Simon's algorithm

runs on a quantum computer and solves an "oracle"-problem (see below) exponentially faster than any classical algorithm!

Simon's problem:

given a circuit that implements an unknown function $f: \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ with the property that

$$f(x) = f(x') \iff x = x' \text{ or } x = x' \oplus s \quad (s \neq 0)$$

:

Find s!

(only by choice of inputs x and reading output $f(x)$ of circuit)

Note: $s \in \mathbb{Z}_2^n \setminus \{0\}$ defines a subgroup $H = \{0, s\}$ of $(\mathbb{Z}_2^n, \oplus)$ with the property that $f|x H = \text{const.}$ for all $x \in \mathbb{Z}_2^n$; the task is to find that hidden subgroup H.

Classical algorithm

1) naive trial and error:

- draw random x and $x' \neq x \in \mathbb{Z}_2^n$
- ask oracle: $f(x) \overset{?}{=} f(x')$ — no! (back to first step)

$\downarrow$ yes!

$s = x \oplus x'$

prob. of success in one try:

$p = \frac{1}{2^n - 1} \rightarrow O(2^n)$ queries necessary in order to find s.

a little better: $\rightarrow$

2) draw L numbers $x_1, x_2, \dots, x_L \in \mathbb{Z}_2^n$,

if $\exists\ i,j$: $f(x_i) = f(x_j)$

$$\Rightarrow \quad s = x_i \oplus x_j$$

prob. of success ?

<u>no</u> success with prob.

$$p = 1 \cdot \left(1 - \frac{1}{2^n - 1}\right)\left(1 - \frac{2}{2^n-2}\right) \cdots \left(1 - \frac{L-1}{2^n - L + 1}\right)$$

$$\approx 1 - \frac{1}{2^n} \sum_{\ell=1}^{L-1} \ell \simeq 1 - \frac{L^2}{2^{n+1}}$$

$L \ll 2^n$

$\rightarrow$ p of order 1 if $L = \mathcal{O}(\sqrt{2^n})$

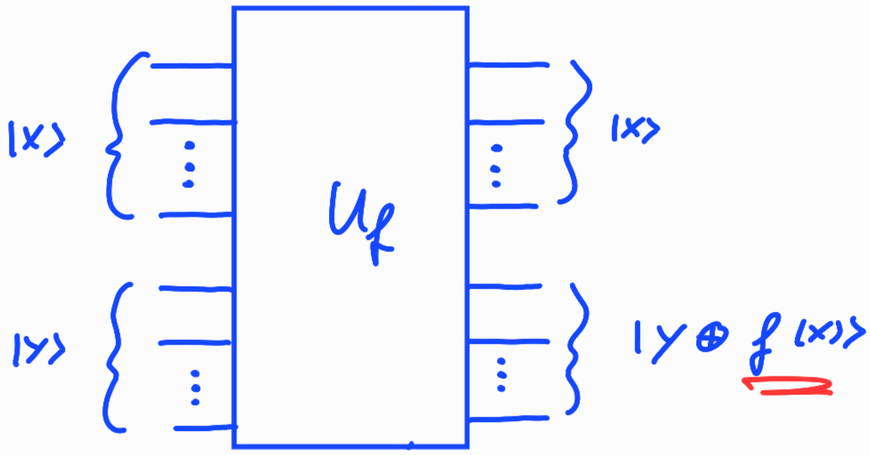
i.e. $\mathcal{O}(2^{n/2})$ queries needed

to find s !

<u>Conclusion:</u> Simon's problem is a <u>hard</u>

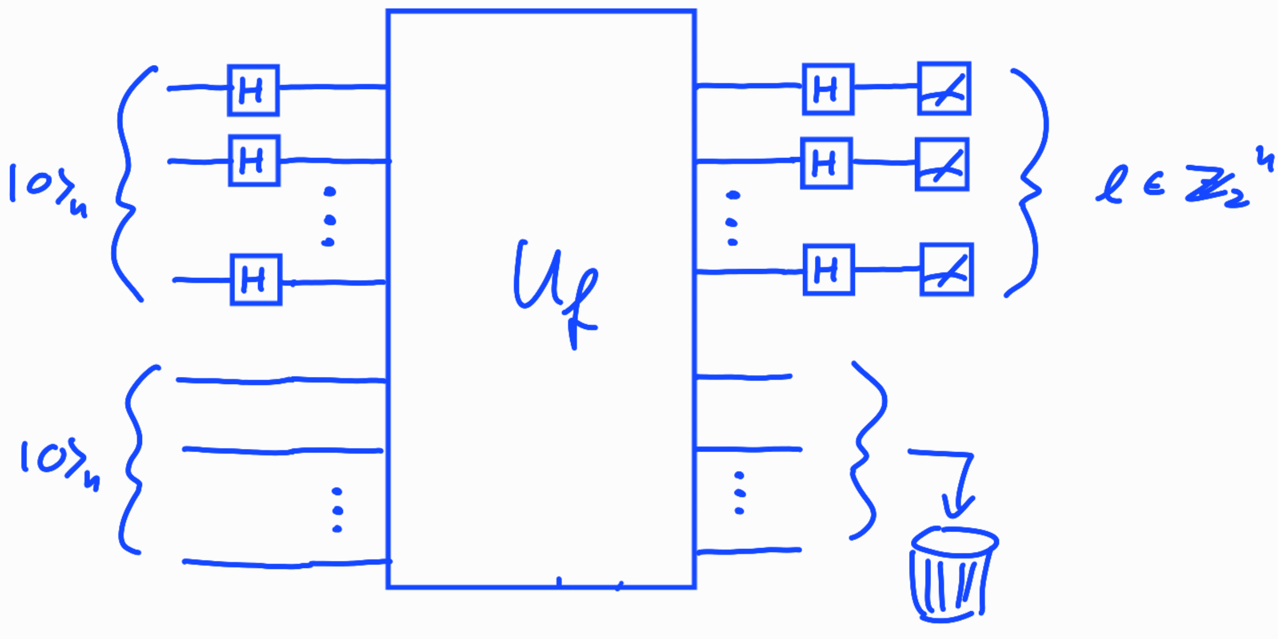
one for classical computers !

