Day 2: Quantum Algorithms

21.07.2020

Overview:

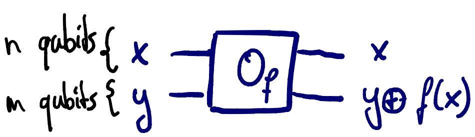
I.) Deutsch-Jozsa algorithm: Oracles, DJ theory, implementation with Qiskit

II.) Grover's algorithm: Grover theory, amplitude amplification, implementation with Qiskit

I. Deutsch-Jozsa algorithm

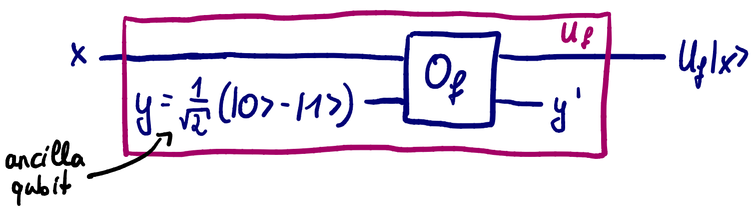
Oracles

- assume we have access to an oracle, e.g. a physical device that we cannot look inside, to which we can pass queries and which returns answers
  $\Rightarrow$ goal: determine some property of the oracle using the minimal number of queries
- on a classical computer, such an oracle is given by a fct. $f: \underbrace{\{0,1\}^n}_{\text{input string}} \to \underbrace{\{0,1\}^m}_{\text{output string}}$
- on a quantum computer, the oracle must be reversible:



O_f: bit oracle, can be seen as a unitary which performs the map $O_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$

$\rightarrow$ for $f: \{0,1\}^n \to \{0,1\}$, we can construct U_f:



$$O_f|x\rangle|y\rangle = \frac{1}{\sqrt{2}}\left(|x\rangle|0 \oplus f(x)\rangle - |x\rangle|1 \oplus f(x)\rangle\right) = \begin{cases} \frac{1}{\sqrt{2}}|x\rangle(|0\rangle - |1\rangle) = |x\rangle|y\rangle, & \text{if } f(x) = 0 \\ \frac{1}{\sqrt{2}}|x\rangle(|1\rangle - |0\rangle) = -|x\rangle|y\rangle, & \text{if } f(x) = 1 \end{cases}$$

$$= (-1)^{f(x)}|x\rangle|y\rangle$$

$\Rightarrow$ indep. of $|y\rangle$ $\Rightarrow$ U_f: phase oracle, which performs the map $U_f|x\rangle = (-1)^{f(x)}|x\rangle$

Hadamard on n qubits: recall that $H|0\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $H|1\rangle = |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

⇒ for $x \in \{0,1\}$: $|x\rangle - \boxed{H} - |y\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x |1\rangle) = \frac{1}{\sqrt{2}}((-1)^{0\cdot x}|0\rangle + (-1)^{1\cdot x}\cdot|1\rangle)$

$$= \frac{1}{\sqrt{2}} \sum_{k\in\{0,1\}} (-1)^{k\cdot x} |k\rangle$$

⇒ for $x \in \{0,1\}^n$:

$$|x\rangle \left\{ \begin{array}{l} |x_0\rangle - \boxed{H} - |y_0\rangle \\ |x_1\rangle - \boxed{H} - |y_1\rangle \\ \quad\vdots \qquad\qquad \vdots \\ |x_{n-1}\rangle - \boxed{H} - |y_{n-1}\rangle \end{array} \right\} |y\rangle = H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{k\in\{0,1\}^n} (-1)^{\overset{\text{inner product}}{k\cdot x}} |k\rangle$$

↳ every $|y_i\rangle$ is either $|+\rangle$ or $|-\rangle$
⇒ $|y\rangle$ must be a superposition of all possible 2^n bit strings

e.g. $|x\rangle = |01\rangle$:

$$\left. \begin{array}{l} |0\rangle - \boxed{H} - |+\rangle \\ |1\rangle - \boxed{H} - |-\rangle \end{array} \right\} |y\rangle = |+\rangle \otimes |-\rangle = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$$

Deutsch-Jozsa algorithm

- We are given a function $f: \{0,1\}^n \to \{0,1\}$, realized by an oracle, of which we know that it is either constant (→ all inputs map to the same output) or balanced (# inputs that map to '0' and '1' is equal)
- Goal: Determine whether f is constant or balanced
- classical solution: we need to ask the oracle at least twice, but if we get twice the same output, we need to ask again, ...

