Day 2: Quantum Algorithms

21.07.2020

<u>Overview:</u>

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

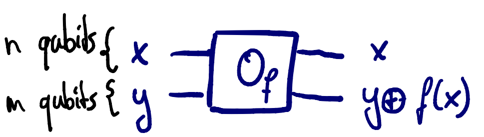
Oracles

- 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

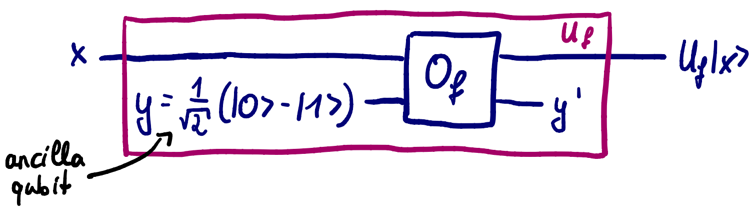
- on a classical computer, such an oracle is given by a fct. $f: \underbrace{\{0,1\}^n}_{\text{input string}} \rightarrow \underbrace{\{0,1\}^m}_{\text{output string}}$

- 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 $f: \{0,1\}^n \rightarrow \{0,1\}$, 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 $U_f|x\rangle = (-1)^{f(x)}|x\rangle$

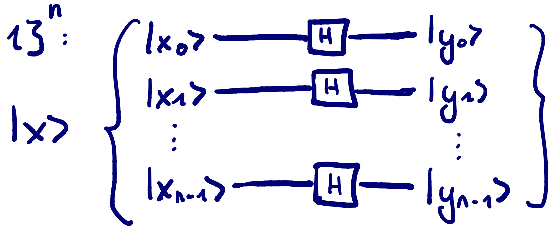
Hadamard on n qubits:

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

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

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

$\Rightarrow$ for $x \in \{0,1\}^n$:

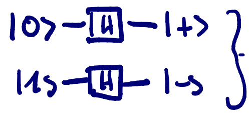


$$|y\rangle = H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{k\in\{0,1\}^n} (-1)^{\overset{\text{inner product}}{\downarrow}\, k\cdot x} |k\rangle$$

$\hookrightarrow$ every $|y_i\rangle$ is either $|+\rangle$ or $|-\rangle$

$\Rightarrow$ $|y\rangle$ must be a superposition of all possible 2^n bit strings

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



$|y\rangle = |+\rangle \otimes |-\rangle = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$

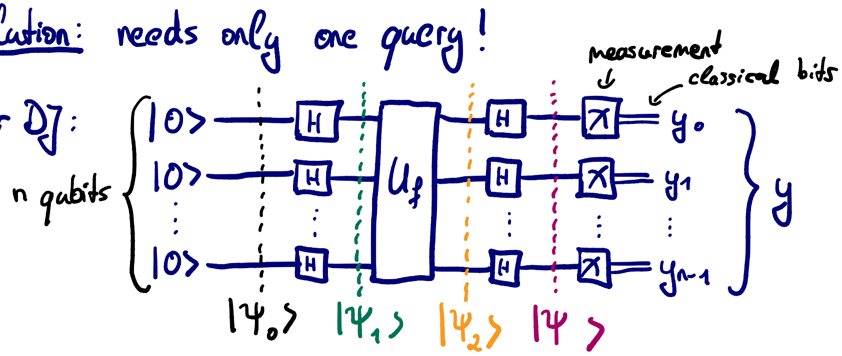
Deutsch-Jozsa algorithm

- 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 ($\to$ 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, ...

  $\to$ 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 $\to$ is the coin fair?
- quantum solution: needs only one query!

