# Quantum computation: lecture 4

- 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 $a \in \{0,1\}^n \setminus \{0\}$

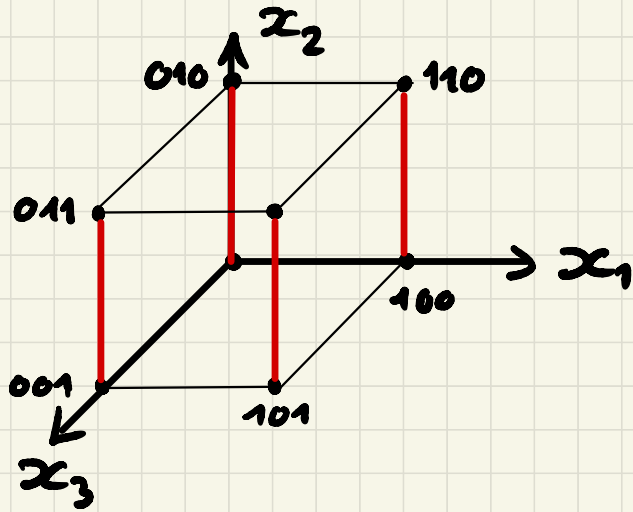NB: · $X$ to be defined later

· $a$ is unknown

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

- <u>Classically</u>, this requires $O(2^n)$ calls (see below)

- Simon's quantum algorithm finds the vector $a$
with probability $\geq 1 - \varepsilon$ in runtime $\text{poly}(n) \cdot |\log \varepsilon|$
(& 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, $|X| = \dfrac{2^n}{2} = 2^{n-1}$.

# Classical algorithm

- draw randomly pairs of points in $\{0,1\}^n$ (with replacement) : $(x^{(1)}, y^{(1)}) \ldots (x^{(q)}, y^{(q)})$

- 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 $f(x^{(j)}) \neq f(y^{(j)})$ $\forall_{1 \leq j \leq q}$ then declare failure

## Lemma

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

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

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

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

$$= \frac{1}{2^n - 1} \quad \left(\begin{array}{l} \text{for a given } x, \text{ there} \\ \text{is a unique corr. } y \end{array}\right)$$

## 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

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

$$H = \text{sub-group of } G \ \& \ \text{sub-vector space}$$

$$\underline{\text{unknown}} \nearrow \quad = \text{span}\{h^{(1)}, \ldots, h^{(k)}\} \quad k\text{-dimensional}$$

$$\underset{\text{lin. independent}}{} \longrightarrow \text{subspace}$$

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

$$\text{iff} \quad x \ominus y \in H$$

## Cardinalities

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

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

with $|X| = |G/H| = |G|/|H| = 2^{n-k}$
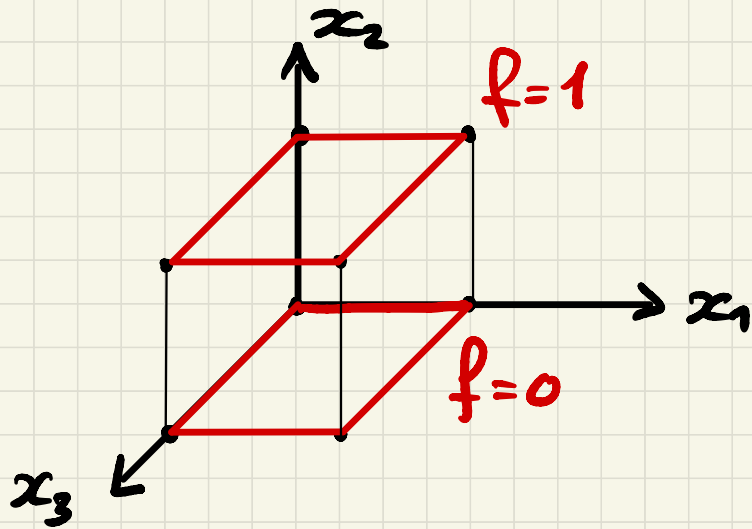
$\downarrow$ Lagrange's thm

$\downarrow$ quotient group

- <u>Equivalence relation</u>: $x \sim y$ iff $x \ominus y \in H$

- The group $G$ can then be divided into $2^{n-k}$ <u>equivalence classes</u>, namely there exist $v^{(1)} \ldots v^{(2^{n-k})}$, representatives of each class, such that

