Title: Entanglement of assistance and random distillation

Date: Nov 21, 2007 04:00 PM

URL: http://pirsa.org/07110068

Abstract: A class of operations distinct to entangled states shared between more than two parties is their conversion to entangled states shared between fewer parties. The extent to which these can be achieved in the regime of local operations and classical communication provides an operational characterisation of multiparty states, for example in the \"entanglement of assistance\" and related quantities. I will give a brief overview of this topic and discuss our results showing qualitatively different behaviour when the parties receiving the final state are not chosen beforehand.

Entanglement of assistance and random distillation[1]

Ben Fortescue Hoi-Kwong Lo

Center for Quantum Information and Quantum Control
Dept. of Electrical and Computer Engineering and Dept. of Physics
University of Toronto

Perimeter Institute, 21st November 2007

[1] Phys. Rev. Lett. 98, 260501 (2007), arXiv:0709.4059 (2007)

Entanglement of assistance and random distillation[1]

Ben Fortescue   Hoi-Kwong Lo

Center for Quantum Information and Quantum Control
Dept. of Electrical and Computer Engineering and Dept. of Physics
University of Toronto

Perimeter Institute, 21st November 2007

[1] Phys. Rev. Lett. 98, 260501 (2007), arXiv:0709.4059 (2007)

Outline

Introduction

If several parties share an entangled state, and want to convert it through local operations and classical communication (LOCC) to a state shared between fewer parties, what can and can't they achieve?

Introduction

If several parties share an entangled state, and want to convert it through local operations and classical communication (LOCC) to a state shared between fewer parties, what can and can't they achieve?

Does how we choose the parties matter?

Entanglement of assistance

First proposed by DiVincenzo *et al* (1998) and Cohen (1998)

Entanglement of assistance

First proposed by DiVincenzo *et al* (1998) and Cohen (1998)

For a three-party pure state $|\Psi\rangle_{ABC}$, entanglement measure E, the entanglement of assistance $E_a(\rho_{AB}) = \max(p_i E(\psi_i))$, maximised over decompositions $\rho_{AB} = \mathrm{tr}_C|\Psi_{ABC}\rangle\langle\Psi_{ABC}| = \sum_i p_i \psi_i$.

Entanglement of assistance

First proposed by DiVincenzo *et al* (1998) and Cohen (1998)

For a three-party pure state $|\Psi\rangle_{ABC}$, entanglement measure E, the entanglement of assistance $E_a(\rho_{AB}) = \max(p_i E(\psi_i))$, maximised over decompositions $\rho_{AB} = \mathrm{tr}_C |\Psi_{ABC}\rangle\langle\Psi_{ABC}| = \sum_i p_i \psi_i$.

Highest expected entanglement of Alice and Bob after Charlie makes a measurement and broadcasts his result. (Not general LOCC).

Properties of entanglement of assistance

Properties of entanglement of assistance

1. For three-party pure states, can be defined by reference to ρ_{AB} only.

Properties of entanglement of assistance

1. For three-party pure states, can be defined by reference to ρ_{AB} only.
2. Can be calculated for pure-state concurrence of assistance of two qubits (Laustsen, Verstraete, Van Enk (2003)), or for asymptotic distillable entanglement (Smolin et al, (2005))

Properties of entanglement of assistance

1. For three-party pure states, can be defined by reference to ρ_{AB} only.
2. Can be calculated for pure-state concurrence of assistance of two qubits (Laustsen, Verstraete, Van Enk (2003)), or for asymptotic distillable entanglement (Smolin et al, (2005))
3. Not a bipartite measure or tripartite monotone (Gour & Spekkens (2006))

General LOCC

General LOCC

Can instead consider expected entanglement after general LOCC.
"Assisted entanglement" or "Entanglement of collaboration" C.

General LOCC

Can instead consider expected entanglement after general LOCC.
"Assisted entanglement" or "Entanglement of collaboration" C.
For three parties:

1. For E=distillable entanglement, pure state, many copies, $C = E_a = \min\{S(\rho_A), S(\rho_B)\}$ (Smolin et al, (2005)). (S=Von Neumann entropy)

General LOCC

Can instead consider expected entanglement after general LOCC.
"Assisted entanglement" or "Entanglement of collaboration" C.
For three parties:

1. For E=distillable entanglement, pure state, many copies, $C = E_a = \min\{S(\rho_A), S(\rho_B)\}$ (Smolin et al, (2005)). (S=Von Neumann entropy)
2. For E=concurrence, single copy, pure state, $C = E_a$. (Gour (2006))

General LOCC

Can instead consider expected entanglement after general LOCC.
"Assisted entanglement" or "Entanglement of collaboration" C.
For three parties:

1. For E=distillable entanglement, pure state, many copies, $C = E_a = \min\{S(\rho_A), S(\rho_B)\}$ (Smolin et al, (2005)). (S=Von Neumann entropy)
2. For E=concurrence, single copy, pure state, $C = E_a$. (Gour (2006))
3. For > 3 parties:
   For E=distillable entanglement, pure state, many copies, $C = \min\{S(AT), S(B\overline{T})\}$ (Horodecki, Oppenheim & Winter (2005))

Definitions - chosen parties

Definitions - chosen parties

For an m-party pure-state $\psi_{P_1 \dots P_m}$, being converted to EPR pairs $|\Phi\rangle_{P_i P_j}$ shared between *specified* parties P_i, P_j under m-party LOCC.

Definitions - chosen parties

For an m-party pure-state $\psi_{P_1 \ldots P_m}$, being converted to EPR pairs $|\Phi\rangle_{P_iP_j}$ shared between *specified* parties P_i, P_j under m-party LOCC.

$$\psi \underbrace{\rightarrow}_{LOCC} |\Phi\rangle^{\otimes M}_{P_iP_j}$$

$$E_{A_{ij}} \equiv \max(\langle M \rangle)$$

(Assisted distillable entanglement).

Definitions - chosen parties

For an m-party pure-state $\psi_{P_1 \ldots P_m}$, being converted to EPR pairs $|\Phi\rangle_{P_i P_j}$ shared between *specified* parties P_i, P_j under m-party LOCC.

$$\psi \underbrace{\rightarrow}_{LOCC} |\Phi\rangle_{P_i P_j}^{\otimes M}$$

$$E_{A_{ij}} \equiv \max(\langle M \rangle)$$

(Assisted distillable entanglement).

$$\text{Asymptotically } \psi^{\otimes N} \rightarrow |\Phi\rangle_{P_i P_j}^{\otimes M}, \quad M, N \rightarrow \infty$$

$$E_{A_{ij}}^{\infty} \equiv \max \frac{M}{N}$$

Specified entanglement

Specified entanglement

Maximising over all pairs - "specified entanglement" E_{sp}.

$$E_{sp}(\psi) \equiv \max_{ij} E_{A_{ij}}$$

$$E_{sp}^{\infty}(\psi) \equiv \max_{ij} E_{A_{ij}}^{\infty}$$

Bounds on E_A

Bounds on E_A

Multiple copies

$$E^{\infty}_{A_{ij}}(\psi) \leq \min(S(P_i), S(P_j))$$

Hence $E^{\infty}_{sp}(\psi) \leq$ second largest $S(P_i)$.

