Lecture 16 - The role of entanglement in q. speedups

Outline

- Brief recap of entanglement
- Correlations: local and non-local
- GHZ game
- Bravyi, Gosset, König result (quantum advantage for shallow circuits)

Recapping entanglement

Suppose we have $|\psi\rangle_{AB} \in H_A \otimes H_B$

If $\nexists$ $|\alpha\rangle \in H_A$, $|\beta\rangle \in H_B$ s.t $|\psi\rangle_{AB} = |\alpha\rangle_A |\beta\rangle_B$

then we say $|\psi\rangle$ is entangled

This is bipartite entanglement.

E.g. Bell states $|\phi_+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$

Let $f: \{0,1\}^n \to \{0,1\}^n$ be 1-to-1, then

$\frac{1}{2^{n/2}} \sum_x |x\rangle_A |f(x)\rangle_B$ is entangled across A-B

States that can be mapped to Bell pairs with local unitaries on A and B (i.e. $U_A \otimes U_B$) are called maximally entangled.

States can also be less than maximally entangled, though we won't go into that. If you want some intuition about this consider

$$\text{Seq}(|\psi\rangle) = \sup_{\substack{|\alpha\rangle \in \mathcal{H}_A \\ |\beta\rangle \in \mathcal{H}_B}} |{}_{AB}\langle \psi | \alpha \rangle_A |\beta\rangle_B|^2$$

(geometric entanglement)

In other words, sep measures the overlap between $|\psi\rangle_{AB}$ and the closest separable state. For maximally entangled states $\text{sep}(|\psi\rangle) = \frac{1}{\min(\dim(\mathcal{H}_A), \dim(\mathcal{H}_B))}$

For separable states $\text{sep}(|\psi\rangle) = 1$. Things in between are non-maximally entangled states.

E.g. $|\psi\rangle = \frac{|00\rangle + |01\rangle + |10\rangle}{\sqrt{3}}$

(note that $\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$ is separable since it's just $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$)

Other measures of entanglement include entanglement entropy (Von Neumann entropy), LOCC distillability, Schmidt rank and others.

Multi-partite entanglement - same idea but for multiple systems

E.g.: $|GHZ\rangle_{ABC} = \frac{|000\rangle_{ABC} + |111\rangle_{ABC}}{\sqrt{2}}$

(also cat state)

Cannot be expressed as tensor product of states on A, B or C (or even AB and C, AC and B etc).

$$|W\rangle_{ABC} = \frac{|001\rangle + |010\rangle + |100\rangle}{\sqrt{3}}$$

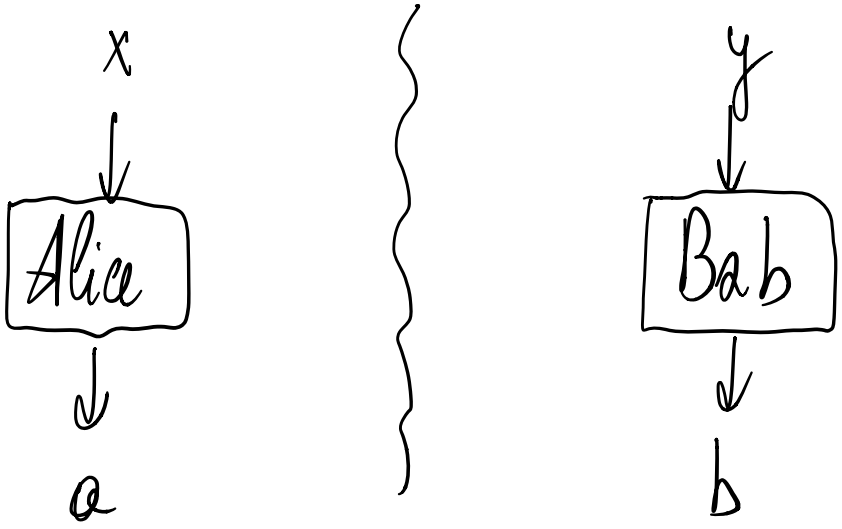
Correlations

Why is entanglement important?

Many reasons mostly having to do with correlations.

Consider the following scenario

2 parties separated by a great distance. Each gets a 1 bit input and produces a 1 bit output. Want to examine distribution of their outputs, given their inputs.



