Concentration of Measure Effects in Quantum Information

Patrick Hayden (McGill University)

Overview

- Superdense coding
- Random states and random subspaces
- Superdense coding of quantum states
- Quantum mechanical encryption

Information theory

- A practical question:
  - How to best make use of a given communications resource?
- A mathematico-epistemological question:
  - How to quantify uncertainty and information?
- Shannon:
  - Solved the first by considering the second.
  - ~~A~~ *mathematical* theory of communication [1948]

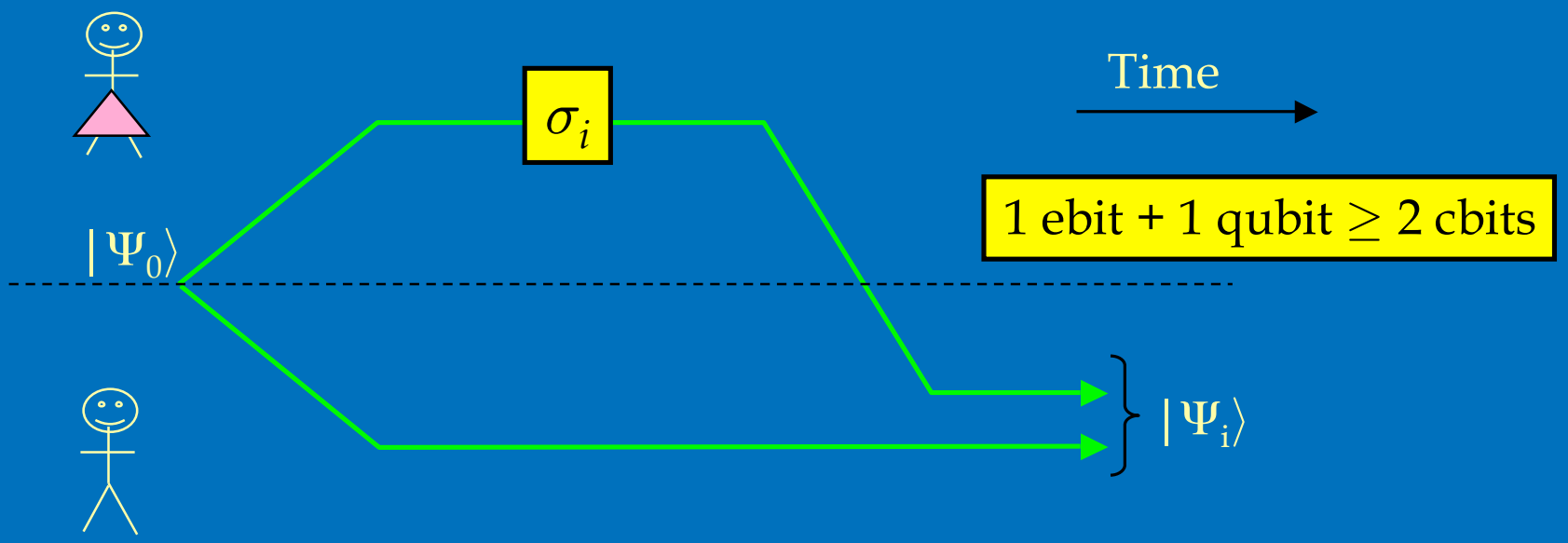
The

A challenge to the physicists

- John Pierce [1973]:
  - I think that I have never met a physicist who understood information theory. I wish that physicists would stop talking about reformulating information theory and would give us a general expression for the capacity of a channel with quantum effects taken into account rather than a number of special cases.

