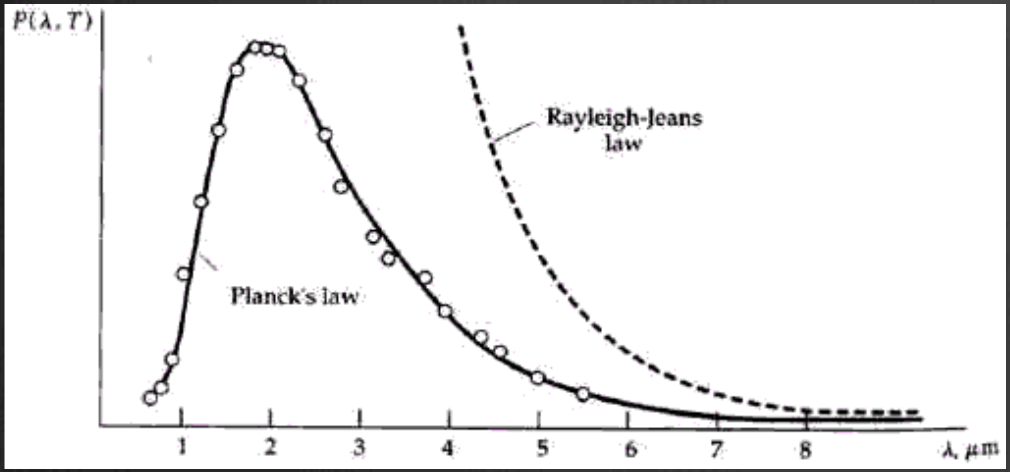
Quantum information and the monogamy of entanglement

Aram Harrow
MIT (UCL until Jan 2015)

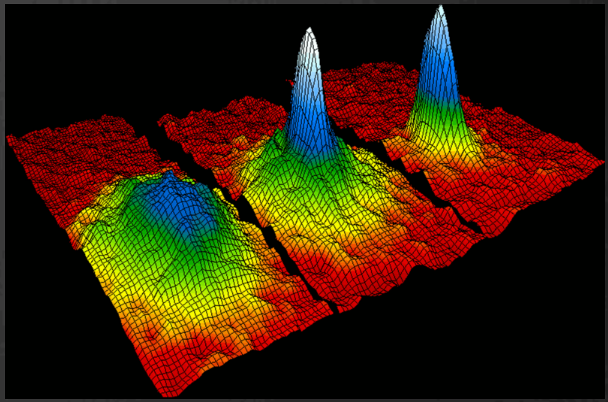
Quantum mechanics

Blackbody radiation paradox:
How much power does a hot object emit at wavelength λ?

Classical theory (1900): const / λ^4
Quantum theory (1900 – 1924): $$\frac{c_1}{\lambda^5(e^{c_2/\lambda} - 1)}$$



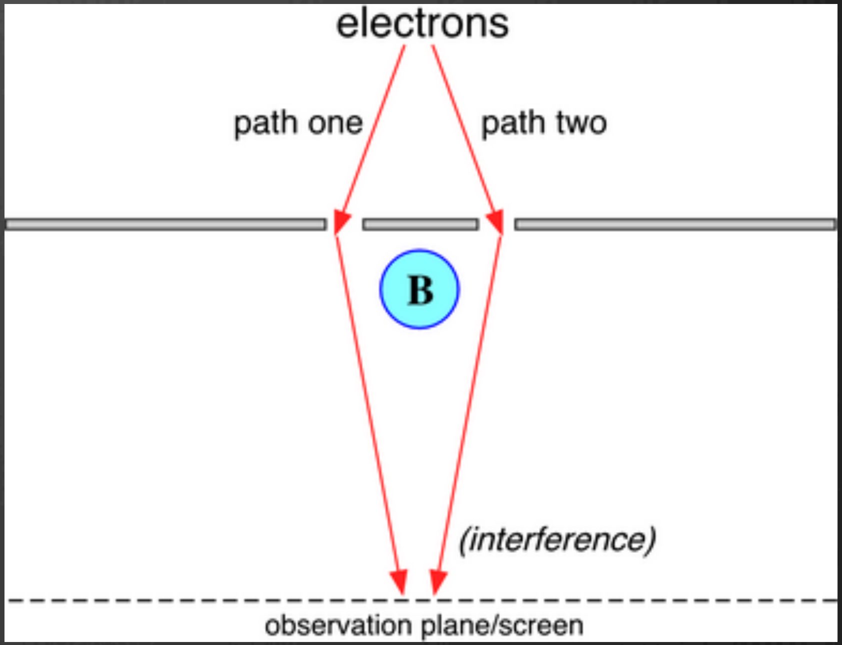
Bose-Einstein condensate (1995)



