Making entanglement

Andrew Childs

MIT Center for Theoretical Physics
IBM T. J. Watson Research Center

Debbie Leung

IBM T. J. Watson Research Center

Frank Verstraete

SISTA/ESAT, University of Leuven

Guifré Vidal

Caltech Institute for Quantum Information

arxiv.org/abs/quant-ph/0207052

Outline

- The resource model of information theory
- Entanglement as a resource
- Some uses of entanglement
- How to (optimally) make entanglement

Resources in (quantum) information theory

Information is a resource.

- Physical
- Fungible

Examples:

	Static	Dynamic
Classical	$\text{cbits}_{A\to B}$ $\text{cbits}_{B\to A}$ sbits	Channel
Quantum	$\text{qubits}_{A\to B}$ $\text{qubits}_{B\to A}$ ebits	Unitary gate Hamiltonian Quantum operation

Quantum information theory is about the interconversion of informational resources.

What is entanglement?

Entangled pure state:

$$|\psi\rangle_{AB} \neq |\phi\rangle_A |\eta\rangle_B$$

Canonical example: EPR pair

$$|\Psi^+\rangle = \frac{|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B}{\sqrt{2}}$$

Entanglement = non-classical correlations

- Violation of Bell inequalities
- Can be used to perform classically impossible tasks!

Quantifying entanglement

Consider a bipartite state $|\psi\rangle$.

Any such state has a Schmidt decomposition:

$$|\psi\rangle = \sum_j \sqrt{p_j} |j\rangle_A |\tilde{j}\rangle_B$$

where $\sum_j p_j = 1$ and $\{|j\rangle_A\}$, $\{|\tilde{j}\rangle_B\}$ are orthonormal bases.

Entanglement:

$$E(|\psi\rangle) = -\sum_j p_j \log p_j$$

measured in *ebits*.

$$1 \text{ ebit} = E(|\Psi^+\rangle)$$

Entanglement is fungible

Theorem. Asymptotically, states with the same entanglement are interconvertible.

[Bennett et al. 95]

Entanglement concentration

$$n \text{ copies of } |\psi\rangle \xrightarrow{\text{LO}} nE(|\psi\rangle) \text{ ebits}$$

Entanglement dilution

$$nE(|\psi\rangle) \text{ ebits} \xrightarrow{\text{LOCC}} n \text{ copies of } |\psi\rangle$$

Entanglement: What is it good for?

- Superdense coding [Bennett, Wiesner 92]
- Quantum teleportation [Bennett et al. 93]
- Quantum key distribution [Lo, Chau 98]
- Entanglement-assisted classical communication
  ... through unidirectional channels [Shor et al. 99]
  ... through bidirectional channels [Bennett et al. 02]
- Remote state preparation [Lo 00, Bennett et al. 00]
- Data hiding [DiVincenzo et al. 00]
- Quantum Vernam cipher [Leung 00]

⋮

Superdense coding

[Bennett, Wiesner 92]

$$1 \text{ ebit} + 1 \text{ qubit}_{A\to B} \quad\longrightarrow\quad 2 \text{ cbits}_{A\to B}$$

- Alice and Bob share one ebit $|\Psi^+\rangle$.
- Alice encodes two bits by choosing one of four unitary operators:

$$\begin{array}{cc} 00 & I \\ 01 & X \\ 10 & Y \\ 11 & Z \end{array}$$

- Alice applies this operator to her half of $|\Psi^+\rangle$ and then sends her qubit to Bob. Bob gets one of four possible states:

$$\begin{aligned} (I \otimes I)|\Psi^+\rangle &= \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle) &= |\Psi^+\rangle \\ (X \otimes I)|\Psi^+\rangle &= \tfrac{1}{\sqrt{2}}(|01\rangle + |10\rangle) &= |\Phi^+\rangle \\ (Y \otimes I)|\Psi^+\rangle &= \tfrac{1}{\sqrt{2}}(|01\rangle - |10\rangle) &= |\Phi^-\rangle \\ (Z \otimes I)|\Psi^+\rangle &= \tfrac{1}{\sqrt{2}}(|00\rangle - |11\rangle) &= |\Psi^-\rangle \end{aligned}$$

  Note that these four states are orthogonal.

