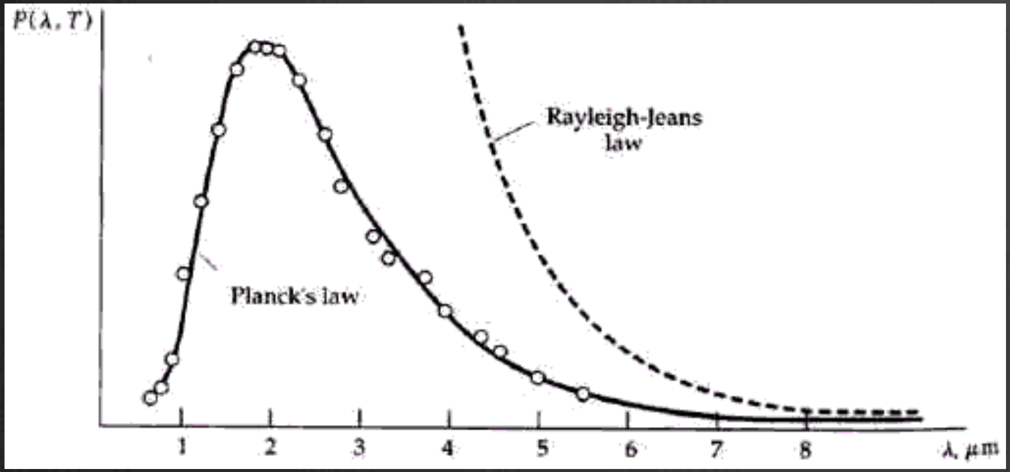
Quantum information and the monogamy of entanglement

Aram Harrow (MIT)
Brown SUMS
March 9, 2013

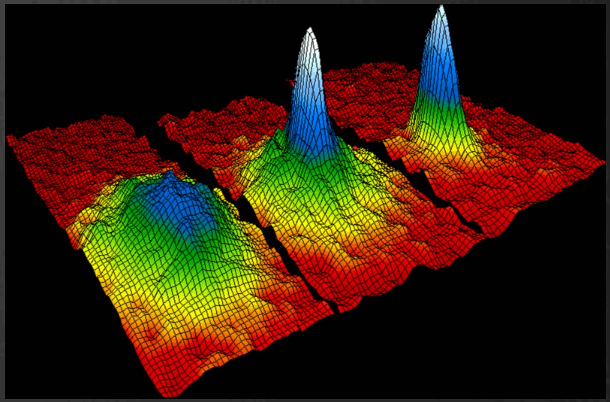
Quantum mechanics

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

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



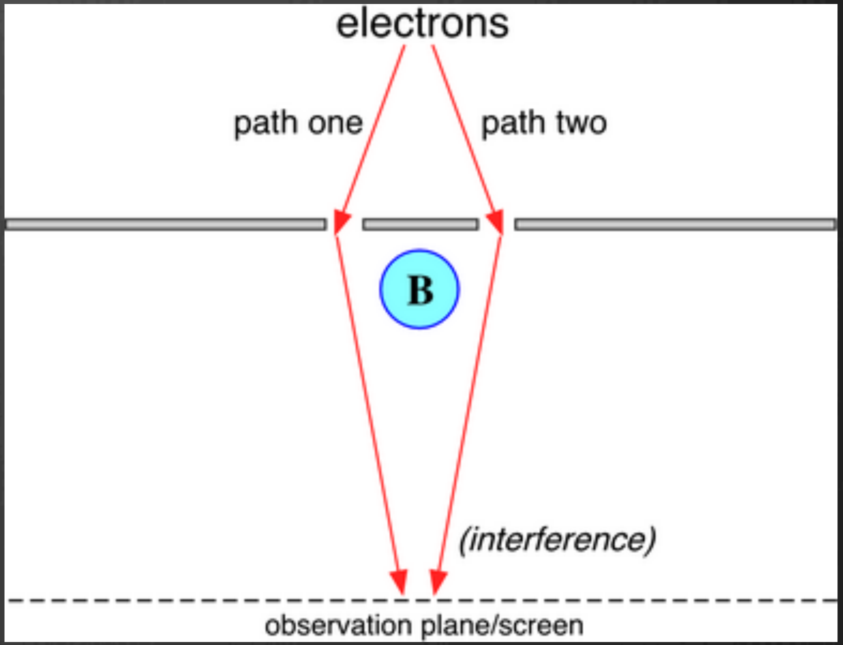
Bose-Einstein condensate (1995)



