Computational basis states & Hadamard

given $N = 2^n$, we can identify

$\{0,1,2,\dots,N-1\}$ with $\{0,1\}^n$ by binary representation

Accordingly for $i \in \{0,1\}^n$

$|i\rangle = |i_1,\dots,i_n\rangle$ is a computational basis state which is also associated with a number in $\{0,1,\dots 2^n-1\}$.

Let H be the Hadamard gate. Determine

$$H^{\otimes n}|i\rangle = \frac{1}{\sqrt{2^n}} \sum_{j\in\{0,1\}^n} (-1)^{i\cdot j} |j\rangle \quad \text{for } i\in\{0,1\}^n$$

Deutsch - Jozsa:

Describe the Deutsch - Jozsa problem:

Deutsch - Jozsa (1992)

solution with single oracle call Cleve et al. 1998

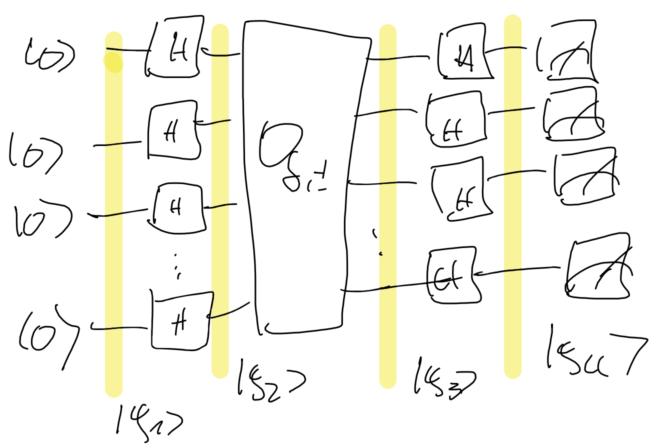
Problem: given $x \in \{0,1\}^N$ with $N = 2^n$

with either

(a) x is constant $\hat{=}$ $x_i = x_j \; \forall i,j$

(b) $N/2$ of the $x_i = 0$ and $\frac{N}{2}$ of the $x_i = 1$ (balanced)

quantum algorithm



$$\Rightarrow |\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{i \in \{0,1\}^n} |i\rangle$$

$$|\psi_3\rangle = O_{f,\pm} \left(\frac{1}{\sqrt{2^n}} \sum_{i \in \{0,1\}^n} |i\rangle \right)$$

$$= \frac{1}{\sqrt{2^n}} \sum_{i \in \{0,1\}^n} (-1)^{x_i} |i\rangle$$

$$|\psi_4\rangle = \frac{1}{2^n} \sum_{i \in \{0,1\}^n} (-1)^{x_i} \sum_{j \in \{0,1\}^n} (-1)^{i \cdot j} |j\rangle$$

$$= \frac{1}{2^n} \sum_{i \in \{0,1\}^n} \sum_{j \in \{0,1\}^n} (-1)^{x_i + i \cdot j} |j\rangle$$

What is the coefficient of $|0\rangle^{\otimes n}$?

answer: $i \cdot 0 = 0 \Rightarrow$ have to consider

$$\frac{1}{2^n} \sum_{i \in \{0,1\}^n} (-1)^{x_i} = \begin{cases} 1 & \text{if all } x_i = 0 \\ -1 & \text{if all } x_i = 1 \\ 0 & \text{if } x \text{ is balanced} \end{cases}$$

$\Rightarrow$ Final measurement gives $|0\rangle^{\otimes n}$ with prob. 1 if and only if x is constant.

classical algorithm

deterministic without error:

need in worst-case scenario $2^{n-1}+1$ queries

$\Rightarrow$ exponential separation

randomized algorithm

check k randomly chosen x_i
if they are all equal assume
x constant otherwise assume x balanced.

error prob. decreases exponentially with k in case of balanced case.

$\Rightarrow O(1) \Rightarrow$ No quantum speed-up

:(

Simon's Algorithm

First exponential speed-up !

