Erasing correlations, destroying entanglement and other new challenges for quantum information theory

quant-ph/0511219

Aram Harrow, Bristol

Peter Shor, MIT

QIP, 19 Jan 2006

outline

- General rules for reversing protocols
- Coherent erasure of classical correlations
- Disentangling power of quantum operations

Everything is a resource

qubit	[q ! q]	|0i^A ! |0i^B and |1i^A ! |1i^B
ebit	[qq]	the state (|0i^A|0i^B + |1i^A|1i^B)/ p 2
~~cbit~~	~~[c ! c]~~	~~|0i^A ! |0i^B|0i^E and |1i^A ! |1i^B|1i^E~~
cobit	[q ! qq]	|0i^A ! |0i^A|0i^B and |1i^A ! |1i^A|1i^B

resource inequalities

super-dense coding:

[q ! q] + [qq] **>** 2[~~c ! c~~] 2 [q ! qq]

In fact, [q ! q] + [qq] = 2 [q ! qq]

Undoing things is also a resource

reversal	meaning
[q ! q]^{y} = [q Ã q]	(relation between time-reversal and exchange symmetry)
[qq]^{y} = -[qq]	(disentangling power)
[q ! qq]^{y} = [q Ã qq] (?)	|0i^{A} |0i^{B} ! |0i^{A} and |1i^{A} |1i^{B} ! |1i^{A} (coherent erasure??)

What good is coherent erasure?

$\alpha|0i^A + \beta|1i^A$! $\alpha|0i^A|0i^B + \beta|1i^A|1i^B$ (using [q ! qq])

! $\alpha|0i^B + \beta|1i^B$ (using [qq ! q])

[q ! qq] + [qq ! q] $\overset{=}{\cancel{\geq}}$ [q ! q]

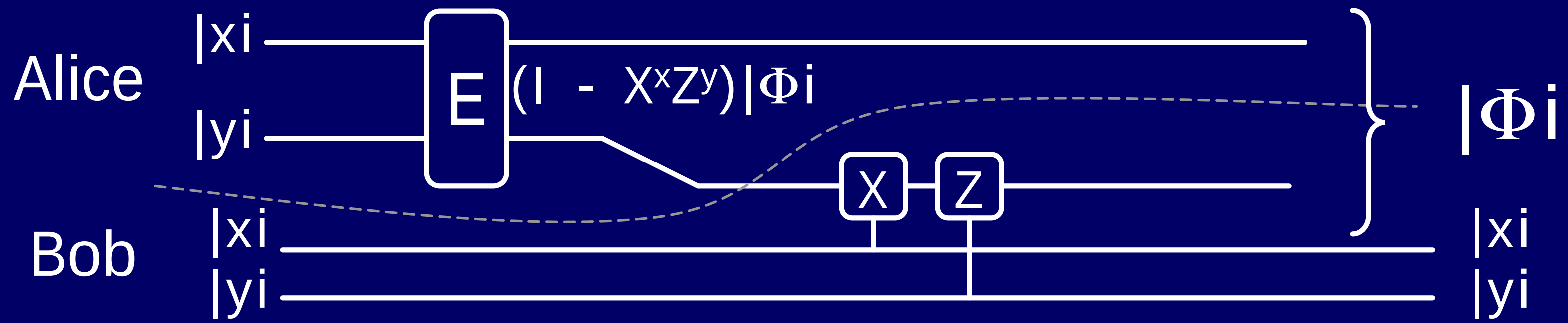
[qq ! q] $\overset{=}{\cancel{\geq}}$ [q ! q] - [q ! qq]

= [q ! qq] - [qq]

= ([q ! q] - [qq]) / 2

entanglement-assisted communication only

In fact, these are all equalities! (Proof: reverse SDC.)



application to unitary gates

U is a bipartite unitary gate (e.g. CNOT)

Known:

U **>** C[c ! c] implies U **>** C[q ! qq]

Time reversal means:

U^{y} **>** C [q Ã qq]

= C [qq Ã q] - C [qq]

Corollary: If entanglement is free then $C_{!}^{E}(U) = C_{\tilde{A}}^{E}(U^{y})$.

