CSE 596 Lecture Fri 12/6 Fall 2019

Simon's Problem: Suppose we are given $f:\{0,1\}^n \to \{0,1\}^n$ such that f has a "hidden key string" $s \in \{0,1\}^n$ such that

$$\forall x, y \in \{0,1\}^n: f(x) = f(y) \iff y = x \oplus s$$

bitwise XOR.

Note: If $s = 0^n$, then this becomes $f(x) = f(y) \iff x = y$, which is the definition of f being 1:1. For all other s, f is 2:1.

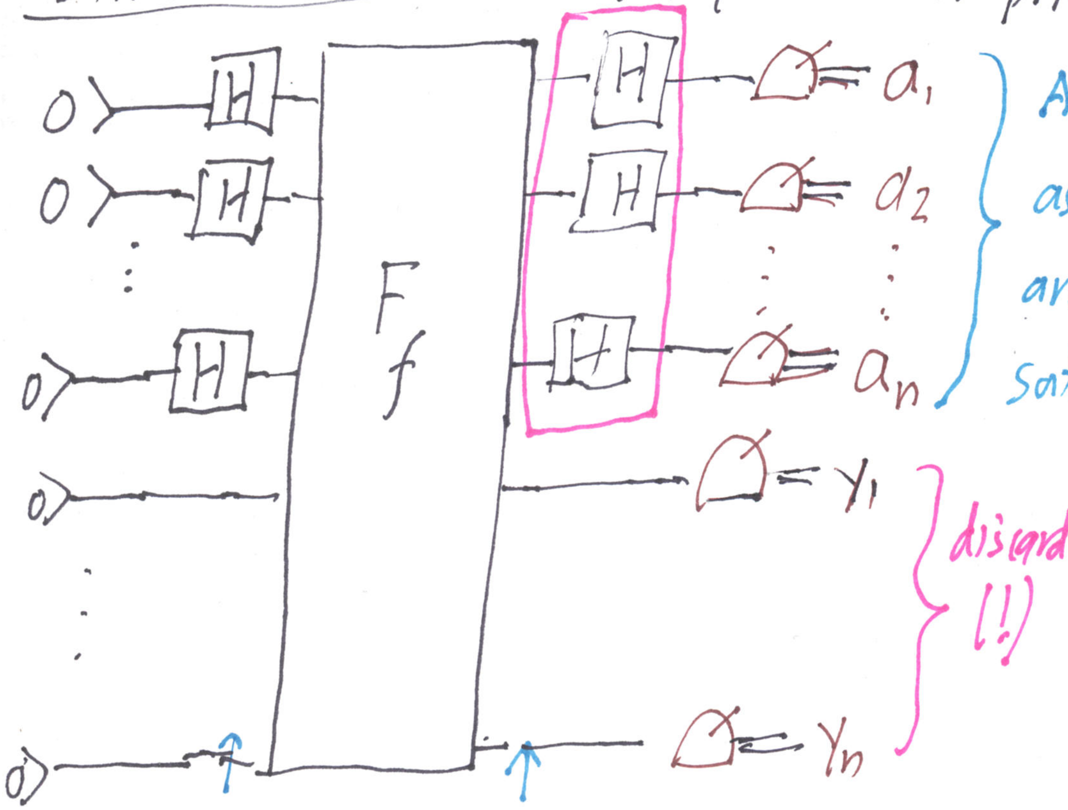
A classical algorithm M is given a "black box" oracle for f. That is, M can write strings u on its oracle tape and instantly get the value $f(u)$, but cannot inspect any code for computing f.

Daniel Simon proved in 1993 that the task of distinguishing the $s = 0^n$ and $s \neq 0^n$ cases is not in $BPP^{[f]}$ where $[f]$ means a black box for a general given such f, not any particular f. In fact, he proved that it requires exponential time classically.

Then he proved quantum circuits can find s w.h.p. in $n^{O(1)}$ size (= time)

This doesn't put a specific language into BQP, because $[f]$ is given in an auxiliary manner — as $[F_f]$ in the quantum case. But it does show a strong separation from "the same (?) manner of BPP."

Simons Circuits on 2n qubits: n primary and n "ancillas"?

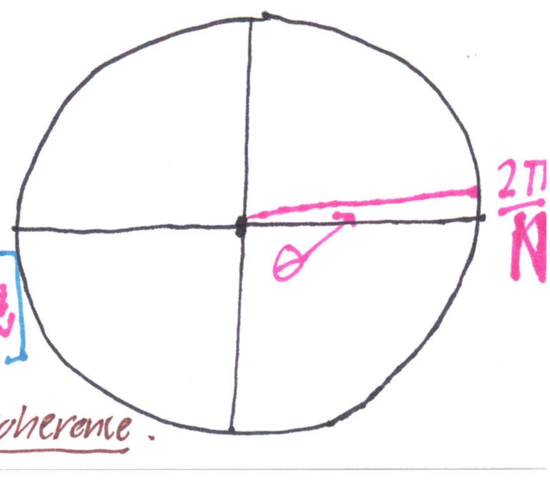


creates $\sum_{x \in \{0,1\}^n} \frac{|x\rangle|0^n\rangle}{\sqrt{2^n}}$ $\qquad \sum_{x \in \{0,1\}^n} \frac{|x\rangle|f(x)\rangle}{\sqrt{2^n}}$

Add $\langle x, \vec{a} \rangle = 0$ as an equation. The analysis shows **s** always satisfies it. When $s \neq 0^n$, analysis shows it narrows down the space by half with prob. $\geq 1/2$. So $O(n)$ iterations are w.h.p. enough to solve for s uniquely. If you force 0^n, then f is 1-1. definitely: so this is "$RQP^{[f]}$".