$x, y, a, b \in \{0, 1\}$. Want $Pr(a, b | x, y) \equiv p(a, b | x, y)$

What can we say about $p(a, b | x, y)$ if Alice and Bob can't talk to each other?

Alice's input can't influence Bob's output and vice-versa.

$$p(a | x, y) = p(a | x)$$

$$p(b|x,y) = p(b|y)$$

In this case we say their correlations are non-signalling.

But classically more is true. Alice's output is determined by her input and local randomness. Same for Bob. They could also have pre-shared information that could also be randomized. Encode all that in a variable we'll denote as λ. If this is the case then

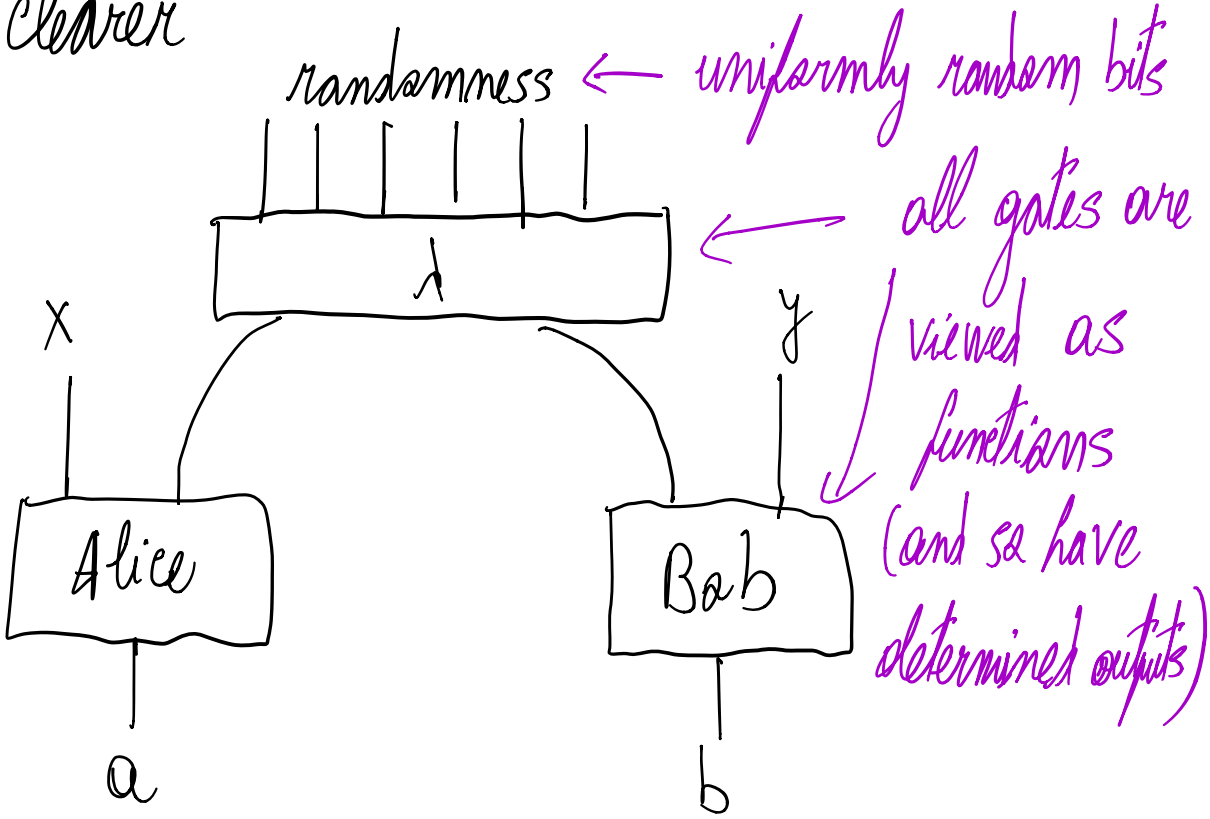
$$p(a,b|x,y) = \sum_{\lambda} p(a|x,\lambda) \cdot p(b|y,\lambda) \cdot p(\lambda)$$

↑ local correlations

Alice and Bob's responses are determined by

their local contexts and shared randomness.