Bounds on E_A

Multiple copies

$$E^{\infty}_{A_{ij}}(\psi) \leq \min(S(P_i), S(P_j))$$

Hence $E^{\infty}_{sp}(\psi) \leq$ second largest $S(P_i)$.

Single copy

For a single copy E_A can be bound using the concurrence of assistance G_A.

$$E_{A_{ij}}(\psi) \leq G_{A_{ij}}(\psi)$$

Definitions - random parties

Alternatively, we try to make as many EPRs as we can, irrespective of which parties share them - "total entanglement" E_t.

Definitions - random parties

Alternatively, we try to make as many EPRs as we can, irrespective of which parties share them - "total entanglement" E_t.

$$|\psi\rangle^{\otimes N}_{P_1 \dots P_m} \longrightarrow \bigotimes_{ij} |\Phi\rangle^{\otimes N_{P_i P_j}}_{P_i P_j}$$

$$E_t^{\infty}(\psi) = \sup \frac{\sum_{ij} N_{P_i P_j}}{N}$$

Definitions - summary

Definitions - summary

1. "Assisted entanglement" E_A^∞ - how many EPRs we can make through LOCC between two chosen parties from a multiparty state.

Definitions - summary

1. "Assisted entanglement" E_A^∞ - how many EPRs we can make through LOCC between two chosen parties from a multiparty state.
2. "Specified entanglement" E_{sp}^∞ - the assisted entanglement, maximised over all pairs.

Definitions - summary

1. "Assisted entanglement" E_A^∞ - how many EPRs we can make through LOCC between two chosen parties from a multiparty state.
2. "Specified entanglement" E_{sp}^∞ - the assisted entanglement, maximised over all pairs.
3. "Total entanglement" E_t^∞ - how many EPRs we can make through LOCC from a multiparty state, irrespective of who shares them.

2 New results - random distillation and the W state

- EPR from W
- Bounds

Specified parties

For the three-party W state shared between Alice, Bob and Charlie:

$$|W\rangle = \frac{1}{\sqrt{3}}(|100\rangle + |010\rangle + |001\rangle)_{ABC} :$$

Specified parties

For the three-party W state shared between Alice, Bob and Charlie:

$$|W\rangle = \frac{1}{\sqrt{3}}(|100\rangle + |010\rangle + |001\rangle)_{ABC} :$$

$$E_{sp}(W) = 2/3$$
$$E_{sp}^{\infty}(W) = H_2(1/3) \approx 0.92$$

Specified parties

For the three-party W state shared between Alice, Bob and Charlie:

$$|W\rangle = \frac{1}{\sqrt{3}}(|100\rangle + |010\rangle + |001\rangle)_{ABC} :$$

$$E_{sp}(W) = 2/3$$
$$E_{sp}^{\infty}(W) = H_2(1/3) \approx 0.92$$

Can't reliably make 1 EPR per W for specified parties.

Random parties

What if we don't specify the parties?

Random parties

What if we don't specify the parties?
Surprisingly...

Theorem 1.

$$E_t^{\infty}(W) \geq 1$$

Random parties

What if we don't specify the parties?
Surprisingly...

Theorem 1.

$$E_t^{\infty}(W) \geq 1$$

Can always make an EPR between *random* parties.

Random parties

What if we don't specify the parties?
Surprisingly...

Theorem 1.

$$E_t^{\infty}(W) \geq 1$$

Can always make an EPR between *random* parties.
(Optimal for a single copy, conjectured to be optimal for many copies)

The protocol 1

Alice, Bob and Charlie each apply the unitary

$$|1\rangle \longrightarrow |1\rangle, \quad |0\rangle \longrightarrow \sqrt{1-\epsilon^2}|0\rangle + \epsilon|2\rangle$$

The protocol 1

Alice, Bob and Charlie each apply the unitary

$$|1\rangle \longrightarrow |1\rangle, \quad |0\rangle \longrightarrow \sqrt{1-\epsilon^2}|0\rangle + \epsilon|2\rangle$$

then

$$|W\rangle_{ABC} \longrightarrow (1-\epsilon^2)|W\rangle + \frac{\epsilon}{\sqrt{3}}(|021\rangle + |201\rangle + |012\rangle + |210\rangle + |102\rangle + |120\rangle) + O(\epsilon^2)$$

The protocol 2

All 3 parties perform the projection

$$A = |0\rangle\langle 0| + |1\rangle\langle 1|, \quad B = |2\rangle\langle 2|$$

The protocol 2

All 3 parties perform the projection

$$A = |0\rangle\langle 0| + |1\rangle\langle 1|, \quad B = |2\rangle\langle 2|$$

Possible outcomes:

1. All 3 parties get "A", (prob $(1-\epsilon^2)^2$), share a W again, unitaries+measurements repeated.

The protocol 2

All 3 parties perform the projection

$$A = |0\rangle\langle 0| + |1\rangle\langle 1|, \quad B = |2\rangle\langle 2|$$

Possible outcomes:

1. All 3 parties get "A", (prob $(1-\epsilon^2)^2$), share a W again, unitaries+measurements repeated.
2. One party (e.g. Alice) gets "B" (total prob $2\epsilon^2(1-\epsilon^2)$), then state is $|2\rangle_A \otimes \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{BC}$. Bob and Charlie share an EPR.

The protocol 2

All 3 parties perform the projection

$$A = |0\rangle\langle 0| + |1\rangle\langle 1|, \quad B = |2\rangle\langle 2|$$

Possible outcomes:

1. All 3 parties get "A", (prob $(1-\epsilon^2)^2$), share a W again, unitaries+measurements repeated.
2. One party (e.g. Alice) gets "B" (total prob $2\epsilon^2(1-\epsilon^2)$), then state is $|2\rangle_A \otimes \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{BC}$. Bob and Charlie share an EPR.
3. 2 or more parties get "B" (prob $O(\epsilon^4)$).

The protocol 2

All 3 parties perform the projection

$$A = |0\rangle\langle 0| + |1\rangle\langle 1|, \quad B = |2\rangle\langle 2|$$

Possible outcomes:

1. All 3 parties get "A", (prob $(1-\epsilon^2)^2$), share a W again, unitaries+measurements repeated.
2. One party (e.g. Alice) gets "B" (total prob $2\epsilon^2(1-\epsilon^2)$), then state is $|2\rangle_A \otimes \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{BC}$. Bob and Charlie share an EPR.
3. 2 or more parties get "B" (prob $O(\epsilon^4)$).

