The princess and the EPR pair

$\Big|$  $\Big\rangle$ $+$ $\Big|$  $\Big\rangle$

$\sqrt{2}$

or

Entanglement spread, communication complexity and information theory.

Aram Harrow
University of Bristol

April 22, 2010

quantum information basics

	Deterministic	Randomized	Quantum
basic unit of information	bit $\{0,1\}$	distribution $p \in \mathbb{R}^2$ $p_0 + p_1 = 1$	qubit $\lvert\psi\rangle = a\lvert 0\rangle + b\lvert 1\rangle \in \mathbb{C}^2$ $\lvert a\rvert^2 + \lvert b\rvert^2 = 1$
n bits	2^n states	2^n dimensions	2^n dimensions
basic unit of computation	NAND, XOR, etc.	stochastic matrices	unitary matrices
measurement	no problem	Bayes' rule	collapses state
correlation	not defined	$p^{AB}(a,b) \neq p^A(a) \cdot p^B(b)$	entanglement $\lvert\psi\rangle \neq \lvert\alpha\rangle \otimes \lvert\beta\rangle$

entanglement

- An old mystery of quantum theory:
  "[not] one, but rather the characteristic trait of quantum mechanics, the one that enforces its entire departure from classical lines of thought."
  ---Schrödinger, 1935

- Spooky action at a distance
  "This makes the reality of [quantities] P and Q depend upon the process of measurement carried out on the first system, which does not disturb the second system in any way. No reasonable definition of reality could be expected to permit this."
  --- Einstein, Podolsky and Rosen [EPR], 1935

- canonical form:
  EPR pair

$$|\Phi_2\rangle = \frac{|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

entanglement as resource

entanglement as resource

- Bell's theorem [1964] describes a set of distributed measurements on $|\Phi_2\rangle$ that produce outcomes inconsistent with any correlated classical probability distribution.

entanglement as resource

- Bell's theorem [1964] describes a set of distributed measurements on $|\Phi_2\rangle$ that produce outcomes inconsistent with any correlated classical probability distribution.
- Super-dense coding [Bennett-Wiesner '92] is a scheme for transmitting two classical bits (cbits) using one qubit and one EPR pair.

entanglement as resource

- Bell's theorem [1964] describes a set of distributed measurements on $|\Phi_2\rangle$ that produce outcomes inconsistent with any correlated classical probability distribution.
- Super-dense coding [Bennett-Wiesner '92] is a scheme for transmitting two classical bits (cbits) using one qubit and one EPR pair.
- Teleportation [BBCJPW93] is a method for sending one qubit using two classical bits and one EPR pair.

entanglement as resource

- Bell's theorem [1964] describes a set of distributed measurements on $|\Phi_2\rangle$ that produce outcomes inconsistent with any correlated classical probability distribution.
- Super-dense coding [Bennett-Wiesner '92] is a scheme for transmitting two classical bits (cbits) using one qubit and one EPR pair.
- Teleportation [BBCJPW93] is a method for sending one qubit using two classical bits and one EPR pair.
- Quantum key distribution achieves information-theoretic security using entanglement either implicitly [BB84] or explicitly [E91].

entanglement as resource

- Bell's theorem [1964] describes a set of distributed measurements on $|\Phi_2\rangle$ that produce outcomes inconsistent with any correlated classical probability distribution.
- Super-dense coding [Bennett-Wiesner '92] is a scheme for transmitting two classical bits (cbits) using one qubit and one EPR pair.
- Teleportation [BBCJPW93] is a method for sending one qubit using two classical bits and one EPR pair.
- Quantum key distribution achieves information-theoretic security using entanglement either implicitly [BB84] or explicitly [E91].
- Quantum computing exploits the exponential scaling to perform calculations that are hard to simulate classically.

general entangled states

Two-party entanglement:

Alice and Bob share $|\psi\rangle = \sum_{ij} c_{ij} \, |i\rangle \otimes |j\rangle$.

general entangled states

Two-party entanglement:

Alice and Bob share $|\psi\rangle = \sum_{ij} c_{ij}\, |i\rangle \otimes |j\rangle$.

With free LO (local operations) + CC (classical communication):

general entangled states

Two-party entanglement:
Alice and Bob share $|\psi\rangle = \sum_{ij} c_{ij} |i\rangle \otimes |j\rangle$.

With free LO (local operations) + CC (classical communication):

- Local unitaries transform any state to a standard form: $|\psi\rangle \sim \sum_i \sqrt{\lambda_i}\, |i\rangle \otimes |i\rangle$. (Proof: use singular value decomposition.)

general entangled states

Two-party entanglement:

Alice and Bob share $|\psi\rangle = \sum_{ij} c_{ij}\, |i\rangle \otimes |j\rangle$.

With free LO (local operations) + CC (classical communication):

- Local unitaries transform any state to a standard form: $|\psi\rangle \sim \sum_i \sqrt{\lambda_i}\, |i\rangle \otimes |i\rangle$. (Proof: use singular value decomposition.)
- The $\{\lambda_i\}$ (Schmidt coeffs) are Schur-monotone under LOCC: i.e., if $|\psi\rangle \rightarrow |\psi'\rangle$ then λ is majorized by λ'.

general entangled states

Two-party entanglement:

Alice and Bob share $|\psi\rangle = \sum_{ij} c_{ij} |i\rangle\otimes|j\rangle$.

With free LO (local operations) + CC (classical communication):

- Local unitaries transform any state to a standard form: $|\psi\rangle \sim \sum_i \sqrt{\lambda_i}\, |i\rangle\otimes|i\rangle$. (Proof: use singular value decomposition.)
- The $\{\lambda_i\}$ (Schmidt coeffs) are Schur-monotone under LOCC: i.e., if $|\psi\rangle\rightarrow|\psi'\rangle$ then λ is majorized by λ'.
- Concentration and dilution [BBPS96] reduce many copies of $|\psi\rangle$ to $-\sum_i \lambda_i \log \lambda_i$ EPR pairs per copy.

general entangled states

Two-party entanglement:
Alice and Bob share $|\psi\rangle = \sum_{ij} c_{ij} |i\rangle \otimes |j\rangle$.

With free LO (local operations) + CC (classical communication):

- Local form:
  $|\psi\rangle$ ~ composition.)

- The { nder LOCC:
  i.e., if

But what if classical communication isn't free?

- Concentration and dilution [BBPS96] reduce many copies of $|\psi\rangle$ to $-\sum_i \lambda_i \log \lambda_i$ EPR pairs per copy.

a different metaphor: superselection constraints

a different metaphor: superselection constraints

The state space is partitioned according to some observable, such as total particle number.

$$\left(\begin{array}{c} * \\ \hline * \\ * \\ \hline * \\ * \\ * \end{array}\right)$$

a different metaphor: superselection constraints

The state space is partitioned according to some observable, such as total particle number.

