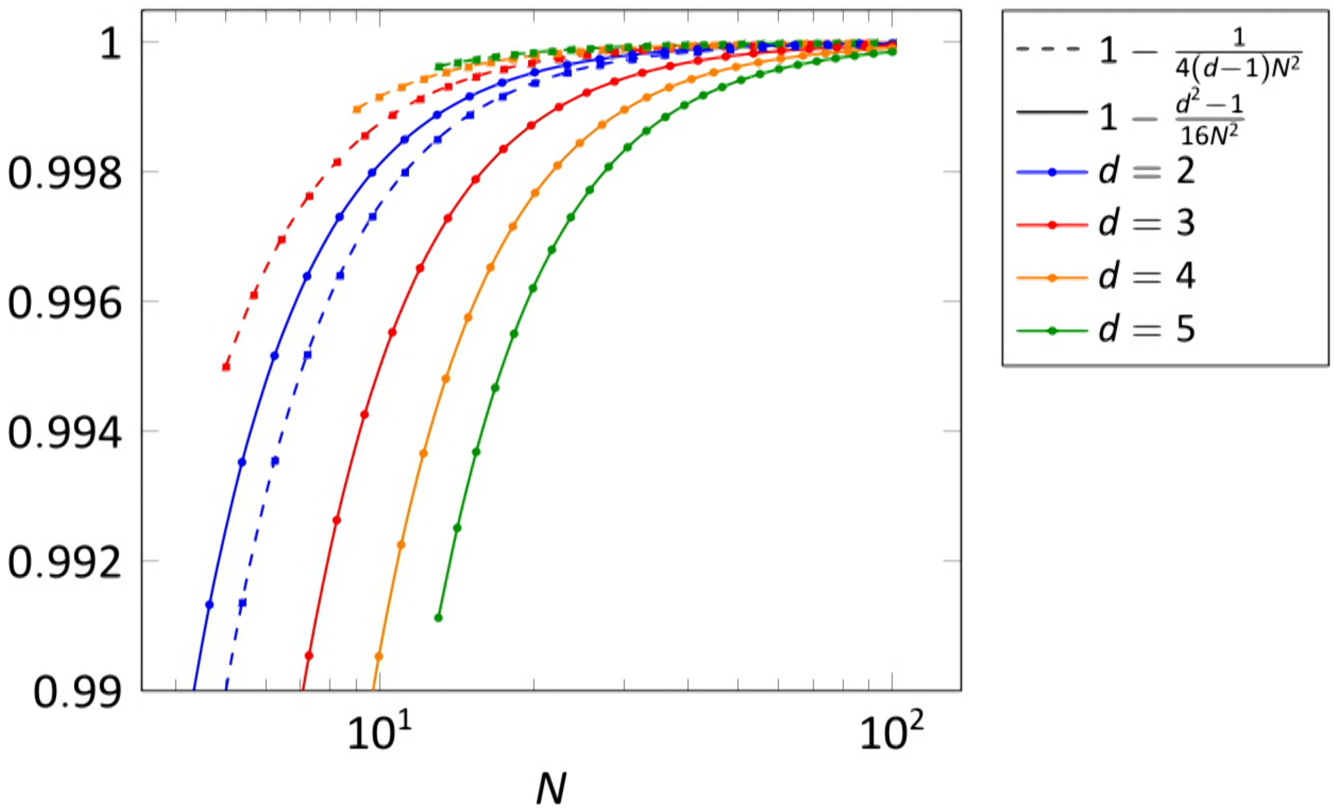
Main result 3: Converse bound

For an arbitrary PBT protocol,

$$F_d \leq \begin{cases} \dfrac{\sqrt{N}}{d} & \text{if } N \leq d^2/2, \\ 1 - \dfrac{d^2-1}{16N^2} & \text{else.} \end{cases}$$

- Tighter for $d > 2$ than converse bound $F_d \leq 1 - \frac{1}{4(d-1)N^2} + O(N^{-3})$ from [Ishizaka 2015].

Converse bounds: comparison



Open problems

- [Mozrzymas et al. 2017] derive the following closed expression of F_d^* in the fully optimized case:

$$F_d^* = d^{-N-2} \max_{c_\mu} \sum_{\alpha \vdash_d N-1} \left(\sum_{\mu = \alpha + \square} \sqrt{c_\mu d_\mu m_\mu} \right)^2,$$

where the optimization is over all sets of nonnegative coefficients $\{c_\mu\}$ such that

$$\sum_{\mu \vdash_d N} \frac{c_\mu d_\mu m_\mu}{d^N} = 1.$$

- Open problem: Determine asymptotics of F_d^* using (extension of) our methods (or in another way)!

References

Beigi, S. and R. König (2011). *New Journal of Physics* 13.9, p. 093036. arXiv: 1101.1065 [quant-ph].

Buhrman, H. et al. (2014). *SIAM Journal on Computing* 43.1, pp. 150–178. arXiv: 1009.2490 [quant-ph].

Ishizaka, S. (2015). *arXiv preprint*. arXiv: 1506.01555 [quant-ph].

Ishizaka, S. and T. Hiroshima (2008). *Physical Review Letters* 101.24, p. 240501. arXiv: 0807.4568 [quant-ph].

— (2009). *Physical Review A* 79.4, p. 042306. arXiv: 0901.2975 [quant-ph].

Johansson, K. (2001). *Annals of Mathematics* 153.1, pp. 259–296. arXiv: math/9906120 [math.CO].

Keyl, M. and R. F. Werner (2005). World Scientific, pp. 458–467. arXiv: quant-ph/0102027.

Mozrzymas, M. et al. (2017). *arXiv preprint*. arXiv: 1707.08456 [quant-ph].

Studziński, M. et al. (2017). *Scientific Reports* 7, p. 10871. arXiv: 1612.09260 [quant-ph].

Thank you very much for your attention!