- Bob measures in the basis $\{|\Psi^\pm\rangle, |\Phi^\pm\rangle\}$ and acquires two bits of information.

Quantum teleportation [Bennett et al. 93]

$$1 \text{ ebit} + 2 \text{ cbits}_{A\to B} \quad \longrightarrow \quad 1 \text{ qubit}_{A\to B}$$

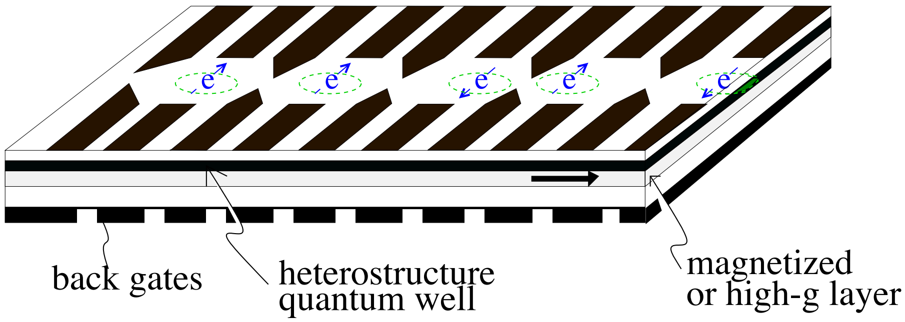
- Alice and Bob share one ebit $|\Psi^+\rangle$.
- Alice has a qubit $|\eta\rangle = \alpha|0\rangle + \beta|1\rangle$. The joint state is

$$\begin{aligned} |\eta\rangle|\Psi^+\rangle &= \tfrac{1}{\sqrt{2}}(\alpha|0\rangle + \beta|1\rangle)(|00\rangle + |11\rangle) \\ &= \tfrac{1}{2}(\quad |\Psi^-\rangle \quad |\eta\rangle \\ &\qquad + |\Phi^-\rangle \; X|\eta\rangle \\ &\qquad + |\Phi^+\rangle \; Y|\eta\rangle \\ &\qquad + |\Psi^+\rangle \; Z|\eta\rangle \;) \end{aligned}$$

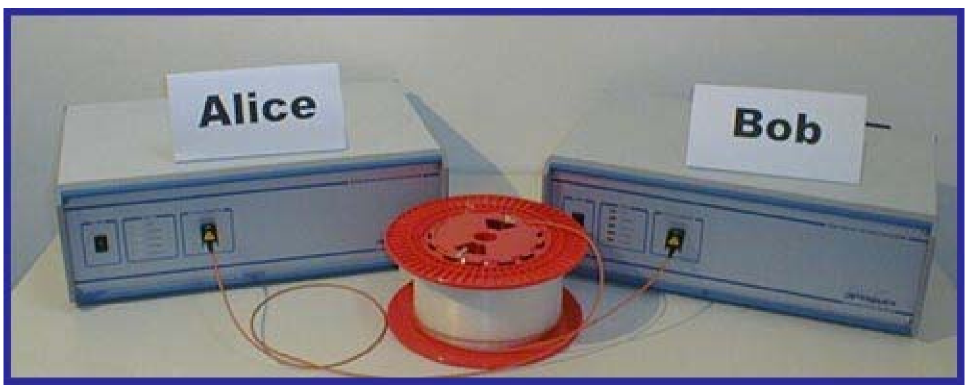
  where the first two qubits belong to Alice and the third belongs to Bob.
- Alice measures her two qubits in the basis $\{|\Psi^\pm\rangle, |\Phi^\pm\rangle\}$ and sends the resulting two classical bits to Bob.
- Bob applies I, X, Y, Z as appropriate to recover $|\eta\rangle$.