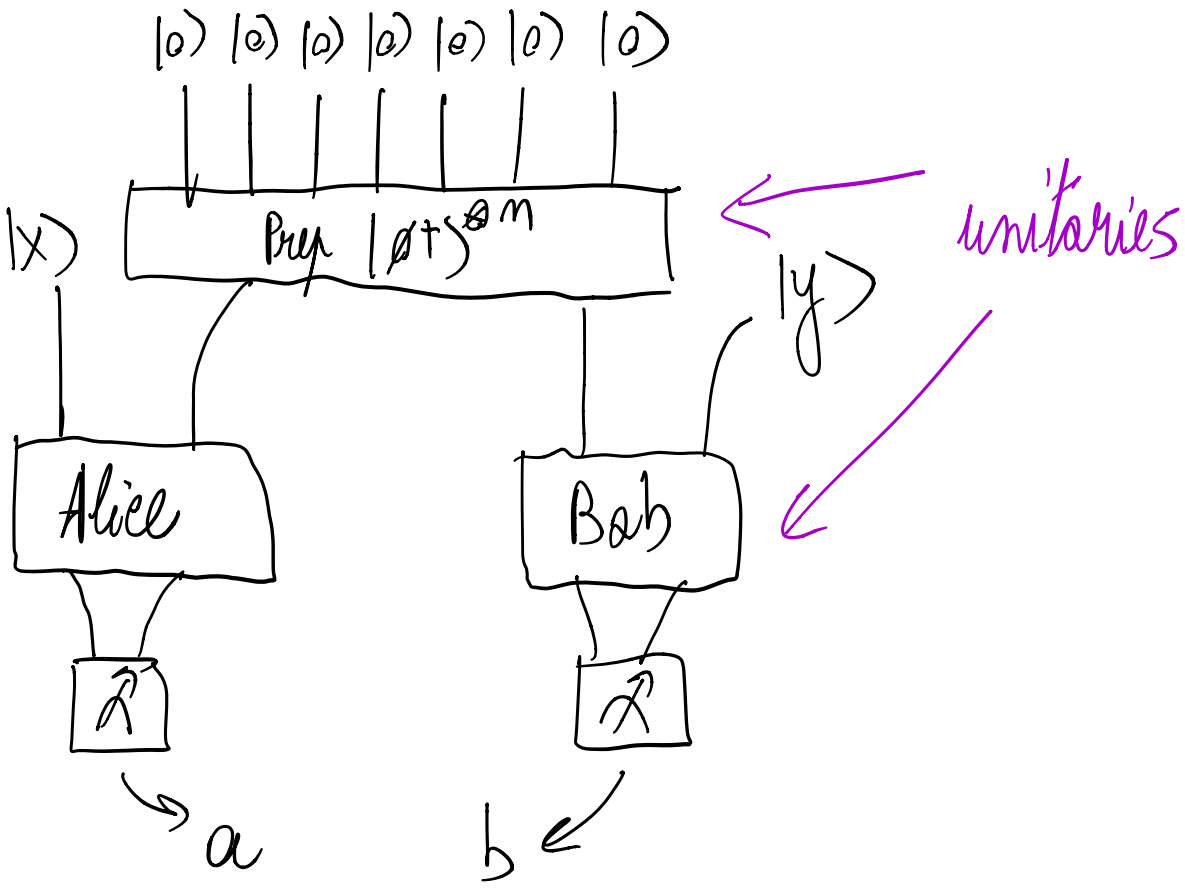
We can also represent this as a circuit to make things clearer



This 2-layer circuit produces local correlations.

Quantumly this is no longer the case!

Consider the following analogous quantum circuit



Can show that there are simple unitaries for Alice and Bob such that

$$p(a,b|x,y) \neq \sum_{\lambda} p(a|x,\lambda) \cdot p(b|y,\lambda) \cdot p(\lambda)$$

Entanglement produces non-local correlations!

However correlations will still be non-signalling!

Entanglement doesn't allow for instantaneous communication

$$p(a,b|x,y) = \sum_{\lambda} p(a|x,\lambda)\cdot p(b|y,\lambda)\cdot p(\lambda)$$

(these define Bell inequalities)

$$p(a,b|x,y) = \left| \langle a,b| \; U_A(x) \otimes U_B(y) \, |\phi^+\rangle \right|^2$$

We can now use these ideas to define games (or problems) for which the win condition is given by having some sort of non-local correlations in the output.