Measurements and unitary evolutions are constrained to respect this partition.

$$\left(\begin{array}{c} * \\ \hline * \\ * \\ \hline * \\ * \\ * \end{array}\right)$$

$$\left(\begin{array}{c|cc|ccc} * & & & & & \\ \hline & * & * & & & \\ & * & * & & & \\ \hline & & & * & * & * \\ & & & * & * & * \\ & & & * & * & * \end{array}\right)$$

entanglement as conserved quantity

Idea:

If Alice and Bob are allowed only local unitaries (LU) then the Schmidt coefficients of their state remain exactly the same.

Or less precisely, the ‘amount’ of entanglement is conserved.

entanglement as conserved quantity

Idea:

If Alice and Bob are allowed only local unitaries (LU) then the Schmidt coefficients of their state remain exactly the same.

Or less precisely, the 'amount' of entanglement is conserved.

So the state $|\psi\rangle$ is LU equivalent to $\sum_k \sqrt{p_k} |k\rangle_A |k\rangle_B |\Phi_2\rangle_{AB}^{\otimes k}$ with the # of EPR pairs (*k*) conserved under LU .

entanglement as conserved quantity

Idea:

If Alice and Bob are allowed only local unitaries (LU) then the Schmidt coefficients of their state remain exactly the same.

Or less precisely, the 'amount' of entanglement is conserved.

So the state $|\psi\rangle$ is LU equivalent to $\sum_k \sqrt{p_k}|k\rangle_A|k\rangle_B|\Phi_2\rangle_{AB}^{\otimes k}$ with the # of EPR pairs (k) conserved under LU .

Really?

entanglement as conserved quantity

Idea:

If Alice and Bob are allowed only local unitaries (LU) then the Schmidt coefficients of their state remain exactly the same.

Or less precisely, the 'amount' of entanglement is conserved.

So the state $|\psi\rangle$ is LU equivalent to $\sum_k \sqrt{p_k}|k\rangle_A|k\rangle_B|\Phi_2\rangle_{AB}^{\otimes k}$ with the # of EPR pairs (k) conserved under LU .

Really?

1. $|\Phi_2\rangle^{\otimes k}$ and $|\Phi_2\rangle^{\otimes l}$ are only approximately orthogonal.

entanglement as conserved quantity

Idea:

If Alice and Bob are allowed only local unitaries (LU) then the Schmidt coefficients of their state remain exactly the same.

Or less precisely, the ‘amount’ of entanglement is conserved.

So the state $|\psi\rangle$ is LU equivalent to $\sum_k \sqrt{p_k}|k\rangle_A|k\rangle_B|\Phi_2\rangle_{AB}^{\otimes k}$ with the # of EPR pairs (k) conserved under LU .

Really?

1. $|\Phi_2\rangle^{\otimes k}$ and $|\Phi_2\rangle^{\otimes l}$ are only approximately orthogonal.
2. Technically we can only approximately decompose $|\psi\rangle$ into

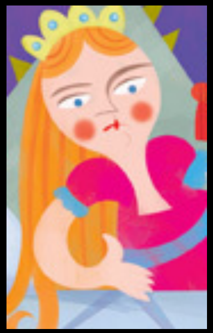
$$\sum_{k\geq 0} \sqrt{p_k}|k\rangle_A|k\rangle_B|\Phi_{\lfloor 2^{\epsilon k}\rfloor}\rangle_{AB}$$

implications

1. Any transformation using local unitaries and Q qubits of communication has off-diagonal blocks decaying as $\leq 2^{Q-\frac{|k-\ell|}{2}}$

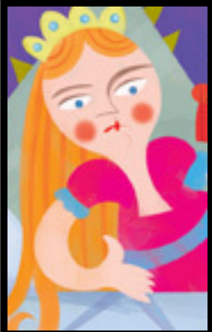
$$\begin{pmatrix} * & * & * & * & * & * \\ * & * & * & * & * & * \\ * & * & * & * & * & * \\ * & * & * & * & * & * \\ * & * & * & * & * & * \\ * & * & * & * & * & * \end{pmatrix}$$

2. 'Exotic' states, such as $|01\rangle^{\otimes n} \pm |\Phi_2\rangle^{\otimes n} / \sqrt{2}$, should be difficult to create, and are potentially valuable.



A bipartite fairy tale

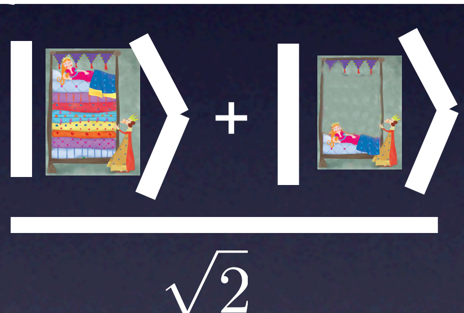
Traditional version: A mysterious woman appears at the castle claiming to be a princess. That night, a single pea placed under twenty mattresses keeps her from sleeping. The prince realises that she is genuine and immediately asks her to marry him.



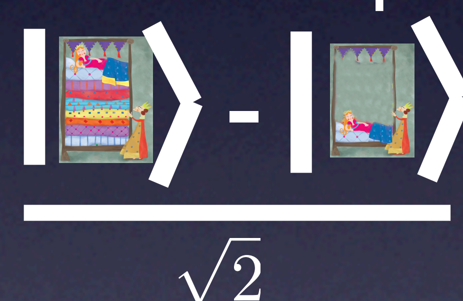
A bipartite fairy tale

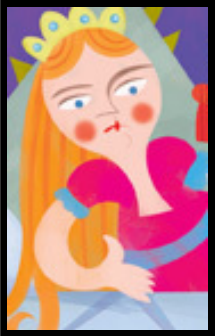
Traditional version: A mysterious woman appears at the castle claiming to be a princess. That night, a single pea placed under twenty mattresses keeps her from sleeping. The prince realises that she is genuine and immediately asks her to marry him.