In limit of many rounds, small ϵ, 2 *random* parties always get an EPR.

A classical analogue

A classical analogue

1. 3 bits $\{1, 0, 0\}$ randomly distributed between Alice, Bob and Charlie.

A classical analogue

1. 3 bits $\{1, 0, 0\}$ randomly distributed between Alice, Bob and Charlie.
2. Each party checks their bit. Parties with a 0 pick an integer $J' \in \{1 \ldots K\}$ (K large).

A classical analogue

1. 3 bits $\{1, 0, 0\}$ randomly distributed between Alice, Bob and Charlie.
2. Each party checks their bit. Parties with a 0 pick an integer $J' \in \{1 \ldots K\}$ (K large).
3. In each round (publically announced), parties with a 0 privately generate a new random integer $J \in \{1 \ldots K\}$. If $J = J'$ that party publically announces that they have a 0, protocol terminates, otherwise repeat.

A classical analogue

1. 3 bits $\{1,0,0\}$ randomly distributed between Alice, Bob and Charlie.
2. Each party checks their bit. Parties with a 0 pick an integer $J' \in \{1 \ldots K\}$ (K large).
3. In each round (publically announced), parties with a 0 privately generate a new random integer $J \in \{1 \ldots K\}$. If $J = J'$ that party publically announces that they have a 0, protocol terminates, otherwise repeat.
4. When protocol terminates remaining 2 parties either have $\{1,0\}$ or $\{0,1\}$ and they (but not an eavesdropper) know which - they share a random bit.

A classical analogue

1. 3 bits $\{1, 0, 0\}$ randomly distributed between Alice, Bob and Charlie.
2. Each party checks their bit. Parties with a 0 pick an integer $J' \in \{1 \dots K\}$ (K large).
3. In each round (publically announced), parties with a 0 privately generate a new random integer $J \in \{1 \dots K\}$. If $J = J'$ that party publically announces that they have a 0, protocol terminates, otherwise repeat.
4. When protocol terminates remaining 2 parties either have $\{1, 0\}$ or $\{0, 1\}$ and they (but not an eavesdropper) know which - they share a random bit.

In limit of many rounds, large K, 2 random parties always get a shared secure bit.

Finite rounds

For finite rounds, increase ϵ as fewer rounds remain. Use ϵ_N for N remaining arounds.

Finite rounds

For finite rounds, increase ϵ as fewer rounds remain. Use ϵ_N for N remaining arounds.

Optimum $\epsilon_N = \frac{1}{\sqrt{N+1}}$.
Prob(EPR)=$\frac{N}{N+1}$.

Finite rounds

For finite rounds, increase ϵ as fewer rounds remain. Use ϵ_N for N remaining arounds.

Optimum $\epsilon_N = \frac{1}{\sqrt{N+1}}$.
Prob(EPR)$=\frac{N}{N+1}$.

Protocol beats $E_{sp}(W)$ for $N \geq 3$, beats $E_{sp}^{\infty}(W)$ for $N \geq 12$.

Tripartite distillation

Can get any 3-qubit state $|\alpha\rangle_{ABC}$ from W at an asymptotic rate $\geq 1/2$:

Tripartite distillation

Can get any 3-qubit state $|\alpha\rangle_{ABC}$ from W at an asymptotic rate $\geq 1/2$:

- Distill $|W\rangle_{ABC}^{\otimes N} \to |\Phi\rangle_{AB}^{\otimes \frac{N}{3}} |\Phi\rangle_{BC}^{\otimes \frac{N}{3}} |\Phi\rangle_{AC}^{\otimes \frac{N}{3}}$, $N \to \infty$

Tripartite distillation

Can get any 3-qubit state $|\alpha\rangle_{ABC}$ from W at an asymptotic rate $\geq 1/2$:

- Distill $|W\rangle_{ABC}^{\otimes N} \to |\Phi\rangle_{AB}^{\otimes \frac{N}{3}} |\Phi\rangle_{BC}^{\otimes \frac{N}{3}} |\Phi\rangle_{AC}^{\otimes \frac{N}{3}}$, $N \to \infty$
- Teleport $|\alpha\rangle_{A}^{\otimes \frac{N}{6}} \to |\alpha\rangle_{ABC}^{\otimes \frac{N}{6}}$, likewise for Bob and Charlie.

Upper-bounding the EPR yield - 3 parties

How large can E_t^{∞} be?

Upper-bounding the EPR yield - 3 parties

How large can E_t^∞ be?

Linden *et al* (2005)

For LOCC on pure ρ_{ABC}:

$$\langle E_r(\rho_{BC})\rangle_{\mathrm{final}} - E_r(\rho_{BC})_{\mathrm{initial}} \leq S(\rho_A)_{\mathrm{initial}} - \langle S(\rho_A)\rangle_{\mathrm{final}}$$

Upper-bounding the EPR yield - 3 parties

How large can E_t^∞ be?

Linden *et al* (2005)

For LOCC on pure ρ_{ABC}:

$$\langle E_r(\rho_{BC})\rangle_{\mathrm{final}} - E_r(\rho_{BC})_{\mathrm{initial}} \leq S(\rho_A)_{\mathrm{initial}} - \langle S(\rho_A)\rangle_{\mathrm{final}}$$

leading to

Theorem 2.

$$E_t^\infty(\sigma_{ABC}) \leq \min\{S(\sigma_{BC}) + E_r^\infty(\sigma_{BC}), S(\sigma_{AC}) + E_r^\infty(\sigma_{AC}), S(\sigma_{AB}) + E_r^\infty(\sigma_{AB})\}$$

(E_r =relative entropy of entanglement)

Upper-bounding the EPR yield - M parties

Upper-bounding the EPR yield - M parties

Theorem 3.

For an M-party pure state $\sigma_{A_1 \ldots A_M}$.

$$E_t^{\infty}(\sigma) \leq E_r^{\infty}(\sigma)$$

(follows from Plenio & Vedral (2001))

Upper-bounding the EPR yield - M parties

Theorem 3.

For an M-party pure state $\sigma_{A_1 \ldots A_M}$.

$$E_t^{\infty}(\sigma) \leq E_r^{\infty}(\sigma)$$

(follows from Plenio & Vedral (2001))
In general looser than 3-party bound, but same result for W

$$E_t^{\infty}(W) \leq E_r^{\infty}(W) \leq E_r(W) = \log_2(9/4) \approx 1.17$$

Upper-bounding the EPR yield - M parties

Theorem 3.