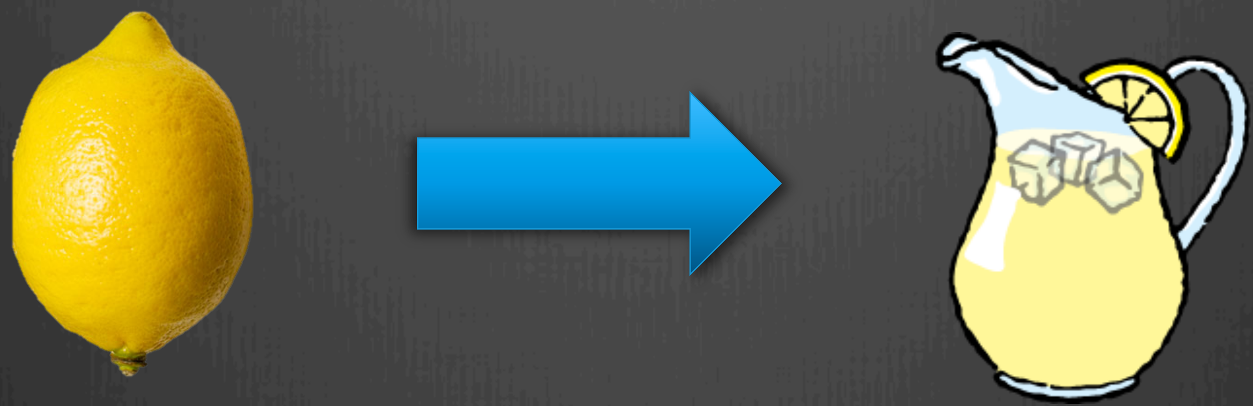
QM has also explained:
- the stability of atoms
- the photoelectric effect
- everything else we've looked at

Difficulties of quantum mechanics

- Heisenberg's uncertainty principle
- Topological effects
- Entanglement
- Exponential complexity:
  Simulating N objects requires effort ~exp(N)



The doctrine of quantum information



- Abstract away physics to device-independent fundamentals: “qubits”
- operational rather than foundational statements: Not “what is quantum information” but “what can we do with quantum information.”

Product and entangled states

state of system A

$$\alpha_0|0\rangle + \alpha_1|1\rangle \quad \otimes \quad \beta_0|0\rangle + \beta_1|1\rangle$$

state of system B

→ product joint state of A and B

$$\alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|10\rangle + \alpha_1\beta_1|11\rangle$$

$|00\rangle := |0\rangle \otimes |0\rangle$ etc.

Entangled
"Not product" := "entangled"
cf. correlated random variables

e.g. $$\frac{|00\rangle + |11\rangle}{\sqrt{2}} \neq |\alpha\rangle \otimes |\beta\rangle$$

The power of [quantum] computers
One qubit $\equiv$ 2 dimensions
n qubits $\equiv$ 2^n dimensions

[quantum] entanglement vs. [classical] correlation

Make comparable using density matrices

Entangled state

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

$$|\psi\rangle\langle\psi| = \frac{|00\rangle\langle 00| + |11\rangle\langle 11| + |00\rangle\langle 11| + |11\rangle\langle 00|}{2}$$

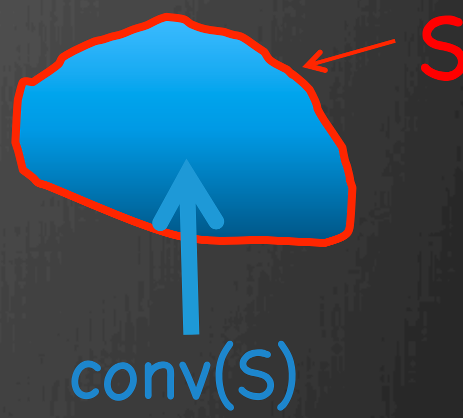
Correlated state

By contrast, a random mixture of $|00\rangle$ and $|11\rangle$ is

$$\frac{|00\rangle\langle 00| + |11\rangle\langle 11|}{2}$$

How to distinguish? off-diagonal elements not enough

when is a mixed state entangled?



Definition: ρ is separable (i.e. not entangled) if it can be written as

$$\rho = \sum_i p_i |\alpha_i\rangle\langle\alpha_i| \otimes |\beta_i\rangle\langle\beta_i|$$

$\in \text{conv}\{|\alpha\rangle\langle\alpha| \otimes |\beta\rangle\langle\beta|\}$

probability distribution

unit vectors

Difficulty: This is hard to check.

Heuristic: All separable states are PPT (Positive under Partial Transpose).
Problem: So are some entangled states.

Why care about Sep testing?

1. validate experiment	Creating entanglement is a major experimental challenge. Even after doing tomography on the created states, how do we know we have succeeded?
2. understand noise and error correction	How much noise will ruin entanglement? How can we guard against this? Need good characterizations of entanglement to answer.
3. other q. info tasks	Sep testing is equivalent to many tasks without obvious connections, such as communication rates of q. channels. [H.-Montanaro, 1001.0017]
4. relation to optimization and simulation	described later (see also 1001.0017)

limits on entanglement testing

Detecting pure-state entanglement is easy, so detecting mixed-state entanglement is hard

[H-Montanaro, 1001.0017]

1. Given $|\psi\rangle \in (\mathbb{C}^d)^{\otimes N}$, how close is $|\psi\rangle$ to a state of the form $|\alpha_1\rangle \otimes |\alpha_2\rangle \otimes \ldots \otimes |\alpha_N\rangle$?

