Lecture 12.

Bernstein-Vazirani algorithm.

Let $s \in \mathbb{B}^n$ be a string (element) and consider a function $f_s : \mathbb{B}^n \to \mathbb{B}$ given by $f_s(x) := x \cdot s = x_1 s_1 + x_2 s_2 + \dots + x_n s_n \pmod 2$.

Problem: given that $g : \mathbb{B}^n \to \mathbb{B}$ is a function of type f_s for some $s \in \mathbb{B}^n$, find s.

Let's discuss a classical algorithm first. Any element $x = (x_1 x_2 \dots x_n) \in \mathbb{B}^n$ gives rise to a linear equation on the coordinates of $s = s_1 s_2 \dots s_n$!

$$f_s(x) = x_1 s_1 + x_2 s_2 + \dots + x_n s_n.$$

Taking a linearly independent collection of n elements in $\mathbb{B}^n$ we will get a system of n linear eq-ns with n unknowns, which has a unique solutions. The solution is exactly $s = (s_1 s_2 \dots s_n)$.

<u>Example.</u> Let $f_s : \mathbb{B}^3 \to \mathbb{B}$ be a function with

$f_s(001) = 1$

$f_s(111) = 0$

$f_s(100) = 1.$

Find s.

We get the system of eq-ns
$$\begin{cases} 0 \cdot s_1 + 0 \cdot s_2 + 1 \cdot s_3 = s_3 = 1 \\ 1 \cdot s_1 + 1 \cdot s_2 + 1 \cdot s_3 = s_1 + s_2 + s_3 = 0 \\ 1 \cdot s_1 + 0 \cdot s_2 + 0 \cdot s_3 = s_1 = 1 \end{cases}$$

The unique solution is $s=101$.

Here is the quantum algorithm.

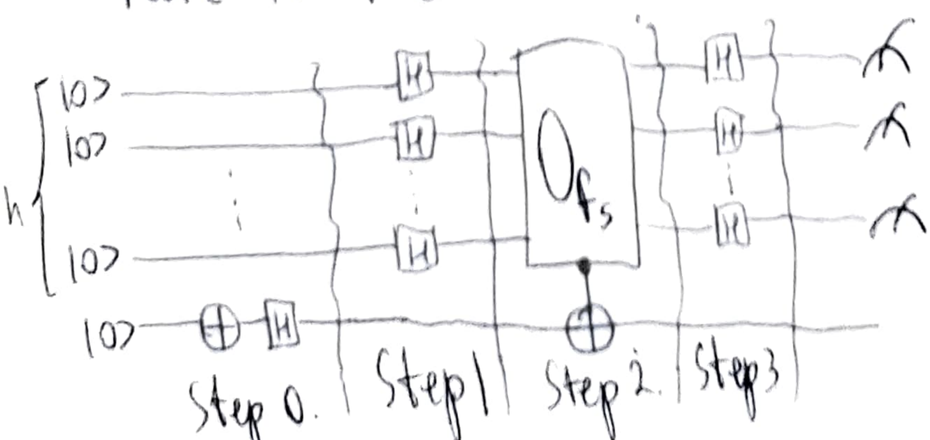
Step 1. $H^{\otimes n}|0^n\rangle|-\rangle = \frac{1}{\sqrt{2^n}}\sum_{i=0}^{2^n-1}|i\rangle|-\rangle$ (prepare the 'generic superposition' state).

Step 2. Use the oracle for f_s: $\frac{1}{\sqrt{2^n}}\sum_{i=0}^{2^n-1}(-1)^{s\cdot i}|i\rangle|-\rangle$.

Notice that we have used $f_s(|i\rangle)=s\cdot i$, also $H^{\otimes n}(|s\rangle)=$
$= \frac{1}{\sqrt{2^n}}\sum_{i=0}^{2^n-1}(-1)^{s\cdot i}|i\rangle$ as we have seen before!

Step 3. Apply $H^{\otimes n}$ again. Using the observation above and $H^2=Id$, we get $H^{\otimes n}\left(\frac{1}{\sqrt{2^n}}\left(\sum_{i=0}^{2^n-1}(-1)^{s\cdot i}|i\rangle\right)\right)\otimes|-\rangle=$
$= H^{\otimes n}(H^{\otimes n}(|s\rangle))\otimes|-\rangle = |s\rangle\otimes|-\rangle$.

Here is the circuit



Simon's problem.

Given: a map $f: \mathbb{B}^n \to \mathbb{B}^n$, satisfying the condition

$$f(x)=f(y) \iff x=y \text{ or } x=y\oplus s \text{ for some (fixed) } s\in\mathbb{B}.$$

Here $y\oplus s=(y_1\oplus s_1, y_2\oplus s_2, \dots, y_n\oplus s_n)$.