For an M-party pure state $\sigma_{A_1 \ldots A_M}$.

$$E_t^{\infty}(\sigma) \leq E_r^{\infty}(\sigma)$$

(follows from Plenio & Vedral (2001))
In general looser than 3-party bound, but same result for W

$$E_t^{\infty}(W) \leq E_r^{\infty}(W) \leq E_r(W) = \log_2(9/4) \approx 1.17$$

"Lower bound on upper bound" (Galvão, Plenio & Virmani, 2000)

$$E_r^{\infty}(W) \geq \log_2(3) - 5/9 \approx 1.03$$

(Can't prove conjecture using E_r alone)

GHZ-like states

GHZ-like states

(Plenio & Vedral (2005)) For states

$$|GHZ'\rangle = \alpha|000\rangle + \beta|111\rangle.$$

GHZ-like states

(Plenio & Vedral (2005)) For states

$$|GHZ'\rangle = \alpha|000\rangle + \beta|111\rangle,$$

$$E_r^\infty(GHZ') = E_{sp}(GHZ') = H_2(|\alpha|^2)$$

GHZ-like states

(Plenio & Vedral (2005)) For states

$$|GHZ'\rangle = \alpha|000\rangle + \beta|111\rangle,$$

$$E_r^\infty(GHZ') = E_{sp}(GHZ') = H_2(|\alpha|^2)$$

No advantage to random distillation.

3. More general states
   - 3-qubit classes
   - More parties

W and GHZ class

Dür *et al*, (2000)

Pure 3 qubit states can be divided into 2 classes (W and GHZ), single copies from different classes not interconvertible through SLOCC.

W and GHZ class

Dür *et al*, (2000)

Pure 3 qubit states can be divided into 2 classes (W and GHZ), single copies from different classes not interconvertible through SLOCC.

What random distillation properties do these classes have?

Symmetric states - simple protocol

Symmetric states - simple protocol

1. For 3-qubit symmetric state, pick a basis where Alice measuring $|0\rangle$ corresponds to large Bob-Charlie entanglement.

$$|\psi_1\rangle_{ABC} = |0\rangle_A(\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle)_{BC} + |1\rangle_{BC}(\ldots)$$

Symmetric states - simple protocol

1. For 3-qubit symmetric state, pick a basis where Alice measuring $|0\rangle$ corresponds to large Bob-Charlie entanglement.

$$|\psi_1\rangle_{ABC} = |0\rangle_A(\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle)_{BC} + |1\rangle_{BC}(\dots)$$

2. Perform the W distillation protocol repeatedly, seeking measurement of $|0\rangle$. In general, failed rounds change coefficients $\alpha, \beta, \gamma, \delta$.

Symmetric states - simple protocol

1. For 3-qubit symmetric state, pick a basis where Alice measuring $|0\rangle$ corresponds to large Bob-Charlie entanglement.

$$|\psi_1\rangle_{ABC} = |0\rangle_A(\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle)_{BC} + |1\rangle_{BC}(\dots)$$

2. Perform the W distillation protocol repeatedly, seeking measurement of $|0\rangle$. In general, failed rounds change coefficients $\alpha, \beta, \gamma, \delta$.
3. Hard to calculate $\langle S_{BC}\rangle$, so use the concurrence $\langle q \equiv 2|\beta\gamma - \alpha\delta|\rangle$. S convex in q, hence can lower-bound S.

Symmetric states - simple protocol

1. For 3-qubit symmetric state, pick a basis where Alice measuring $|0\rangle$ corresponds to large Bob-Charlie entanglement.

$$|\psi_1\rangle_{ABC} = |0\rangle_A(\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle)_{BC} + |1\rangle_{BC}(\ldots)$$

2. Perform the W distillation protocol repeatedly, seeking measurement of $|0\rangle$. In general, failed rounds change coefficients $\alpha, \beta, \gamma, \delta$.
3. Hard to calculate $\langle S_{BC}\rangle$, so use the concurrence $\langle q \equiv 2|\beta\gamma - \alpha\delta|\rangle$. S convex in q, hence can lower-bound S.
4. For a symmetric state $E_t \geq 3 \times \langle S_{BC}\rangle$.

Symmetric states - simple protocol

1. For 3-qubit symmetric state, pick a basis where Alice measuring $|0\rangle$ corresponds to large Bob-Charlie entanglement.

$$|\psi_1\rangle_{ABC} = |0\rangle_A(\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle)_{BC} + |1\rangle_{BC}(\dots)$$

2. Perform the W distillation protocol repeatedly, seeking measurement of $|0\rangle$. In general, failed rounds change coefficients $\alpha, \beta, \gamma, \delta$.
3. Hard to calculate $\langle S_{BC}\rangle$, so use the concurrence $\langle q \equiv 2|\beta\gamma - \alpha\delta|\rangle$. S convex in q, hence can lower-bound S.
4. For a symmetric state $E_t \geq 3 \times \langle S_{BC}\rangle$.

Protocol:filter to symmetric state, then do random distillation.

Results

Results

For all W–class states

$$|W'\rangle = (\alpha|100\rangle + \beta|010\rangle + \gamma|001\rangle + \delta|000\rangle)$$

($\{\alpha, \beta, \gamma, \delta\} \in \mathbb{R}$, and $\alpha, \beta, \gamma > 0, \delta \geq 0$.)

Results

For all W–class states

$$|W'\rangle = (\alpha|100\rangle + \beta|010\rangle + \gamma|001\rangle + \delta|000\rangle)$$

($\{\alpha, \beta, \gamma, \delta\} \in \mathbb{R}$, and $\alpha, \beta, \gamma > 0, \delta \geq 0$.)

Theorem 4.

$$E_t^{\infty}(W) \geq E_{sp}^{\infty}(W)$$

Random distillation is always advantageous for the W class.

Results

For all W–class states

$$|W'\rangle = (\alpha|100\rangle + \beta|010\rangle + \gamma|001\rangle + \delta|000\rangle)$$

$(\{\alpha, \beta, \gamma, \delta\} \in \mathbb{R}$, and $\alpha, \beta, \gamma > 0, \delta \geq 0.)$

Theorem 4.

$$E_t^\infty(W) \geq E_{sp}^\infty(W)$$

Random distillation is always advantageous for the W class.
For GHZ class, random distillation is sometimes advantageous.
E.g. for

$$|\psi_G\rangle = \alpha(|100\rangle + |010\rangle + |001\rangle) + \epsilon|111\rangle, \quad \epsilon = \sqrt{1 - 3\alpha^2}, \alpha \geq 7/32$$

Multi-party W state

$$|W_M\rangle = \frac{1}{\sqrt{M}}\left(|\underbrace{00\ldots0}_{M-1}1\rangle + (\text{permutations})\right)$$

$(W_3 = W,\ W_2 = EPR)$

Multi-party W state

$$|W_M\rangle = \frac{1}{\sqrt{M}}\left(|\underbrace{00\ldots0}_{M-1}1\rangle + (\text{permutations})\right)$$

$(W_3 = W,\ W_2 = EPR)$

Random distillation protocol takes $W_M \to W_{M-1}$ (randomly shared). Eventually to EPR.