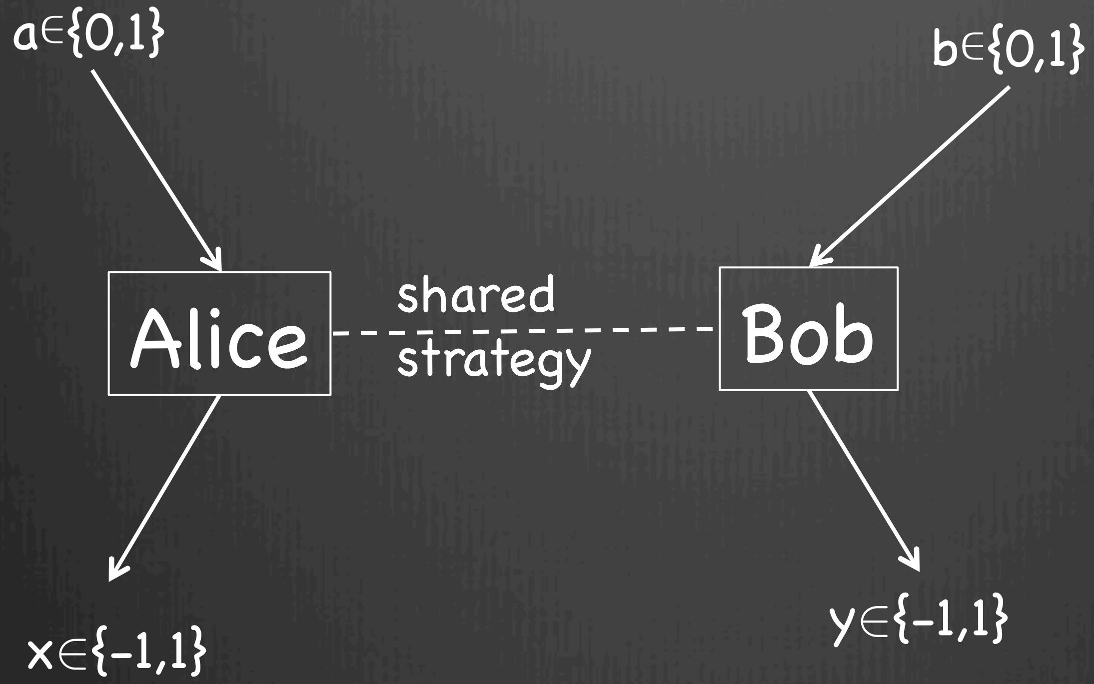
2. With one copy of $|\psi\rangle$ this is impossible to estimate. We give a simple test that works for two copies.

3. Combine this with
   a) [Aaronson-Beigi-Drucker-Fefferman-Shor 0804.0802]
   b) a widely believed assumption (the "exponential time hypothesis")
   c) other connecting tissue (see our paper)

to prove that testing whether a d-dimensional state is approximately separable requires time $\geq d^{\log(d)}$.

4. This rules out any simple heuristic (e.g. checking eigenvalues).

CHSH game



a	b	x,y
0	0	same
0	1	same
1	0	same
1	1	different

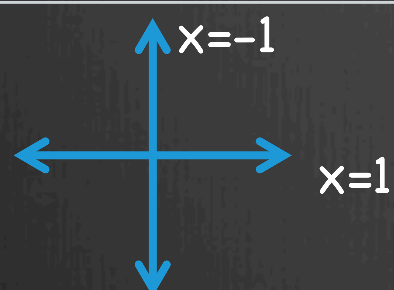
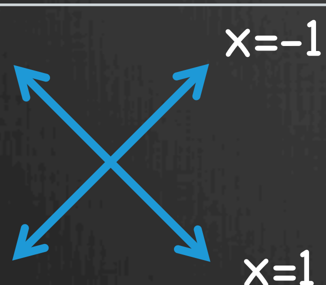
Goal: $xy = (-1)^{ab}$

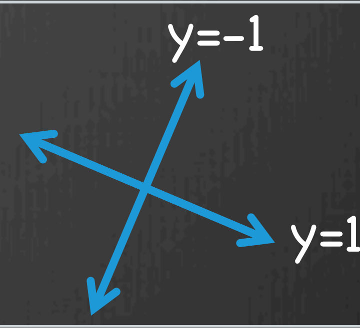
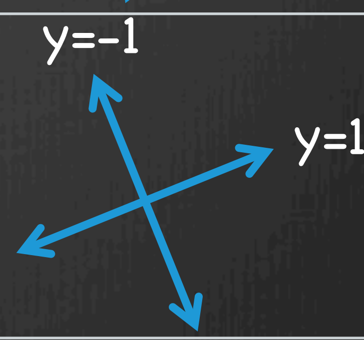
Max win probability is 3/4. Randomness doesn't help.

