Quantum computation: lecture 5

- Simon's problem
- Classical method(s) of resolution
- Simon's quantum algorithm

  Part I: quantum circuit

Simon's problem

Let $f : \{0,1\}^n \to X$ be a function

such that $f(x) = f(y)$ iff:

- either $x = y$
- or $x \oplus a = y$ for some $a \in \{0,1\}^n \setminus \{0\}$

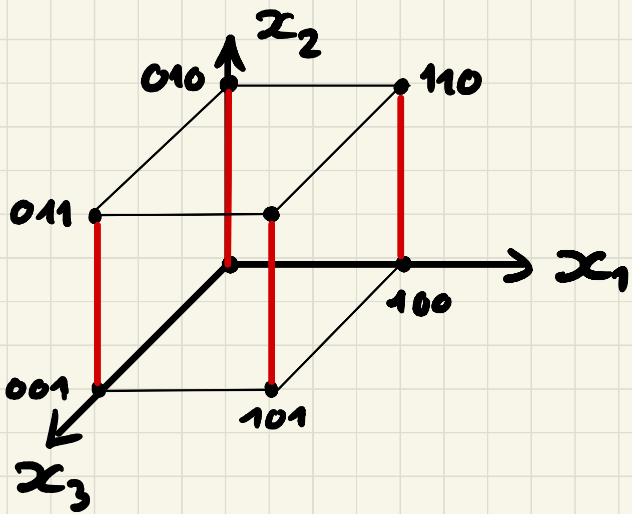
NB: • X to be defined later

- a is unknown

Our aim: to discover the value of $a \neq 0$ by asking as few questions as possible to the oracle f.

- **Classically**, this requires $O(2^n)$ calls (see below)
- Simon's quantum algorithm finds the vector a with probability $\geq 1-\varepsilon$ in runtime $\mathrm{poly}(n) \cdot |\log \varepsilon|$ (& similar number of calls to the oracle)

Example with $n=3$



$a = (0,1,0)$

$f(x \oplus a) = f(x) \quad \forall x \in \{0,1\}^3$

Image space X must be of cardinality 4 here.

In general, $|X| = \frac{2^n}{2} = 2^{n-1}$.

Classical algorithm

- draw randomly pairs of points in $\{0,1\}^n$ (with replacement) : $(x^{(1)}, y^{(1)}) \dots (x^{(q)}, y^{(q)})$
- if for one such pair (say j), $f(x^{(j)}) = f(y^{(j)})$, compute $a = x^{(j)} \ominus y^{(j)}$ ($= x^{(j)} \oplus x^{(j)}$ by the way) and declare success
- on the contrary, if $f(x^{(j)}) = f(y^{(j)})$ $\forall 1 \leq j \leq q$ then declare failure

Lemma

$$\mathbb{P}(\text{success}) \leq \frac{q}{2^n - 1}$$

(So in order to ensure $\mathbb{P}(\text{success}) \geq 1-\varepsilon$, $q \geq (2^n-1)(1-\varepsilon)$ draws are needed)

Proof: $\mathbb{P}(\text{success}) = \mathbb{P}\left(\exists\, 1 \leq j \leq q \text{ with } f(x^{(j)}) = f(y^{(j)})\right)$

$$\leq \sum_{j=1}^{q} \underbrace{\mathbb{P}\left(f(x^{(j)}) = f(y^{(j)})\right)}_{= \frac{1}{2^n-1}} \leq q/_{2^n-1} \quad \#$$

(for a given x, there is a unique corr. y)

Slightly better (classical) algorithm

Bday pb: random sampling in a set on N elements

$\longrightarrow$ order $\sqrt{N}$ trials until you see two identical elements

$\Rightarrow O(2^{n/2})$ draws needed only,

but this is still exponential in n

Slight generalization

$G = \{0,1\}^n$ = group = vector space

H = sub-group of G & sub-vector space

unknown

$= \text{span}\{h^{(1)}, \ldots, h^{(k)}\}$ k-dimensional subspace

lin. independent

$f : \{0,1\}^n \longrightarrow X$ s.t. $f(x) = f(y)$

iff $x \oplus y \in H$

Cardinalities

- $|G| = 2^n$
- H k-dimensional $\Longrightarrow |H| = 2^k$
- so f takes possibly 2^{n-k} values $= |X|$