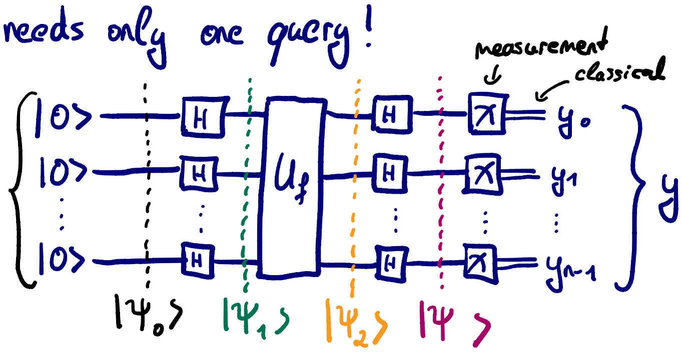
  → at most $\frac{N}{2} + 1 = 2^{n-1} + 1$ queries, n: # input bits, $N = 2^n$: # realizable bit strings

  demonstrative example: 2^n different ways to throw a coin → is the coin fair?

- quantum solution: needs only one query!

Circuit for DJ:

n qubits



Claim: If the outcome y equals the bitstring $\underbrace{00\ldots0}_{n}$, then f is constant, otherwise it is balanced

Proof: Let us check the state after every step:

- $|\psi_0\rangle = |00\ldots0\rangle = |0\rangle^{\otimes n}$
- $|\psi_1\rangle = H^{\otimes n}|\psi_0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} \underbrace{(-1)^{\overset{00\ldots0}{\overset{\shortparallel}{x\cdot\psi_0}}}}_{=+1} |x\rangle = \frac{1}{\sqrt{2^n}} \cdot \sum_{x\in\{0,1\}^n} |x\rangle$
- $|\psi_2\rangle = U_f \cdot |\psi_1\rangle \underset{\text{linearity}}{=} \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} U_f|x\rangle = \frac{1}{\sqrt{2^n}} \cdot \sum_{x\in\{0,1\}^n} (-1)^{f(x)} \cdot |x\rangle$
- $|\psi_3\rangle = H^{\otimes n} \cdot |\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} \cdot H^{\otimes n}|x\rangle = \frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} \cdot \sum_{k\in\{0,1\}^n} (-1)^{k\cdot x} \cdot |k\rangle$

$$= \sum_{k\in\{0,1\}^n} \underbrace{\left[\frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{f(x)+k\cdot x}\right]}_{=:c_k} \cdot |k\rangle =: \sum_{k\in\{0,1\}^n} c_k |k\rangle$$

$\Rightarrow$ probability to measure the zero-string $|00\ldots0\rangle$:

$$P[y=00\ldots0] \overset{\text{Born rule}}{=} |\langle 00\ldots0|\psi_3\rangle|^2 = \Big|\sum_{k\in\{0,1\}^n} c_k \cdot \underbrace{\langle 00\ldots0|k\rangle}_{=\begin{cases}1, & k=00\ldots0\\ 0, & \text{else (orthogonal)}\end{cases}}\Big|^2 = |c_{00\ldots0}|^2$$

$$= \Big|\frac{1}{2^n} \cdot \underbrace{\sum_{x\in\{0,1\}^n} (-1)^{f(x)}}_{=\begin{cases}+2^n, & \text{if } f(x)\equiv 0\\ -2^n, & \text{if } f(x)\equiv 1\\ 0, & \text{if } f(x) \text{ balanced}\end{cases}}\Big|^2 = \begin{cases}1, & \text{if } f \text{ const.}\\ 0, & \text{if } f \text{ balanced}\end{cases}$$

$\blacksquare$