Today:Quantum Computing + Wrap-up

- Quantum Wire
- Quantum Information
- Quantum Measurements
- Quantum Gates
- Quantum Circuit
- Quantum Algorithm for Factoring.

Preliminaries

Quantum Wire Carries a vector in complex 2-dimensional space.

n-**Quantum wires** Carry a vector in complex 2^n-dimensional space.

Measurement Can read, say, the first i "qubits": Result: i classical bits + $n-i$ qubits, as follows: Let initial configuration: $\sum_x \alpha_x |x\rangle$. For $x' \in \{0,1\}^i$, let $p_{x'} = \sum_{y \in \{0,1\}^{n-i}} \alpha^2_{x' \circ y}$. Then see x' with probability $p_{x'}$ and $n-i$ qubits are in state $\sum_y \frac{\alpha_{x' \circ y}}{\sqrt{p_{x'}}} v_{x' \circ y}$.

Gates c-qubit gate is a "linear map $G : \mathbb{C}^{2^c} \to \mathbb{C}^{2^c}$ such that $\langle G(x), G(y) \rangle =$

$\langle x, y \rangle$" (referred to as unitary operator). Interesting gates are:

- Hadamard Gate: $\begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix}$
- Quantum NOT Gate: Maps $|a, b\rangle$ to $|a, b \oplus \neg a\rangle$.
- Quantum AND Gate: Maps $|a, b, c\rangle$ to $|a, b, c \oplus (a \wedge b)\rangle$.

Above gates suffice to approximate any other quantum gate to within arbitrary precision.

Quantum Circuit n quantum wires + m gates + measurement at the end.

What can Q-Circuits Do?

3 Famous Algorithms:

- Simon's algorithm to detect collisions (promise + oracle problem).
- Shor's algorithm to factor integers
- Grover's algorithm to search for NP witnesses (oracle problem).

Simon's problem

Given: $f : \{0,1\}^n \to \{0,1\}^n$.
Yes Instance: Exists $s \in \{0,1\}^n$ such that $f(x) = f(y) \Leftrightarrow y = x + s$.
No Instance: f is $1-1$. Task: Decide which case.

Simon's Algorithm

(Omitting normalizing constants)

$$\begin{aligned} |0^{2n}\rangle &\to \sum_x |x0^n\rangle \\ &\to \sum_x |xf(x)\rangle \\ &\to \sum_{x,y} (-1)^{\langle x,y\rangle} |yf(x)\rangle \end{aligned}$$

- Now measure all $2n$ qubits.
- In NO instance: All $2n$ bit strings equally likely.
- In YES instance: y-part has inner product 0 with s.
- Repeat experiment $O(n)$ time and get a full rank collection of y's, s is the (unique) vector orthogonal to all.

Shor's algorithm

Key insight: Simon's algorithm discover's periods in groups. Can apply to other groups. Technical issues arise if group is not "nice", but can be dealt with.

Idea: To find factors of N, suffices to find r such that $a^r = 1 (\mod N)$. So need to consider the map $r \mapsto a^r (modN)$ and find kernel of this map. Simon considers the map $x \mapsto f(x)$ and finds kernel of this map.

Idealized algorithm

$$\begin{aligned} |00\rangle &\to \sum_i |i0\rangle \\ &\to \sum_i |ia^i\rangle \\ &\to \sum_{i,j} (\omega)^{ij} |ja^i\rangle (\text{ where } \omega^N = 1) \end{aligned}$$

Now measuring j gives random multiples of N/r.

Actual algorithm: Issues

Can't do N-ary Fourier transform.

Shor's fix: Pick $Q = 2^k$, $Q \gg N$. Then the Fourier transform can be implemented effectively.

But now j reported is not a random multiple of N/r, but rather an integer such that $[rj]$ is small modulo Q. Can use integer programming in $O(1)$ variables to find r.

Details omitted.

Wrap-up

Saw lower bound techniques.

Power of randomness, and some algebra.

Main take-away messages: Computation captures many remarkable phenomena.

"Proof of existence of colors".

"Pseudo-randomness".

"Knowledge complexity of interaction".

Seemingly unrelated tasks can be fundamentally related. Relationship becomes evident when one focusses on computational implications. Shor's factoring; Connection between PCP and inapproximability. Trevisan's extractor; Lipton's hardness for permanent.

Future?

More derandomizations (Factorization of polynomials, Polynomial identity testing, RL).

Better understanding of circuit complexity. (Is second level of EXP hierarchy the best possible?).