Circuit for DJ:



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:

- $|\Psi_0\rangle = |00\ldots0\rangle = |0\rangle^{\otimes n}$
- $|\Psi_1\rangle = H^{\otimes n}|\Psi_0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} \underbrace{(-1)^{x\cdot\Psi_0}}_{=+1} |x\rangle = \frac{1}{\sqrt{2^n}} \cdot \sum_{x\in\{0,1\}^n} |x\rangle$, where $\Psi_0 = 00\ldots0$
- $|\Psi_2\rangle = U_f \cdot |\Psi_1\rangle \overset{\text{linearity}}{=} \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} U_f|x\rangle = \frac{1}{\sqrt{2^n}} \cdot \sum_{x\in\{0,1\}^n} (-1)^{f(x)} \cdot |x\rangle$
- $|\Psi_3\rangle = H^{\otimes n} \cdot |\Psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} \cdot H^{\otimes n}|x\rangle = \frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} \cdot \sum_{k\in\{0,1\}^n} (-1)^{k\cdot x} \cdot |k\rangle$

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

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

$$P[y=00\ldots0] \overset{\text{Born rule}}{=} |\langle 00\ldots0|\Psi_3\rangle|^2 = \Big|\sum_{k\in\{0,1\}^n} c_k \cdot \underbrace{\langle 00\ldots0|k\rangle}_{=\begin{cases}1, & k=00\ldots0\\ 0, & \text{else (orthogonal)}\end{cases}}\Big|^2 = |c_{00\ldots0}|^2$$

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

$\blacksquare$

II. Grover's algorithm

- algorithm "searching an unsorted database" with $N = 2^n$ elements in $\mathcal{O}(\sqrt{N})$ time   rather: find x s.t. $f(x) = 1$

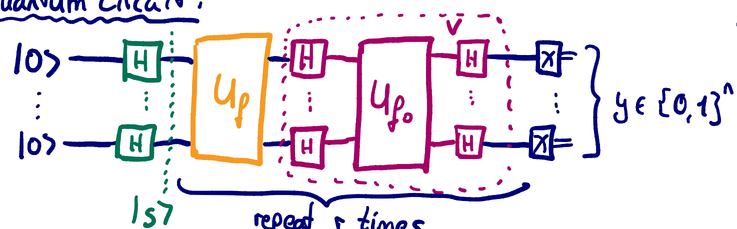
  $\rightsquigarrow$ classical alg. needs on average $\frac{N}{2} = \mathcal{O}(N)$ time

- goal: find ω, given an oracle U_f with $f: \{0,1\}^n \to \{0,1\}$, $f(x) = \begin{cases} 1, & \text{if } x = \omega \\ 0, & \text{else} \end{cases}$, $f_0(x) = \begin{cases} 0, & \text{if } x = 00..0 \\ 1, & \text{else} \end{cases}$

  phase oracle: $U_f |x\rangle = (-1)^{f(x)} |x\rangle$ $\Rightarrow$ $U_f: |\omega\rangle \to -|\omega\rangle$, $|x\rangle \to |x\rangle \; \forall x \neq \omega$ $\Rightarrow U_{f_0}: |0\rangle^{\otimes n} \to |0\rangle^{\otimes n}$, $|x\rangle \to -|x\rangle \; \forall x \neq 00..0$

  $\hookrightarrow U_f = \mathbb{1} - 2|\omega\rangle\langle\omega|$ $\hookrightarrow U_{f_0} = 2|0\rangle\langle 0|^{\otimes n} - \mathbb{1}$

- quantum circuit:



Claim: $y = \omega$ (with high prob.)

Proof: Let us define the uniform superposition state $|s\rangle := H^{\otimes n} |0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle$

and $V := H^{\otimes n} \cdot U_{f_0} \cdot H^{\otimes n} = H^{\otimes n} \cdot 2|0\rangle\langle 0|^{\otimes n} \cdot H^{\otimes n} - H^{\otimes n} H^{\otimes n} = 2|s\rangle\langle s| - \mathbb{1}$

$\Rightarrow$ Grover's algorithm carries out the operation $(V \cdot U_f)^r$ on the state $|s\rangle$.

Let Σ be the plane spanned by $|s\rangle$ and $|\omega\rangle$ and let $|\omega^\perp\rangle$ be the state orthogonal to $|\omega\rangle$ in Σ: $|\omega^\perp\rangle := \frac{1}{\sqrt{2^n - 1}} \sum_{x \neq \omega} |x\rangle$

$\Rightarrow |s\rangle = \sqrt{\frac{2^n - 1}{2^n}} |\omega^\perp\rangle + \frac{1}{\sqrt{2^n}} |\omega\rangle =: \cos\frac{\theta}{2} |\omega^\perp\rangle + \sin\frac{\theta}{2} |\omega\rangle$