Goal: find s.

Rmk. If we get lucky to spot $x\neq y$ with ~~x⊕~~ $f(x)=f(y)$, then s can be found via

$$s=x\oplus y=(x_1\oplus y_1, x_2\oplus y_2, \dots, x_n\oplus y_n).$$

Again, we first present a (probabilistic classical algorithm. Consider the following problem.

Problem. Given a group of K people, what is the probability that two of them have a Birthday on the same day (assume there are N days in a year)?

Solution: we compute the probability that no people in the group were born on the same day (complimentary event):

$$P\left(\begin{matrix}\text{no pair of people}\\ \text{born on the same day}\end{matrix}\right)=\underset{\substack{\uparrow\\ \text{1st person}\\ \text{can be born}\\ \text{on any day}}}{\frac{N}{N}}\cdot\underset{\substack{\uparrow\\ \text{any day}\\ \text{except 1st}\\ \text{guy's B-day}}}{\frac{N-1}{N}}\cdot \ldots \cdot\frac{N-K+1}{N}=\prod_{i=0}^{K-1}\left(1-\frac{i}{N}\right).$$

...

Technical lemma. $e^{-x} \geqslant 1-x$.

Proof. Let $f(x) = e^{-x} - 1 + x$, then $f(0) = 0$ and

$$f'(x) = -e^{-x} + 1 \text{ is } \begin{cases} > 0, & x > 0 \\ < 0, & x < 0, \end{cases}$$

implying $f(x)$ is decreasing for $x < 0$ and increasing for $x > 0$. The statement follows.

It follows that

$$P\begin{pmatrix}\text{no pair has B-day} \\ \text{on the same day}\end{pmatrix} = \prod_{i=0}^{k-1}\left(1 - \frac{i}{N}\right) \underset{\substack{\text{T. lemma for} \\ \text{each } \frac{i}{N} \text{ in} \\ \text{place of } x}}{\leqslant} \prod_{i=0}^{k-1} e^{-i/N} =$$

$$= e^{-\frac{1}{N}\sum_{i=0}^{k-1} i} = e^{-\frac{k(k-1)}{2N}}$$

Finally

$$P\begin{pmatrix}\text{2 people born} \\ \text{on the same day}\end{pmatrix} = 1 - P\begin{pmatrix}\text{no pair has} \\ \text{B-day on the same day}\end{pmatrix} \geqslant$$

$$\geqslant 1 - e^{-\frac{k(k-1)}{2N}}.$$

Rmk. ① If $k = 2\sqrt{N}$, then $e^{-4} \leqslant e^{-\frac{k(k-1)}{2N}} \leqslant \underset{0.05}{e^{-3}}$, so

$P(\text{failure}) \leqslant 5\%$.

② The correspondence

days in a year $\longleftrightarrow$ elements of $\mathbb{B}^n$

people's B-days $\longleftrightarrow$ randomly chosen el-ts in $\mathbb{B}^n$

gives a classical probabilistic algorithm with probability of finding s being at least $1 - e^{-\frac{k(k-1)}{N}}$ where $N = 2^n = |\mathbb{B}^n|$ and k is the number of trials on $x \in \mathbb{B}^n$.

Lecture 13.

Simon's algorithm.

Now let's take a look at the quantum algorithm.

Step 1. We start with the state $|0^n\rangle|0^n\rangle$ of 2n qubits and apply the Hadamard operator to the first $\underbrace{n}_{\text{qubits}}$ to get the state $\frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle|0^n\rangle$

Step 2. Application of the oracle gives rise to the state $\frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle|f_s(i)\rangle$. Next we measure the second n-tuple of qubits and get ~~a~~ state $\frac{1}{\sqrt{2}}(|k\rangle+|k\oplus s\rangle)\otimes|f_s(k)\rangle$ for some $0\le k\le N-1$ (recall that $f_s(k)=f_s(k\oplus s)$).

Step 3. Act with $H^{\otimes n}$ again to produce the state

$$|\sigma\rangle=\frac{1}{\sqrt{2N}}\sum_{j=0}^{N-1}(-1)^{i\cdot j}(1+(-1)^{s\cdot j})|j\rangle.$$ (we have used that $(-1)^{(i\oplus s)\cdot j}=(-1)^{i\cdot j+s\cdot j}$).

Notice that the amplitude of $|j\rangle$ in $|\sigma\rangle$ is 0 if $s\cdot j=1$ and nonzero if $s\cdot j=0$.

It follows that measuring n qubits results (collapses) to a $|j\rangle$ with $s\cdot j=0$. A linear equation on $(s_1,\dots,s_n)$ has been obtained. We run the algorithm repeatedly until getting n linearly independent eq-ns. This allows to find the hidden string s.