The quest for asymmetric unitary gate capacities

Problem: If U is nonlocal, it has nonzero quantum capacities in both directions. Are they equal?

Yes, if U is 2£2.

No, in general, but for a dramatic separation we will need a gate that violates time-reversal symmetry.

the construction:

(U_m acts on 2^m **£** 2^m dimensions)

$U_m|xi^A|0i^B = |xi^A|xi^B$ for 0 **6** $x < 2^m$

$U_m|xi^A|yi^B = |xi^A|y\text{-}1i^B$ for $0 < y$ **6** $x < 2^m$

$U_m|xi^A|yi^B = |xi^A|yi^B$ for 0 **6** $x < y < 2^m$

et voilà l'asymétrie!

$U_m|xi^A|0i^B$ = $|xi^A|xi^B$ for 0 **6** x < 2^m

$U_m|xi^A|yi^B$ = $|xi^A|y\text{-}1i^B$ for 0 < y **6** x < 2^m

$U_m|xi^A|yi^B$ = $|xi^A|yi^B$ for 0 **6** x < y < 2^m

U_m **>** m[q ! qq]

Upper bound by simulation:

m[q ! qq] + O((log m)(log m/ε)) ([q ! q] + [q Ã q]) **&** U_m

Similarly, U_m^y **>** m[q Ã qq] and

m[q Ã qq] + O((log m)(log m/ε)) ([q ! q] + [q Ã q]) **&** U_m^y

Meaning: U_m ¼ m [q ! qq]

and U_m^y ¼ m [q Ã qq] (almost worthless w/o ent. assistance!)

disentanglement

clean resource inequalities:

$$\alpha \overset{\text{clean}}{\geq} \beta$$

means that $\alpha^{\otimes n}$ can be asymptotically converted to $\beta^{\otimes n}$ while discarding only o(n) entanglement.

(equivalently: while generating a sublinear amount of local entropy.)

Example: $[q ! q] \overset{\text{clean}}{>} [qq]$ and $[q ! q] \overset{\text{clean}}{>} -[qq]$

Example: $U_m \overset{\text{clean}}{>} m[qq]$, but can only destroy $O(\log^2 m)$ [qq]

$U_m^y \overset{\text{clean}}{>} -m[qq]$, but can only create $O(\log^2 m)$ [qq]

You can't just throw it away

Q: Why not?

A: Given unlimited EPR pairs, try creating the state

$$\frac{1}{\sqrt{2}}\left(|00\rangle_{AB}^{\otimes n} + |\Phi_-\rangle_{AB}^{\otimes n}\right)$$

Hayden & Winter [quant-ph/0204092] proved that this requires ¼n bits of communication.

more relevant examples

Entanglement dilution:

$|\psi i_{AB}$ is partially entangled. $E = S(\psi^A)$.

$|\Phi i^{- nE+o(n)}$! $|\psi i^{- n}$

Even $|\Phi i^{- 1}$! $|\psi i^{- n}$ requires $\Omega(n^{½})$ cbits (in either direction).

OR a size $O(n^{½}/\varepsilon)$ embezzling state [q-ph/0205100, Hayden-van Dam]

Quantum Reverse Shannon Theorem for general inputs

[Bennett, Devetak, Harrow, Shor, Winter]

Input $\rho^{- n}$ requires $I(A;B)_\rho$ [c ! c] + $H(N(\rho))$ [qq].

Superpositions of different $\rho^{- n}$ mean consuming superpositions of different amounts of entanglement: we need either extra cbits, embezzling, or another source of entanglement spread.

summary

- new ideas
  - coherent erasure
  - clean protocols
  - entanglement spread
- new results
  - asymmetric unitary gate capacities
  - QRST and other converses
- new directions
  - formalizing entanglement spread
  - clean protocols involving noisy resources (cbits?)

READ ALL ABOUT IT!

quant-ph/0511219