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

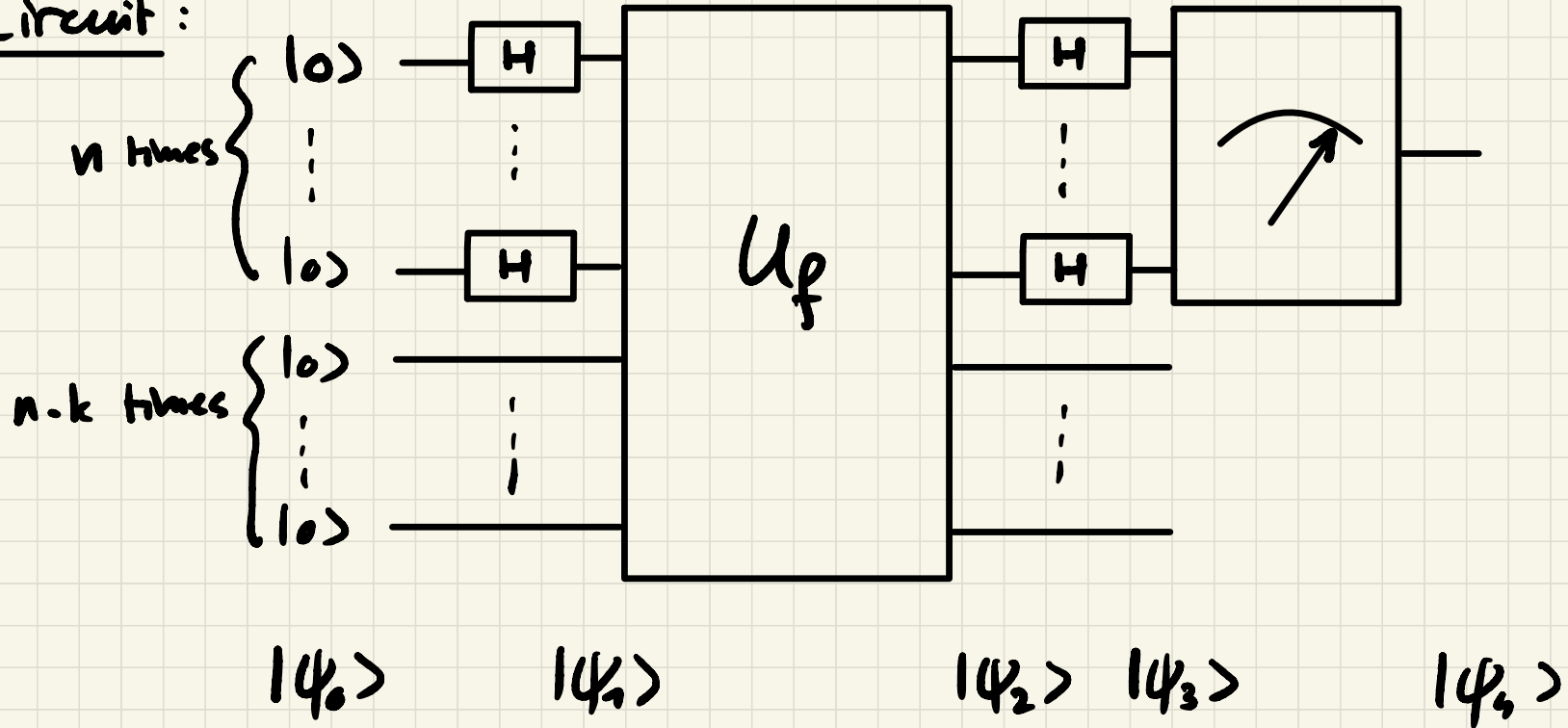disjoint union

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



$x_2$

$f=1$

$x_1$

$f=0$

$x_3$

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

$|X| = 2$

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

# Simon's quantum algorithm



Circuit:

n times $\left\{ \begin{array}{c} |0\rangle \\ \vdots \\ |0\rangle \end{array} \right.$

n-k times $\left\{ \begin{array}{c} |0\rangle \\ \vdots \\ |0\rangle \end{array} \right.$

$H$ — $U_f$ — $H$ — measurement

$|\psi_0\rangle$ $\quad$ $|\psi_1\rangle$ $\quad\quad$ $|\psi_2\rangle$ $\;$ $|\psi_3\rangle$ $\quad\quad$ $|\psi_4\rangle$

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

**Stage 1:**

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

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

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

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

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

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

## Stage 3:

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

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

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

So

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

Now: 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 $\{0,1\}^n$

$\left( \text{and note that } (H^\perp)^\perp = H \right)$

$\left( \triangle \text{ slight notation overload} \right)$

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

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

  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

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

  so this sum is equal to $0$.

Finally, we obtain:

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

To be continued next week...