Quantum computation: lecture 6

- Simon's algorithm
  - Part I reminder
  - Part II:
    - measurement process
    - probabilistic analysis

Short recap of last week:

Simon's problem: find the hidden subgroup $H \subset G$ with as few as possible calls to the oracle $f : \{0,1\}^n \to X$ satisfying $f(x) = f(y)$ whenever $x \oplus y \in H$

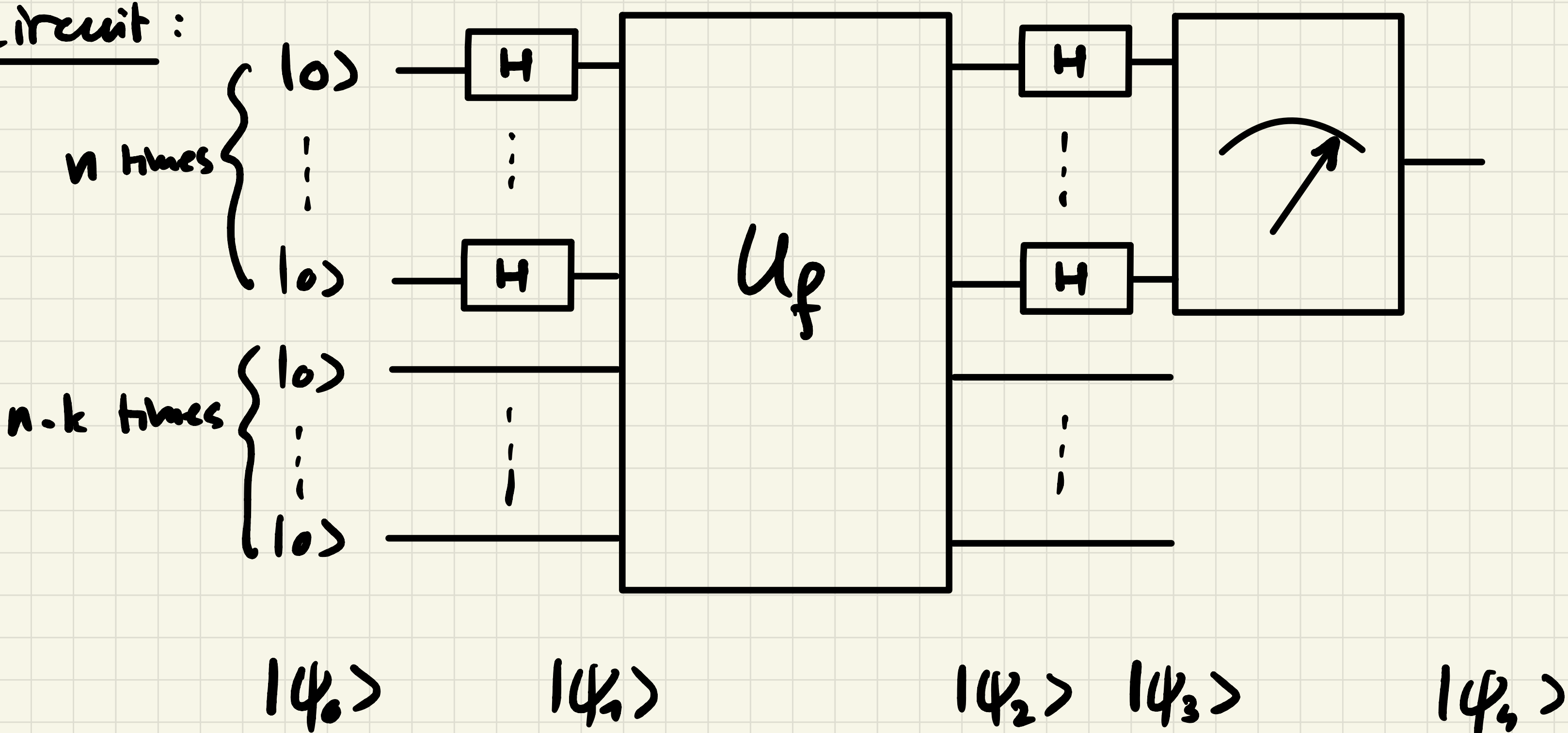
Here: $G = \{0,1\}^n$

H = k-dimensional subspace of G

Recall also : $H^\perp = \{x \in \{0,1\}^n : x \cdot h = 0 \;\; \forall h \in H\}$