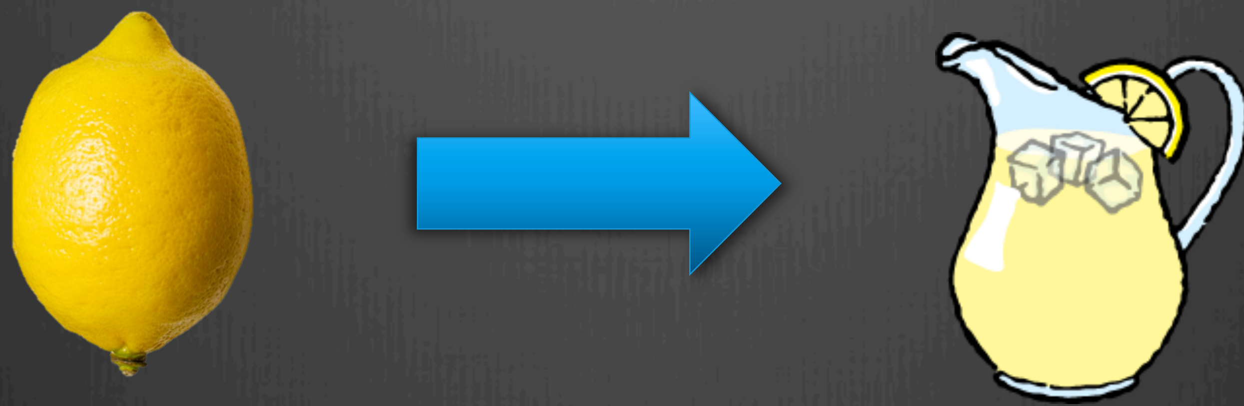
QM has also explained:
- the stability of atoms
- the photoelectric effect
- everything else we've looked at

Difficulties of quantum mechanics

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

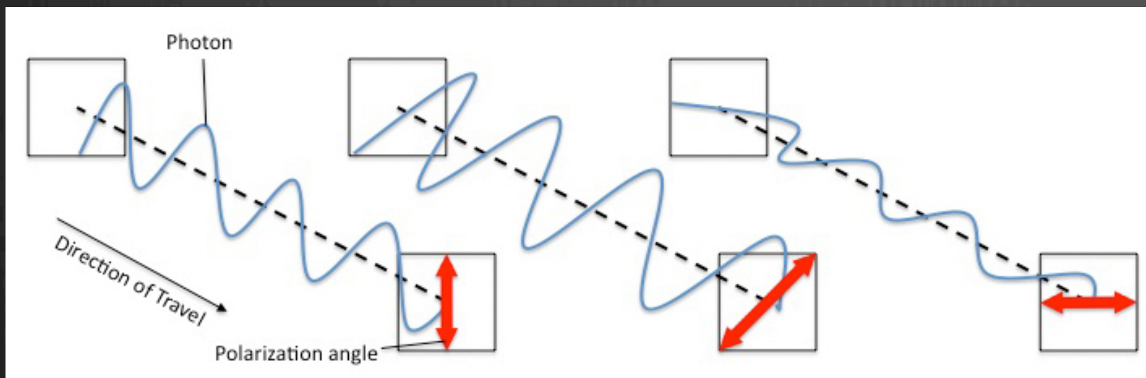


The doctrine of quantum information



- 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.”

