Query complexity / promise problem

Instead of input $i_1, \dots, i_n \in B_n$ have:

- Black box / oracle that computes some $f: B_m \to B_n$
- May have a priori promise on f
- Want to determine some property of f
- Only access to f is querying the oracle with its inputs
- Use of f (classical) or U_f (quantum) counts as one step of computation

* Query complexity : least # times that oracle needs to be queried.

- Example (balanced vs constant)

<u>Input</u> : black box for $f: B_n \to B_1$

<u>Promise</u>: f is either a) a const f^n (i.e. $f(x) = 0$ or 1 for all x)

or b) "balanced" $f(x) = 0$ for exactly half possible x

<u>Problem</u>: determine f is const or balanced with certainty

<u>Classically</u> $2^n/2 + 1$ queries are necessary and sufficient

<u>Quantumly</u> 1 query suffices

DJ algorithm (1992)

Have $U_f |x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$ $\quad |x\rangle(e^{i\theta}|y\rangle) = (e^{i\theta}|x\rangle)|y\rangle$ difference if sum over

(we use "phase kickback" to encode f-values as $\pm$ sign rather than $0/1$)

- Set the output to $|\alpha\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} = H|1\rangle \left(= HX|0\rangle\right)$

- $|x\rangle\left(\frac{|0\rangle - |1\rangle}{2}\right) \xrightarrow{\text{oracle}} |x\rangle\left(\frac{|f(x)\rangle - |1 \oplus f(x)\rangle}{\sqrt{2}}\right) = \begin{cases} |x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} \\ |x\rangle \frac{|1\rangle - |0\rangle}{\sqrt{2}} \end{cases} = (-1)^{f(x)}|x\rangle|\alpha\rangle$

Now do this in superpos^n over all x's

$$\frac{1}{\sqrt{2^n}} \sum_{\text{all } x} |x\rangle|\alpha\rangle \xrightarrow{U_f} \left(\frac{1}{\sqrt{2^n}} \sum_{\text{all } x} (-1)^{f(x)} |x\rangle\right)|\alpha\rangle$$

So 1 query gives $|\xi_f\rangle = \frac{1}{\sqrt{2^n}} \sum_{\text{all } x} (-1)^{f(x)} |x\rangle$

Key observation f const vs f bal $\Rightarrow$ so $|\xi_{f\,\text{const}}\rangle \perp |\xi_{f\,\text{bal}}\rangle$

all signs same / exactly half signs are $\pm$ s

Orthogonality $\Leftrightarrow$ can perfectly distinguish with a quantum measurement

but allow only mmts in standard $|0\rangle|1\rangle$ basis.

Recall $|0\rangle\dots|0\rangle \xrightarrow{\otimes^n H} \frac{1}{\sqrt{2^n}}\sum_{\text{all } x}|x\rangle = \pm|\xi_{f_{\text{const}}}\rangle$

$\otimes^n H$ since $HH=I$

So write $|\eta_f\rangle = \otimes^n H|\xi_f\rangle$

then $|\eta_{f_{\text{const}}}\rangle \perp |\eta_{f_{\text{bal}}}\rangle$

f const $|\eta_{f_{\text{const}}}\rangle = \pm|0\dots0\rangle$

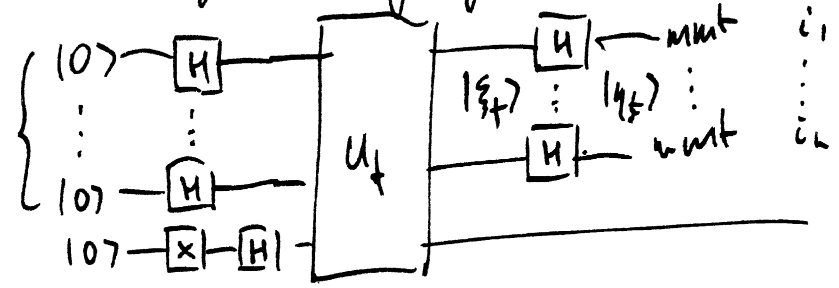
f bal $|\eta_{f_{\text{bal}}}\rangle = \sum_{\text{all } x\neq 0\dots0} a_x|x\rangle$ ← since $\perp |\eta_{f_{\text{const}}}\rangle = \pm|0\dots0\rangle$

So the mmts of the n qubits distinguishes

f const (mmt gives $0\dots0$)

f bal (mmt gives some $i_1\dots i_n\neq 0\dots0$)

Circuit diagram for DJ algorithm



Uses 1 query + $\underbrace{(1+(n+1)+n+n)}_{3n+1}$ gates

Remember 1) for some special balanced f^{ns} (2^n-1 of all f_a labelled by $a\in B_n$)
get $|\eta_f\rangle = |a\rangle$ so get a with certainty → see BV algorithm

2) Can we decide any yes/no question $f: B_n \to B_1$ by quantum algorithm with few queries? NO!

- SAT problem (NP complete): given f, is there an x with $f(x)=1$

Can show (cf later) any quantum algorithm solving this problem with probability $(1-\epsilon)$ with $0<\epsilon<\frac{1}{2}$ needs at least $O(\sqrt{2^n})$ queries, classically need $O(2^n)$ queries.

(Achieved by Grover's algorithm)

3) If tolerate error in result, there is a classical probabilistic algorithm with order $O(\log(1/\epsilon))$ queries, i.e. constant for constant ϵ, as follows:

choose K (fixed later) to match ϵ

choose K x-values uniformly at random and obtain $f(x)$

all same → const : f const → correct answer probability 1

not all same → bal : f bal → $p(\text{same}) = \frac{2}{2^k} < \epsilon$ fails $\Rightarrow k > \log(1/\epsilon)+1$