Physical systems

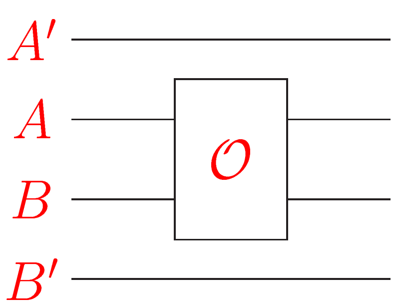
- Adjacent quantum dots



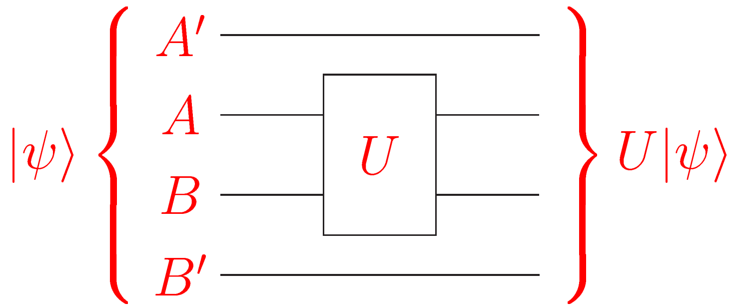
- Distant labs connected by optical fiber



General model:

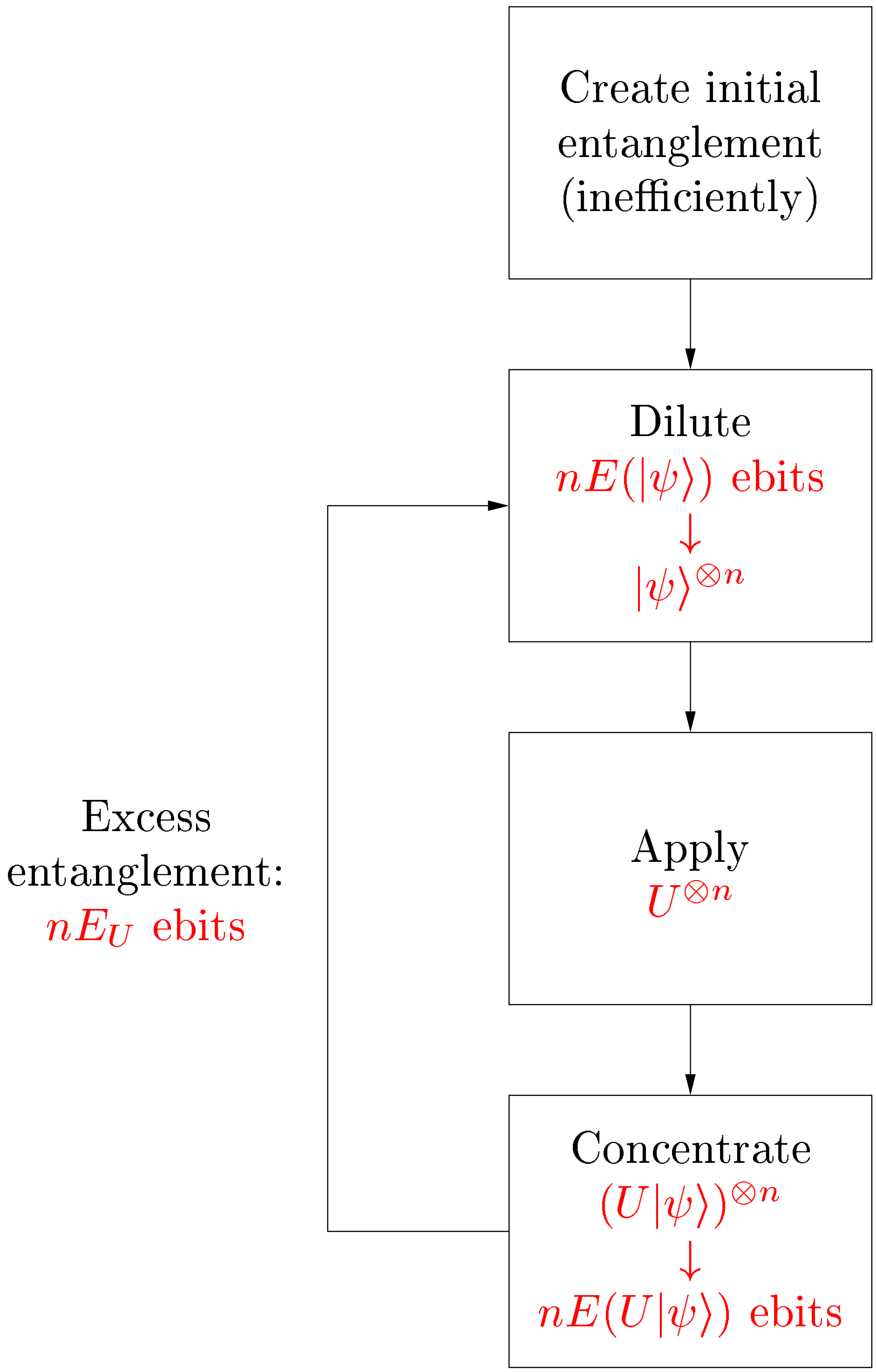


How to make entanglement



Choose $|\psi\rangle$ so that $U|\psi\rangle$ is more entangled than $|\psi\rangle$.

Entanglement production cycle



Entanglement generating capacity

$$E_U = \sup_{|\psi\rangle \in AA'BB'} \left[E(U|\psi\rangle) - E(|\psi\rangle) \right]$$

Three technical points:

- Mixed states
- Asymptotic vs. one-shot capacity
- Ancillary systems

Mixed states

Theorem. For unitary interactions, the optimal input state is always pure.

[Bennett, Harrow, Leung, Smolin 02]

Proof:

$$
\begin{aligned}
E'_U &= \sup_\rho [D(U\rho U^\dagger) - E_c(\rho)] \\
&\leq \sup_\rho [E_c(U\rho U^\dagger) - E_c(\rho)] \\
&= \sup_\rho \frac{1}{n}[E_f((U\rho U^\dagger)^{\otimes n}) - E_f(\rho^{\otimes n})] + \epsilon \\