CHSH with entanglement

Alice and Bob share state $\frac{|00\rangle + |11\rangle}{\sqrt{2}}$

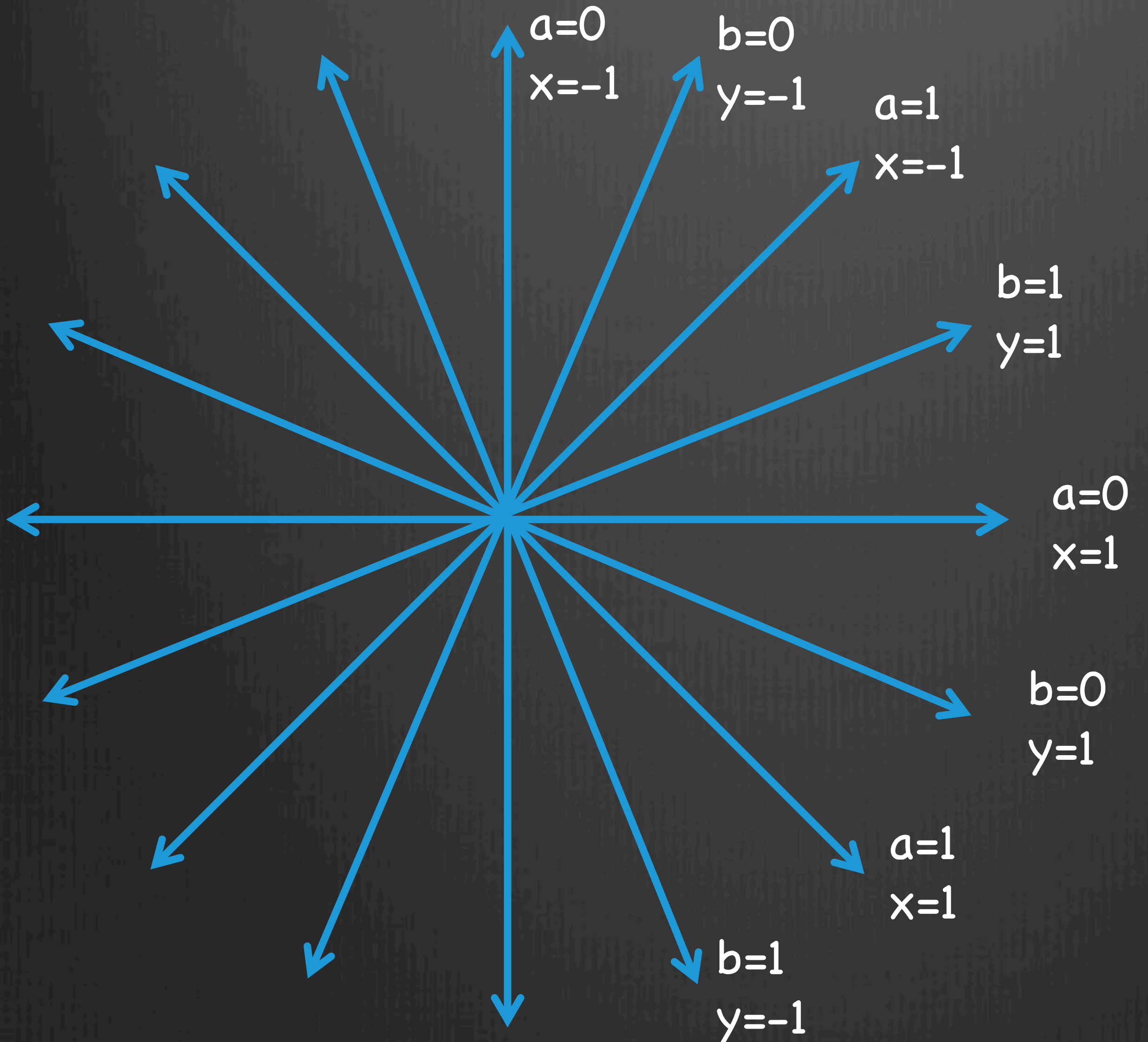
Based on inputs a,b they choose measurement angles.
Measurement outcomes determine outputs x,y.