Superdense coding

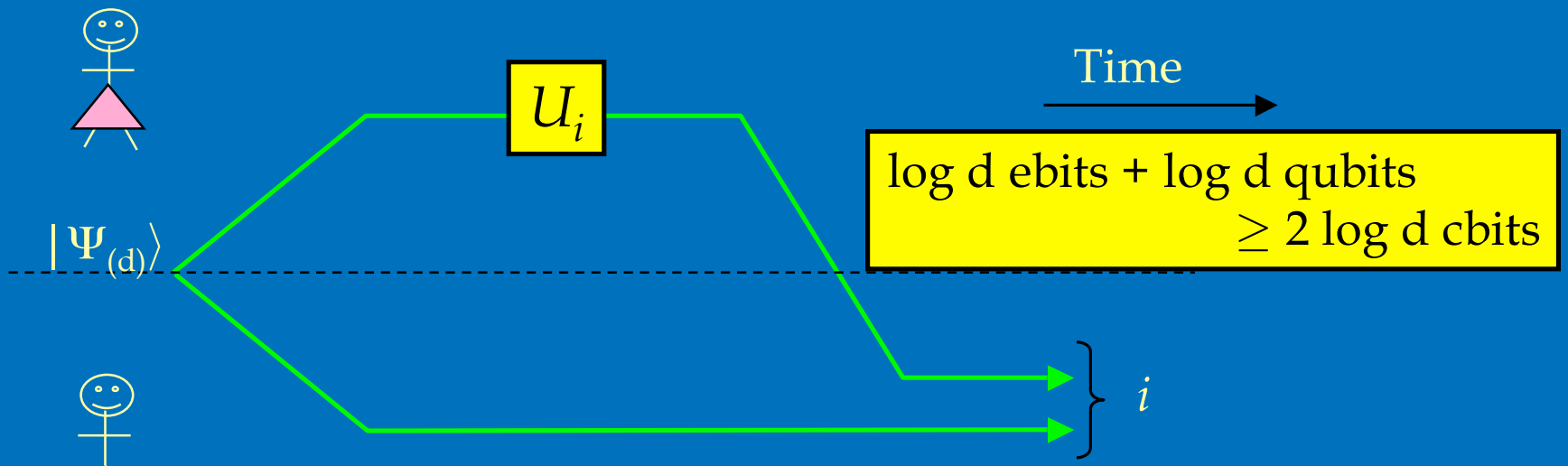
To send $i \in \{0,1,2,3\}$



$$|\Psi_0\rangle = |00\rangle + |11\rangle \quad |\Psi_2\rangle = |00\rangle - |11\rangle$$
$$|\Psi_1\rangle = |01\rangle + |10\rangle \quad |\Psi_3\rangle = |01\rangle - |10\rangle$$

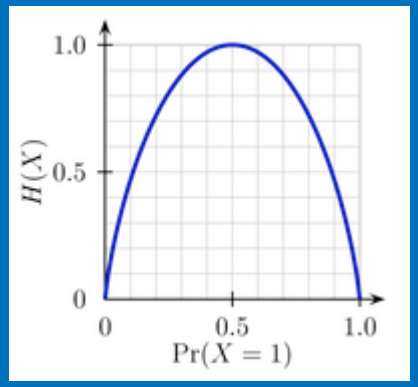
More generally...

Superdense coding: To send $i \in \{1,\ldots,d^2\}$



$$|\Psi_{(d)}\rangle = |00\rangle + |11\rangle + \cdots + |dd\rangle$$

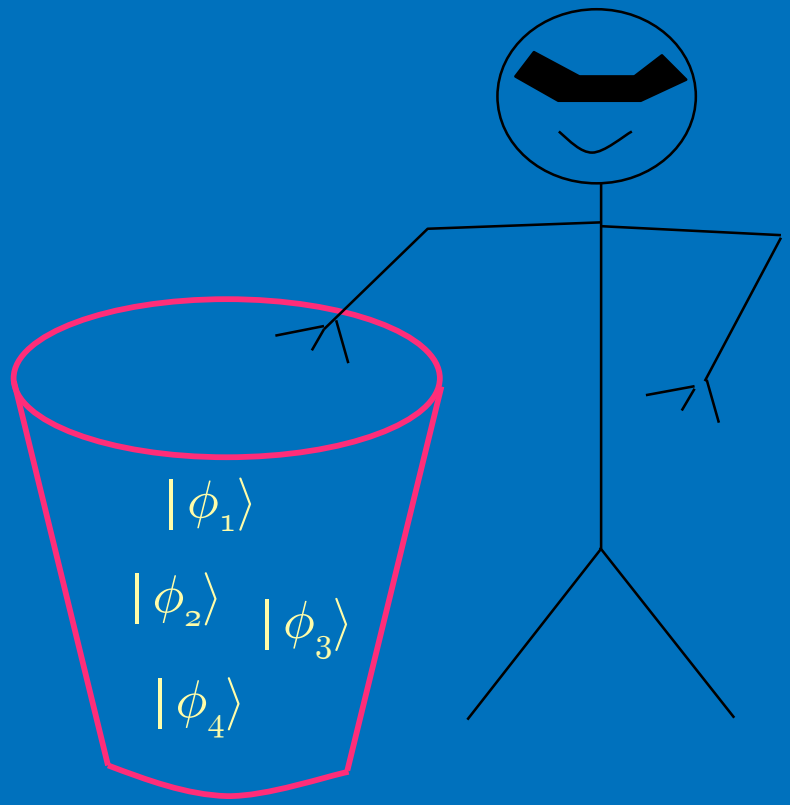
Quantifying uncertainty



- Entropy: $H(X) = -\sum_x p(x) \log_2 p(x)$
- Proportional to entropy of statistical physics
- Term suggested by von Neumann (more on him later)
- Can arrive at definition axiomatically:
  - $H(X,Y) = H(X) + H(Y)$ for independent X, Y, etc.
- Operational point of view…

Mixing quantum states: The density operator

Draw $|\phi_x\rangle$ with probability p(x)



Perform a measurement $\{|0\rangle, |1\rangle\}$:

Probability of outcome j:

$$q_j = \sum_x p(x) \; |\langle j|\phi_x\rangle \; |^2$$

$$= \sum_x p(x) \; \mathrm{tr}[\,|j\rangle\langle j|\phi_x\rangle\langle\phi_x|\,]$$