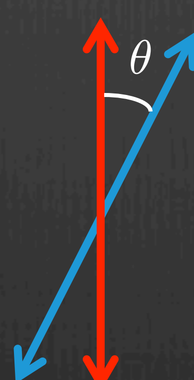
example: photon polarization



Photon polarization **states**: ↕ ↔ ⤢ ⤡

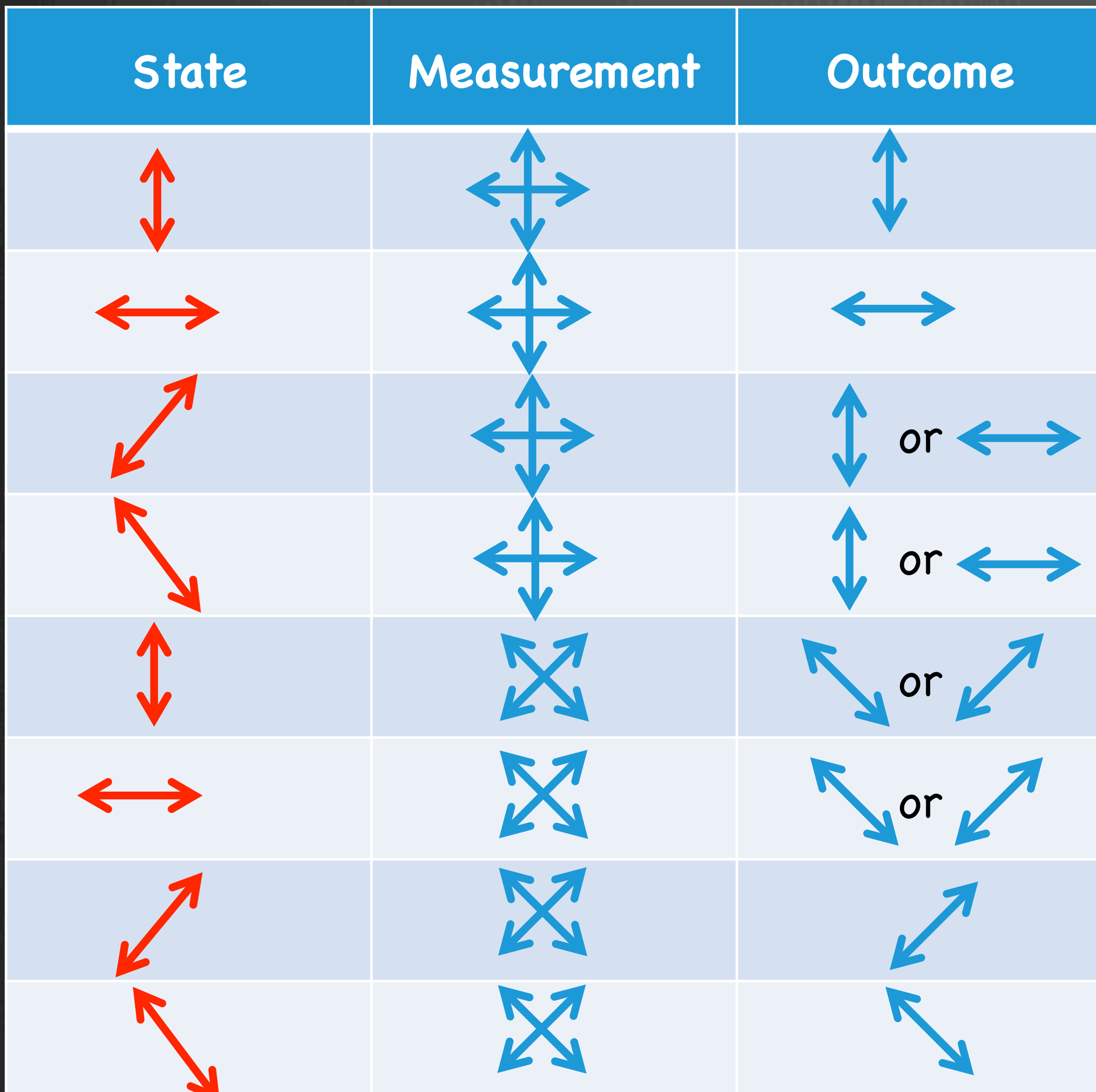
Measurement: Questions of the form
"Are you ⤢ or ⤡ ?"

