Meeting 7.1: BQP and QMA

I. BQP, gate (in)dependence, and the Solovay-Kitaev theorem

II. QMA and local Hamiltonian problem

ROUGH PLAN FOR REMAINDER OF SEMESTER

Next time: Simon's and Shor's algorithms

Week 8: Quantum error correction, stabilizer formalism, and $\mathbb{Z}/2$ homology

Weeks 9+: topological quantum computation and TQFT

Time remaining: Khovanov homology?

student talks

I. BQP, gate (in)dependence, and the Solovay-Kitaev theorem

Last time, I ended by flashing this definition (taken from the textbook of Kitaev et al.):

Let

$$F: \{0,1\}^n \to \{0,1\}^m$$

be a function. A circuit U "computes" F to precision ε $(0 \leq \varepsilon < 1/2)$ if for any $x \in \{0,1\}^n$

$$\sum_{z=0}^{2^{N-m}-1} \left| \langle F(x), z | U | x, 0^{N-n} \rangle \right|^2 \geq 1 - \varepsilon.$$

forgot last time

(U has width N)

Why is this a good definition?

For convenience, assume $m = 1$.

Do measurement

$M_0 = |0\rangle\langle 0| \otimes Id_{(\mathbb{C}^2)^{N-1}}$ $M_1 = |1\rangle\langle 1| \otimes Id_{(\mathbb{C}^2)^{\otimes N-1}}$ on

$U|x, 0^{N-n}\rangle$. Probability of correct outcome $f(x)$ is

$\langle x, 0^{N-n} | U^\dagger M_{f(x)}^\dagger M_{f(x)} U | x, 0^{N-n}\rangle$

Write

$$U|x,0\rangle = |f(x)\rangle \otimes \left(\sum_z c_z |z\rangle \right) + |\overline{f(x)}\rangle \otimes \left(\sum_z d_z |z\rangle \right)$$

where $\sum_z |c_z|^2 + |d_z|^2 = 1$. Then

$$M_{f(x)} U|x,0\rangle = |f(x)\rangle \otimes \sum c_z |z\rangle, \text{ so}$$

$$P(\text{outcome } f(x)) = \sum_{z=0}^{2^{N-m}-1} \left| \langle f(x), z | U | x, 0^{N-n}\rangle \right|^2 \geq 1 - \varepsilon.$$

Intuition:

U computes F if for all x,
$U|x, 0^{N-n}\rangle$ is "close" to a state of the form $|F(x)\rangle \otimes |\text{junk}\rangle$.

Here's another fair definition:

U computes F to precision ε if for any $x \in \{0,1\}^n$

$$\langle F(x), x, 0^{N-m-n} | U | x, 0^{N-n} \rangle \geq 1 - \varepsilon$$

Claim: Two definitions are equivalent. (ε's differ, but by controlled amount)

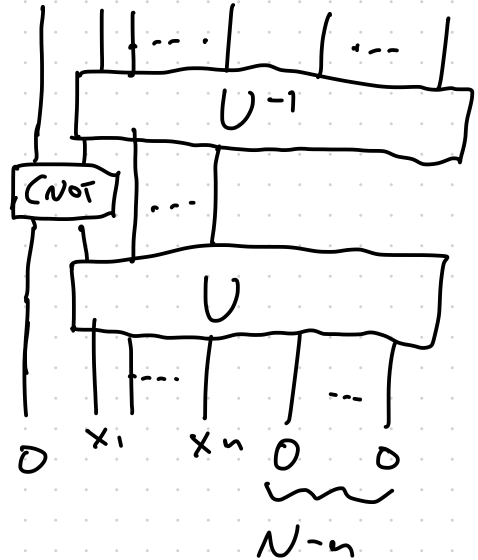
Proof: For convenience, assume $m = 1$.

(1) $\Rightarrow$ (2): Use uncomputation. If U satisfies

$$\sum_{z=0}^{2^{N-m}} \left| \langle F(x), z | U | x, 0^{N-n} \rangle \right|^2 \geq 1 - \varepsilon.$$

then build circuit V as follows:

V :



(2) $\Rightarrow$ (1): Immediate from definitions. $\square$

What should be the correct definition of what it means for a quantum computer to compute a decision problem

$$F: \{0,1\}^* \longrightarrow \{0,1\} = \{No, Yes\} ?$$

Issue: now input bit string has variable + unbounded length!

Fix: use a different circuit for every bit string, or at least every different length $n = |x|$.

But careful! Where should these circuits come from?

A classical polynomial time algorithm!

Def'n [BQP($\mathcal{G}$, ε)]

Fix a quantum universal gate set $\mathcal{G}$ and $0 < \varepsilon < 1/2$.

A decision problem $f: \{0,1\}^* \to \{0,1\} = \{\text{No}, \text{Yes}\}$ is in BQP($\mathcal{G}$, ε) if there exists a classical, polynomial time algorithm that when input $x \in \{0,1\}^*$, prints a diagram of a quantum circuit (w/ gate set $\mathcal{G}$) U_x that computes $f(x)$ to precision ε.

Dependence on $\mathcal{G}$ and ε?