$$= \mathrm{tr}[\; |j\rangle\langle j| \; \rho \;],$$

where $\rho = \sum_x p(x) \; |\phi_x\rangle\langle\phi_x|$

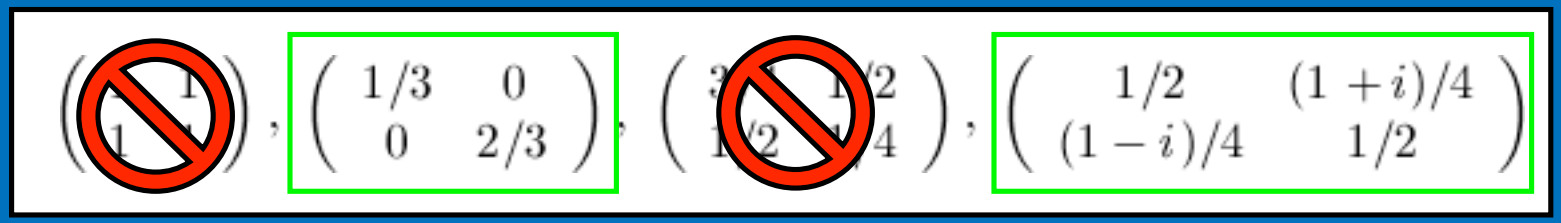
Outcome probability is linear in ρ

Properties of the density operator

- ρ is Hermitian:
  - $\rho^\dagger = [\sum_x p(x) |\phi_x\rangle\langle\phi_x|]^\dagger = \sum_x p(x) [|\phi_x\rangle\langle\phi_x|]^\dagger = \rho$
- ρ is positive semidefinite:
  - $\langle\omega|\rho|\omega\rangle = \sum_x p(x) \langle\omega|\phi_x\rangle\langle\phi_x|\omega\rangle \geq 0$
- $\mathrm{tr}[\rho] = 1$:
  - $\mathrm{tr}[\rho] = \sum_x p(x)\, \mathrm{tr}[|\phi_x\rangle\langle\phi_x|] = \sum_x p(x) = 1$
- Ensemble ambiguity:
  - $I/2 = \frac{1}{2}[|0\rangle\langle 0| + |1\rangle\langle 1|] = \frac{1}{2}[|+\rangle\langle +| + |-\rangle\langle -|]$

The density operator: examples

Which of the following are density operators?



Quantifying uncertainty

- Let $\rho = \sum_x p(x) |\phi_x\rangle\langle\phi_x|$ be a density operator
- von Neumann entropy:

$$H(\rho) = - \text{tr} [\rho \log \rho]$$

- Equal to Shannon entropy of ρ eigenvalues
- Analog of a joint random variable:
  - ρ_{AB} describes a composite system $A \otimes B$
  - $H(A)_\rho = H(\rho_A) = H(\text{tr}_B \rho_{AB})$

Quantifying uncertainty: Examples

- $H(|\phi\rangle\langle\phi|) =$
- $H(I/2) =$
- $H(\rho \otimes \sigma) =$
- $H(I/2^n) =$
- $H(p\rho \oplus (1\text{-}p)\sigma) =$

Surprises in high dimension

- Choose a random pure quantum state:
  $\phi \in_{\mathrm{R}} \mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$

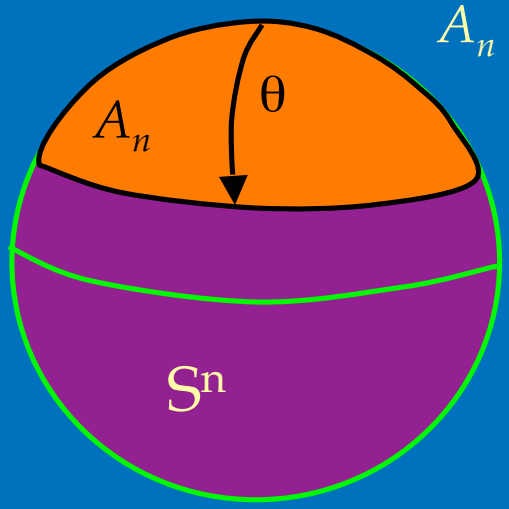
- What can we expect of ϕ? $(d_A \leq d_B)$

$$\mathbb{E} H(\phi_A) \geq \log d_A - \frac{d_A}{2 \ln 2 \, d_B}$$

- On average, states are highly entangled

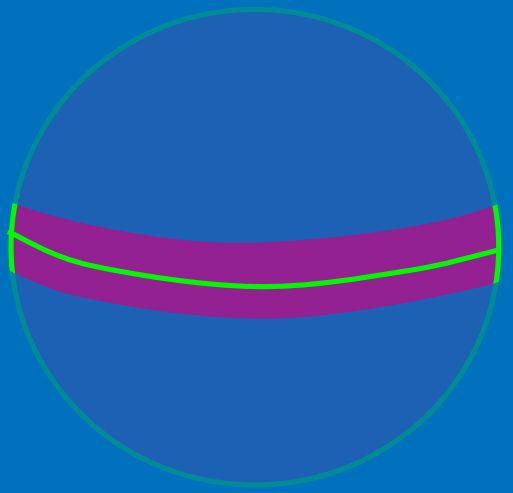
Lubkin, Lloyd, Page, Foong & Kanno, Sanchez-Ruiz, Sen…

Concentration of measure



$A_n \sim \exp[-n\, f(\theta)]$

$$\sim \frac{1}{\sqrt{n}}$$



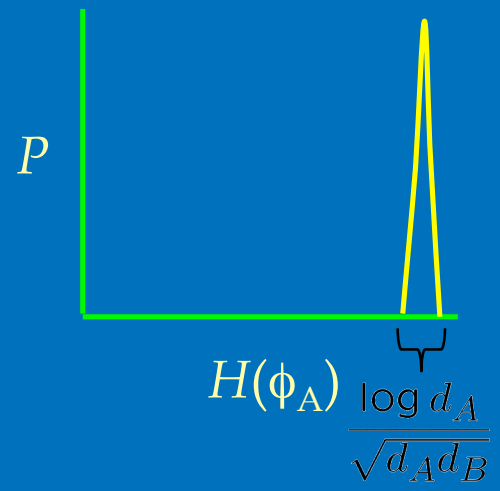
LEVY: Given an η-Lipschitz function $f : S^n \to \mathbb{R}$ with median M, the probability that a random $x \in_R S^n$ is further than ε from M is bounded above by $\exp(-n\varepsilon^2 C/\eta^2)$ from some $C > 0$.