Quantum version: Our heroine is so delicate that she can distinguish



from any orthogonal state. In particular, she can distinguish it from

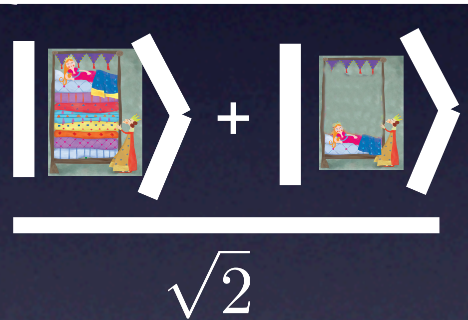




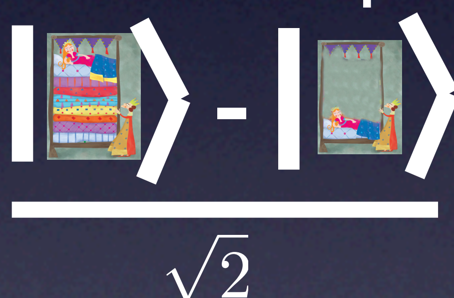
A bipartite fairy tale

Traditional version: A mysterious woman appears at the castle claiming to be a princess. That night, a single pea placed under twenty mattresses keeps her from sleeping. The prince realises that she is genuine and immediately asks her to marry him.

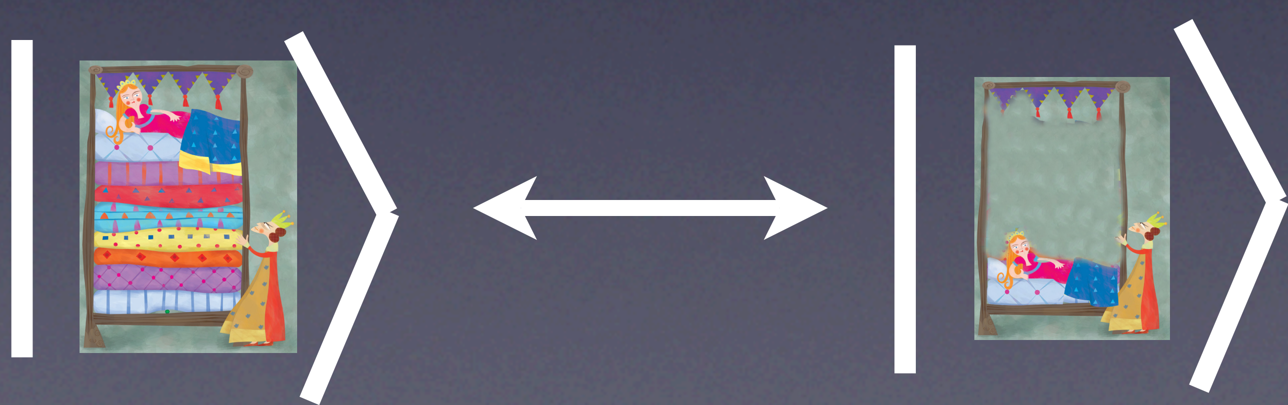
Quantum version: Our heroine is so delicate that she can distinguish



from any orthogonal state. In particular, she can distinguish it from

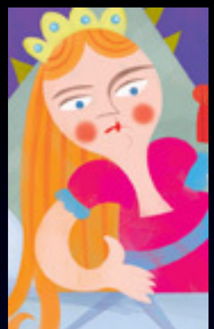


However! Adding or removing lots of mattresses is difficult.



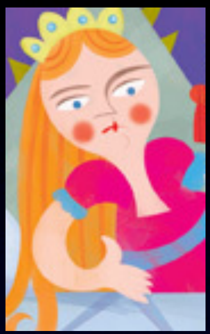
requires

Should he marry her?



Distinguishing (|  ⟩ + |  ⟩) / $\sqrt{2}$ from (|  ⟩ - |  ⟩) / $\sqrt{2}$ with a reversible quantum circuit allows us to apply a phase (-1) to one of the states.

Should he marry her?

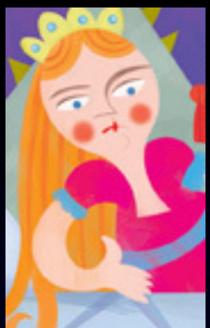


Distinguishing (|⟩ + |⟩) / √2 from (|⟩ - |⟩) / √2 with a reversible quantum circuit allows us to apply a phase (-1) to one of the states.

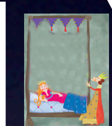
But $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ in the (|⟩ ± |⟩) / √2 basis is equivalent to

$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ in the |⟩ , |⟩ basis.

Should he marry her?



Distinguishing $\dfrac{|$$\rangle + |$$\rangle}{\sqrt{2}}$ from $\dfrac{|$$\rangle - |$$\rangle}{\sqrt{2}}$ with a reversible quantum circuit allows us to apply a phase (-1) to one of the states.

But $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ in the $\dfrac{|$$\rangle \pm |$$\rangle}{\sqrt{2}}$ basis is equivalent to

$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ in the $|$$\rangle$, $|$$\rangle$ basis.

This performs $|$$\rangle \longleftrightarrow |$$\rangle$

Conclusion: The “princess” is stronger than she looks!

The relevance to entanglement

The relevance to entanglement

- Performing $|01\rangle^{\otimes n} \leftrightarrow |\Phi_2\rangle^{\otimes n}$ requires transmitting n qubits.

$|01\rangle^{\otimes n} = \big|$  $\big\rangle$

$|\Phi_2\rangle^{\otimes n} = \big|$  $\big\rangle$

The relevance to entanglement

- Performing $|01\rangle^{\otimes n} \leftrightarrow |\Phi_2\rangle^{\otimes n}$ requires transmitting n qubits.

$|01\rangle^{\otimes n} =$ |  $\rangle$ $\qquad |\Phi_2\rangle^{\otimes n} =$ |  $\rangle$

- Therefore, distinguishing $|01\rangle^{\otimes n} \pm |\Phi_2\rangle^{\otimes n} / \sqrt{2}$ requires transmitting n/2 qubits.
  Why? Because any measurement in the $\{|\alpha\rangle, |\beta\rangle\}$ basis using Q qubits of communication implies that the operation $|\alpha\rangle\langle\alpha| - |\beta\rangle\langle\beta|$ can be performed using 2Q qubits of communication.

The relevance to entanglement

- Performing $|01\rangle^{\otimes n} \leftrightarrow |\Phi_2\rangle^{\otimes n}$ requires transmitting n qubits.

  $|01\rangle^{\otimes n} =$ $|$  $\rangle$ $|\Phi_2\rangle^{\otimes n} =$ $|$  $\rangle$

- Therefore, distinguishing $|01\rangle^{\otimes n} \pm |\Phi_2\rangle^{\otimes n} / \sqrt{2}$ requires transmitting n/2 qubits.

  Why? Because any measurement in the $\{|\alpha\rangle, |\beta\rangle\}$ basis using Q qubits of communication implies that the operation $|\alpha\rangle\langle\alpha| - |\beta\rangle\langle\beta|$ can be performed using 2Q qubits of communication.

- This bound holds even given unlimited EPR pairs.