&= \sup_\rho \frac{1}{n} \sum_i p_i [E((U|\psi_i\rangle)^{\otimes n}) - E(|\psi_i\rangle^{\otimes n})] + \epsilon \\
&= \sup_\rho \sum_i p_i [E(U|\psi_i\rangle) - E(|\psi_i\rangle)] \\
&= \sup_{\rho,i} [E(U|\psi_i\rangle) - E(|\psi_i\rangle)] \\
&= E_U
\end{aligned}
$$

□

Asymptotic vs. one-shot

Theorem. $E_U^{(n)} = nE_U$

[Bennett, Harrow, Leung, Smolin 02]

Proof:

The entanglement can only increase by application of U. For each use of U, the maximum increase is given by E_U. Thus $E_U^{(n)} \leq nE_U$.

By using the optimal input n times, $E_U^{(n)} \geq nE_U$. $\square$

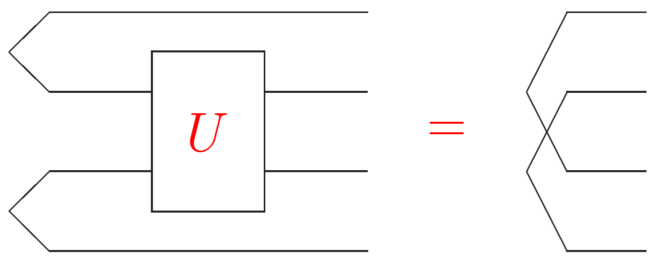
Using ancillas

Consider $U = \mathrm{SWAP}$:

$$U|\alpha\rangle|\beta\rangle = |\beta\rangle|\alpha\rangle$$

Clearly $E(|\psi\rangle_{AB}) = E(U|\psi\rangle_{AB})$.

But:



In general, you can make more entanglement when ancillary systems are available. This makes it hard to compute E_U!