Application to entropy

- Choose a random pure quantum state:
$$\phi \in_{\mathrm{R}} \mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B} \quad (d_A \leq d_B)$$

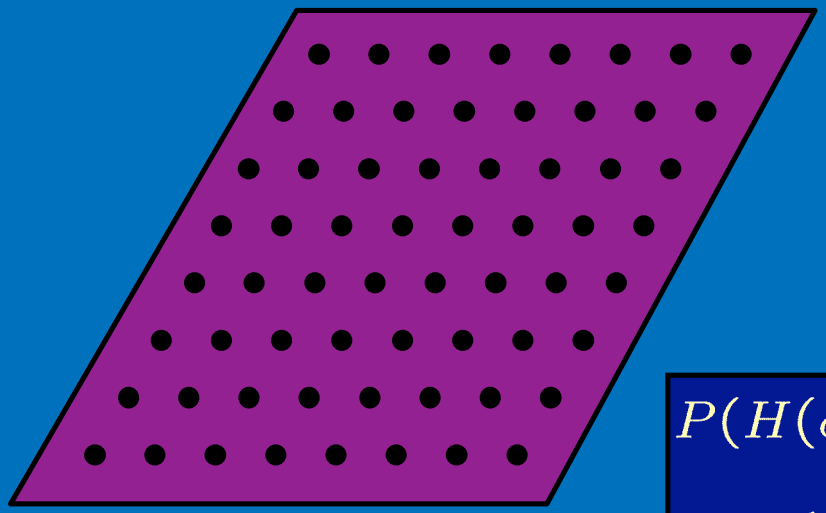
$$\mathbb{E} H(\phi_A) \geq \log d_A - \beta$$

$$P(H(\phi_A) < \log d_A - \alpha - 2\beta) \leq \exp\left(\frac{(1 - d_A d_B) C \alpha^2}{(\log d_A)^2}\right)$$



Random subspaces

$S \subset \mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$



1) Choose a fine net N of states on S.
2) P(Not all states in N highly entangled) $\leq |N|\ P$(One state isn't)
3) True for sufficiently fine N implies true for all of S.

$$P(H(\phi_A) < \log d_A - \alpha - 2\beta) \leq \exp\left(\frac{(1 - d_A d_B) C \alpha^2}{(\log d_A)^2}\right)$$

$$|N| \leq \left(\frac{C}{\epsilon}\right)^{2s}$$

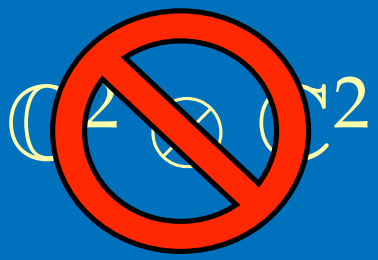
THEOREM: There exist subspaces of dimension $Cd_Ad_B\alpha^3/(\log d_A)^3$, *all* of whose states have entanglement at least $\log d_A - \alpha - 2\beta$. The probability that a random subspace does goes to 1 with d_Ad_B.

In qubit language…

- In a bipartite system of n by n+o(n) qubits, there exists a subspace of $2n$ – o(n) qubits in which all states have at least n – $o(1)$ ebits of entanglement.
- The subspace of nearly maximally entangled states is almost as big as the *whole* system!