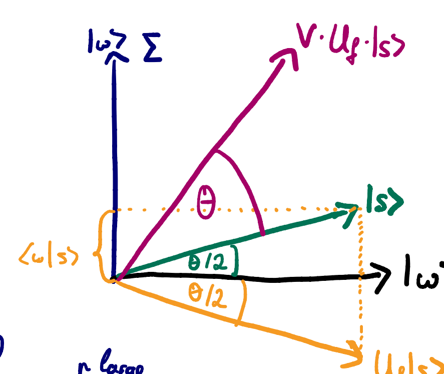
define θ s.t. $\sin\frac{\theta}{2} = \frac{1}{\sqrt{2^n}}$
$\Rightarrow \theta = 2 \cdot \arcsin \frac{1}{\sqrt{2^n}}$

protocol:

1.) Prepare $|s\rangle$

2.) Apply $U_f = \mathbb{1} - 2|\omega\rangle\langle\omega|$ $\rightsquigarrow$ reflection at $|\omega^\perp\rangle$

3.) Apply $V = 2|s\rangle\langle s| - \mathbb{1}$ $\rightsquigarrow$ reflection at $|s\rangle$



$\Rightarrow V \cdot U_f$ corresponds to a rotation by an angle θ

$\Rightarrow$ after r applications of 2.) & 3.), the state is rotated by $r \cdot \theta$

$\hookrightarrow$ choose r, s.t. $r \cdot \theta + \frac{\theta}{2} \overset{!}{=} \frac{\pi}{2}$ $\Rightarrow r = \frac{\pi}{2\theta} - \frac{1}{2} = \frac{\pi}{4 \cdot \arcsin \frac{1}{\sqrt{2^n}}} - \frac{1}{2} \overset{n \text{ large}}{\approx} \frac{\pi}{4}\sqrt{2^n} = \mathcal{O}(\sqrt{N})$

$\Rightarrow$ after r calls to the oracle, the final meas. will result in state $|\omega\rangle$ with min. probability

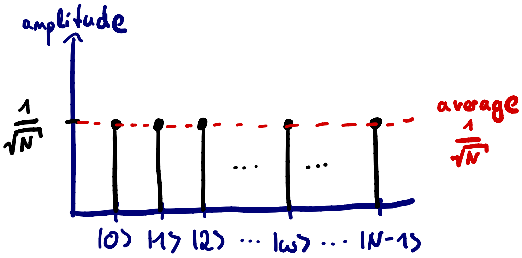
$$p(\omega) \geq 1 - \sin^2\frac{\theta}{2} = 1 - \frac{1}{2^n}$$ (if )

$\square$

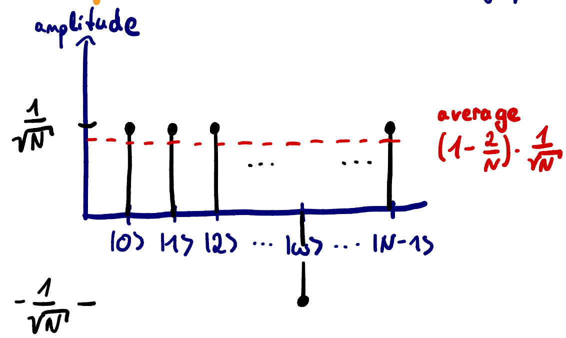
Amplitude amplification

The general idea behind Grover's algorithm is amplitude amplification. Let us have a look at the amplitudes at each step in Grover's algorithm:

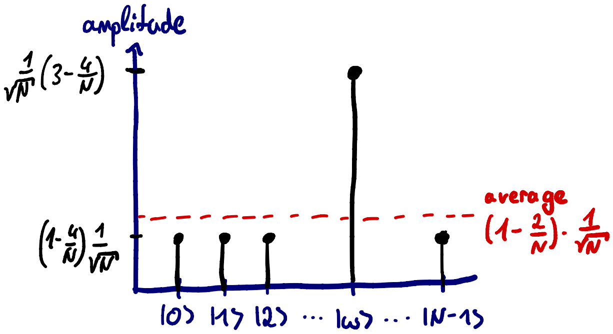
1.) $|s\rangle := H^{\otimes n}|0\rangle^{\otimes n}$