Peter Shor in 1993-94 observed: What if we replace the second Hadamard transform by the QFT, which is just the ordinary Discrete Fourier Transform but on $N = 2^n$ elements. And what if $f(x)$ is the definite function a^x modulo M where $M = pq$ is a product of two odd primes and $a < M$ is not a multiple of p or q:

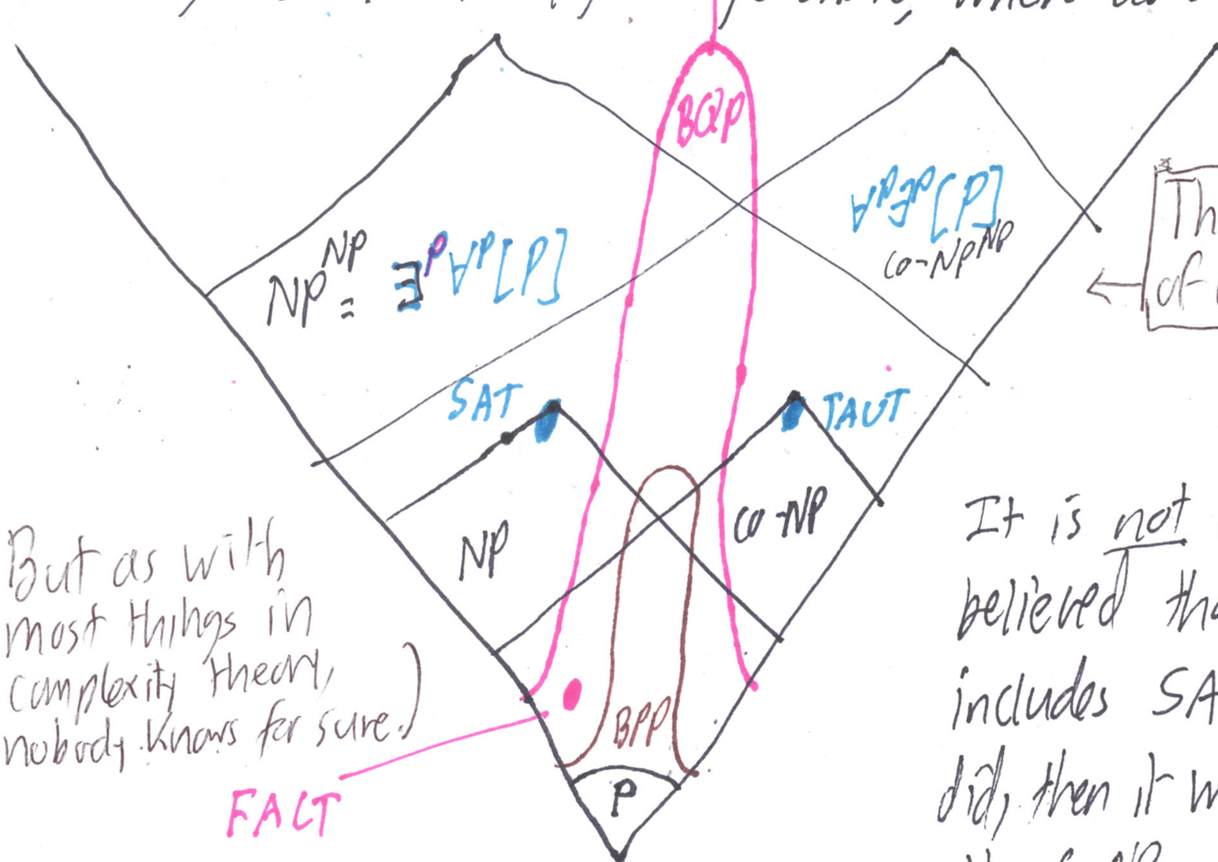
$\hookrightarrow$ Shor's Theorem: FACTORING $\in$ BQP.



Issue 0: The QFT involves exponentially tiny angles. Standard n^2-sized QCs involve rotations by $\frac{2\pi}{N}$ or $T_N = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{N}} \end{bmatrix}$

Issue 1: These can be approximated by circuits of ordinary T-gates, but with great concrete size blowup and decoherence.

Presuming BQP really is feasible, where does it lie?



The picture most of us believe.

(But as with most things in complexity theory, nobody knows for sure.)

It is <u>not</u> commonly believed that BQP includes SAT. If it did, then it would include all of NP and co-NP.

<u>Theorem</u>: $BQP \subseteq PSPACE$. In fact, every $L \in BQP$ can be accepted by a poly-time oracle TM $M^{\#sat}$ where $\#sat(\phi)$ gives the <u>number</u> of satisfying assignments of a formula ϕ. You can count all the satisfying assgts. by looping thru $x \in \{0,1\}^n$ in linear space.

I had an idea for trying to show $BQP \subseteq NP^{NP^{NP}}$, the third level of the <u>polynomial hierarchy PH</u>, which you might understand better as the class of languages L such that for some predicate $R(x,u,v,w)$ in P and polynomial $q(n)$,

But newest evidence hints $BQP \not\subseteq PH$

$$x \in L \Leftrightarrow (\exists u : |u| \leq q(n))(\forall v : |v| \leq q(n))(\exists w : |w| \leq q(n))\, R(x,u,v,w).$$

$\boxed{\text{END}}$