Multi-party W state

$$|W_M\rangle = \frac{1}{\sqrt{M}}\left(|\underbrace{00\ldots0}_{M-1}1\rangle + (\text{permutations})\right)$$

$(W_3 = W,\ W_2 = EPR)$
Random distillation protocol takes $W_M \rightarrow W_{M-1}$ (randomly shared). Eventually to EPR. Hence:

$$E_{sp}^{\infty}(W_M) = H_2(1/M)$$
$$E_t^{\infty}(W_M) \geq 1$$

Multi-party W state

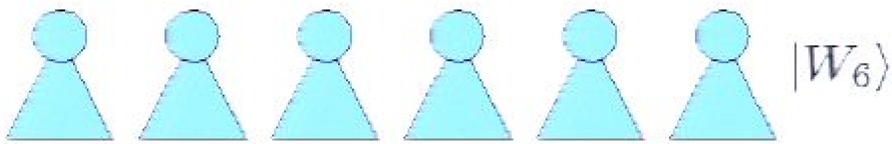
$$|W_M\rangle = \frac{1}{\sqrt{M}}\left(|\underbrace{00\ldots0}_{M-1}1\rangle + (\text{permutations})\right)$$

$(W_3 = W,\ W_2 = EPR)$
Random distillation protocol takes $W_M \to W_{M-1}$ (randomly shared). Eventually to EPR. Hence:

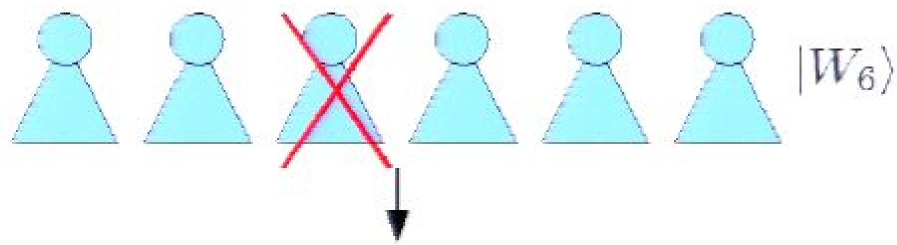
$$E_{sp}^{\infty}(W_M) = H_2(1/M)$$
$$E_t^{\infty}(W_M) \geq 1$$

Can always get an EPR between random parties even though probability between specified parties is arbitrarily small.