Simon's quantum algorithm

Circuit:



Last time, we computed:

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

Recall G is divided into 2^{n-k} equivalence classes $\{ E_j = H \oplus v^{(j)},\ 1 \leq j \leq 2^{n-k} \}$

$$\begin{cases} v^{(j)} = \text{representative of class } E_j \\ f_j = \text{value of } f \text{ on } E_j \end{cases}$$

Measurement process

⚠ Here, the first n qubits are entangled with the last n-k qubits in state $|\psi_3\rangle$, so the partial measurement of the first n qubits is more difficult to describe than in the case of Deutsch-Josza's algorithm.

In general, a measurement is described in QM by a complete collection of orthogonal projectors $\{P_j, 1 \leq j \leq d\}$:

- $\forall 1 \leq j \leq d, \quad P_j = P_j^{+} = P_j^2$
- $\sum_{j=1}^{d} P_j = I$

(<u>Ex</u>: $P_j = |\varphi_j\rangle\langle\varphi_j|$, where $\{|\varphi_j\rangle, 1 \leq j \leq d\}$ is an orthonormal basis of the Hilbert space H)

Then if the system is in state $|\psi\rangle$ before the measurement, the outcome state i

$$|\psi'\rangle = \frac{P_j|\psi\rangle}{\|P_j|\psi\rangle\|}$$

with probability

$$\| P_j|\psi\rangle\|^2 = \langle\psi|P_j^\dagger P_j|\psi\rangle \overset{\text{proj.}}{=} \langle\psi|P_j|\psi\rangle$$

In our case, the measurement of the first n qubits is described by the following complete collection of projectors:

$$\{ P_y = |y\rangle\langle y| \otimes I_{n-k} \, , \; y \in \{0,1\}^n \}$$

For a given $y_0 \in \{0,1\}^n$, let us compute the outcome probability $\langle \psi_3 | P_{y_0} | \psi_3 \rangle$ of state $\frac{P_{y_0}|\psi_3\rangle}{\| P_{y_0}|\psi_3\rangle \|} = |y_0\rangle \otimes \begin{pmatrix} \text{Some state we do} \\ \text{not care about} \end{pmatrix}$

$$\langle \psi_3 | P_{y_0} | \psi_3 \rangle$$

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

$$\left(|y_0\rangle\langle y_0| \otimes I_{n-k} \right) \left(\sum_{y' \in H^\perp} \frac{1}{2^{n-k}} \sum_{j'=1}^{2^{n-k}} (-1)^{v^{(j')} \cdot y'} |y'\rangle \otimes |f_{j'}\rangle \right)$$

$$= \sum_{y, y' \in H^\perp} \frac{1}{2^{2(n-k)}} \cdot \sum_{j, j'=1}^{2^{n-k}} (-1)^{v^{(j)} \cdot y + v^{(j')} \cdot y'} \underbrace{\langle y | y_0 \rangle}_{= \delta_{y y_0}} \underbrace{\langle y_0 | y' \rangle}_{= \delta_{y_0 y'}} \cdot \underbrace{\langle f_j | f_{j'} \rangle}_{= \delta_{j j'}}$$

So the above quadruple sum simplifies to:

- 0 if $y_0 \notin H^\perp$
- and if $y_0 \in H^\perp$, we obtain:

$$\frac{1}{2^{2(n-k)}} \sum_{j=1}^{2^{n-k}} \underbrace{(-1)^{v^{(i)} \cdot y_0 + v^{(j)} \cdot y_0}}_{=1} = \frac{2^{n-k}}{2^{2(n-k)}} = \frac{1}{2^{n-k}}$$

i.e. the outcome probabilities are uniform over $H^\perp$.

Simon's algorithm is then the following:

- run $n-k$ times the above circuit
  $\rightarrow$ outputs $y^{(1)} \dots y^{(n-k)}$ uniformly and independently distributed on $H^\perp$
- if $y^{(1)} \dots y^{(n-k)}$ are linearly independent, then these form a <u>basis</u> of $H^\perp$, which is of dimension $n-k$.