  Why? Because for any m, the same argument applies to the states

  $$|\Phi_2\rangle^{\otimes m} \otimes (|01\rangle^{\otimes n} \pm |\Phi_2\rangle^{\otimes n} / \sqrt{2})$$

The general rule:

The general rule:

- If $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_r$, then preparing $|\psi\rangle = \sum_i \sqrt{\lambda_i}\, |i\rangle \otimes |i\rangle$ from EPR pairs requires $\log(r\lambda_1)/2$ qubits of communication (i.e. the "entanglement spread" of $|\psi\rangle$).
  Why? r and λ_1 each change by at most 2 for each qubit sent.
  For EPR pairs $r\lambda_1 = 1$.
  [P. Hayden, A. Winter. quant-ph/0204092]

The general rule:

- If $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_r$, then preparing $|\psi\rangle = \sum_i \sqrt{\lambda_i}\, |i\rangle \otimes |i\rangle$ from EPR pairs requires $\log(r\lambda_1)/2$ qubits of communication (i.e. the "entanglement spread" of $|\psi\rangle$).
  Why? r and λ_1 each change by at most 2 for each qubit sent.
  For EPR pairs $r\lambda_1 = 1$.
  [P. Hayden, A. Winter. quant-ph/0204092]
- Approximate versions also exist.

The general rule:

- If $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_r$, then preparing $|\psi\rangle = \sum_i \sqrt{\lambda_i}\, |i\rangle \otimes |i\rangle$ from EPR pairs requires $\log(r\lambda_1)/2$ qubits of communication (i.e. the "entanglement spread" of $|\psi\rangle$).
  Why? r and λ_1 each change by at most 2 for each qubit sent.
  For EPR pairs $r\lambda_1 = 1$.
  [P. Hayden, A. Winter. quant-ph/0204092]
- Approximate versions also exist.
- If $|\psi\rangle = \sum_k \sqrt{p_k}\, |k\rangle|k\rangle|\Phi_2\rangle^{\otimes k}$, then
  $\log(r) \approx \max\{k : p_k > 0\}$ and $\log(\lambda_1) \approx -\min\{k : p_k > 0\}$.
  So the spread of $|\psi\rangle \approx$ the diameter of the support of p.

The general rule:

- If $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_r$, then preparing $|\psi\rangle = \sum_i \sqrt{\lambda_i}\, |i\rangle \otimes |i\rangle$ from EPR pairs requires $\log(r\lambda_1)/2$ qubits of communication (i.e. the "entanglement spread" of $|\psi\rangle$).
  Why? r and λ_1 each change by at most 2 for each qubit sent.
  For EPR pairs $r\lambda_1 = 1$.
  [P. Hayden, A. Winter. quant-ph/0204092]
- Approximate versions also exist.
- If $|\psi\rangle = \sum_k \sqrt{p_k}\, |k\rangle|k\rangle|\Phi_2\rangle^{\otimes k}$, then
  $\log(r) \approx \max\{k : p_k > 0\}$ and $\log(\lambda_1) \approx -\min\{k : p_k > 0\}$.
  So the spread of $|\psi\rangle \approx$ the diameter of the support of p.
- Corollary: For $|01\rangle^{\otimes n} + |\Phi_2\rangle^{\otimes n} / \sqrt{2}$, $r\lambda_1 \approx 2^n$. Therefore creating the state requires $\approx n/2$ qubits of communication.

Application to information theory

Application to information theory

- Traditionally spread has been thought as a "sublinear" phenomenon, and as a result, has been neglected.

Application to information theory

- Traditionally spread has been thought as a "sublinear" phenomenon, and as a result, has been neglected.
- Example: If $|\psi\rangle$ is an entangled state, then $|\psi\rangle^{\otimes n}$ is very close to a state with spread $O(\sqrt{n})$.
  Therefore, $O(\sqrt{n})$ bits of communication are necessary and sufficent to prepare $|\psi\rangle^{\otimes n}$ from EPR pairs. (a.k.a. entanglement dilution.) [Harrow and Lo; quant-ph/0204096]

Application to information theory

- Traditionally spread has been thought as a "sublinear" phenomenon, and as a result, has been neglected.
- Example: If $|\psi\rangle$ is an entangled state, then $|\psi\rangle^{\otimes n}$ is very close to a state with spread $O(\sqrt{n})$.
  Therefore, $O(\sqrt{n})$ bits of communication are necessary and suffcent to prepare $|\psi\rangle^{\otimes n}$ from EPR pairs. (a.k.a. entanglement dilution.) [Harrow and Lo; quant-ph/0204096]
- However, even in i.i.d. settings, entanglement spread can be size $O(n)$.

Example: Channel simulation

$$A \;\text{———}\; \boxed{N} \;\text{———}\; B$$

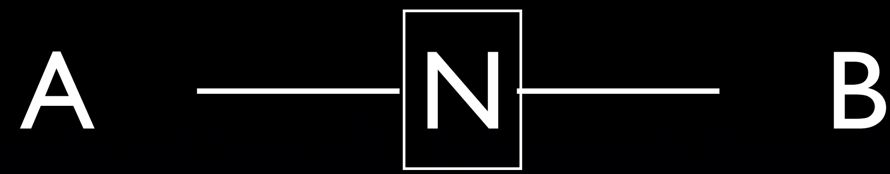
Example: Channel simulation

$$A \;\text{———}\; \boxed{N} \;\text{———}\; B$$

<u>Shannon's (noisy coding) theorem:</u>

Any noisy channel N using input distribution p^A can code at rate $C_{N,p} = H(A)_p + H(B)_p - H(AB)_p$.

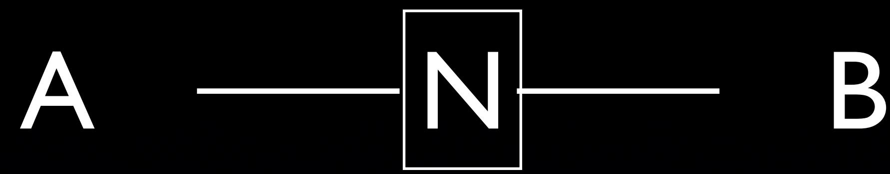
Example: Channel simulation



<u>Shannon's (noisy coding) theorem:</u>

Any noisy channel N using input distribution p^A can code at rate $C_{N,p} = H(A)_p + H(B)_p - H(AB)_p$.

Example: Channel simulation



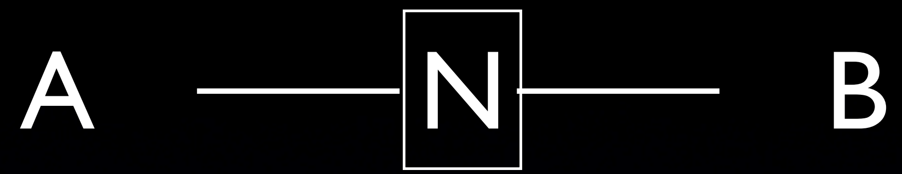
Shannon's (noisy coding) theorem:

Any noisy channel N using input distribution p^A can code at rate $C_{N,p} = H(A)_p + H(B)_p - H(AB)_p$.