Rule: Pr[⤢ | ↕] = $\cos^2(\theta)$



Uncertainty principle:
No photon will yield a definite answer to both measurements.

Quantum key distribution



Protocol:

1. Alice chooses a random sequence of bits and encodes each one using either

2. Bob randomly chooses to measure with either

3. They publically reveal their choice of axes and discard pairs that don't match.

4. If remaining bits are perfectly correlated, then they are also secret.

Quantum Axioms

Classical probability

$$p = \begin{pmatrix} p_1 \\ p_2 \\ \vdots \\ p_N \end{pmatrix} \in \mathbb{R}_+^N$$

$$\sum_{i=1}^{N} p_i = 1 \qquad p_i \geq 0$$

Quantum mechanics

$$\alpha = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_N \end{pmatrix} \in \mathbb{C}^N$$

$$\sum_{i=1}^{N} |\alpha_i|^2 = 1$$

Measurement

Quantum state: $\alpha \in C^N$

Measurement: An orthonormal basis $\{v_1, \ldots, v_N\}$

Outcome:

$\Pr[v_i \mid \alpha] = |\langle v_i, \alpha \rangle|^2$

More generally, if M is Hermitian, then $\langle \alpha, M\alpha \rangle$ is observable.

Example:

$$v_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, v_2 = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \ldots$$

$\Pr[v_i \mid \alpha] = |\alpha_i|^2$

Product and entangled states

state of system A

$$\begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix}$$

state of system B

$$\begin{pmatrix} \beta_1 \\ \beta_2 \end{pmatrix}$$

joint state of A and B

$$\begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix} \otimes \begin{pmatrix} \beta_1 \\ \beta_2 \end{pmatrix} = \begin{pmatrix} \alpha_1\beta_1 \\ \alpha_1\beta_2 \\ \alpha_2\beta_1 \\ \alpha_2\beta_2 \end{pmatrix}$$

<u>probability analogue:</u>
independent random variables

Entanglement
"Not product" := "entangled" $\sim$ correlated random variables

e.g. $\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$

The power of [quantum] computers
One qubit $\equiv \mathbb{C}^2$
n qubits $\equiv \mathbb{C}^{2^n}$

Measuring entangled states

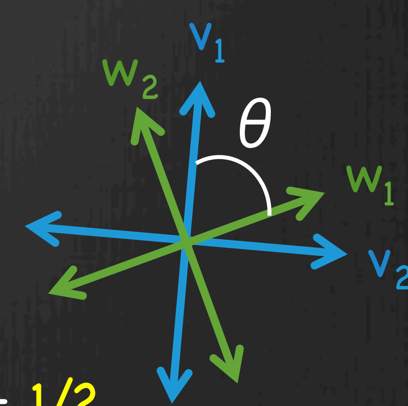
joint state $\frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\1\end{pmatrix}$

Rule: Pr[A observes $\updownarrow$ and B observes $\updownarrow$] = $\cos^2(\theta) / 2$

General rule: Pr[A,B observe v,w | state α] = $|\langle v\otimes w, \alpha\rangle|^2$

Instantaneous signalling?

Alice measures $\{v_1,v_2\}$, Bob measures $\{w_1,w_2\}$.