Simon's algorithm uses quantum gate that implements $f: \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ in a reversible manner:



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

Circuit for Simon's algorithm:



(i) (ii) (iii) (iv) (v)

procedure:

(i) prepare $|0\rangle_n |0\rangle_n$

(ii) apply $H^{\otimes n} \otimes \mathbb{1}_n$ (= D.F.T. on 1st reg.)

(iii) apply U_f

(iv) apply $H^{\otimes n} \otimes \mathbb{1}_n$ (= D.F.T. on 1st reg.)

(v) measure 1st register $\rightarrow l_i \in \mathbb{Z}_2^n$

- repeat (i) – (v) $\Rightarrow l_1, \ldots, l_k$

until linear system

$$l_1 \cdot s = 0$$

$$l_2 \cdot s = 0$$

$$\vdots$$

$$l_n \cdot s = 0$$

has unique solution $s \neq 0$!

$\rightarrow$ s is solution of Simon's problem!

How does it work? step by step:

$$|0\rangle_n|0\rangle_n \xrightarrow{H^{\otimes n}\otimes 1\!\!1_n} \frac{1}{2^{n/2}}\sum_i |i\rangle_n |0\rangle_n$$

$$\xrightarrow{U_f} 2^{-n/2}\sum_i |i\rangle\, |f(i)\rangle$$

$$\xrightarrow{H^{\otimes n}\otimes 1\!\!1_n} 2^{-n}\sum_{i,j} (-1)^{i\cdot j}\,|j\rangle\,|f(i)\rangle = |\psi'\rangle$$

→ measurement of 1st register yields outcome ℓ with prob.

$$p_\ell = \langle\psi'|\ |\ell\rangle\langle\ell|\otimes 1\!\!1_n\ |\psi'\rangle$$

$$= 2^{-2n}\sum_{i,m}\underbrace{(-1)^{i\cdot\ell}(-1)^{m\cdot\ell}}_{=(-1)^{(i\oplus m)\cdot\ell}}\ \underbrace{\langle f(i)|f(m)\rangle}_{=\delta_{i,m}+\delta_{i,m\oplus s}}$$

$$= 2^{-2n}\sum_m\Big((-1)^{\overbrace{(m\oplus m)\cdot\ell}^{=0}} + (-1)^{\overbrace{(m\oplus m\oplus s)\cdot\ell}^{=s}}\Big)$$

→

$$\rightarrow \quad p_\ell = 2^{-2n} \sum_{m=0}^{2^n-1} \left(1 + (-1)^{s\cdot\ell}\right)$$

$$= \begin{cases} 2^{1-n} & : \quad s\cdot\ell = 0 \\ 0 & : \quad s\cdot\ell = 1 \end{cases}$$

!

$\rightarrow$ outcome ℓ is a random element from the $(n-1)$-dimensional linear subspace

$$S^\perp = \{\ell\cdot s = 0 \mid \ell \in \mathbb{Z}_2^n\}$$

of $\mathbb{Z}_2^n$

$\rightarrow$ $k = n + O(n)$ rand. vectors $\ell_1, \dots, \ell_n \in S^\perp$ span with high prob. $S^\perp$

(c.f. Problem sheet 3)

$\rightarrow$ linear system $\ell_i \cdot s = 0 \quad i = 1, \dots, k$ determines s

→ Simon's algorithm finds solution s with only $k = \mathcal{O}(n)$ queries!

- "precision requirements" on
  - state preparation
  - gate transformations
  - coherence
  - state measurements

?

→ later!

- crucial part of Simon's alg. is DFT over $\mathbb{Z}_2^n$ with $H^{\otimes n}$

↑ matches order 2 of hidden subg. $H = \{0, s\}$

→

next lecture: efficient quantum circuit for general DFT over $\mathbb{Z}_N$!

$\rightarrow$ application in Shor's algorithm for integer factorization