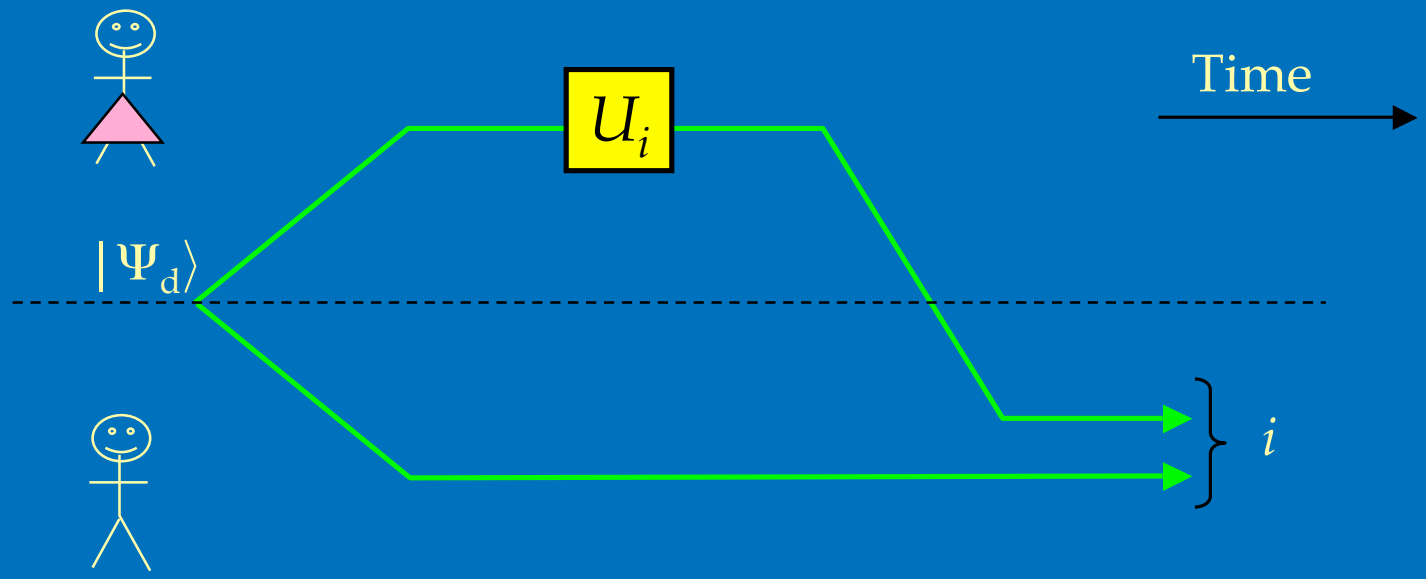
Compare to pairs of qubits

- The subspace spanned by two or more Bell pairs always contains some product states. (No subspaces of entangled states, let alone *maximally* entangled states.)



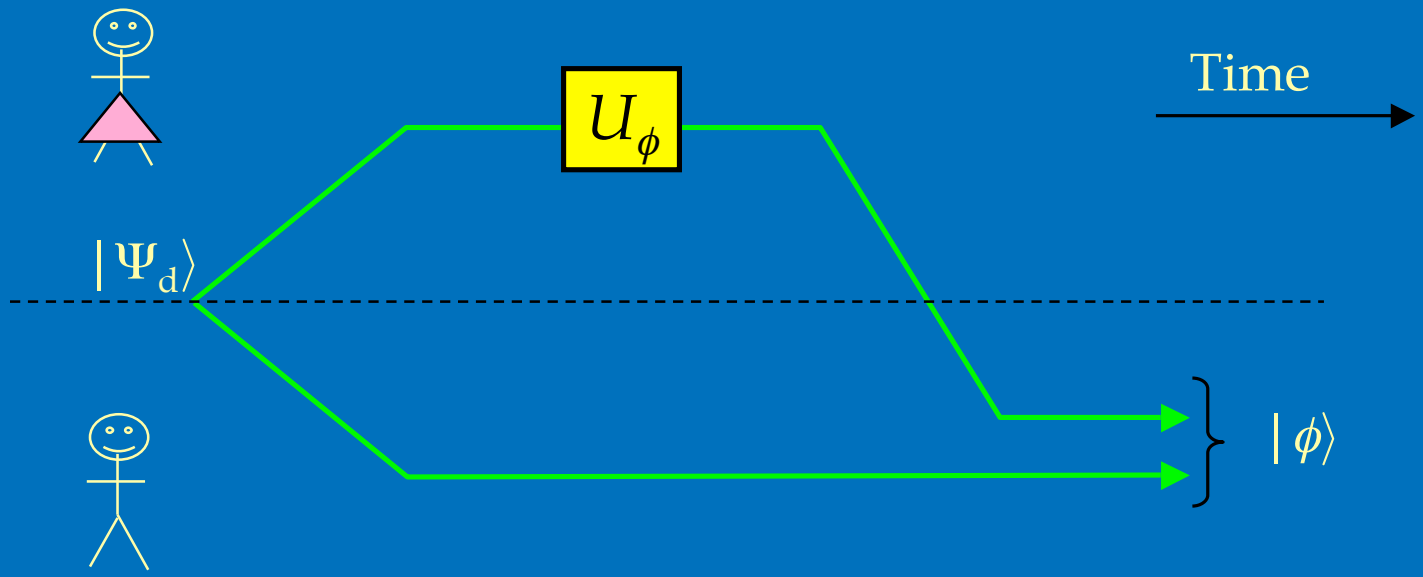
What's this good for?

Superdense coding: To send $i \in \{1,\ldots,d^2\}$



What's this good for?