(Classical) Reverse Shannon Theorem: N can be simulated on $p^{\otimes n}$ using communication $C_{N,p}$ and shared randomness $R_{N,p} = H(AB)_p - H(A)_p$.

[BSST01,Cuff08]

Example: Channel simulation



Shannon's (noisy coding) theorem:

Any noisy channel N using input distribution p^A can code at rate $C_{N,p} = H(A)_p + H(B)_p - H(AB)_p$.

(Classical) Reverse Shannon Theorem: N can be simulated on $p^{\otimes n}$ using communication $C_{N,p}$ and shared randomness $R_{N,p} = H(AB)_p - H(A)_p$.

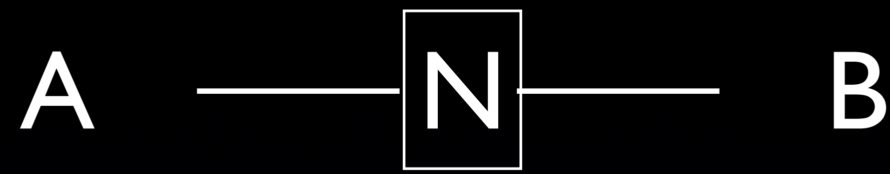
[BSST01,Cuff08]

On general inputs:

The capacity and simulation cost are replaced by $C(N) = \max_p C_{N,p}$.

Randomness cost for simulation is $\max_p H(B)_p - C(N)$.

Example: Channel simulation



<u>Shannon's (noisy coding) theorem:</u>

Any noisy channel N using input distribution p^A can code at rate $C_{N,p} = H(A)_p + H(B)_p - H(AB)_p$.

<u>(Classical) Reverse Shannon Theorem</u>: N can be simulated on $p^{\otimes n}$ using communication $C_{N,p}$ and shared randomness $R_{N,p} = H(AB)_p - H(A)_p$.

[BSST01,Cuff08]

<u>On general inputs</u>:

The capacity and simulation cost are replaced by $C(N) = \max_p C_{N,p}$.

Randomness cost for simulation is $\max_p H(B)_p - C(N)$.

Simulating quantum channels

Simulating quantum channels

- Coding with quantum channels: Using shared EPR pairs, a quantum channel $\mathcal{N}$ can send noiseless qubits at rate $\max_\rho Q_{\mathcal{N},\rho} = \max_\rho (H(A)_\rho + H(B)_\rho - H(AB)_\rho) / 2$.

Simulating quantum channels

- Coding with quantum channels: Using shared EPR pairs, a quantum channel $\mathcal{N}$ can send noiseless qubits at rate $\max_\rho Q_{\mathcal{N},\rho} = \max_\rho (H(A)_\rho + H(B)_\rho - H(AB)_\rho) / 2$.
- Quantum Reverse Shannon Theorem: For a quantum channel $\mathcal{N}$ and an input distribution ρ, $\mathcal{N}^{\otimes n}$ can be simulated on $\rho^{\otimes n}$ using $Q_{\mathcal{N},\rho}$ qubits of communication and $E_{\mathcal{N},\rho} = H(B)_\rho - Q_{\mathcal{N},\rho}$ shared EPR pairs. [BDHSW; arXiv:0912.5537]

Simulating quantum channels

- Coding with quantum channels: Using shared EPR pairs, a quantum channel $\mathcal{N}$ can send noiseless qubits at rate $\max_\rho Q_{\mathcal{N},\rho} = \max_\rho (H(A)_\rho + H(B)_\rho - H(AB)_\rho) / 2$.
- Quantum Reverse Shannon Theorem: For a quantum channel $\mathcal{N}$ and an input distribution ρ, $\mathcal{N}^{\otimes n}$ can be simulated on $\rho^{\otimes n}$ using $Q_{\mathcal{N},\rho}$ qubits of communication and $E_{\mathcal{N},\rho} = H(B)_\rho - Q_{\mathcal{N},\rho}$ shared EPR pairs. [BDHSW; arXiv:0912.5537]
- However, it does not follow that $\mathcal{N}^{\otimes n}$ can be simulated on arbitrary inputs using $\max_\rho(Q_{\mathcal{N},\rho})$ qubits of communication and $\max_\rho(E_{\mathcal{N},\rho})$ shared EPR pairs!

Simulating quantum channels

- Coding with quantum channels: Using shared EPR pairs, a quantum channel $\mathcal{N}$ can send noiseless qubits at rate $\max_\rho Q_{\mathcal{N},\rho} = \max_\rho (H(A)_\rho + H(B)_\rho - H(AB)_\rho) / 2$.
- Quantum Reverse Shannon Theorem: For a quantum channel $\mathcal{N}$ and an input distribution ρ, $\mathcal{N}^{\otimes n}$ can be simulated on $\rho^{\otimes n}$ using $Q_{\mathcal{N},\rho}$ qubits of communication and $E_{\mathcal{N},\rho} = H(B)_\rho - Q_{\mathcal{N},\rho}$ shared EPR pairs. [BDHSW; arXiv:0912.5537]
- However, it does not follow that $\mathcal{N}^{\otimes n}$ can be simulated on arbitrary inputs using $\max_\rho(Q_{\mathcal{N},\rho})$ qubits of communication and $\max_\rho(E_{\mathcal{N},\rho})$ shared EPR pairs!
- Problem: suppose that the input to $\mathcal{N}^{\otimes n}$ is $(\rho^{\otimes n} + \sigma^{\otimes n})/2$ with $Q_{\mathcal{N},\rho} = Q_{\mathcal{N},\sigma}$ but $E_{\mathcal{N},\rho} > E_{\mathcal{N},\sigma}$. Then the naive method of combining the two simulations will require creating $n(E_{\mathcal{N},\rho} - E_{\mathcal{N},\sigma})$ entanglement spread.