From this basis, compute the basis of the dual space H, via a classical algorithm (Gauss elimination - runtime $O(n^3)$).
In this case, declare success.

- If $y^{(1)} \ldots y^{(n-k)}$ are not linearly independent then declare failure and restart the algorithm. (NB: In practice, one can do better.)

<u>Claim</u>: $\text{prob}(\text{success}) \geq \frac{1}{4}$

<u>Proof</u>: • $\text{prob}(y^{(1)} \neq 0) = 1 - \frac{1}{2^{n-k}}$

• $\text{prob}(y^{(2)} \notin \underbrace{\text{span}(y^{(1)})}_{=\{0, y^{(1)}\}} \mid y^{(1)} \neq 0) = 1 - \frac{2}{2^{n-k}} = 1 - \frac{1}{2^{n-k-1}}$

• $\text{prob}(y^{(3)} \notin \underbrace{\text{span}(y^{(1)}, y^{(2)})}_{4 \text{ elements}} \mid y^{(1)}, y^{(2)} \text{ lin indep}) = 1 - \frac{4}{2^{n-k}}$

$= 1 - \frac{1}{2^{n-k-2}}$

- - -

$$\text{prob}\left(y^{(n-k)} \notin \text{span}\left(y^{(1)} .. y^{(n-k-1)}\right) \,\middle|\, y^{(1)} .. y^{(n-k-1)} \text{ lin indep.}\right)$$

$$= 1 - \frac{2^{n-k-1}}{2^{n-k}} = 1 - \frac{1}{2}$$

So finally,

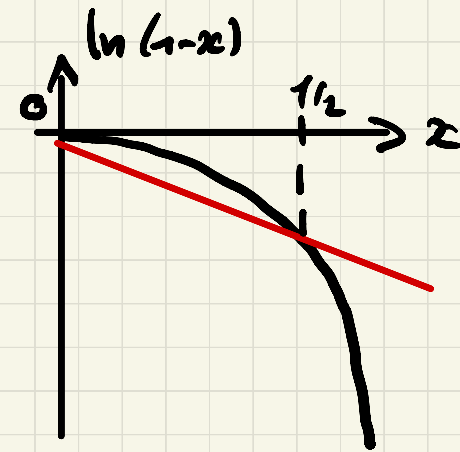
$$\text{prob(success)} = \text{prob}\left(y^{(1)} \ldots y^{(n-k)} \text{ are lin. indep.}\right)$$

$$= \prod_{j=0}^{n-k-1} \left(1 - \frac{1}{2^{n-k-j}}\right) \underset{\substack{\uparrow \\ \ell = n-k-j}}{=} \prod_{\ell=1}^{n-k} \left(1 - \frac{1}{2^{\ell}}\right)$$

Furthermore:

$$\text{prob}(\text{success}) = \exp\left(\sum_{\ell=1}^{n-k} \ln\left(1-\frac{1}{2^\ell}\right)\right) \quad \text{and}$$

using $\ln(1-x) \geq -(2\ln 2)x$ for $0 \leq x \leq \frac{1}{2}$



So prob (success)

$$\geq \exp\Big(-(2\ln 2)\underbrace{\sum_{\ell=1}^{n-k} \frac{1}{2^\ell}}_{\leq 1}\Big)$$

$$\geq \exp(-2\ln 2)$$

$$= 2^{-2} = 1/4 \qquad \#$$

Of course, a success probability of only $\frac{1}{4}$ is not satisfactory; we would like a success prob. $\geq 1-\varepsilon$. Let us therefore repeat independently the whole algorithm T times:

$$\text{prob(failure after } T \text{ attempts)}$$
$$= \text{prob(failure)}^T \leq \left(\frac{3}{4}\right)^T \leq \varepsilon$$
$$\text{if } T \geq \frac{|\ln \varepsilon|}{|\ln 3/4|}$$

<u>Conclusion:</u> We obtain a success prob. $\geq 1-\varepsilon$ after $O((n-k)\cdot|\ln\varepsilon|)$ calls to the quantum oracle U_f (& a polynomial runtime dominated by the $O(n^3)$ computation of the dual basis). This is to be compared to the $\Omega(2^n)$ calls to the oracle f of any classical algorithm.