Deutsch's algorithm

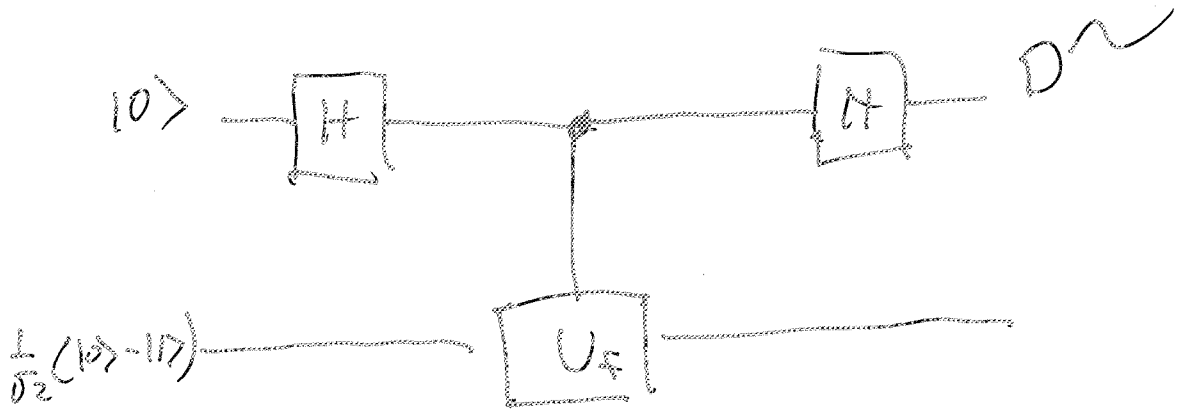
$f : \{0,1\} \to \{0,1\}$

Is $f(0) = f(1)$ or $f(0) \neq f(1)$?

How many times to evaluate $f(x)$ to answer this ?

Classical - twice

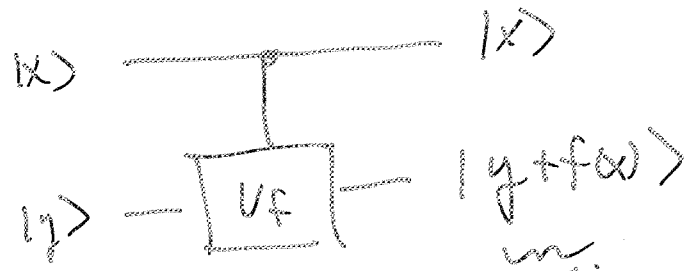
Quantum - once



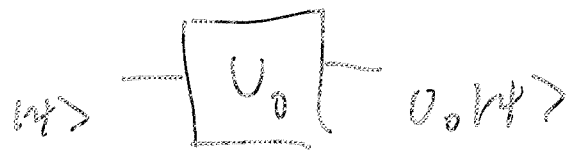
$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

f - controlled not



Second problem



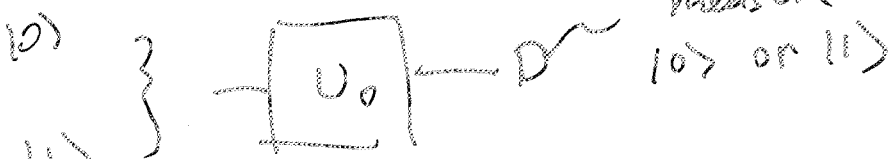
U_0 eigenvalues ± 1

Don't know eigenstates

Want 2 qubits

one in +1 eigen state

one in −1 eigenstate



Do many times, find $\langle 0|U_0|0\rangle$,

$\langle 0|U_0|1\rangle$, -- etc.

Find eigenstates and produce them.

Use gate many times.

Quantum strategy : singlet state

$$|\phi_s\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle)$$

Invariant under local unitaries

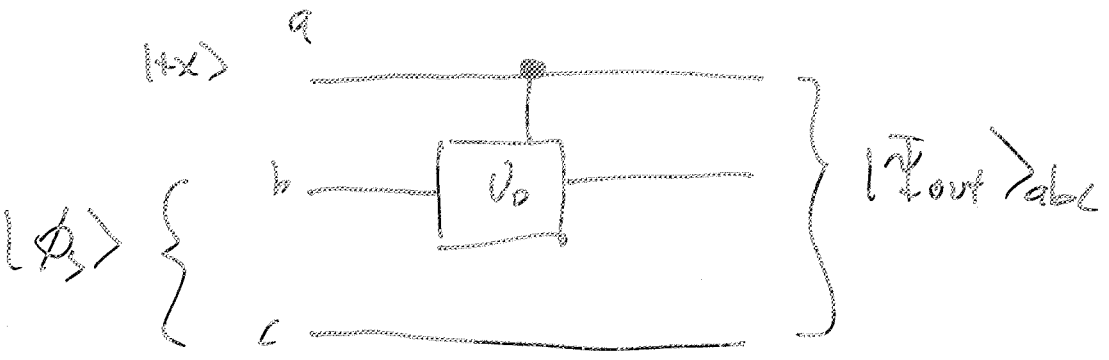
$$U \otimes U |\phi_s\rangle = e^{i\theta} |\phi_s\rangle$$