GHZ game

3 players: Alice, Bob, Charlie.

Can have pre-shared strategy but can't communicate during the game

Given inputs $x, y, z \in \{0, 1\}$. Inputs are chosen uniformly at random from $\{000, 011, 101, 110\}$ (i.e. $x \oplus y \oplus z = 0$)

Output $a, b, c \in \{0, 1\}$

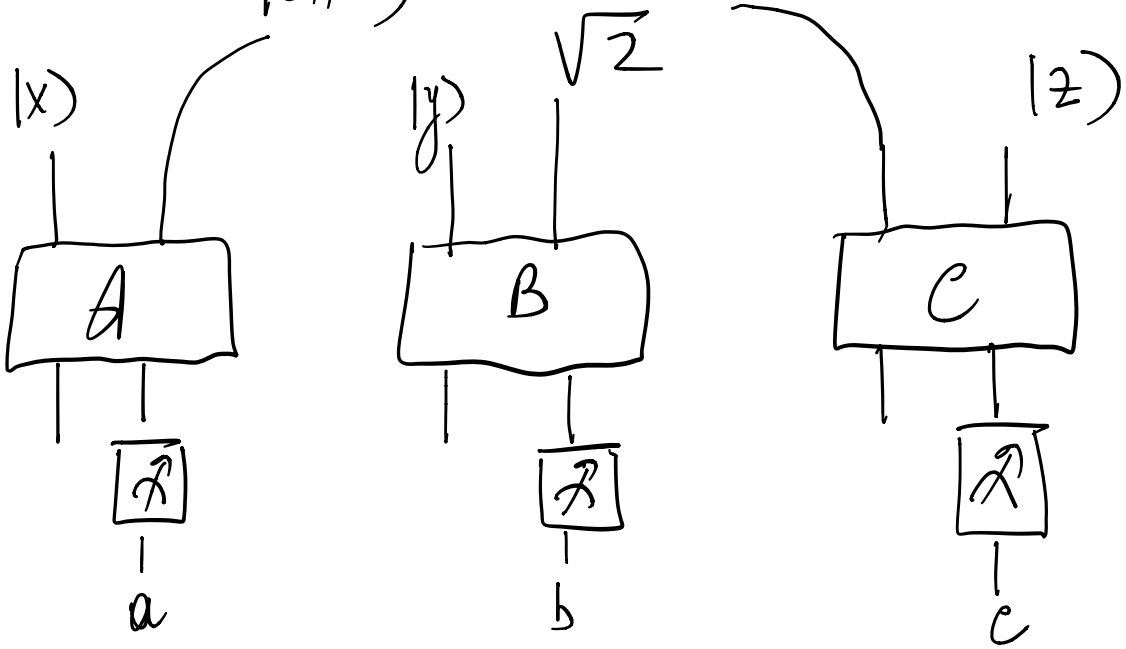
Win condition

- for $x = y = z = 0$ must have $a \oplus b \oplus c = 0$
- for all other inputs $a \oplus b \oplus c = 1$

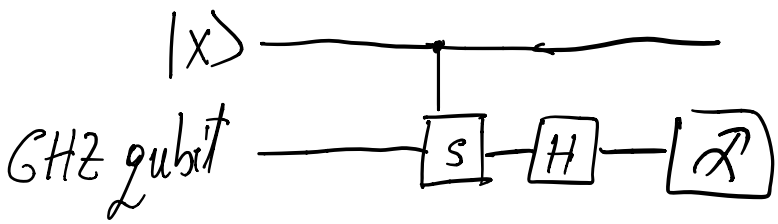
No classical strategy!