Simulating quantum channels

- Coding with quantum channels: Using shared EPR pairs, a quantum channel $\mathcal{N}$ can send noiseless qubits at rate $\max_\rho Q_{\mathcal{N},\rho} = \max_\rho (H(A)_\rho + H(B)_\rho - H(AB)_\rho) / 2$.
- Quantum Reverse Shannon Theorem: For a quantum channel $\mathcal{N}$ and an input distribution ρ, $\mathcal{N}^{\otimes n}$ can be simulated on $\rho^{\otimes n}$ using $Q_{\mathcal{N},\rho}$ qubits of communication and $E_{\mathcal{N},\rho} = H(B)_\rho - Q_{\mathcal{N},\rho}$ shared EPR pairs. [BDHSW; arXiv:0912.5537]
- However, it does not follow that $\mathcal{N}^{\otimes n}$ can be simulated on arbitrary inputs using $\max_\rho(Q_{\mathcal{N},\rho})$ qubits of communication and $\max_\rho(E_{\mathcal{N},\rho})$ shared EPR pairs!
- Problem: suppose that the input to $\mathcal{N}^{\otimes n}$ is $(\rho^{\otimes n} + \sigma^{\otimes n})/2$ with $Q_{\mathcal{N},\rho} = Q_{\mathcal{N},\sigma}$ but $E_{\mathcal{N},\rho} > E_{\mathcal{N},\sigma}$. Then the naive method of combining the two simulations will require creating $n(E_{\mathcal{N},\rho} - E_{\mathcal{N},\sigma})$ entanglement spread.
- This requires either extra communication (forward or back) or embezzling states.

The general goal: LOSE

The general goal: LOSE

- Definition: LOSE (local operations and shared entanglement) operations can be performed with local operations and arbitrary shared entangled states, but no communication.

The general goal: LOSE

- Definition: LOSE (local operations and shared entanglement) operations can be performed with local operations and arbitrary shared entangled states, but no communication.
- Determining membership in LOSE, even approximately, is NP-hard. [Gutoski, arXiv:0805.2209]

The general goal: LOSE

- Definition: LOSE (local operations and shared entanglement) operations can be performed with local operations and arbitrary shared entangled states, but no communication.
- Determining membership in LOSE, even approximately, is NP-hard. [Gutoski, arXiv:0805.2209]
- Question: When do EPR pairs help reduce the communication cost of a task?
  Trivial examples: creating a shared entangled state; super-dense coding.

The general goal: LOSE

- Definition: LOSE (local operations and shared entanglement) operations can be performed with local operations and arbitrary shared entangled states, but no communication.
- Determining membership in LOSE, even approximately, is NP-hard. [Gutoski, arXiv:0805.2209]
- Question: When do EPR pairs help reduce the communication cost of a task?
  Trivial examples: creating a shared entangled state; super-dense coding.
- Question: When do other forms of entanglement help more than EPR pairs?
  Simulating noisy quantum channels. More examples to follow.

The general goal: LOSE

- Definition: LOSE (local operations and shared entanglement) operations can be performed with local operations and arbitrary shared entangled states, but no communication.
- Determining membership in LOSE, even approximately, is NP-hard. [Gutoski, arXiv:0805.2209]
- Question: When do EPR pairs help reduce the communication cost of a task?
  Trivial examples: creating a shared entangled state; super-dense coding.
- Question: When do other forms of entanglement help more than EPR pairs?
  Simulating noisy quantum channels. More examples to follow.
- Communication complexity: Special case in which Alice holds $x \in \{0,1\}^n$, Bob holds $y \in \{0,1\}^n$ and they want to compute the bit $f(x,y)$.

Uses of non-standard entanglement:
1. Embezzling states

Uses of non-standard entanglement: 1. Embezzling states

- When communication is not free, EPR pairs are one of the weakest forms of entanglement.

Uses of non-standard entanglement: 1. Embezzling states

- When communication is not free, EPR pairs are one of the weakest forms of entanglement.
- On the other hand, there is a family of $k \times k$-qubit "embezzling states" [van Dam and Hayden. quant-ph/0201041]

$$|\zeta_k\rangle \propto \sum_{i=1}^{2^k} \frac{1}{\sqrt{i}} |i\rangle \otimes |i\rangle$$

such that for any $n \times n$-qubit entangled state $|\psi\rangle$, Alice and Bob can map $|\zeta_k\rangle$ to $|\zeta_k\rangle \otimes |\psi\rangle$ with no communication, up to error $O(n/k)$.

Uses of non-standard entanglement: I. Embezzling states

- When communication is not free, EPR pairs are one of the weakest forms of entanglement.
- On the other hand, there is a family of $k \times k$-qubit "embezzling states" [van Dam and Hayden. quant-ph/0201041]

$$|\zeta_k\rangle \propto \sum_{i=1}^{2^k} \frac{1}{\sqrt{i}} |i\rangle \otimes |i\rangle$$

such that for any $n \times n$-qubit entangled state $|\psi\rangle$, Alice and Bob can map $|\zeta_k\rangle$ to $|\zeta_k\rangle \otimes |\psi\rangle$ with no communication, up to error $O(n/k)$.

- The proper definition of "free entanglement" is thus closer to "an embezzling state of arbitrary finite size" than "unlimited EPR pairs." In particular, the entangled state in LOSE operations can be taken to be an embezzling state w.l.o.g.

Uses of non-standard entanglement: 2. Non-local measurement

Uses of non-standard entanglement: 2. Non-local measurement

Measurement using reference states: Given $|\alpha\rangle^{\otimes m-1}$, we can determine whether an input state is equal to or orthogonal $|\alpha\rangle$ up to error $1/m$.

Uses of non-standard entanglement: 2. Non-local measurement

Measurement using reference states: Given $|\alpha\rangle^{\otimes m-1}$, we can determine whether an input state is equal to or orthogonal $|\alpha\rangle$ up to error 1/m.

$$\overbrace{|\alpha\rangle \quad |\alpha\rangle \quad |\alpha\rangle \quad |\alpha\rangle \quad |\alpha\rangle}^{\text{m-1 copies}} \quad |\beta\rangle$$

Uses of non-standard entanglement: 2. Non-local measurement

Measurement using reference states: Given $|\alpha\rangle^{\otimes m-1}$, we can determine whether an input state is equal to or orthogonal $|\alpha\rangle$ up to error $1/m$.

m-1 copies

$|\alpha\rangle \quad |\alpha\rangle \quad |\alpha\rangle \quad |\alpha\rangle \quad |\alpha\rangle \quad |\beta\rangle$

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

Contained in symmetric subspace

$\langle\alpha|\beta\rangle=0$

Overlap 1/m with symmetric subspace

Uses of non-standard entanglement: 2. Non-local measurement

Measurement using reference states: Given $|\alpha\rangle^{\otimes m-1}$, we can determine whether an input state is equal to or orthogonal $|\alpha\rangle$ up to error $1/m$.

m-1 copies

$|\alpha\rangle \quad |\alpha\rangle \quad |\alpha\rangle \quad |\alpha\rangle \quad |\alpha\rangle \quad |\beta\rangle$

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

Contained in symmetric subspace

$\langle\alpha|\beta\rangle=0$

Overlap 1/m with symmetric subspace

Problem reduces to projecting onto symmetric subspace.