When	Alice measures
a=0	
a=1	

When	Bob measures
b=0	
b=1	

win prob
$\cos^2(\pi/8)$
≈ 0.854

CHSH with entanglement



goal: $xy=(-1)^{ab}$

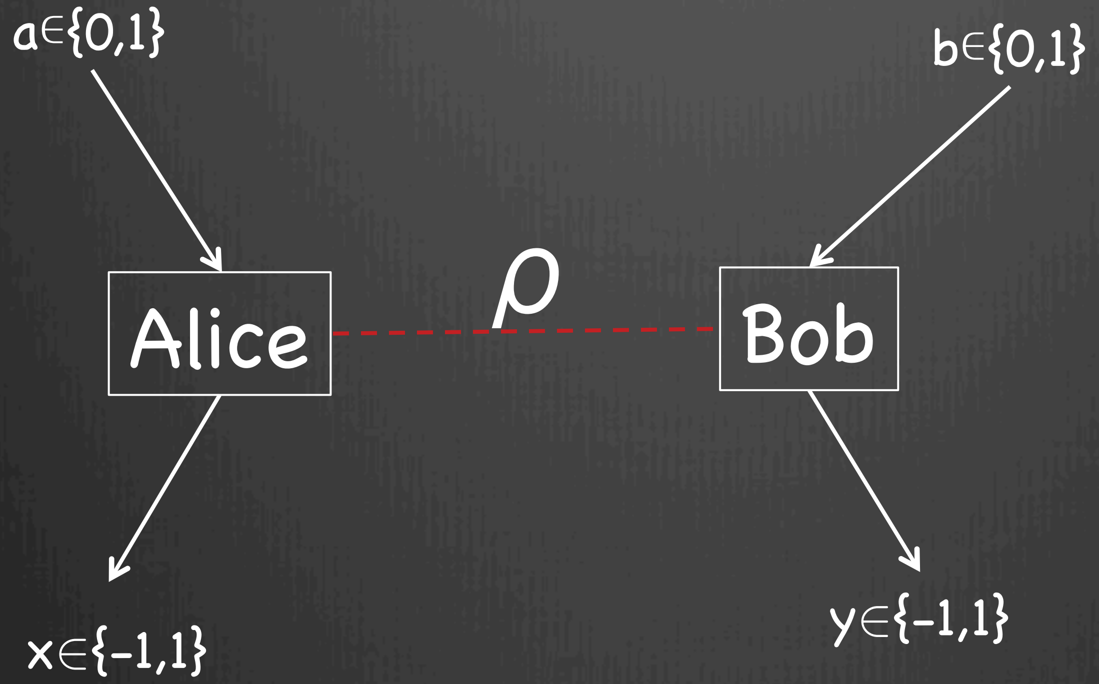
Why it works

Winning pairs are at angle $\pi/8$

Losing pairs are at angle $3\pi/8$

$\therefore \Pr[\text{win}]=\cos^2(\pi/8)$

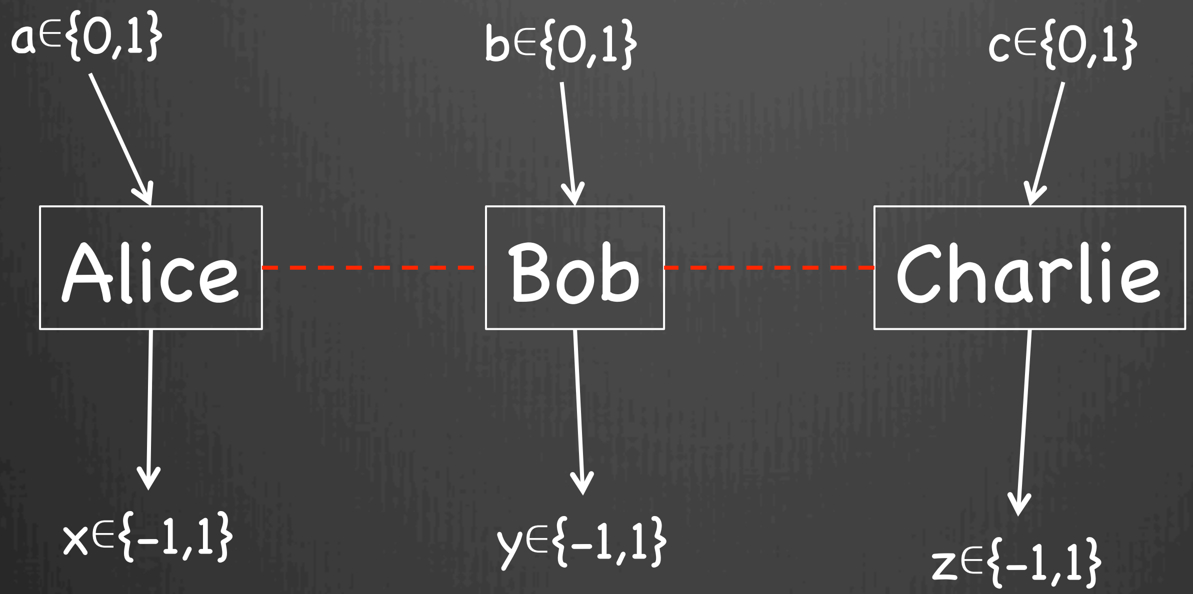
games measure entanglement



ρ separable → Pr[win] ≤ 3/4

conversely, Pr[win] − 3/4 is a measure of entanglement.

Monogamy of entanglement



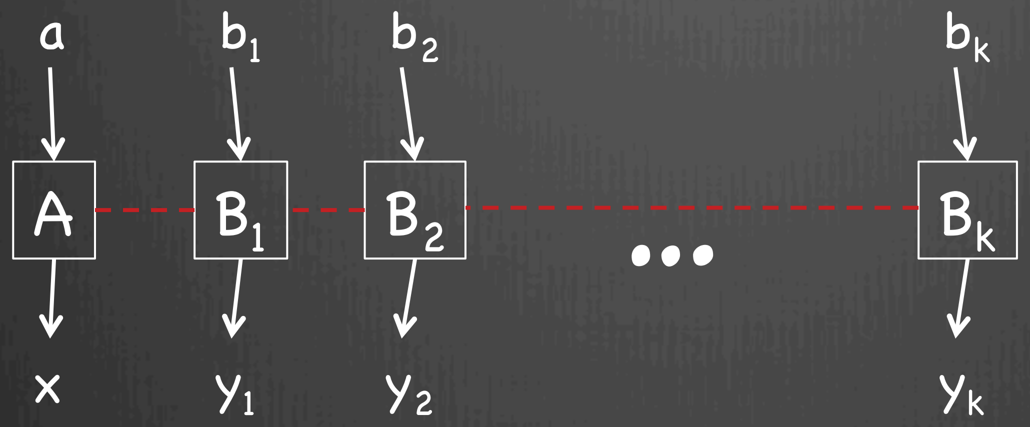
max Pr[AB win] + Pr[AC win] =

max $\Pr[xy = (-1)^{ab}] + \Pr[xz = (-1)^{ac}]$

$< 2\cos^2(\pi/8)$

why? If AB win often, then B is like a "hidden variable" for AC.