But there is a quantum strategy

$$|GHZ\rangle = \frac{|000\rangle_{ABC} + |111\rangle_{ABC}}{\sqrt{2}}$$



A, B and C all do the following



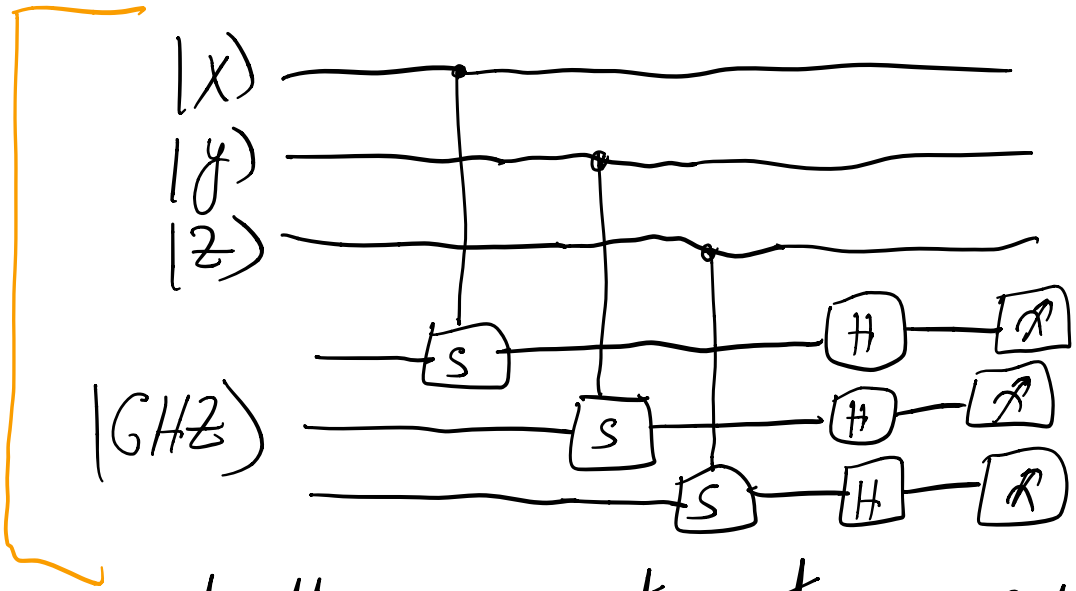
Recall $S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$

$S|0\rangle = |0\rangle$

$S|1\rangle = i|1\rangle$

$(S = T^2;\ S = \sqrt{Z})$

The complete circuit will be



How do the CS gates act on GHZ?

$$CS_{12}\ |x\rangle_1 |GHZ\rangle_2 = |x\rangle \frac{1}{\sqrt{2}} \left(|000\rangle + i^x |111\rangle \right)$$

$\Rightarrow$ after CS gates bottom state is

$$\frac{1}{\sqrt{2}} \left(|000\rangle + i^{x+y+z} |111\rangle \right)$$

But we know $x+y+z=0$ or $x+y+z=2$

If $x+y+z=0 \Rightarrow \frac{1}{\sqrt{2}} \left(|000\rangle + |111\rangle \right)$

If $x+y+z=2 \Rightarrow \frac{1}{\sqrt{2}} \left(|000\rangle - |111\rangle \right)$

$$H^{\otimes n}|0^n\rangle = \frac{1}{2^{n/2}} \sum_w |w\rangle$$

$$H^{\otimes n}|1^n\rangle = \frac{1}{2^{n/2}} \sum_w (-1)^{|w|} |w\rangle$$

$$\Rightarrow \frac{1}{\sqrt{2}} \cdot \frac{1}{2^{3/2}} \left(\sum_w |w\rangle \pm (-1)^{|w|} |w\rangle \right)$$

$$= \boxed{\frac{1}{4} \sum_w \left(1 \pm (-1)^{|w|}\right) |w\rangle}$$

when $x+y+z=0$ we're in + case

$\Rightarrow$ we get w for which $|w| = 0 \mod 2$

i.e $a \oplus b \oplus c = 0$

when $x \oplus y \oplus z = 1$ we're in $-$ case

$\Rightarrow$ we get w for which $|w| = 1 \mod 2$

i.e $a \oplus b \oplus c = 1$

Quantum advantage for shallow circuits

Bravyi, Gosset and König generalized the above idea and proposed a problem that can be solved in constant depth quantumly but not classically!

This is the Hidden Linear Function from HW4. We'll instead look at a more recent problem by Bene Watts, Kothari, Schaeffer and Tal that provides a stronger separation and is a natural generalization of the GHZ game.