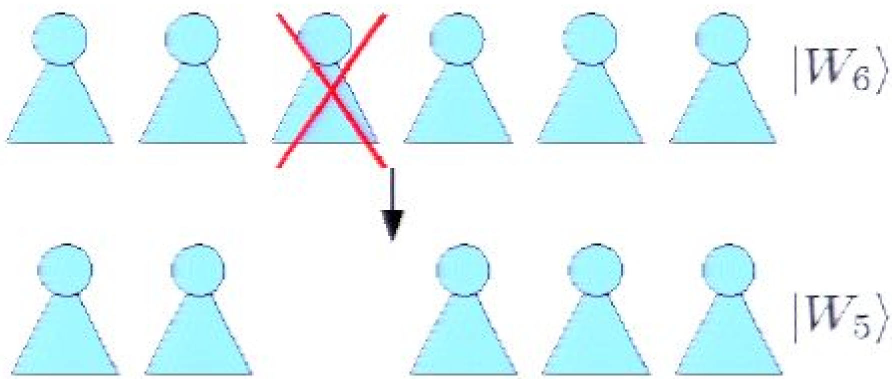
Multi-party W



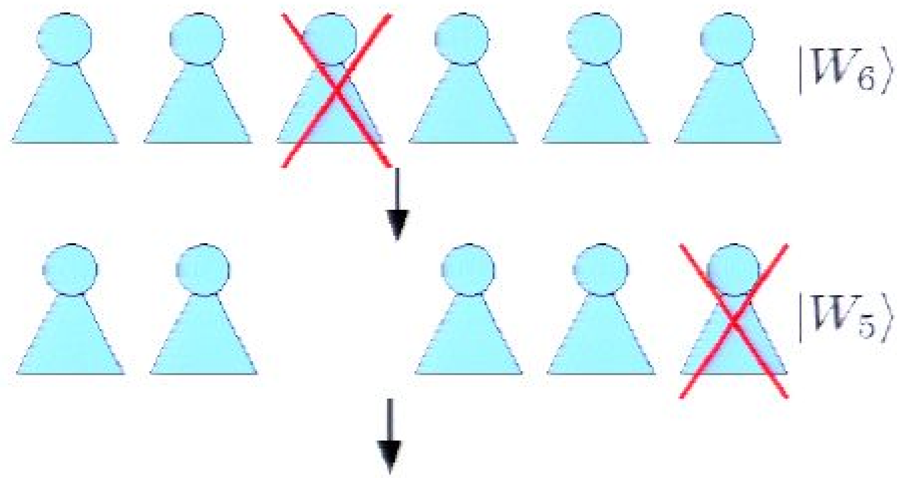
Multi-party W



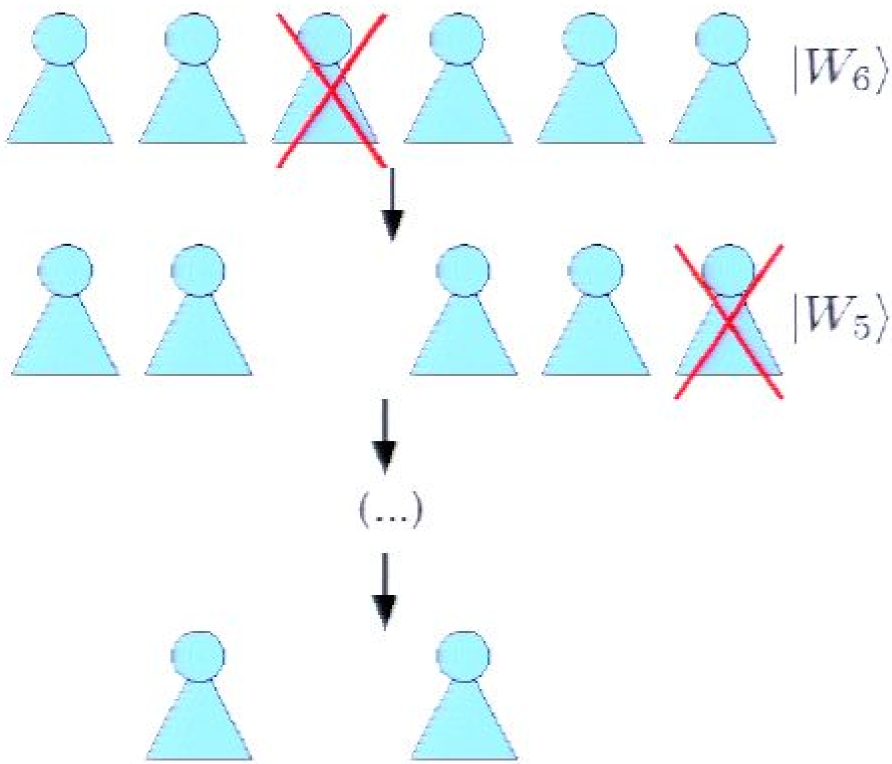
Multi-party W



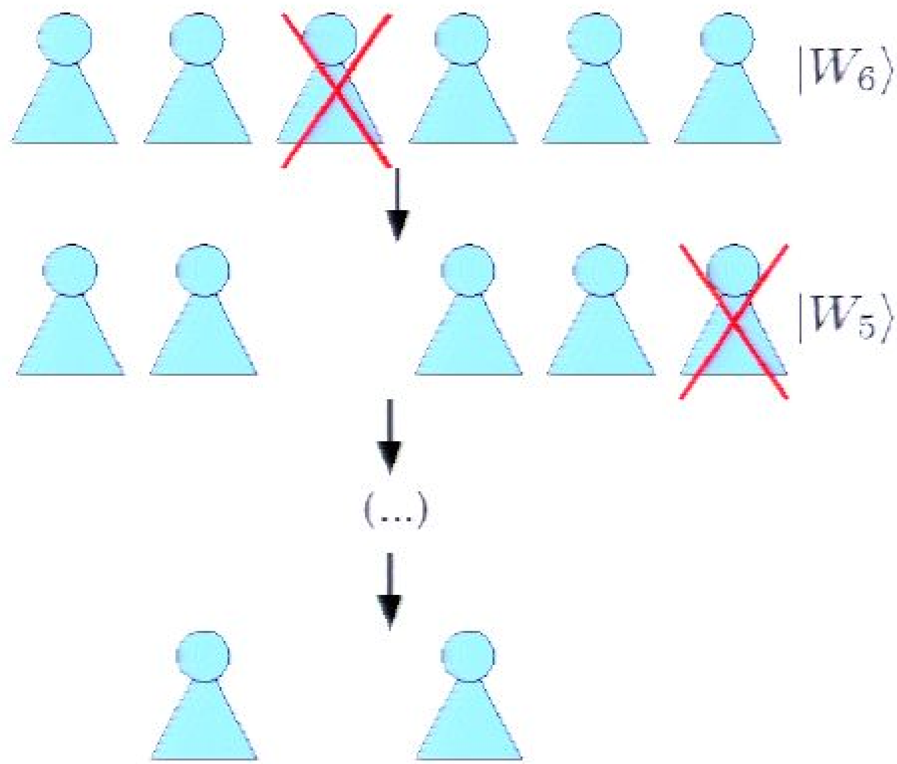
Multi-party W



Multi-party W



Multi-party W



Symmetric Dicke states $\psi(M, N)$

Symmetric superposition of all states of M qubits, N in state 1 e.g.

$$|\psi(4,2)\rangle = \frac{1}{\sqrt{6}}\Big(|0011\rangle + |0110\rangle + |1100\rangle + |1001\rangle + |1010\rangle + |0101\rangle\Big)$$

Symmetric Dicke states $\psi(M, N)$

Symmetric superposition of all states of M qubits, N in state 1 e.g.

$$|\psi(4,2)\rangle = \frac{1}{\sqrt{6}}\Big(|0011\rangle + |0110\rangle + |1100\rangle + |1001\rangle + |1010\rangle + |0101\rangle\Big)$$

Random distillation - can force measurement of $|0\rangle$

$$|\psi(4,2)\rangle \rightarrow |\psi(3,2)\rangle$$

or $|1\rangle$

$$|\psi(4,2)\rangle \rightarrow |\psi(3,1)\rangle$$

Symmetric Dicke states - general result

Generally

Symmetric Dicke states - general result

Generally

$$|\psi(M,N)\rangle \rightarrow |\psi(M',N')\rangle, \text{ or } |\psi(M',M'-N')\rangle \text{ if}$$
$$M' \leq M$$
$$N' \geq (M'-M)+N$$

Symmetric Dicke states - general result

Generally

$$|\psi(M,N)\rangle \to |\psi(M',N')\rangle, \text{ or } |\psi(M',M'-N')\rangle \text{ if}$$
$$M' \leq M$$
$$N' \geq (M'-M)+N$$

Not possible for chosen parties for $\binom{M'}{N'} > \binom{M}{N}$.

4 Redefinition

Problems with using E_t

The condition $E_t > E_{sp}$ can be trivially satisfied in some systems. E.g.

$$|\psi\rangle_{ABC} = |\Phi\rangle_{AB} \otimes |\Phi\rangle_{BC}$$

Problems with using E_t

The condition $E_t > E_{sp}$ can be trivially satisfied in some systems. E.g.

$$|\psi\rangle_{ABC} = |\Phi\rangle_{AB} \otimes |\Phi\rangle_{BC}$$

$E_t = 2$ but $E_{sp} = 1$.

Problems with using E_t

The condition $E_t > E_{sp}$ can be trivially satisfied in some systems. E.g.

$$|\psi\rangle_{ABC} = |\Phi\rangle_{AB} \otimes |\Phi\rangle_{BC}$$

$E_t = 2$ but $E_{sp} = 1$.

Better quantity to consider: E_{rnd}

For $\psi_i \underbrace{\rightarrow}_{LOCC} \{\psi_f, p_f\}$:

$$\langle E_{sp}\rangle = \sum_f p_f E_{sp}(\psi_f)$$

$$E_{rnd} \equiv \max(\langle E_{sp}\rangle)$$

Problems with using E_t

The condition $E_t > E_{sp}$ can be trivially satisfied in some systems. E.g.

$$|\psi\rangle_{ABC} = |\Phi\rangle_{AB} \otimes |\Phi\rangle_{BC}$$

$E_t = 2$ but $E_{sp} = 1$.
Better quantity to consider: E_{rnd}

For $\psi_i \underbrace{\longrightarrow}_{LOCC} \{\psi_f, p_f\}$:

$$\langle E_{sp} \rangle = \sum_f p_f E_{sp}(\psi_f)$$

$$E_{rnd} \equiv \max(\langle E_{sp} \rangle)$$

"The maximum (over protocols) expected maximum (over pairs) assisted entanglement"

Definitions

1. "Assisted entanglement" E_A^∞ - how many EPRs we can make through LOCC between two chosen parties from a multiparty state.

Definitions

1. "Assisted entanglement" E_A^∞ - how many EPRs we can make through LOCC between two chosen parties from a multiparty state.
2. "Specified entanglement" E_{sp}^∞ - the assisted entanglement, maximised over all pairs.