shareability implies separability



CHSH $$\frac{\Pr[AB_1 \text{ win}] + \ldots + \Pr[AB_k \text{ win}]}{k} \le \frac{3}{4} + \frac{c}{\sqrt{k}}$$

any game $$\frac{\Pr[AB_1 \text{ win}] + \ldots + \Pr[AB_k \text{ win}]}{k} \le \text{classical value} + c\sqrt{\frac{\log \min(\dim A, |X|)}{k}}$$

Intuition: Measuring B_2, ..., B_k leaves A,B_1 nearly separable

Proof uses information theory: [Brandão-H., 1210.6367, 1310.0017]

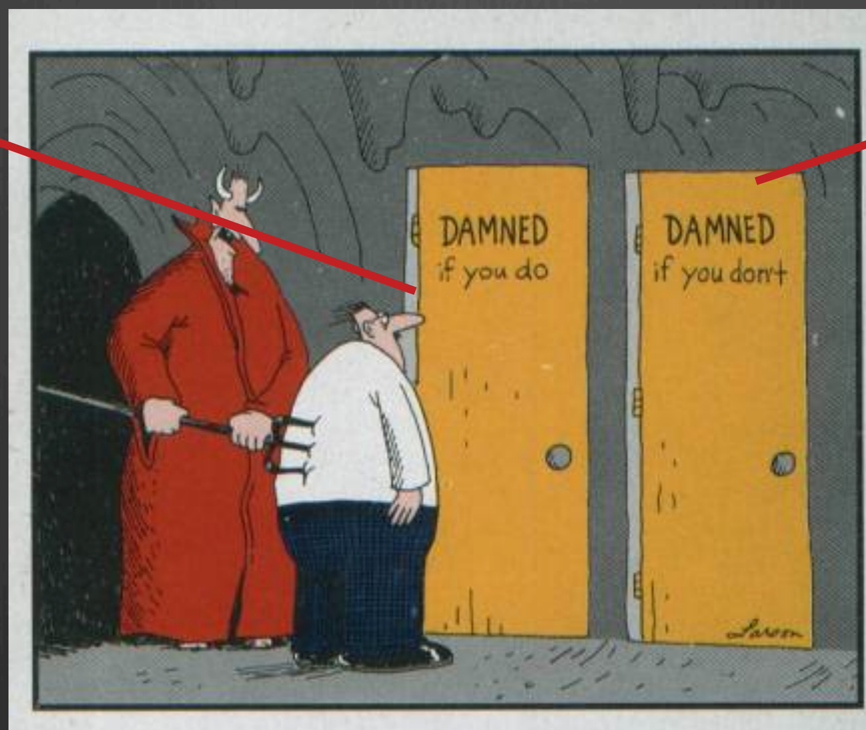
1. conditional mutual information shows game values monogamous
2. other tools show "advantage in non-local games" ≈ "entanglement"

proof sketch

outcome distribution is $p(x,y_1,\ldots,y_k|a,b_1,\ldots,b_k)$

<u>case 1</u>

$p(x,y_1|a,b_1) \approx$
$p(x|a) \cdot p(y_1|b_1)$



"C'mon, c'mon — it's either one or the other."

<u>case 2</u>

$p(x,y_2|y_1,a,b_1,b_2)$
has less mutual information

less sketchy proof sketch

$$\log|X| \geq I(X : Y_1, \ldots, Y_k)$$
$$= I(X : Y_1) + I(X : Y_2|Y_1) + \ldots + I(X : Y_k|Y_1, \ldots, Y_{k-1})$$

∴ for some j we have $I(X : Y_j|Y_1, \ldots, Y_{j-1}) \leq \frac{\log|X|}{k}$

Y_1, …, Y_{j-1} constitute a "hidden variable" which we can condition on to leave X,Y_j nearly decoupled.

Trace norm bound follows from Pinsker's inequality.

what about the inputs?

$$\log|X| \geq \max_{b_1,\ldots,b_k} I(X : Y_1, \ldots, Y_k | A, b_1, \ldots, b_k)$$

$$= \max_{b_1,\ldots,b_{k-1}} \Big(I(X : Y_1 | A, b_1) + I(X : Y_2 | A, b_1, b_2, Y_1) + \ldots +$$