Suppose U is such that

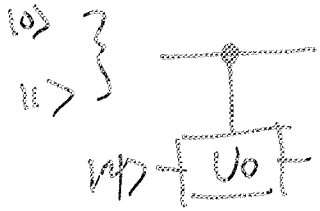
$U|0\rangle = |u_+\rangle$ $\quad U_0|u_+\rangle = |u_+\rangle$

$U|1\rangle = |u_-\rangle$ $\quad U_0|u_-\rangle = -|u_-\rangle$

$$U \otimes U |\phi_s\rangle = \frac{1}{\sqrt{2}}(|u_+\rangle|u_-\rangle - |u_-\rangle|u_+\rangle) = |\phi_s\rangle$$



$$|+x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$



$|0\rangle|\Psi\rangle \to |0\rangle|\Psi\rangle$

$|1\rangle|\Psi\rangle \to |1\rangle U_0|\Psi\rangle$

$$|\Psi_{out}\rangle_{abc} = \frac{1}{2}\{|0\rangle_a(|+\rangle_b|-\rangle_c - |-\rangle_b|+\rangle_c)$$
$$+ |1\rangle_a(|+\rangle_b|-\rangle_c + |-\rangle_b|+\rangle_c)\}$$
$$= \frac{1}{\sqrt{2}}\{|+\rangle_a|+\rangle_b|-\rangle_c - |-\rangle_a|-\rangle_b|+\rangle_c\}$$

Measure a in $|\pm x\rangle$ basis

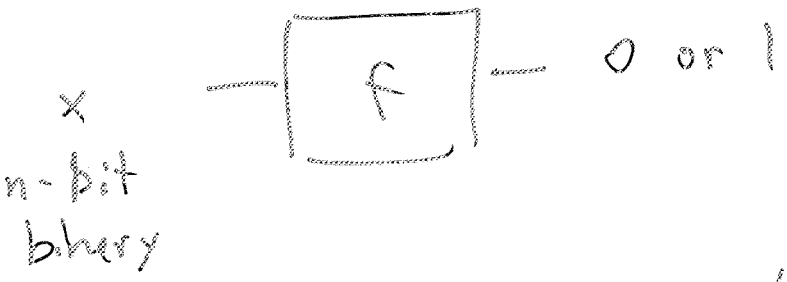
$|+x\rangle$: $|+\rangle_b|-\rangle_c$

$|-x\rangle$: $-|-\rangle_b|+\rangle_c$

One use of controlled-U gate gave us qubits in eigenstates.

Deutsch-Jozsa algorithm:

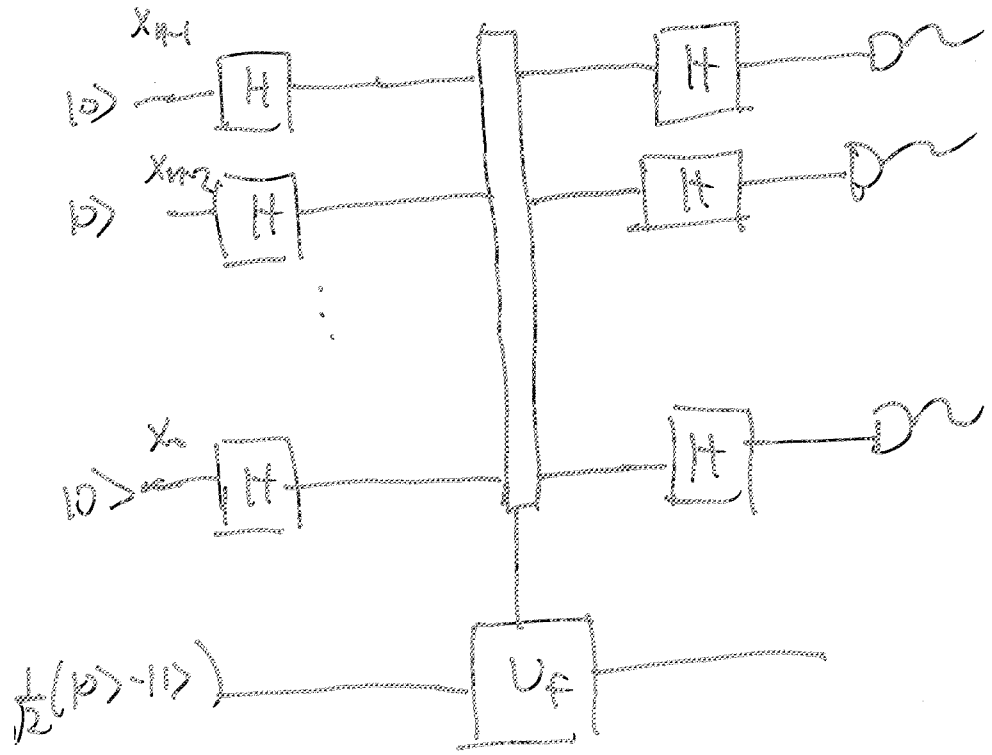
$$f : \{0,1\}^n \to \{0,1\}$$



Promise: $f(x)$ is constant
or $f(x)$ is balanced (0 on half of inputs, 1 on half of inputs)

Which (using box smallest number of times).

Deutsch-Jozsa $\Rightarrow$ one use of box



Look at n - Hadamard gates

Input state to n - Hadamards $|x\rangle$ n-qubits

x n-digit binary $x = x_{n-1}\, x_{n-2} \cdots x_0$

$|x\rangle = |x_{n-1}\rangle |x_{n-2}\rangle \cdots |x_0\rangle$

single Hadamard on $|x_j\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_j}|1\rangle)$

$$|x\rangle = \prod_{j=0}^{n-1} |x_j\rangle \to \left(\frac{1}{\sqrt{2}}\right)^n \prod_{j=0}^{n-1} (|0\rangle + (-1)^{x_j}|1\rangle)$$

$$= \left(\frac{1}{\sqrt{2}}\right)^n \sum_{y=0}^{2^n-1} \left(\prod_{j \text{ such that } y_j = 1} (-1)^{x_j} \right) |y\rangle$$

$y = y_{n-1}\, y_{n-2} \cdots y_0$

$$= \left(\frac{1}{\sqrt{2}}\right)^n \sum_{y=0}^{2^n-1} \left(\prod_{j=0}^{n-1} (-1)^{x_j y_j} \right) |y\rangle$$

$$\prod_{j=0}^{n-1} (-1)^{x_j y_j} = (-1)^{\sum_{j=0}^{n-1} x_j y_j} = (-1)^{\left(\sum_{j=0}^{n-1} x_j y_j \bmod 2\right)}$$

Define $x \cdot y = \sum_{j=0}^{n-1} x_j y_j \bmod 2$

(x, y: n digit binaries)

n Hadamards

$$|x\rangle \longrightarrow \left(\frac{1}{2}\right)^{n/2} \sum_{y=0}^{2^n-1} (-1)^{x \cdot y} |y\rangle$$

f-controlled NOT

$|x\rangle |y\rangle \longrightarrow |x\rangle |y + f(x) \bmod 2\rangle$

($|x\rangle$: n-digit binary (n qubits); $|y\rangle$: one qubit)

So

$$|x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \longrightarrow |x\rangle \otimes \frac{1}{\sqrt{2}}(|f(x)\rangle - |1+f(x)\rangle)$$

$$(-1)^{f(x)} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

State after f-controlled NOT gate

$$\left(\frac{1}{2}\right)^{(n+1)/2} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle \otimes (|0\rangle - |1\rangle)$$

Goes through n-Hadamards

$$\rightarrow \underbrace{\left(\frac{1}{2}\right)^{(n+1)/2} \sum_{x,y=0}^{2^n-1} (-1)^{f(x)+x\cdot y} |y\rangle \otimes (|0\rangle - |1\rangle)}_{|\Psi_{out}\rangle}$$

Look at overlap of $|\Psi_{out}\rangle$ with $|0\rangle^{\otimes n} = |\vec{0}\rangle$

~~$\langle \vec{0} | \Psi_{out} \rangle = \left(\frac{1}{2}\right)^n \sum_{x=0}^{2^n-1} f(x)$~~

$$\langle \vec{0} | \Psi_{out} \rangle = \left(\frac{1}{2}\right)^n \sum_{x=0}^{2^n-1} (-1)^{f(x)}$$

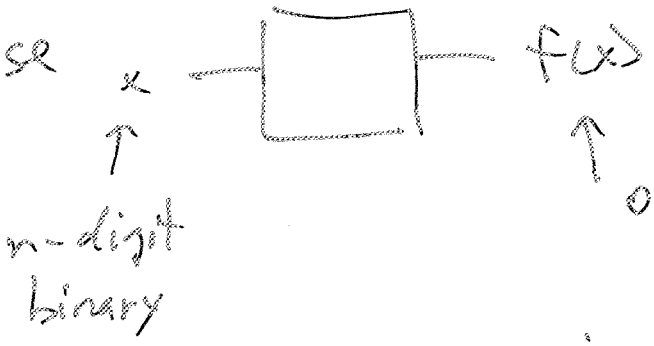
$$= \begin{cases} 0 & \text{if } f(x) \text{ balanced} \\ (-1)^{f(0)} & \text{if } f(x) \text{ constant} \end{cases}$$

Measure each of n qubits in output in computational basis

(1) all give 0 $\Rightarrow$ $f(x)$ constant

(2) not all 0 $\Rightarrow$ $f(x)$ balanced

Bernstein - Vazirani

Suppose 

Suppose $f(x) = a \cdot x$ is linear

(x: n-digit binary)

$$a \cdot x = \sum_{j=0}^{n-1} a_j x_j \mod 2$$

Find a. How many times do we need to evaluate $f(x)$?