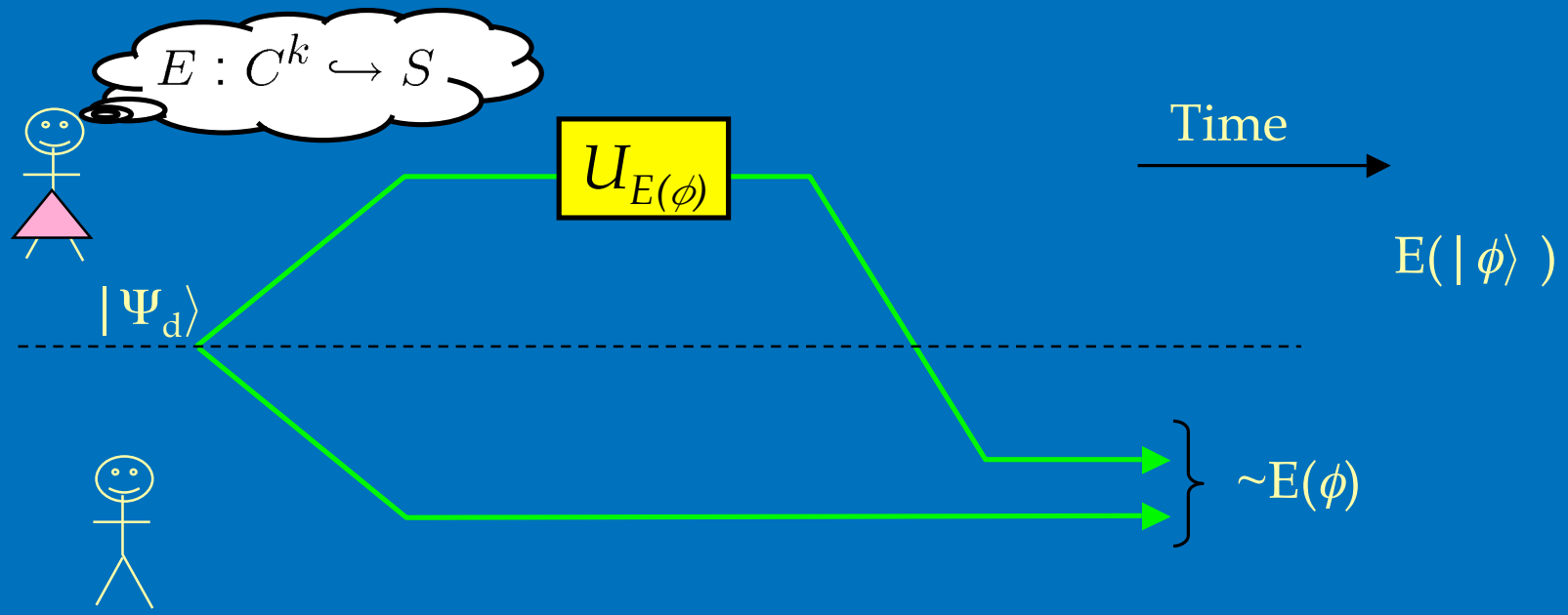
Superdense coding: To send maximally entangled $|\phi\rangle$



Asymptotically, an arbitrary 2 qubit *maximally entangled* quantum state can be communicated using 1 qubit and 1 ebit.

What's this good for?

Superdense coding: To send arbitrary $|\phi\rangle \in C^k$

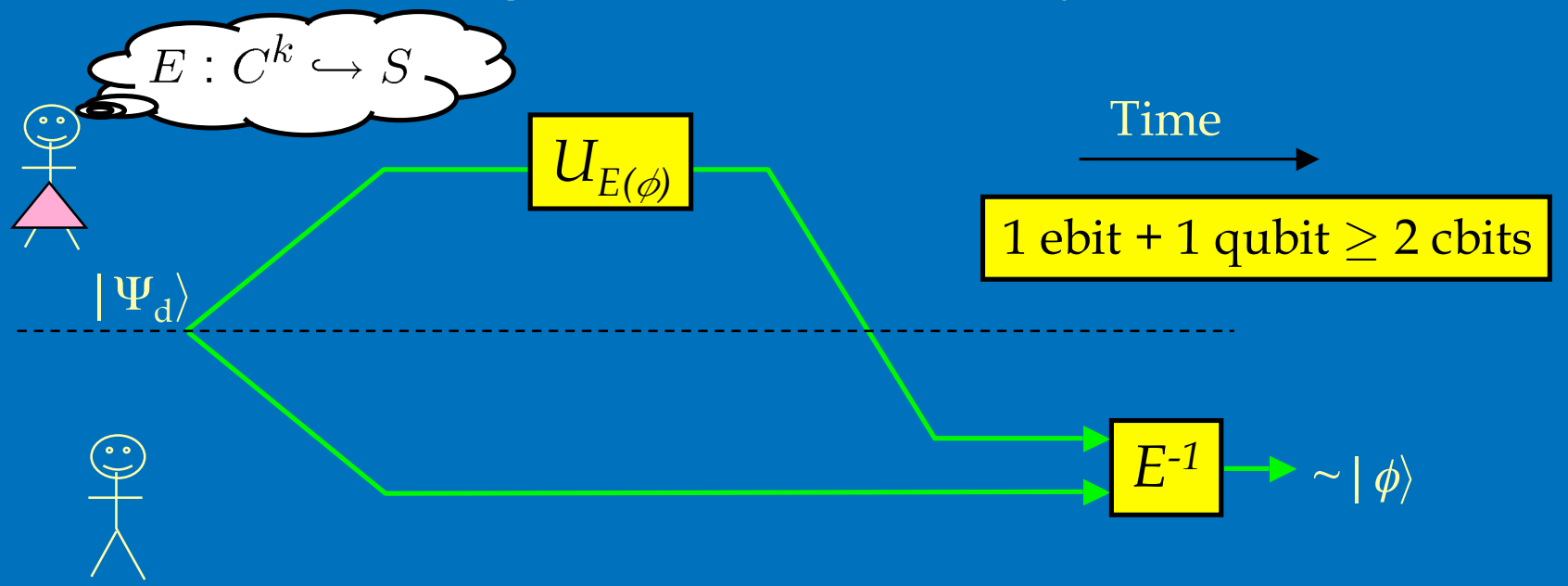


There exists a subspace S of near-full size containing only nearly maximally entangled states.

Asymptotically, an arbitrary 2 qubit quantum state can be communicated using 1 qubit and 1 ebit.

What's this good for?