$$I(X : Y_{k-1} | A, b_1, \ldots, b_{k-1}, Y_1, \ldots, Y_{k-2}) +$$

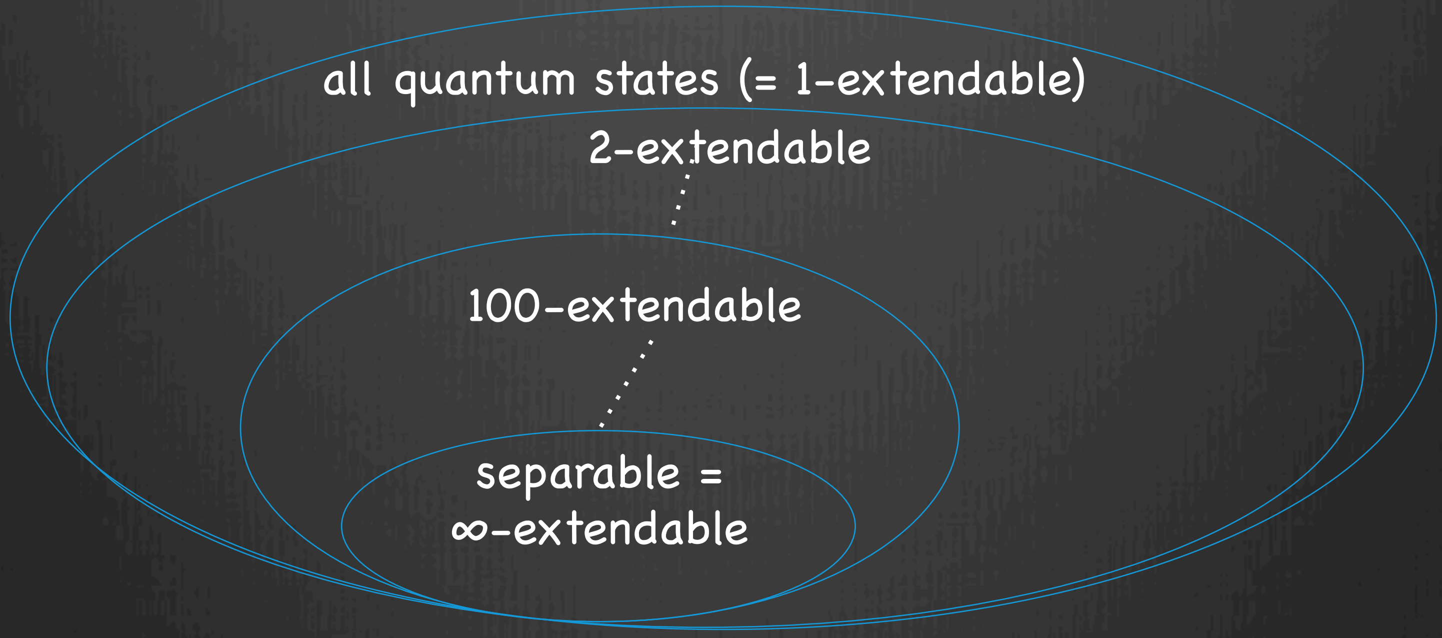
$$\max_{b_k} I(X : Y_k | A, b_1, \ldots, b_k, Y_1, \ldots, Y_{k-1}) \Big)$$

Apply Pinsker here to show that this is
$\gtrsim \| p(X, Y_k \mid A, b_k) - \text{LHV} \|_1^2$

then repeat for $Y_{k-1}, \ldots, Y_1$

A hierachy of tests for entanglement

Definition: ρ^{AB} is k-extendable if there exists an extension $\rho^{AB_1 \ldots B_k}$ with $\rho^{AB} = \rho^{AB_i}$ for each i.



Algorithms: Can search/optimize over k-extendable states in time $d^{O(k)}$.

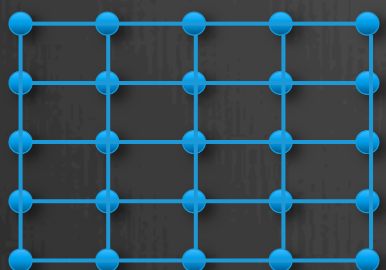
Question: How close are k-extendable states to separable states?

application #1: mean-field approximation

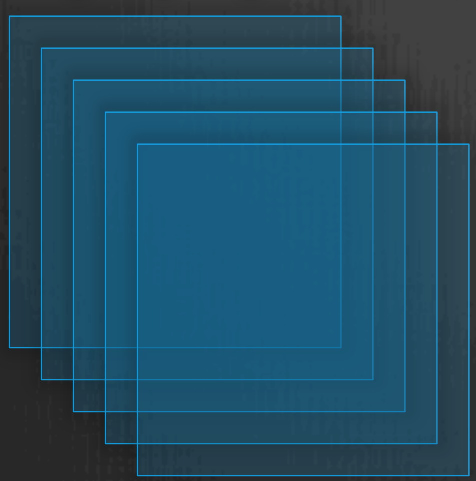
used in limit of high coordination number, e.g.

1-D

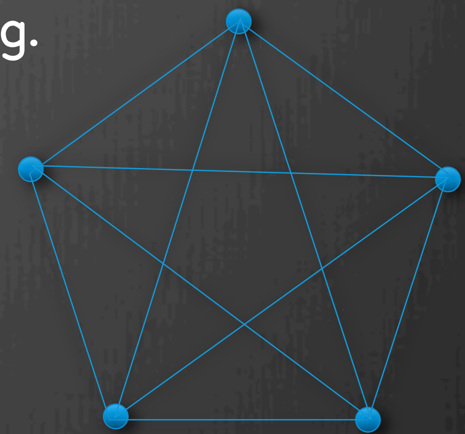
2-D



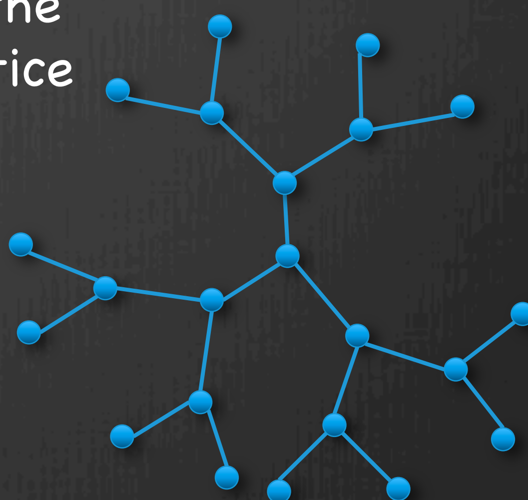
3-D



∞-D



Bethe lattice



mean-field ≅ product states

mean-field ansatz for homogenous systems: $|\alpha\rangle^{\otimes N}$

for inhomogenous systems: $|\alpha_1\rangle \otimes |\alpha_2\rangle \otimes \ldots \otimes |\alpha_N\rangle$