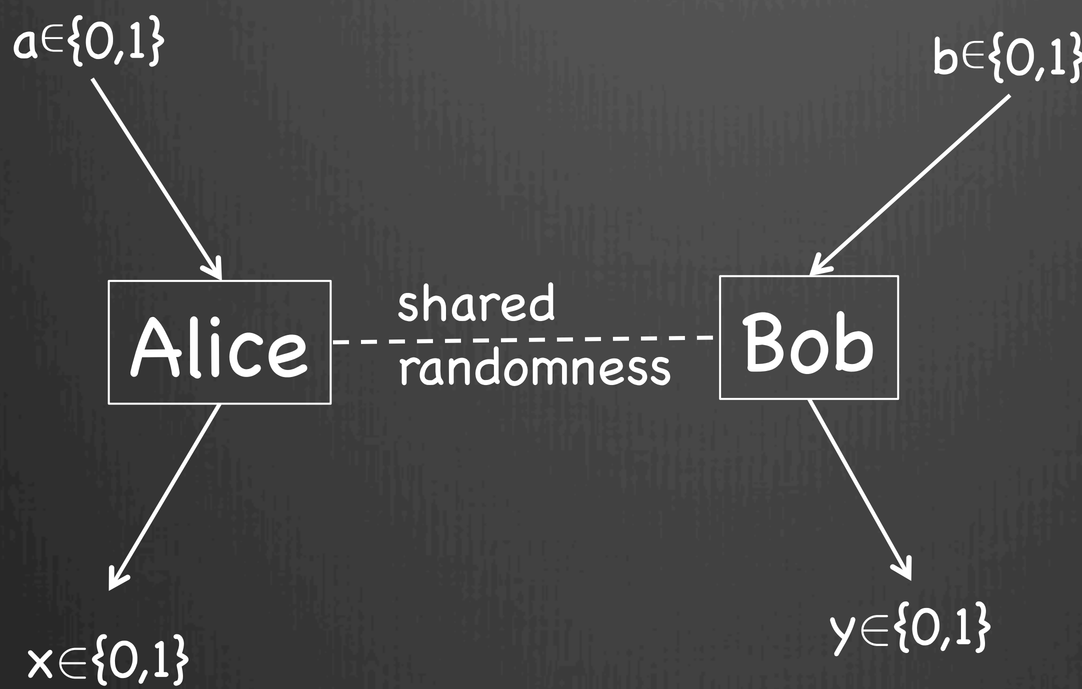


$\Pr[w_1|v_1] = \cos^2(\theta)$ $\quad\Pr[v_1] = 1/2$

$\Pr[w_1|v_2] = \sin^2(\theta)$ $\quad\Pr[v_2] = 1/2$

$\Pr[w_1|$ Alice measures $\{v_1,v_2\}] = \cos^2(\theta)/2 + \sin^2(\theta)/2 = 1/2$

CHSH game



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

Goal: $x \oplus y = ab$

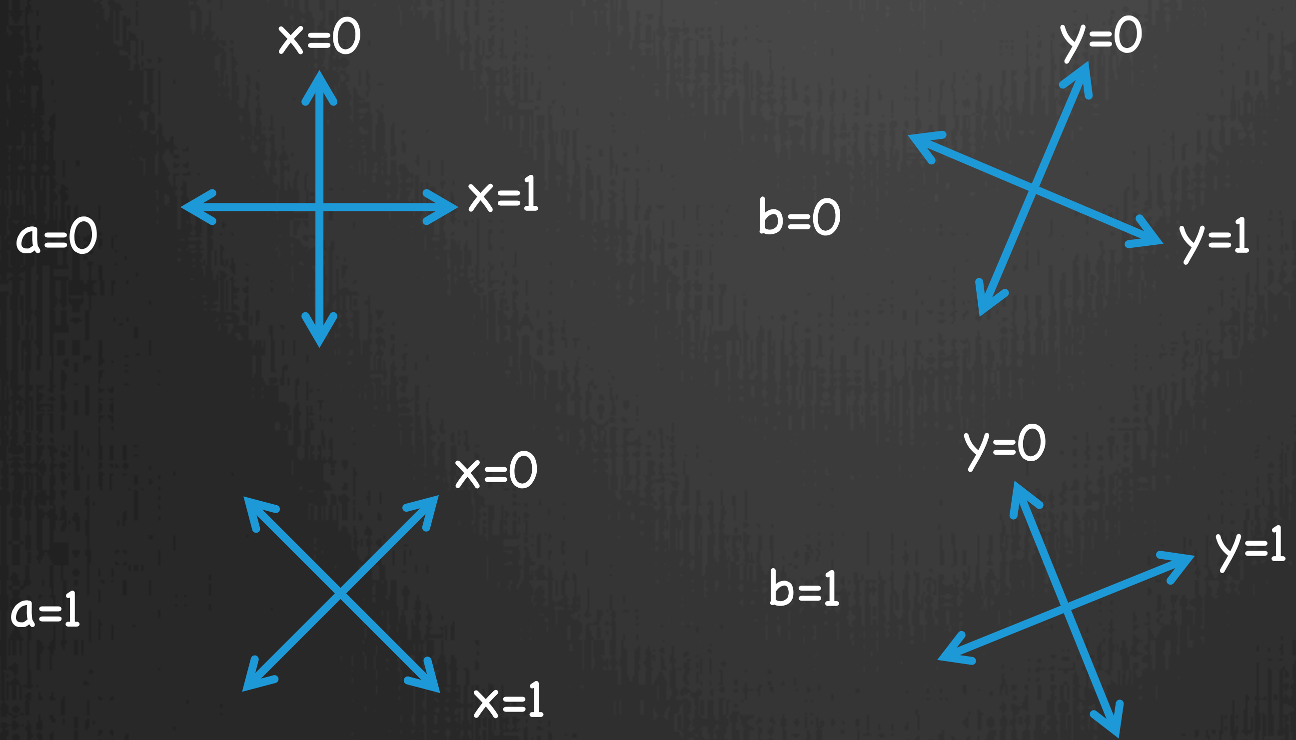
Max win probability is 3/4. Randomness doesn't help.