A possible option for X is therefore $X = G/H$

quotient group

with $|X| = |G/H| = |G|/|H| = 2^{n-k}$

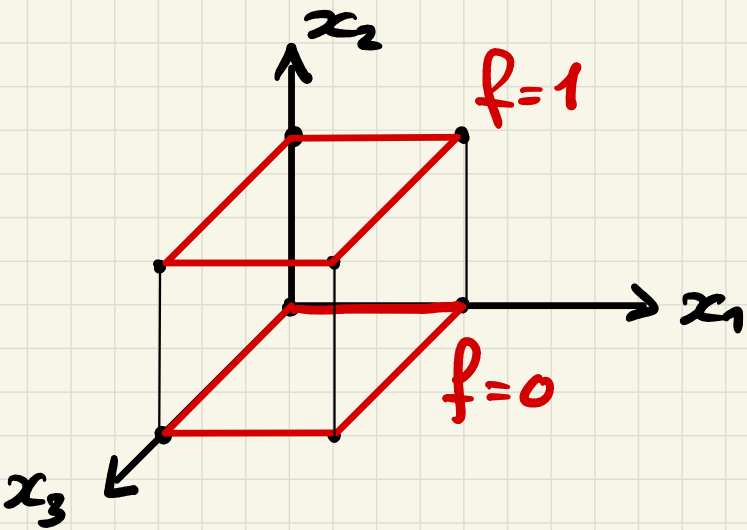
Lagrange's thm

- <u>Equivalence relation</u>: $x \sim y$ iff $x \oplus y \in H$
- The group G can then be divided into 2^{n-k} <u>equivalence classes</u>, namely there exist $v^{(1)} \dots v^{(2^{n-k})}$, representatives of each class, such that

$$G = \bigsqcup_{j=1}^{2^{n-k}} \{ v^{(j)} \oplus H \}$$

disjoint union

Example with $n = 3$ & $k = 2$:



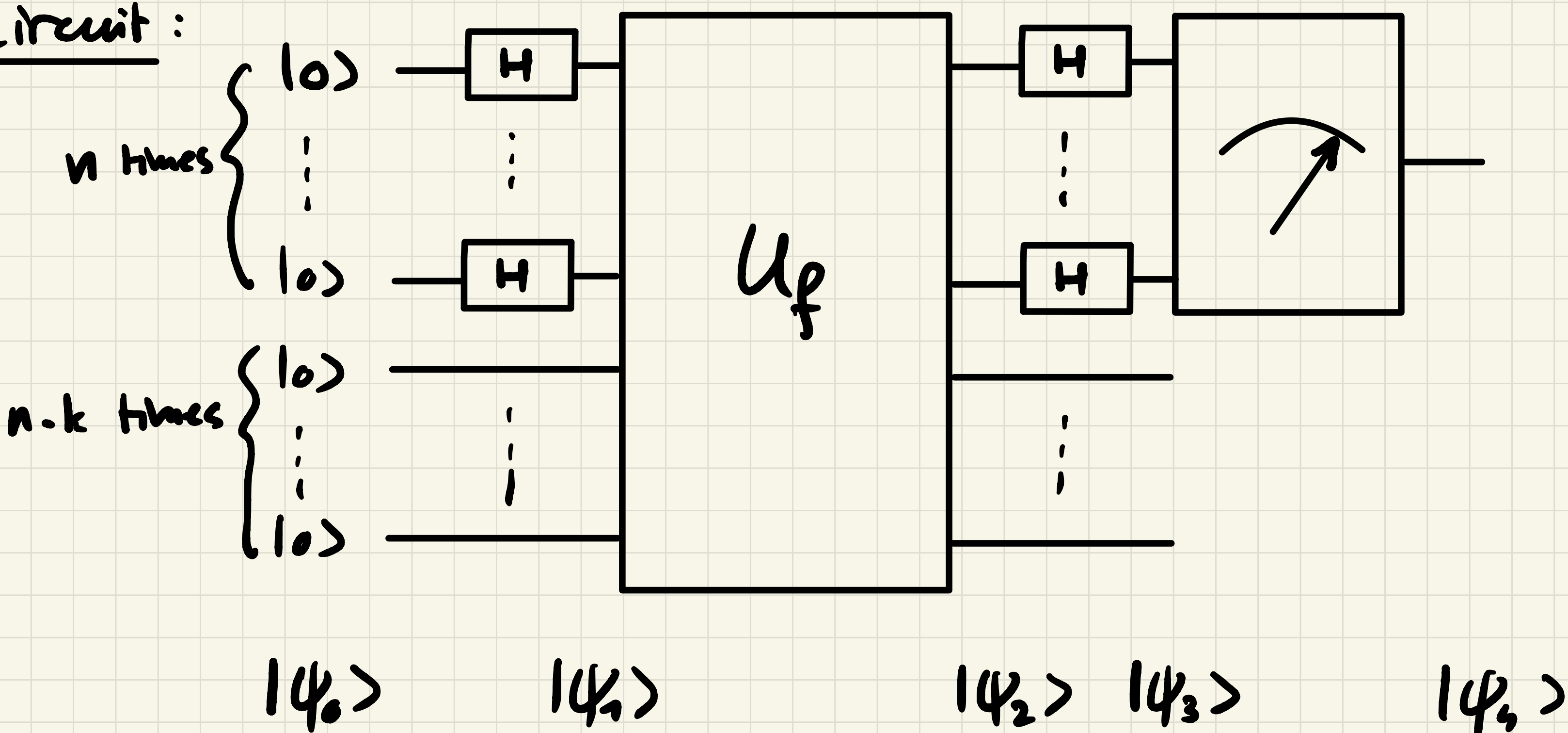
$$H = \{(0,0,0), (1,0,0), (0,1,0), (1,1,0)\}$$

$$|X| = 2$$

eq. classes are H & $H \oplus (0,1,0)$

Simon's quantum algorithm

Circuit:



Stage 0: $|\psi_0\rangle = \underbrace{|0\rangle \otimes \dots \otimes |0\rangle}_{n \text{ times}} \otimes \underbrace{|0\rangle \otimes \dots \otimes |0\rangle}_{n-k \text{ times}}$

Stage 1:

$$|\psi_1\rangle = \left(H^{\otimes n} \otimes I_{n-k}\right) |\psi_0\rangle$$

$$= H^{\otimes n} |0\dots0\rangle \otimes |0\dots0\rangle$$

$$= \frac{1}{2^{n/2}} \sum_{x_1 \dots x_n \in \{0,1\}} |x_1 \dots x_n\rangle \otimes |0\dots0\rangle$$

$$= \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} |x\rangle \otimes |0\dots0\rangle$$

Note that contrary to the D-J algorithm, the n-k ancilla bits are left untouched before the passage through the oracle U_f.

<u>Stage 2</u>: The oracle U_f is defined as:

$$U_f(|x\rangle \otimes |y\rangle) = |x\rangle \otimes |y \oplus f(x)\rangle$$

but here, both y & $f(x)$ are $(n-k)$-dimensional.

So $|\psi_2\rangle = U_f|\psi_1\rangle = \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} |x\rangle \otimes |f(x)\rangle$

<u>Stage 3</u>:

Again, following what was done for D-J's algorithm, we have:

$$H^{\otimes n}|x\rangle = \frac{1}{2^{n/2}} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle$$

so

$$|\psi_3\rangle = \left(H^{\otimes n} \otimes I\right)|\psi_2\rangle = \frac{1}{2^n} \sum_{x,y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle \otimes |f(x)\rangle$$

Let us rewrite this:

Let $v^{(1)} \dots v^{(2^{n-k})}$ be the representatives of the equivalence classes of G.

$$|\psi_3\rangle = \sum_{y \in \{0,1\}^n} \frac{1}{2^n} \sum_{j=1}^{2^{n-k}} \sum_{h \in H} (-1)^{(v^{(j)} \oplus h) \cdot y} \, |y\rangle \otimes |\underbrace{f(v^{(j)} + h)}_{= f(v^{(j)}) = f_j}\rangle$$

(The sum over the x's has been split into two sums: $\sum_{j=1}^{2^{n-k}} \sum_{h \in H}$)

So

$$|\psi_3\rangle = \sum_{y\in\{0,1\}^n} \frac{1}{2^n} \sum_{j=1}^{2^{n-k}} (-1)^{v^{(j)}\cdot y} \left(\sum_{h\in H} (-1)^{h\cdot y}\right) |y\rangle \otimes |f_j\rangle$$

<u>Now</u>: matrix repr: $H = \begin{pmatrix} h^{(1)} \\ \vdots \\ h^{(k)} \end{pmatrix} = k \times n$ matrix

whose kernel $= H^\perp = \{x \in \{0,1\}^n : H \cdot x = 0\}$

is an $(n-k)$-dimensional subspace of $\{0,1\}^n$

(and note that $(H^\perp)^\perp = H$)

(⚠ slight notation overload)

Observe that $\sum_{h \in H} (-1)^{y \cdot h} \in \{0, 2^k\}$:

- if $y \in H^{\perp}$, then $y \cdot h = 0 \quad \forall h \in H$

  so $\sum_{h \in H} (-1)^{y \cdot h} = 2^k$ in this case

- if $y \notin H^{\perp}$, then $\exists h^{(0)} \in H$ s.t. $h^{(0)} \cdot y = 1$, and

  $$\sum_{h \in H} (-1)^{y \cdot h} = \sum_{h' \in H} (-1)^{y \cdot (h^{(0)} + h')} = -\sum_{h' \in H} (-1)^{y \cdot h'}$$

  so this sum is equal to 0.

Finally, we obtain:

$$|\psi_3\rangle = \sum_{y \in H^\perp} \left(\frac{1}{2^{n-k}} \sum_{j=1}^{2^{n-k}} (-1)^{v^{(j)} \cdot h} \right) |y\rangle \otimes |f_j\rangle$$

To be continued next week...