Definitions

1. "Assisted entanglement" E_A^∞ - how many EPRs we can make through LOCC between two chosen parties from a multiparty state.
2. "Specified entanglement" E_{sp}^∞ - the assisted entanglement, maximised over all pairs.
3. "Total entanglement" E_t^∞ - how many EPRs we can make through LOCC from a multiparty state, irrespective of who shares them.
4. "Random entanglement" E_{rnd}^∞ - how many EPRs we can make through LOCC between a pair of parties not *a priori* specified.

E_{rnd} and multiple copies

- Can we have $E_{rnd} > E_{sp}$ for multiple copies of states?

E_{rnd} and multiple copies

- Can we have $E_{rnd} > E_{sp}$ for multiple copies of states?
- E.g. $W^{\otimes 2}$. If one party measures $|00\rangle$, remaining parties share 2 EPR pairs.

E_{rnd} and multiple copies

- Can we have $E_{rnd} > E_{sp}$ for multiple copies of states?
- E.g. $W^{\otimes 2}$. If one party measures $|00\rangle$, remaining parties share 2 EPR pairs.
- Can do protocol with $|00\rangle \rightarrow \sqrt{1-\epsilon^2}|00\rangle + \epsilon|2\rangle$ but no guarantee of success.

E_{rnd} and multiple copies

- Can we have $E_{rnd} > E_{sp}$ for multiple copies of states?
- E.g. $W^{\otimes 2}$. If one party measures $|00\rangle$, remaining parties share 2 EPR pairs.
- Can do protocol with $|00\rangle \to \sqrt{1-\epsilon^2}|00\rangle + \epsilon|2\rangle$ but no guarantee of success.
- However we find:

$$E_{sp}(W^{\otimes 2}) = 2 \times H_2(1/3) \approx 1.837$$
$$E_{rnd} \gtrsim 1.843$$

E_{rnd} and multiple copies

- Can we have $E_{rnd} > E_{sp}$ for multiple copies of states?
- E.g. $W^{\otimes 2}$. If one party measures $|00\rangle$, remaining parties share 2 EPR pairs.
- Can do protocol with $|00\rangle \rightarrow \sqrt{1-\epsilon^2}|00\rangle + \epsilon|2\rangle$ but no guarantee of success.
- However we find:

$$E_{sp}(W^{\otimes 2}) = 2 \times H_2(1/3) \approx 1.837$$
$$E_{rnd} \gtrapprox 1.843$$

- Very small advantage, soon lost for more copies (with this protocol).

No advantage for many copies

No advantage for many copies

Theorem 5.

$$E_{sp}(\psi^{\otimes N}) \to E_{rnd}(\psi^{\otimes N}), \quad N \to \infty$$

No advantage for many copies

Theorem 5.

$$E_{sp}(\psi^{\otimes N}) \to E_{rnd}(\psi^{\otimes N}), \quad N \to \infty$$

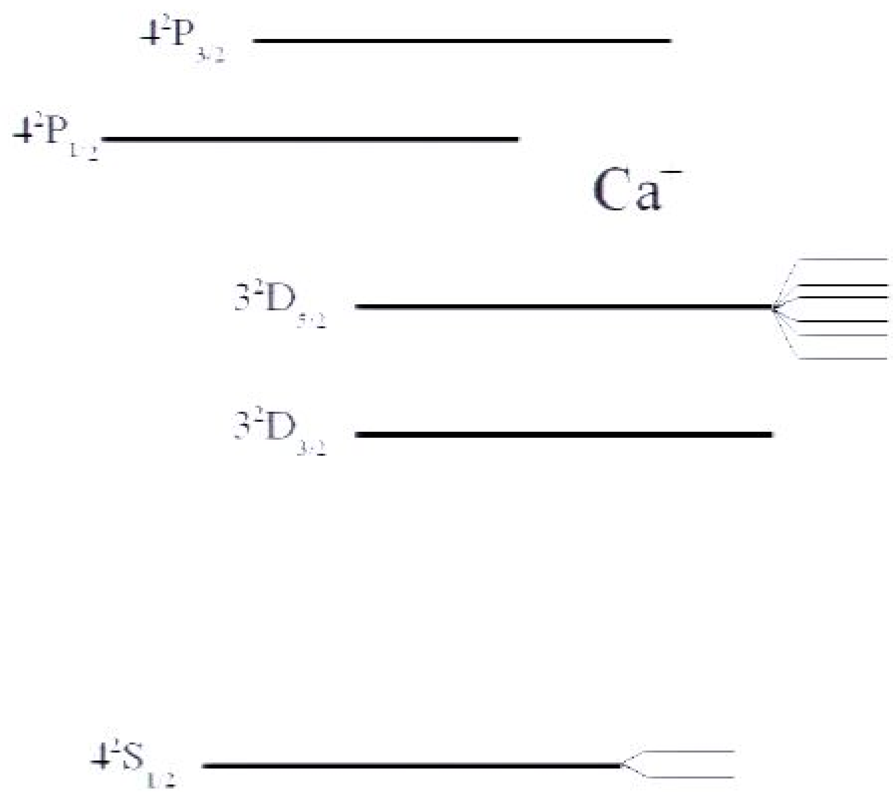
Proof.

(Lo & Popescu (1999))
Probability for a party to increase their distillable EPR pairs through LOCC $\to 0$ as $N \to \infty$.
Hence no increase in S or E_A for any party through LOCC - necessary for advantageous random distillation. □

Experimental random distillation

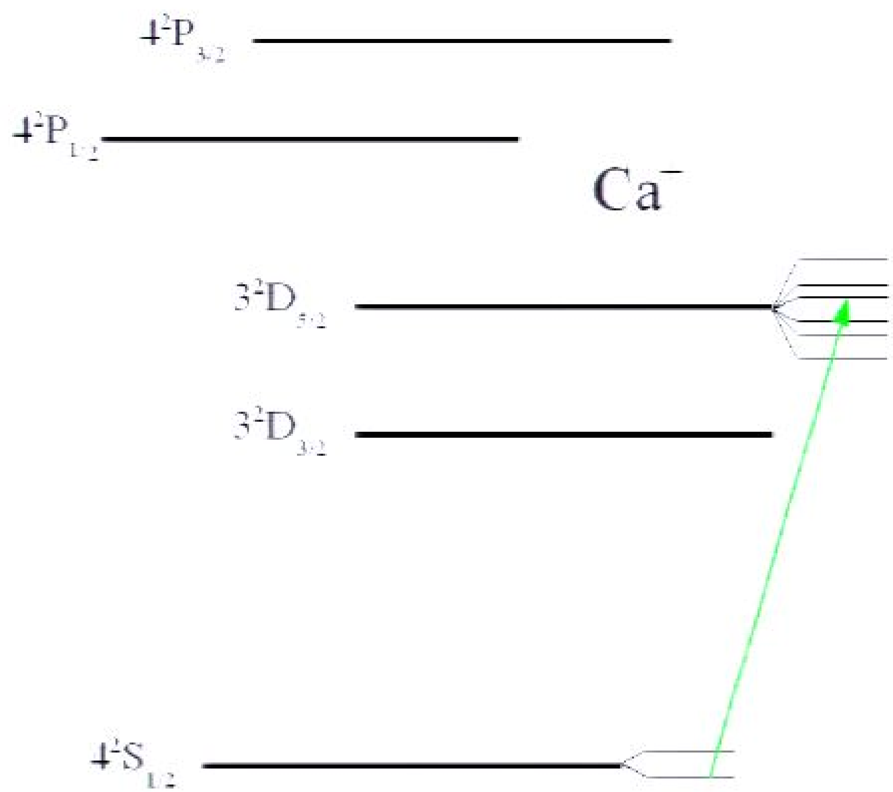
(Experimental QO, Uni. Innsbruck) Potential to implement the W random distillation protocol in trapped ions.