Entanglement capacity of a Hamiltonian

$$E_H = \lim_{t \to 0} (E_{e^{-iHt}}/t) = \sup_{|\psi\rangle} \left[\frac{\mathrm{d}}{\mathrm{d}t} E(e^{-iHt}|\psi\rangle) \right]_{t=0}$$

Using perturbation theory, we find

$$E_{H,|\psi\rangle} = \sum\nolimits_{j,k} \sqrt{p_j p_k} \log(p_j/p_k) \ \mathrm{Im}\langle j\tilde{j}|H|k\tilde{k}\rangle$$

where

$$|\psi\rangle = \sum_j \sqrt{p_j} |j\rangle_{AA'} |\tilde{j}\rangle_{BB'}$$

This is...

- Zero for product states
- Zero for maximally entangled states
- Hard to optimize over $|\psi\rangle$!

Two-qubit Hamiltonians: Canonical form

A general two-qubit Hamiltonian has 15 real parameters. But only two of them are nonlocal!

Fact: Any two-qubit Hamiltonian H is *locally equivalent* to a Hamiltonian of the form

$$\tilde{H} = a\, X \otimes X + b\, Y \otimes Y + c\, Z \otimes Z\,.$$

In other words, there are local Hamiltonians H_A, H_B and local unitary operators U, V so that

$$H = (U \otimes V)\tilde{H}(U^\dagger \otimes V^\dagger) + H_A + H_B\,.$$

[Dür et al. 01]

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \qquad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Ising interaction

Consider $H = Z \otimes Z$ $\qquad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

No ancillas:

$$\begin{aligned} E^*_{ZZ} &= 2 \max_{p \in [0,1]} \sqrt{p(1-p)} \log \frac{p}{1-p} \\ &\approx 1.9123 \end{aligned}$$

[Dür et al. 01]

> **Theorem.** $E_{ZZ} = 1.9123$
>
> [Childs, Leung, Vidal, Verstraete 02]

Proof idea: No pair of terms in the Schmidt decomposition with Schmidt coefficients p_1, p_2 can contribute more than $E^*_{ZZ}/(p_1 + p_2)$. $\square$

$a\,XX + b\,YY$

Upper bound: Simulation.

$a\ X \otimes X + b\ Y \otimes Y$ can be *simulated* using $(a+b)\ Z \otimes Z$.

There exist unitaries H, K so that

$$HZH^\dagger = X \qquad\qquad KZK^\dagger = Y$$

Simulation uses the Lie product formula:

$$e^{i(H_1+H_2)t} = \lim_{n\to\infty} (e^{iH_1 t/n} e^{iH_2 t/n})^n$$

Therefore $E_{aXX+bYY} \le (a+b)E_{ZZ}$.

Lower bound: By an explicit protocol (with no ancillas), $E_{aXX+bYY} \ge (a+b)E_{ZZ}$. [Dür et al. 01]

Summary of known capacities

Gates:

$$\begin{aligned} E_{\text{CNOT}} &= 1 \\ E_{\text{SWAP}} &= 2 \end{aligned}$$

Hamiltonians:

$$E_{aXX+bYY} = 1.9123(a+b)$$

In general, there may be no closed-form expression for the capacity of a given interaction.

Conjecture:

$$\begin{aligned} E_{a(XX+YY)+ZZ} = 2\sup\big[& \sqrt{p_1 p_2}\log(p_1/p_2)\,(\sin n + a\sin(m-l)) \\ & + \sqrt{p_1 p_4}\log(p_1/p_4)\,a\sin l \\ & + \sqrt{p_2 p_4}\log(p_2/p_4)\,(\sin m + a\sin(n-l))\big] \end{aligned}$$

where $p_1, p_2, p_4 > 0$ and $p_1 + 2p_2 + p_4 = 1$.

Open problems

- Calculate capacities for two-qubit gates
- Find an upper bound on the optimal ancilla dimension for a $d_A \times d_B$ dimensional gate or Hamiltonian
- Study entanglement generation by nonunitary quantum operations
- Inverse problem: How much entanglement is needed to simulate a gate (or Hamiltonian)?

  $$E_U \leq \text{ebits needed to simulate } U$$

  When is this achievable?