Lecture 11.

Deutsch-Jozsa algorithm.

Let $f: \mathbb{B}^n \to \mathbb{B}$ be a function that is guaranteed to satisfy one of the two assumptions:

- f is *constant*, i.e. $f \equiv 1$ or $f \equiv 0$.
- f is *balanced*, i.e. $f \equiv 1$ for half the el-ts in $\mathbb{B}^n$ and $f \equiv 0$ for the other half:

$$\exists X \subset \mathbb{B}^n,\ |X| = 2^{n-1},\ f|_X \equiv 1 \text{ and } f|_{\mathbb{B}^n \setminus X} \equiv 0.$$

<u>Task</u>: determine which of the two possibilities occurs.

<u>Rmk</u>. Classically, we have to check $\frac{n}{2}+1$ values (if f is balanced, we know nothing about the subsets except the cardinality). This is to get the result with 100% degree of certainty. If we are happy with getting the right answer not for sure but with a very high probability, this is easy to accomplish. Using k random trials, $P(\text{error}) \leq \frac{1}{2^{k-1}}$ (see HW for details).

Quantum algorithm.

Step 1. Start with $|0^n\rangle$ and apply $H^{\otimes n}$ to get $\frac{1}{\sqrt{2^n}}\sum_{i=0}^{2^n-1}|i\rangle$.

Step 2. Using the oracle for f and an ancilla qubit, get $\frac{1}{\sqrt{2^n}}\sum_{i=0}^{2^n-1}\underset{H(|1\rangle)\text{ (and } |1\rangle = NOT(|0\rangle))}{\underset{\parallel}{|-\rangle}}|i\rangle \rightsquigarrow \frac{1}{\sqrt{2^n}}\sum_{i=0}^{2^n-1}(-1)^{f(i)}|-\rangle|i\rangle$.

Step 3. Apply $H^{\otimes n}$ again. Possible outcomes:

$$\star\ \frac{1}{2^n}\sum_{i=0}^{2^n-1}(-1)^{f(i)}\sum_{j=0}^{2^n-1}(-1)^{i\cdot j}|j\rangle = \begin{cases} |0\rangle, & f\equiv 0 \\ -|0\rangle, & f\equiv 1 \\ \sum_{i=1}^{2^n-1} d_i|i\rangle, & f \text{ is balanced} \end{cases}$$

Indeed, let's compute the amplitude of $|0\rangle$ in $\star$:

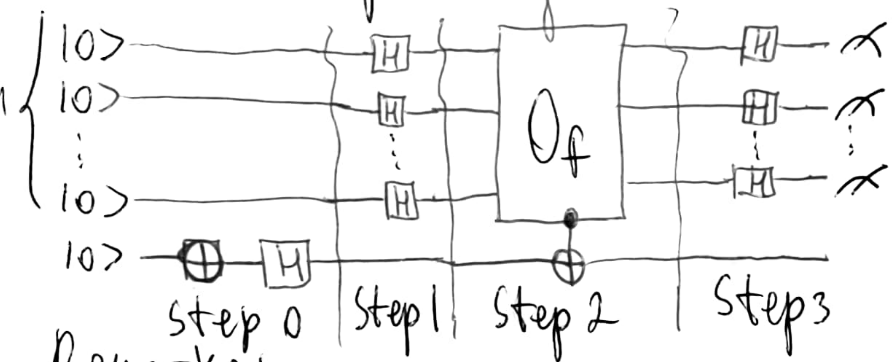
$f\equiv 0$: $\frac{1}{2^n}\sum_{i=0}^{2^n-1}(-1)^0\cdot(-1)^{i\cdot 0} = \frac{2^n}{2^n} = 1$;

$f\equiv 1$: $\frac{1}{2^n}\sum_{i=0}^{2^n-1}(-1)^1\cdot(-1)^{i\cdot 0} = \frac{-2^n}{2^n} = -1$;

f is balanced: $\frac{1}{2^n}\sum_{i=0}^{2^n-1}(-1)^{f(i)}\cdot(-1)^{i\cdot 0} = \frac{1}{2^n}\sum_{i=0}^{2^n-1}(-1)^{f(i)} = 0$

Rmk. We applied f just once (to the vector $\frac{1}{\sqrt{2^n}}\sum_{i=0}^{2^n-1}|i\rangle$).

The corresponding circuit is depicted below:



Remarks:

① $\oplus$ acts on $|-\rangle$ via mapping to $-|-\rangle$. Indeed, $NOT\left(\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right) = \frac{1}{\sqrt{2}}(|1\rangle - |0\rangle) = -|-\rangle$.

② O_f is the oracle, i.e. black box computing f, given initially to us.

③ Step 0 'prepares' a $|-\rangle$ vector from $|0\rangle$.

④ The symbol '$\measuredangle$' stands for 'measure'