Random distillation scheme



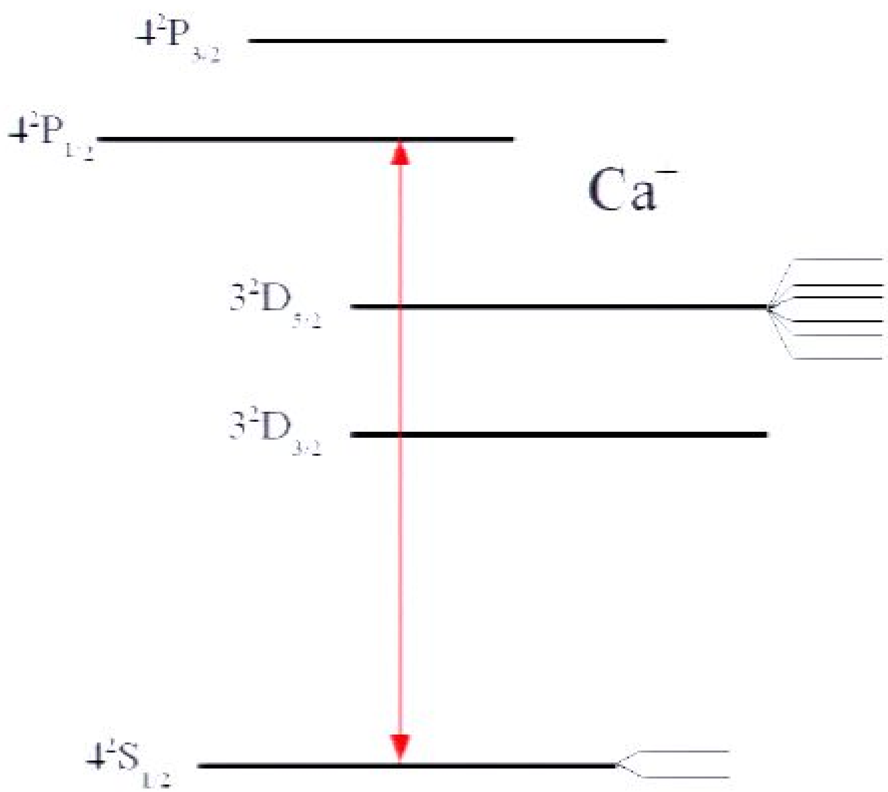
$$\alpha|S\rangle + \beta|D\rangle$$

Random distillation scheme



$$\epsilon(S \to D'), \quad \alpha\sqrt{1-\epsilon^2}|D'\rangle + \alpha\epsilon|S\rangle + \beta|D\rangle$$

Random distillation scheme



$$(S \to P), \quad |S\rangle\langle S|$$

$$\epsilon(S \to D'), \quad \alpha\sqrt{1-\epsilon^2}|D'\rangle + \alpha\epsilon|S\rangle + \beta|D\rangle$$

5 Conclusions

Conclusions

Conclusions

- For LOCC-conversion of M-party states to $< M - party$ states, whether you choose the parties matters.

Conclusions

- For LOCC-conversion of M-party states to $< M - party$ states, whether you choose the parties matters.
- Example, you can eventually get an EPR from a W iff you don't choose the parties.

Conclusions

- For LOCC-conversion of M-party states to $< M - party$ states, whether you choose the parties matters.
- Example, you can eventually get an EPR from a W iff you don't choose the parties.
- Applicable to many states (not just W or 3-party states).

Conclusions

- For LOCC-conversion of M-party states to $< M - party$ states, whether you choose the parties matters.
- Example, you can eventually get an EPR from a W iff you don't choose the parties.
- Applicable to many states (not just W or 3-party states).
- Can get states between random parties that have negligible probability between specified parties.

Conclusions

- For LOCC-conversion of M-party states to $< M - party$ states, whether you choose the parties matters.
- Example, you can eventually get an EPR from a W iff you don't choose the parties.
- Applicable to many states (not just W or 3-party states).
- Can get states between random parties that have negligible probability between specified parties.
- Relative entropy upper-bounds the yield for E_t.

Conclusions

- For LOCC-conversion of M-party states to $< M - party$ states, whether you choose the parties matters.
- Example, you can eventually get an EPR from a W iff you don't choose the parties.
- Applicable to many states (not just W or 3-party states).
- Can get states between random parties that have negligible probability between specified parties.
- Relative entropy upper-bounds the yield for E_t.
- Random distillation is always advantageous for W class, sometimes for GHZ class.

Conclusions

- For LOCC-conversion of M-party states to $< M - party$ states, whether you choose the parties matters.
- Example, you can eventually get an EPR from a W iff you don't choose the parties.
- Applicable to many states (not just W or 3-party states).
- Can get states between random parties that have negligible probability between specified parties.
- Relative entropy upper-bounds the yield for E_t.
- Random distillation is always advantageous for W class, sometimes for GHZ class.
- Provably no advantage in the many-copy limit.

Acknowledgements

Thanks to: Daniel Gottesman, Martin Plenio, Andrew House, Matthias Christandl, Debbie Leung and Andreas Winter.

References

- M. Horodecki, J. Oppenheim and A. Winter, Nature **436**, 673 (2005)
- J. A. Smolin, F. Verstraete and A. Winter, Phys. Rev. A, **72**, 052317 (2005)
- G. Gour, Phys. Rev. A, **72**, 042318 (2005)
- N. Linden, S. Popescu, B. Schumacher and M. Westmoreland, Quant.Inf.Proc, vol 4, 241 (2005)
- M. B. Plenio and V. Vedral, J. Phys. A **34**, 6997 (2001)
- E. F. Galvão, M. B. Plenio and S. Virmani, J. Phys. A, **33**, 8809 (2000)
- H.-K. Lo and S. Popescu Phys. Rev. A, **63**, 022301 (2001)