2.) $U_f|s\rangle = (\mathbb{1} - 2|\omega\rangle\langle\omega|)|s\rangle$ → flip amplitude of $|\omega\rangle$



3.) $V\cdot U_f\cdot|s\rangle = (2|s\rangle\langle s| - \mathbb{1})\cdot U_f\cdot|s\rangle$ → reflect amplitudes about the average amplitude



as for $|\psi\rangle := \sum_i \alpha_i |i\rangle$ $\quad V|\psi\rangle$ yields:

$$(2|s\rangle\langle s| - \mathbb{1})\cdot|\psi\rangle = 2\cdot\frac{1}{N}\cdot\sum_j |j\rangle\cdot\sum_k\langle k|\cdot\sum_i \alpha_i|i\rangle - \sum_i\alpha_i|i\rangle$$

$$= 2\cdot\frac{\sum_k \alpha_k}{N}\cdot\sum_j|j\rangle - \sum_j \alpha_j|j\rangle$$

$$= \sum_j \underbrace{\left(2\cdot\langle\alpha\rangle - \alpha_j\right)}_{\text{reflection of } \alpha_j \text{ about average } \langle\alpha\rangle}|j\rangle$$

(→ if $\alpha_j = \langle\alpha\rangle + \Delta$ then $\alpha_j' = 2\langle\alpha\rangle - \alpha_j = \langle\alpha\rangle - \Delta$)

⇒ by repeating step 2) & 3), the amplitude of $|\omega\rangle$ will increase further ⇒ amplitude amplification!

Multiple marked elements

When we have M marked elements ω_i, we define the winning state as

$$|\omega\rangle := \frac{1}{\sqrt{M}}\sum_{i=1}^{M}|\omega_i\rangle \quad\rightarrow\quad |\omega^\perp\rangle = \frac{1}{\sqrt{N-M}}\cdot\sum_{x\notin\{\omega_1,\dots,\omega_M\}}|x\rangle$$

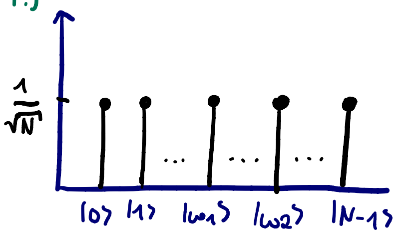
$$\Rightarrow |s\rangle = \frac{\sqrt{N-M}}{\sqrt{N}}\cdot|\omega^\perp\rangle + \sqrt{\frac{M}{N}}\cdot|\omega\rangle =: \cos\frac{\theta}{2}\,|\omega^\perp\rangle + \sin\frac{\theta}{2}\,|\omega\rangle$$

$$\Leftrightarrow \sin\frac{\theta}{2} = \sqrt{\frac{M}{N}}$$ ⇒ angle becomes larger!

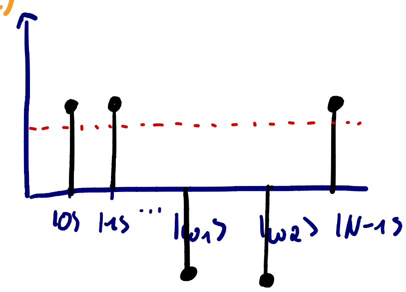
$$\Rightarrow r = \frac{\pi}{4\cdot\arcsin\left(\sqrt{\frac{M}{N}}\right)} - \frac{1}{2} = \mathcal{O}\left(\sqrt{\frac{N}{M}}\right)$$

→ we can see this speedup also when looking at the amplitudes:

1.)

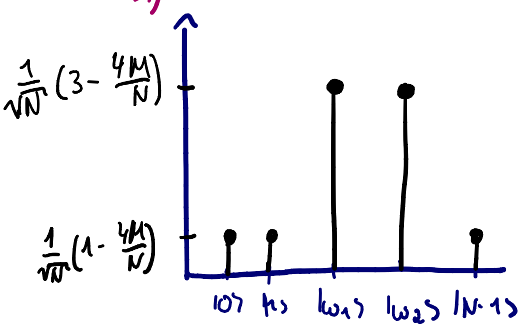


2.)



average $\left(1-\frac{2M}{N}\right)\cdot\frac{1}{\sqrt{N}}$

3.)



⇒ goes faster