CHSH with entanglement

Alice and Bob share state $\frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\1\end{pmatrix}$

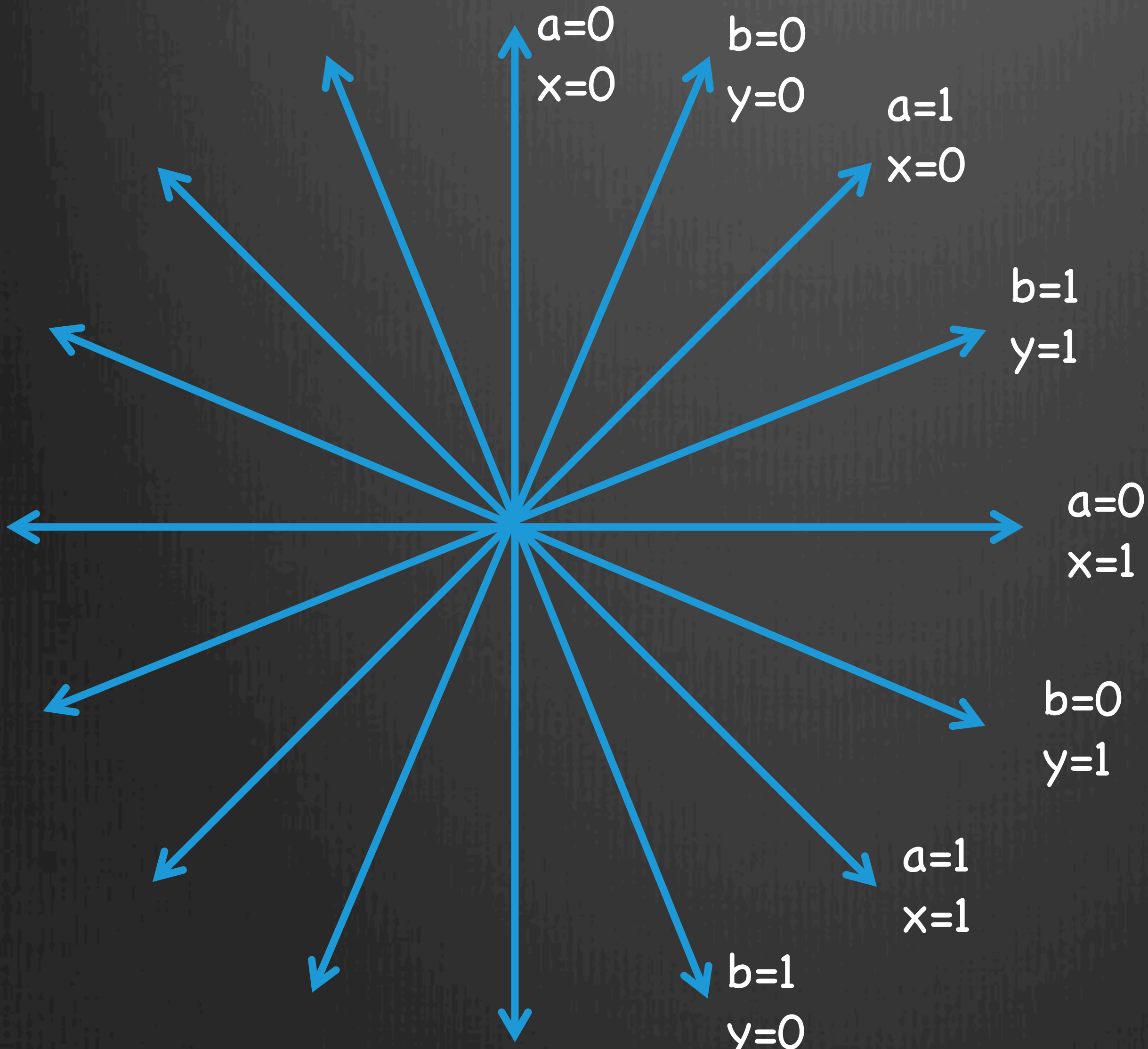
Alice measures

Bob measures



win prob
$\cos^2(\pi/8)$
≈ 0.854

CHSH with entanglement



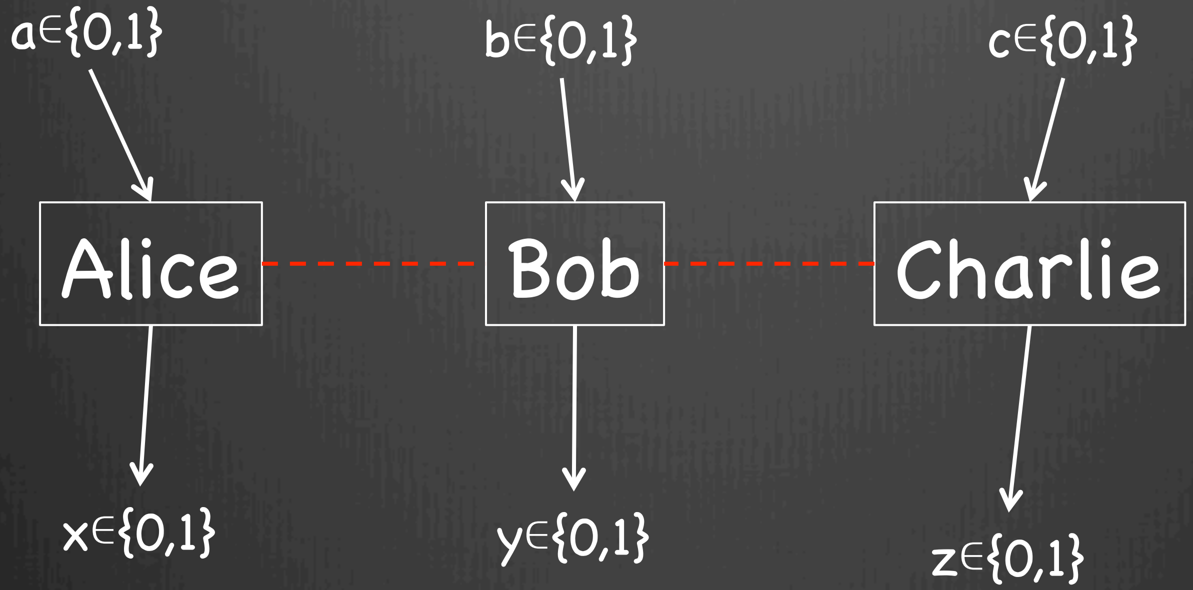
Why it works

Winning pairs are at angle $\pi/8$

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

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

Monogamy of entanglement



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

max Pr[$x \oplus y = ab$] + Pr[$x \oplus z = ac$]

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

Marginal quantum states

Q: What is the state of AB? or AC?