Parity Halving Problem (PHP)

Input: $x \in \{0,1\}^n$, $|x| = 0 \mod 2$

Out: $y \in \{0,1\}^n$ s.t $|y| = \frac{|x|}{2} \mod 2$

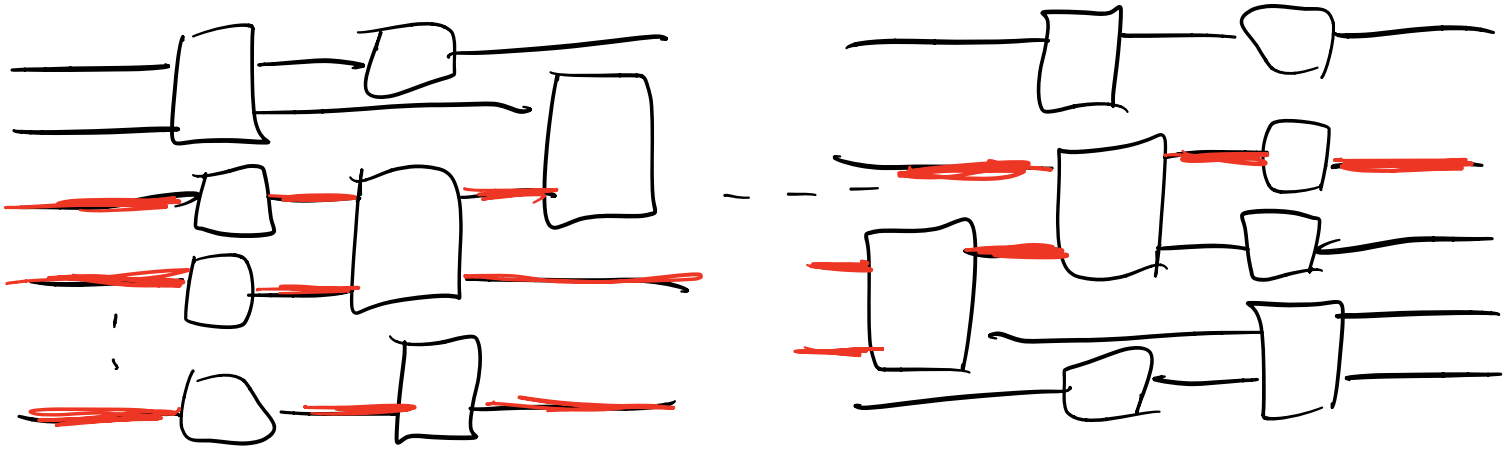
Unsurprisingly the quantum solution is just the generalization of the GHZ game.

1. Start with $|GHZ_n\rangle = \frac{|0^n\rangle + |1^n\rangle}{\sqrt{2}}$
2. Do CS between each input bit of x (or $|x\rangle$) and a qubit in $|GHZ_n\rangle$
3. Hadamard GHZ register
4. Measure.

Analysis is the same as before.

Let's give a proof sketch for why constant depth classical circuits can't solve the problem.

We'll consider circuits with constant fan-in/out ≤ 2 comprised of AND, OR and NOT gates



Red wires highlight light-cone of a particular output. The light-cone is the set of all wires that determine the value of that output.

Suppose the circuit has depth d. $\Rightarrow$ # of input bits in light-cone of any output is at most 2^d

Since $d = O(1)$, each output depends on $O(1)$ input bits.

Similarly, any given input can affect only constant-many outputs. These outputs are the light-cone for that particular input bit.

Roughly, the idea is to then show that there is a set of input bits with disjoint light-cones and that solving PHP reduces to having a classical strategy for the corresponding non-local game.
But we know such a strategy doesn't exist and this concludes the proof.
Remarkably, this can be strengthened in several ways:

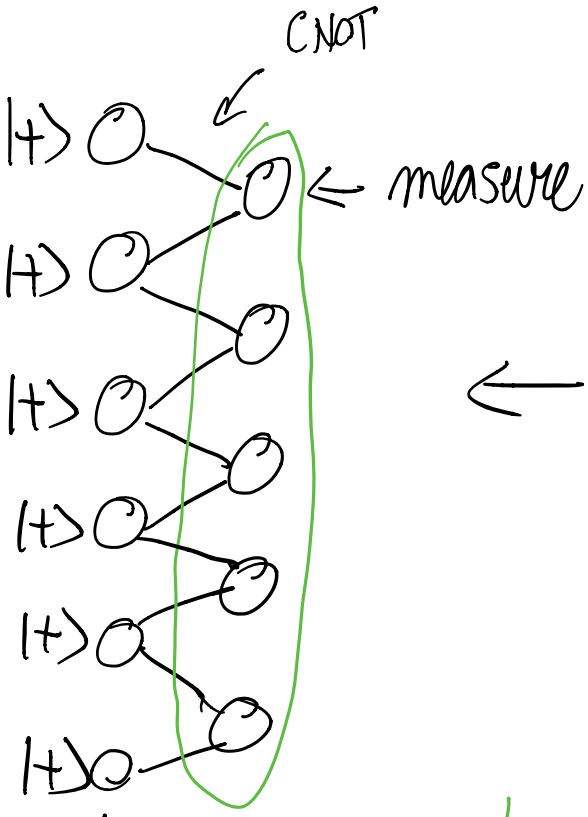
- works for average-case instances
- prob of success of classical circuit is $\frac{1}{2} + \frac{1}{\exp(n)}$
- works even against constant depth circuits with unbounded fan-in!

But wait... can we prepare $|GHZ_n\rangle$ in constant depth?

No! (requires log depth)

However, can prepare poor man's cat state

$$\frac{|z\rangle + |\bar{z}\rangle}{\sqrt{2}}$$ for random $z \in \{0,1\}^n$



← can be done in constant depth

$w \in \{0,1\}^{n-1}$

$$\frac{|z\rangle + |\bar{z}\rangle}{\sqrt{2}}, \quad w_i = z_i \oplus z_{i+1}$$

Relaxed PHP

In: $x \in \{0,1\}^n$, $|x| = 0 \bmod 2$

Out: y, w s.t

$$\exists\, z \in \{0,1\}^n, \quad |y| = \frac{|x|}{2} + z \cdot x \mod 2$$

$$W_i = z_i \oplus z_{i+1}$$

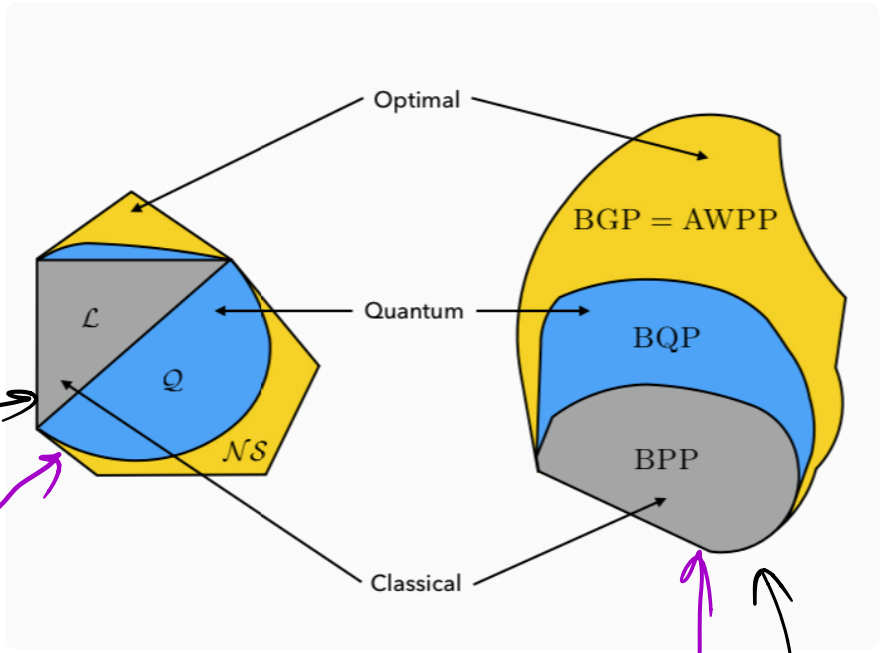
Can be solved in constant depth quantumly!

Cannot be solved in constant depth classically (same results as for PHP)

Correlations seem to play an important role in speed-ups. What about general non-signalling correlations? Turns out those yield the general interference model of computation! Associated complexity class for poly-time comp is called BGP (G is for "general physical theory"; generalizations of QM that allow for non-signalling correlations).
Was shown by Barrett, de Beaudrap, Hoban, Lee

that BGP = AWPP.

So we get this nice picture...



correlations

known containments

(from arxiv: 1702:08483)

conjectured containments

complexity classes

As we'll see in the last lecture, it's hard to generalize this to poly-size circuits.