Superdense coding: To send arbitrary $|\phi\rangle \in C^k$



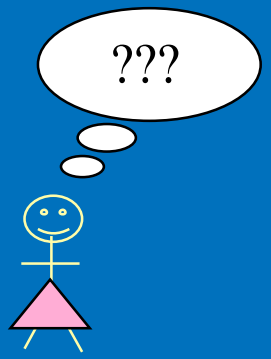
There exists a subspace S of near-full size containing only nearly maximally entangled states.

Asymptotically, an arbitrary 2 qubit quantum state can be communicated using 1 qubit and 1 ebit.

Recurse:

- 1 ebit + 1 qubit $\geq$ 2 qubits
- 2 ebits + (1 ebit + 1 qubit) $\geq$ 4 qubits
- 4 ebits + (3 ebits + 1 qubit) $\geq$ 8 qubits
- 2^r-1 ebits + 1 qubit $\geq$ 2^r qubit
- Send an unbounded amount of quantum information with a single qubit? NO!

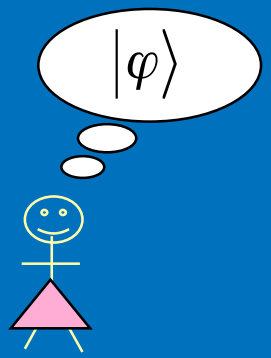
Knowledge is power



Oblivious Alice:

$$1 \text{ ebit} + 1 \text{ qubit} \geq 1 \text{ qubit}$$

All you need in this life is ignorance and confidence, and then success is sure. -Mark Twain



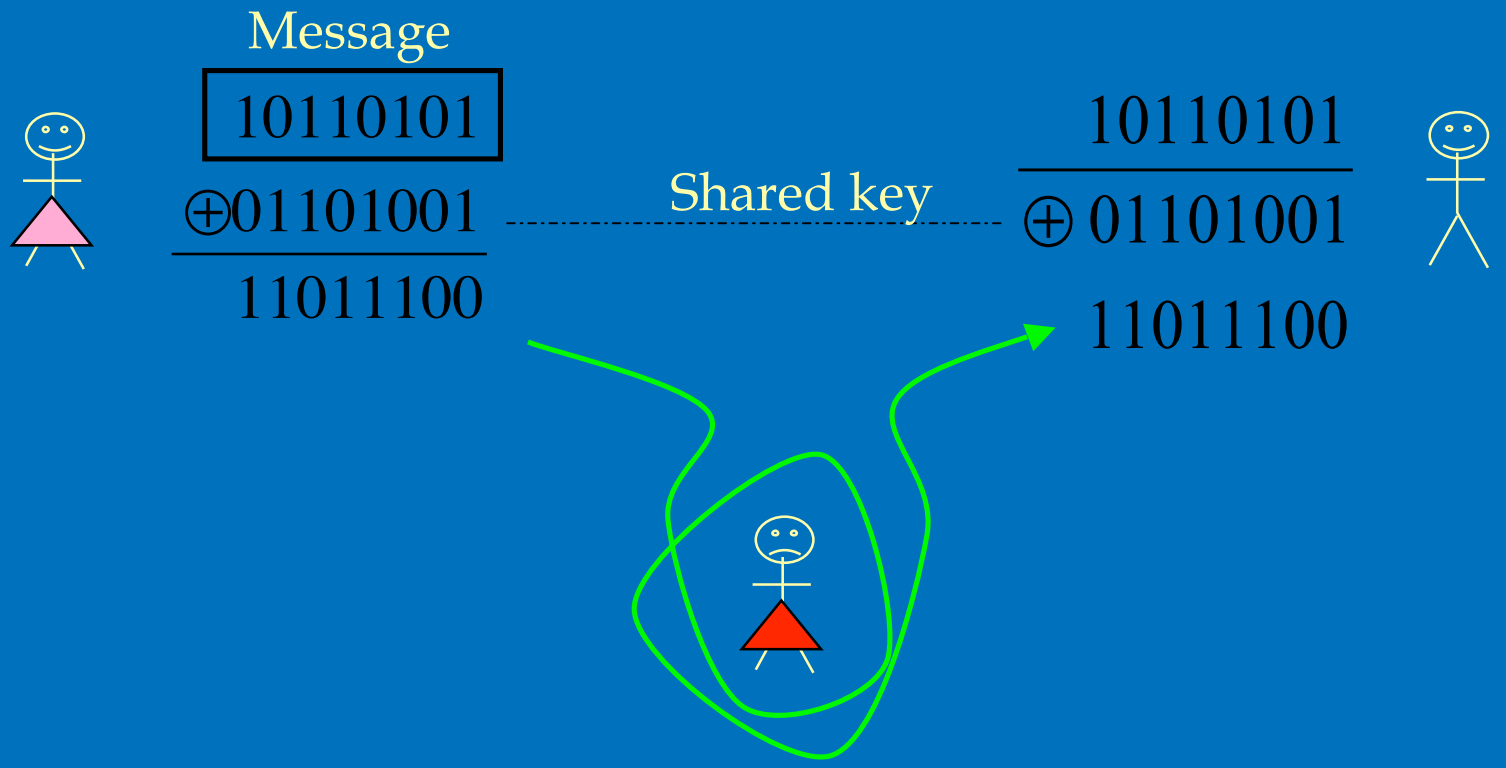
Non-Oblivious Alice:

$$1 \text{ ebit} + 1 \text{ qubit} \geq 2 \text{ qubits}$$

Credit where credit is due

- Accidental quantum information theorists?
  - Milman and Schechtman. “Asymptotic theory of finite dimensional normed spaces”. Springer-Verlag, 1986.
- Others: Gowers, Gromov, Ledoux, Szarek, Talagrand…