Uses of non-standard entanglement:
2. Non-local measurement

Uses of non-standard entanglement: 2. Non-local measurement

- Non-local measurement using reference states: Given *shared states* $|\alpha\rangle^{\otimes m-1}$, Alice and Bob can distinguish $|\alpha\rangle$ from $|\alpha\rangle^{\perp}$ up to error 1/m, using O(log m) qubits of communication.
  [Harrow, Leung, 0803.3066]

Uses of non-standard entanglement: 2. Non-local measurement

- Non-local measurement using reference states: Given *shared states* $|\alpha\rangle^{\otimes m-1}$, Alice and Bob can distinguish $|\alpha\rangle$ from $|\alpha\rangle^{\perp}$ up to error 1/m, using O(log m) qubits of communication.
  [Harrow, Leung, 0803.3066]
- Application: Define the bipartite unitary operator
  $U = I - 2\,|\alpha\rangle\langle\alpha|$, with $|\alpha\rangle = |01\rangle^{\otimes n} + |\Phi\rangle^{\otimes n} / \sqrt{2}$. Then

Uses of non-standard entanglement: 2. Non-local measurement

- Non-local measurement using reference states: Given *shared states* $|\alpha\rangle^{\otimes m-1}$, Alice and Bob can distinguish $|\alpha\rangle$ from $|\alpha\rangle^{\perp}$ up to error 1/m, using O(log m) qubits of communication. [Harrow, Leung, 0803.3066]
- Application: Define the bipartite unitary operator $U = I - 2\,|\alpha\rangle\langle\alpha|$, with $|\alpha\rangle = |01\rangle^{\otimes n} + |\Phi\rangle^{\otimes n} / \sqrt{2}$. Then
  - Simulating U requires O(n) qubits of communication, even using free EPR pairs.

Uses of non-standard entanglement: 2. Non-local measurement

- Non-local measurement using reference states: Given *shared states* $|\alpha\rangle^{\otimes m-1}$, Alice and Bob can distinguish $|\alpha\rangle$ from $|\alpha\rangle^{\perp}$ up to error $1/m$, using $O(\log m)$ qubits of communication.
[Harrow, Leung, 0803.3066]
- Application: Define the bipartite unitary operator
$U = I - 2\,|\alpha\rangle\langle\alpha|$, with $|\alpha\rangle = |01\rangle^{\otimes n} + |\Phi\rangle^{\otimes n} / \sqrt{2}$. Then
    - Simulating U requires O(n) qubits of communication, even using free EPR pairs.
    - With general entanglement, U can be simulated to accuracy ε using $O(\log 1/\varepsilon)$ qubits of communication.

Uses of non-standard entanglement: 2. Non-local measurement

- Non-local measurement using reference states: Given *shared states* $|\alpha\rangle^{\otimes m-1}$, Alice and Bob can distinguish $|\alpha\rangle$ from $|\alpha\rangle^\perp$ up to error $1/m$, using $O(\log m)$ qubits of communication.
  [Harrow, Leung, 0803.3066]
- Application: Define the bipartite unitary operator $U = I - 2\,|\alpha\rangle\langle\alpha|$, with $|\alpha\rangle = |01\rangle^{\otimes n} + |\Phi\rangle^{\otimes n} / \sqrt{2}$. Then
  - Simulating U requires O(n) qubits of communication, even using free EPR pairs.
  - With general entanglement, U can be simulated to accuracy ε using $O(\log 1/\varepsilon)$ qubits of communication.
- Corollary: U can asymptotically create O(n) EPR pairs/use, but can only send O(log(n)) bits/use.

Communication complexity

Communication complexity

- Alice gets $x \in \{0,1\}^n$, Bob gets $y \in \{0,1\}^n$ and they would like to compute $f(x,y)$ using as little communication as possible, allowing a small chance of error.

Communication complexity

- Alice gets $x \in \{0,1\}^n$, Bob gets $y \in \{0,1\}^n$ and they would like to compute $f(x,y)$ using as little communication as possible, allowing a small chance of error.
- Communication can be one-way or two-way.

Communication complexity

- Alice gets $x \in \{0,1\}^n$, Bob gets $y \in \{0,1\}^n$ and they would like to compute $f(x,y)$ using as little communication as possible, allowing a small chance of error.
- Communication can be one-way or two-way.
- Shared randomness is known to help, but by Newman's theorem, $O(\log n)$ bits of shared randomness always suffice.

Communication complexity

- Alice gets $x \in \{0,1\}^n$, Bob gets $y \in \{0,1\}^n$ and they would like to compute $f(x,y)$ using as little communication as possible, allowing a small chance of error.
- Communication can be one-way or two-way.
- Shared randomness is known to help, but by Newman's theorem, $O(\log n)$ bits of shared randomness always suffice.
- Free EPR pairs are known to help, although all known examples simply use them to turn classical communication into quantum communication.

Communication complexity

- Alice gets $x \in \{0,1\}^n$, Bob gets $y \in \{0,1\}^n$ and they would like to compute $f(x,y)$ using as little communication as possible, allowing a small chance of error.
- Communication can be one-way or two-way.
- Shared randomness is known to help, but by Newman's theorem, $O(\log n)$ bits of shared randomness always suffice.
- Free EPR pairs are known to help, although all known examples simply use them to turn classical communication into quantum communication.
- Can non-standard entanglement (e.g. embezzling states) save even more communication?

Communication complexity

Claim: General entanglement is not much better than EPR pairs in reducing communication complexity.

Communication complexity

Claim: General entanglement is not much better than EPR pairs in reducing communication complexity.

Proof: Let $|\psi\rangle = \sum_k \sqrt{p_k}\, |k\rangle|k\rangle|\Phi_2\rangle^{\otimes k}$ be our starting state for a protocol that uses Q qubits of communication. Then Pr[accept] is of the form

Communication complexity

Claim: General entanglement is not much better than EPR pairs in reducing communication complexity.

Proof: Let $|\psi\rangle = \sum_k \sqrt{p_k}\, |k\rangle|k\rangle|\Phi_2\rangle^{\otimes k}$ be our starting state for a protocol that uses Q qubits of communication. Then Pr[accept] is of the form

$$\mathrm{tr} \begin{pmatrix} * & * & * & * & * & * \\ * & * & * & * & * & * \\ * & * & * & * & * & * \\ * & * & * & * & * & * \\ * & * & * & * & * & * \\ * & * & * & * & * & * \end{pmatrix} \begin{pmatrix} p_1 & \sqrt{p_1 p_2} & \sqrt{p_1 p_3} & \cdots \\ \sqrt{p_1 p_2} & p_2 & \sqrt{p_2 p_3} & \\ \sqrt{p_1 p_3} & \sqrt{p_2 p_3} & p_3 & \\ \vdots & & & \ddots \end{pmatrix}$$

Communication complexity

Claim: General entanglement is not much better than EPR pairs in reducing communication complexity.