Just as for BPP, we have

$$BQP(\mathcal{G}_1, \varepsilon_1) = BQP(\mathcal{G}_1, \varepsilon_2)$$

for all $0 < \varepsilon_1 < \varepsilon_2 < 1/2$.

For $\mathcal{G}_1$ have to consider convergence properties of dense subgroups of $U(2)$ and $U(4)$.

Problem: need to convert gates in $\mathcal{G}_1$ to gates in $\mathcal{G}_2$ without too much overhead.

Moreover, the conversion is only APPROXIMATE.

Theorem A3.1: (**Solovay–Kitaev theorem**) Let $\mathcal{G}$ be a finite set of elements in $SU(2)$ containing its own inverses, such that $\langle \mathcal{G} \rangle$ is dense in $SU(2)$. Let $\epsilon > 0$ be given. Then $\mathcal{G}_l$ is an ϵ-net in $SU(2)$ for $l = O(\log^c(1/\epsilon))$, where $c \approx 4$.

In other words, if $G \in SU(2)$, I can find

$$U = G_1 G_2 G_3 \cdots G_\ell \quad , \quad G_i \in \mathcal{G}$$

such that

$$\| U - G \| < \varepsilon$$

where $\ell = O(\log^c(1/\varepsilon))$.

(Assuming $\mathcal{G}_1$ and $\mathcal{G}_2$ both finite and inverse closed.)

Take-away: it's easy to find a short product of elements of $\mathcal{G}$ that is ε-close to G.

Corollary: $BQP(\mathcal{G}_1) = BQP(\mathcal{G}_2)$

Warning: if $\mathcal{G}$ is infinite, $BQP(\mathcal{G})$ can include uncomputable functions

<u>Def</u> $BQP = BQP(\mathcal{G}, 1/3)$

where $\mathcal{G}$ is whatever finite, inverse closed, quantum universal gate set you prefer.

Examples of problems in BQP?

Factoring!

Given an integer n (in binary), output its prime factorization.

Note: Factoring is NOT the same as "Is it prime?"

Already in P.

II. QMA and local Hamiltonian problem

Kitaev's book calls QMA "BQNP."

Three way analogy:

$$P : NP :: BPP : MA :: BQP : QMA$$

QMA is very similar to MA, with two additions:

1. Arthur has a quantum computer!

2. Merlin provides Arthur with a certificate in the form of a quantum state

.

Subtlety: it's possible Merlin only ever needs to use a classical bit string.

It would be better to call QMA

"QMQA".

Then there is a subset

"CMQA"

Unfortunately CMQA is actually called QCMA.

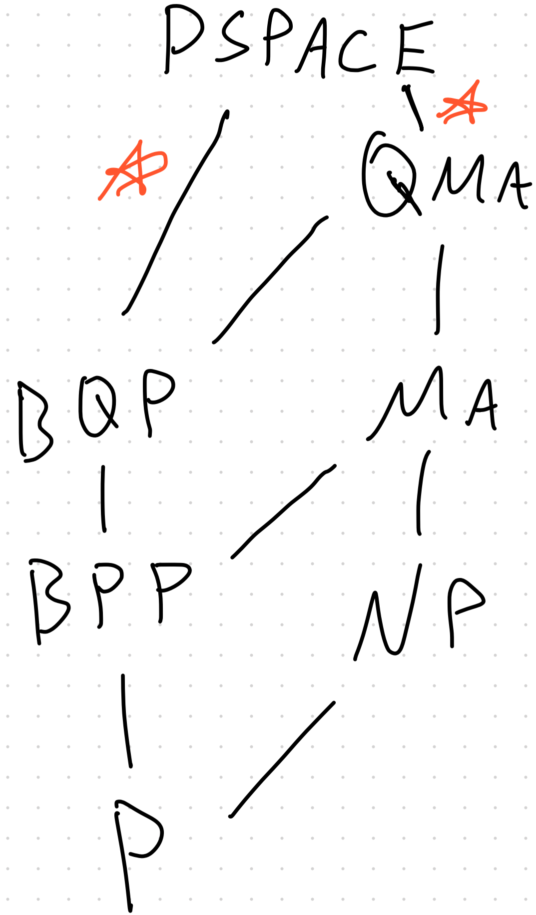
It's not known if

$$P \subsetneq PSPACE!$$

All of these complexity classes are separated by oracles. E.g. exists a decision problem F such that

$$P^F \neq NP^F.$$

(There also exists an F where $P^F = NP^F$.)



IP = PSPACE

but separated by a random oracle!

$$C_1^F \stackrel{?}{=} C_2^F \qquad \forall F$$

Why is BQP $\subseteq$ PSPACE?

Gist: we can sufficiently approximate

$\langle z | U | w \rangle$ for all

$z, w \in \{0,1\}^N$ and width N circuit U.

$$\langle z | U | w \rangle =$$

$$\sum_{x_1, x_2, \ldots, x_\ell} \langle z | G_1 | x_1 \rangle \langle x_1 | G_2 | x_2 \rangle \cdots \langle x_{\ell-1} | G_\ell | x_\ell \rangle$$

$$U = G_1 G_2 \cdots G_\ell$$