Result: Controlled approximation to ground-state energy with no homogeneity assumptions based only on coordination number. [Brandão-H. 1310.0017]

Application: "No low-energy trivial states" conjecture [Freedman-Hastings] states that there exist Hamiltonians where all low-energy states have topological order.
∴ This can only be possible with low coordination number.

application #2: optimization

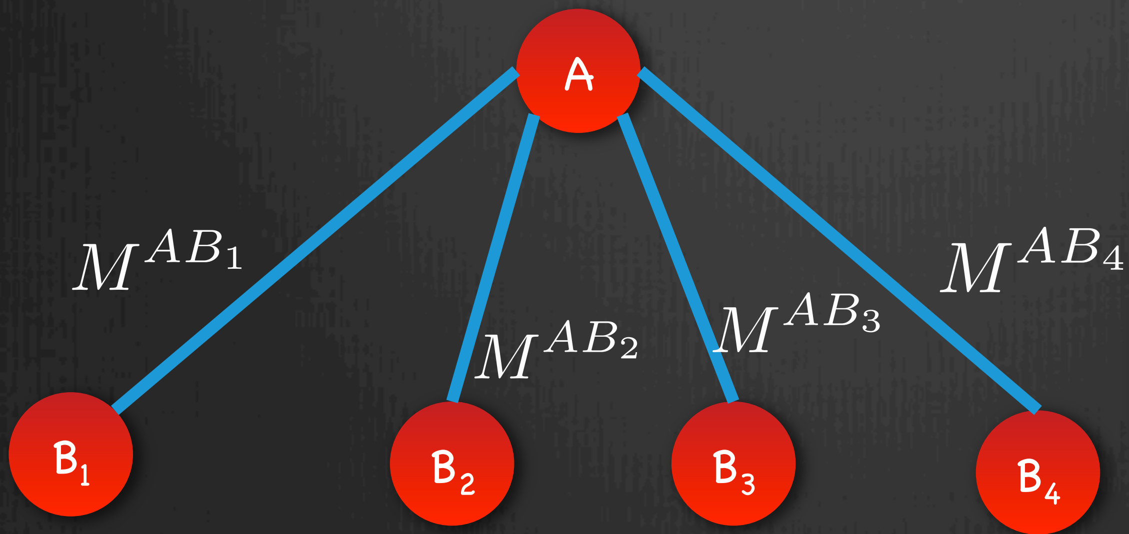
Given a Hermitian matrix M:

- $\max_{\alpha} \langle \alpha | M | \alpha \rangle$ is easy
- $\max_{\alpha, \beta} \langle \alpha \otimes \beta | M | \alpha \otimes \beta \rangle$ is hard

connections to:

- polynomial opt.
- unique games conjecture

Approximate with $\max_{\psi} \langle \psi | \frac{M^{AB_1} + \dots + M^{AB_k}}{k} | \psi \rangle$



Computational effort: $d^{O(k)}$

Key question: approximation error as a function of k and d

speculative application: simulating lightly-entangled quantum systems

Original motivation for quantum computing [Feynman '82]

Nature isn't classical, dammit, and if you want to make a simulation of Nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy.

modern translation: Unentangled quantum systems can be simulated classically but in general we need quantum computers for this.

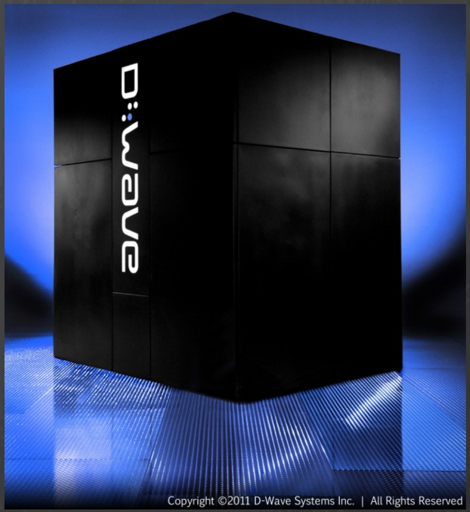
low-entanglement simulation

degree of entanglement

classically simulatable

supports universal classical computing

?



supports universal quantum computing

Open question:
Are there good classical simulations of lightly-entangled quantum systems?

Idea: model k-body reduced density matrices where k scales with entanglement. cf. results for ground states in 1310.0017.

≈0.1ns single-qubit Rabi oscillations
≈2.5ns decoherence time
≈10μs computation time

references

Product test and hardness	1001.0017
New monogamy relations	1210.6367
Application to optimization	1205.4484
Application to mean-field	1310.0017

all papers: http://web.mit.edu/aram/www/