Another application: One-time pad

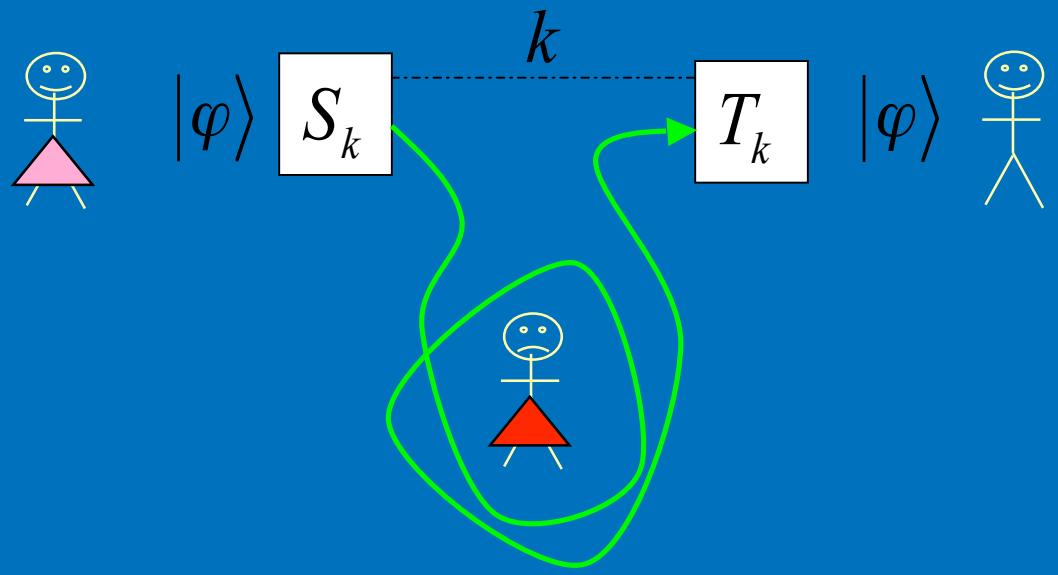


1 bit of key per bit of message necessary and sufficient [Shannon49]

Private quantum channels

$\forall |\varphi\rangle \in \mathbb{C}^d$

$k \in \{1, \ldots, n\}$



Eavesdropper learns nothing:

$$\frac{1}{n}\sum_{k=1}^{n} S_k(\varphi) = \rho_0$$

Lower bound on key length:

$n \geq d^2 \quad (\log n \geq 2 \log d)$

[BR,AMTW 2000]

Relax security criterion

A physical operation R is ϵ-randomizing if for all states φ,

$$\left\| R(\varphi) - \tfrac{I}{d} \right\|_\infty \leq \varepsilon / d .$$

CONSEQUENCE:

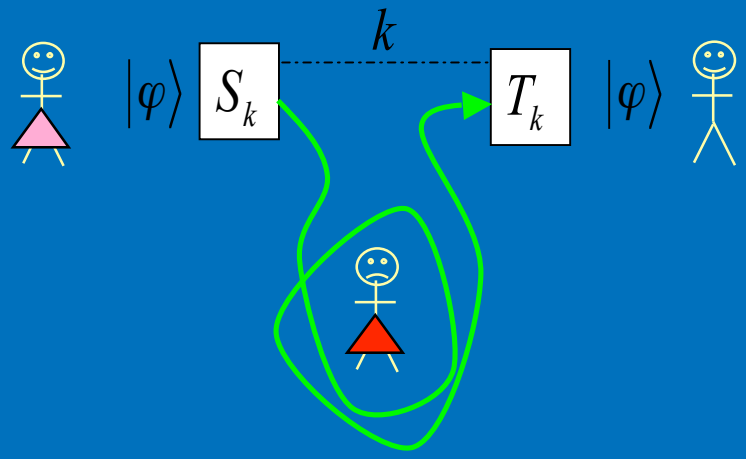
Given $\varepsilon>0$, there exists a choice of unitaries $\{U_k\}$, $k=1,\ldots,n$ such that the map

$$R(\varphi) = \frac{1}{n} \sum_{k=1}^{n} U_k \varphi U_k^*$$

is ϵ-randomizing, with $n = \dfrac{Cd \log d}{\varepsilon^2}$.

Approximate PQC

Can encrypt a quantum state using 1 secret random bit per encrypted qubit asymptotically.



Security:

$$E = \{p_i, \varphi_i\} \Rightarrow I_{\text{Eve}}(E) \leq \varepsilon / \ln 2$$

$$\varepsilon = \frac{1}{poly(l)}$$ *1* bit of key/qubit

$$\varepsilon = \frac{1}{2^{\alpha \cdot l}}$$ *(1+2α)* bits of key/qubit

Conclusions

- General rule: Random states and subspaces exhibit extremal behaviour
  - Entanglement
  - Communication
  - Error-correction
- Many effects do not have good low-dimensional analogues
- Tip of the iceberg: encryption, state identification, data hiding, secret sharing….
- Direction application of the concentration of measure phenomenon to problems in communication