Problem: • $N = 2^n$ identify $\{0,\dots,N-1\}$ with $\{0,1\}^n$

• entrywise addition: $\xi, s \in \{0,1\}^n$: $\xi \oplus s \mathrel{\hat{=}}$ entrywise addition mod2

- example: $(1\,0\,1) \oplus (1\,0\,0) = (0\,0\,1)$

promise: $X = (x_0, \dots, x_{N-1})$ with $x_i \in \{0,1\}^n$

$$\begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ \vdots \\ x_{N-1} \end{bmatrix} = \begin{bmatrix} x_0^0 & x_0^1 & \cdots & x_0^{n-1} \\ \vdots & & & \\ \vdots & & & \\ x_{N-1}^0 & x_{N-1}^2 & \cdots & x_{N-1}^{n-1} \end{bmatrix}$$

there is $s \in \{0,1\}^n$, $s \neq (0,\dots,0)$ s.t.

$x_i = x_\xi$ iff $\underline{i = \xi}$ or $\underline{i = \xi \oplus s}$

Task: find s

Note: Each string appears exactly twice: $x_i = x_{i \oplus s}$ but there

no other pairs $(j, j \oplus s)$

with the same string

Classical algorithm

query k strings at random

$(i_1, i_2, \dots, i_k)$

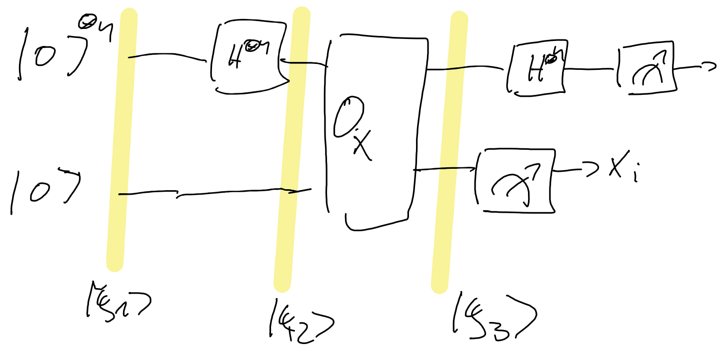
if $x_{i_r} = x_{i_e} \Rightarrow s = i_e + i_r$

done

Birthday paradox: $O(2^{n/2})$

Lecture notes: matching lower bound.

Quantum algorithm



Determine $|\psi_1\rangle$, $|\psi_2\rangle$ & $|\psi_3\rangle$

$$|\psi_1\rangle = |0\rangle^{\otimes n}$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{i \in \{0,1\}^n} |i\rangle$$

$$|\psi_3\rangle = \frac{1}{\sqrt{2^n}} \sum_{i \in \{0,1\}^n} |i\rangle |x_i\rangle$$

$$|\psi_3\rangle = \frac{1}{\sqrt{2^n}} \sum_{i \in \{0,1\}^n} |i\rangle |x_i\rangle$$

Measurement of second register gives random result x_i

x_i corresponds to exactly two strings $i, i \oplus s$

$$\Rightarrow |\psi_4\rangle = \frac{1}{\sqrt{2}} \left(|i\rangle + |i \oplus s\rangle \right) |x_i\rangle$$

Now ignore second register & apply Hadamard:

$$H^{\otimes n} \left(\frac{1}{\sqrt{2}} \left(|i\rangle + |i \oplus s\rangle \right) \right) = \frac{1}{\sqrt{2}} \left(H^{\otimes n} |i\rangle + H^{\otimes n} |i \oplus s\rangle \right)$$

$$= \sum_{\xi \in \{0,1\}^n} \left((-1)^{i \cdot \xi} |\xi\rangle + (-1)^{(i \oplus s) \cdot \xi} |\xi\rangle \right)$$

$$= \sum_{\xi \in \{0,1\}^n} (-1)^{i \cdot \xi} \left(1 + (-1)^{s \cdot \xi} \right) |\xi\rangle$$

Measure: $\left(1 + (-1)^{s \cdot \xi} \right) \neq 0$ only for $s \cdot \xi = 0$

$\Rightarrow$ observe random outcome ξ, which satisfies $s \cdot \xi = 0$

$\Rightarrow$ partial knowledge about s

Observation: if we obtain $n-1$ linear independent $\{ y_1, \dots, y_{n-1} \}$ we can solve the linear eq.

$$\begin{aligned} y_1 \cdot s &= 0 \\ y_2 \cdot s &= 0 \quad \Rightarrow \text{get } s \\ &\vdots \\ y_{n-1} \cdot s &= 0 \end{aligned}$$

There are 2^{n-1} vectors that satisfy $y \cdot s = 0$

Hence running the algorithm $O(n)$ times will produce $n-1$ linear independent y_e with high probability.