Given a state of A, B, C

$$\alpha = \begin{pmatrix} \alpha_{000} \\ \alpha_{001} \\ \alpha_{010} \\ \alpha_{011} \\ \alpha_{100} \\ \alpha_{101} \\ \alpha_{110} \\ \alpha_{111} \end{pmatrix}$$

A: Measure C.
Outcomes {0,1} have probability

$$p_x = |\alpha_{00x}|^2 + |\alpha_{01x}|^2 + |\alpha_{10x}|^2 + |\alpha_{11x}|^2$$

AB are left with $\frac{1}{\sqrt{p_0}} \begin{pmatrix} \alpha_{000} \\ \alpha_{010} \\ \alpha_{100} \\ \alpha_{110} \end{pmatrix}$ or $\frac{1}{\sqrt{p_1}} \begin{pmatrix} \alpha_{001} \\ \alpha_{011} \\ \alpha_{101} \\ \alpha_{111} \end{pmatrix}$

General monogamy relation:
The distributions over AB and AC cannot both be very entangled.

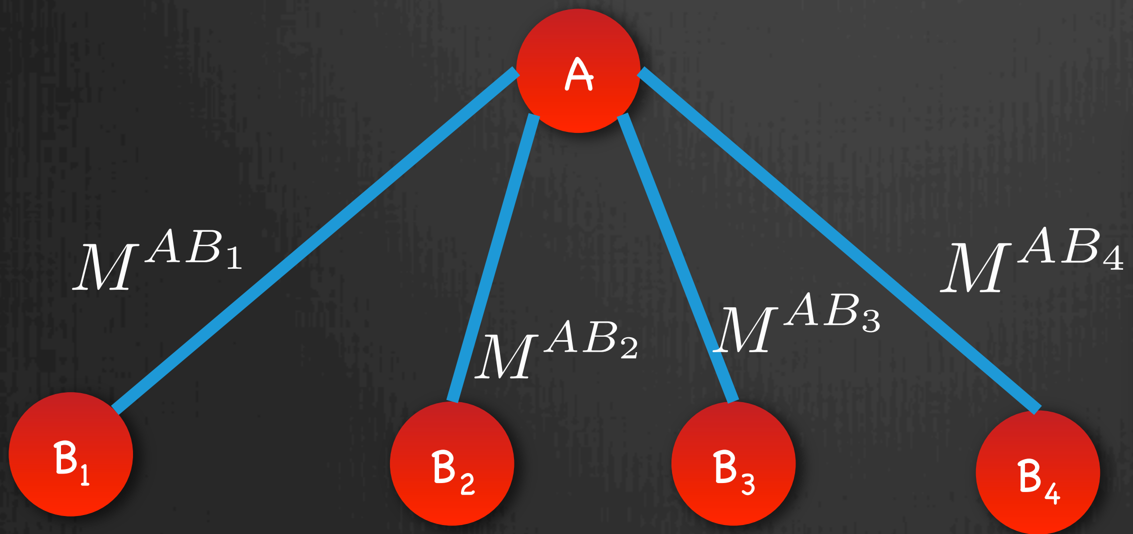
More general bounds from considering $AB_1B_2\ldots B_k$.

Application to 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

Approximate with $\max_{\alpha} \langle \alpha, \dfrac{M^{AB_1} + \cdots + M^{AB_k}}{k} \alpha \rangle$



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

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

For more information

General quantum information:

- M.A. Nielsen and I.L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2000.
- google "David Mermin lecture notes"
- M. M. Wilde, *From Classical to Quantum Shannon Theory*, arxiv.org/abs/1106.1445

Monogamy of Entanglement: arxiv.org/abs/1210.6367

Application to Optimization: arxiv.org/abs/1205.4484