Proof: Let $|\psi\rangle = \sum_k \sqrt{p_k}\, |k\rangle|k\rangle|\Phi_2\rangle^{\otimes k}$ be our starting state for a protocol that uses Q qubits of communication. Then Pr[accept] is of the form

$$\mathrm{tr} \begin{pmatrix} * & * & * & * & * & * \\ * & * & * & * & * & * \\ * & * & * & * & * & * \\ * & * & * & * & * & * \\ * & * & * & * & * & * \\ * & * & * & * & * & * \end{pmatrix} \begin{pmatrix} p_1 & \sqrt{p_1 p_2} & \sqrt{p_1 p_3} & \cdots \\ \sqrt{p_1 p_2} & p_2 & \sqrt{p_2 p_3} & \\ \sqrt{p_1 p_3} & \sqrt{p_2 p_3} & p_3 & \\ \vdots & & & \ddots \end{pmatrix}$$

Thus we can replace $|\psi\rangle$ with a mixture of states with spread $O(Q/\varepsilon)$ and incur error $\leq \varepsilon$.

Open questions

Open questions

- When does entanglement spread help, and when are EPR pairs good enough?

Open questions

- When does entanglement spread help, and when are EPR pairs good enough?
- Can spread be quantified and described as a resource, like EPR pairs?
  (First step: $\log(r\lambda_1)/2+O(\log 1/\varepsilon)$ qubits suffice to produce a state with Schmidt coefficients $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_r$ up to accuracy ε [Harrow & Hayden].)

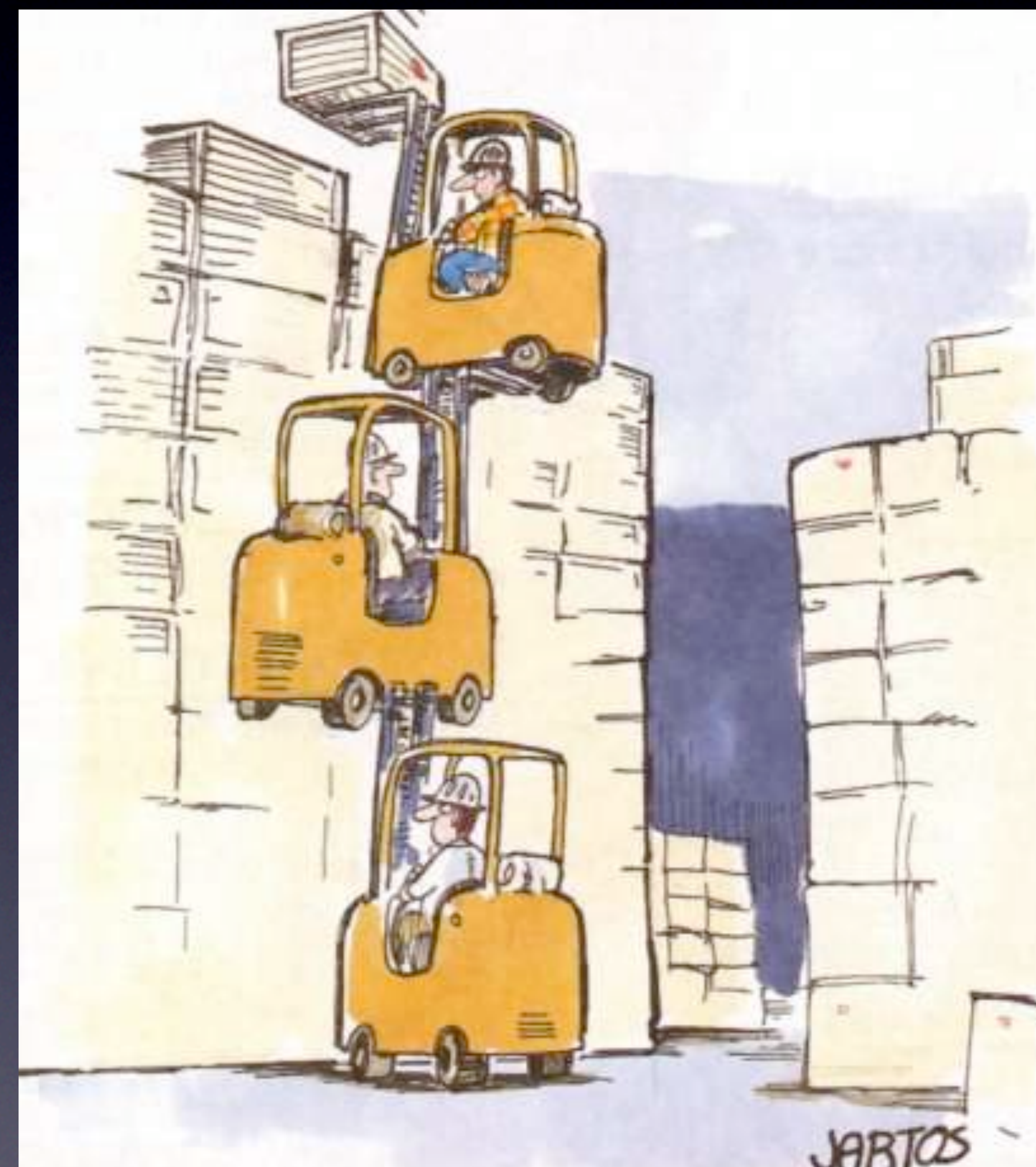
Open questions

- When does entanglement spread help, and when are EPR pairs good enough?
- Can spread be quantified and described as a resource, like EPR pairs?
  (First step: $\log(r\lambda_1)/2+O(\log 1/\varepsilon)$ qubits suffice to produce a state with Schmidt coefficients $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_r$ up to accuracy ε [Harrow & Hayden].)
- Does spread connect to other forms of irreversibiliy in quantum information theory, such as creating noisy entanglement?

Open questions

- When does entanglement spread help, and when are EPR pairs good enough?
- Can spread be quantified and described as a resource, like EPR pairs?
  (First step: $\log(r\lambda_1)/2+O(\log 1/\varepsilon)$ qubits suffice to produce a state with Schmidt coefficients $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_r$ up to accuracy ε [Harrow & Hayden].)
- Does spread connect to other forms of irreversibiliy in quantum information theory, such as creating noisy entanglement?
- In communication complexity, how useful even are EPR pairs? Can spread be used to argue that n EPR pairs are not useful for a Q-qubit protocol when $n \gg Q$?

And they all lived happily ever after.



The end.