Answer
Classical - n times
Quantum - once

Classically input $x = 00\ldots0100\ldots0$ (j^{th} place)

Do n times with different j's, get a.

Quantum

Same circuit

Look at $|\Psi_{out}\rangle$ for $f(x) = a \cdot x$

$$|\Psi_{out}\rangle = \left(\frac{1}{2}\right)^n \sum_{x,y=0}^{2^n-1} (-1)^{x\cdot(a+y)} |y\rangle$$

Exercise: Show that

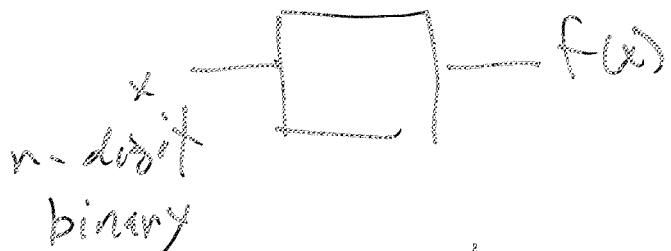
$$\sum_{x=0}^{2^n-1} (-1)^{x\cdot z} = 2^n \delta_{z,0}$$

$$\Rightarrow |\Psi_{out}\rangle = |a\rangle$$

↑ measure in computational basis

This can be used for function property testing.

Typical problem:



Promised f(x) is linear or ε-far from linear. Which?

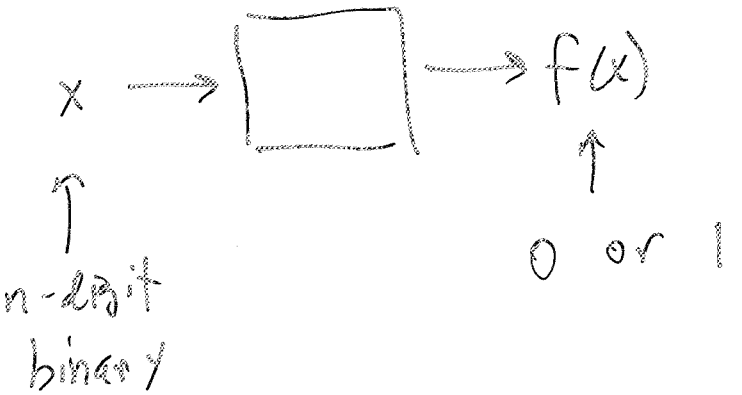
Two functions are ε-far if they disagree on an ε fraction of their inputs or

$$\frac{1}{2^n} \sum_x |(-1)^{f(x)} - (-1)^{g(x)}| > 2\varepsilon$$

f and g are ε-far

f is ε-far from linear if the closest linear function to f is ε-far from f.

Grover Algorithm



$$f(x) = \begin{cases} 1 & x = x_0 \\ 0 & x \neq x_0 \end{cases}$$

x_0 is unknown, we want to find it.

$N = 2^n$ Classically use box $O(N)$ times

Quantum use box $\Theta(\sqrt{N})$ times.

Define $U_f |x\rangle = (-1)^{f(x)} |x\rangle$

or $U_f = I - 2|x_0\rangle\langle x_0|$

$U_0 = I - 2|0\rangle\langle 0|$ $\quad |0\rangle = |$ <ll n 0's $\rangle$

$U_H = (H)^{\otimes n}$

Procedure: Apply $Q = -U_H U_0 U_H U_f$

to initial state $|w_0\rangle = U_H |0\rangle$

$$= \frac{1}{\sqrt{N}} \sum_{x=0}^{2^n-1} |x\rangle$$

Do this $O(\sqrt{N})$ times

Measure state in computational basis.

Result: $|x_0\rangle$ with high probability.

How does this work?

Define $U_{w_0} = U_H U_0 U_H = I - 2|w_0\rangle\langle w_0|$

$$Q = -U_{w_0} U_f$$

Define $S = \text{span}\{|w_0\rangle, |x_0\rangle\}$

Let $|\psi\rangle = c_1 |w_0\rangle + c_2 |k_0\rangle \in S$

$$Q|\psi\rangle = -U_{w_0} U_f |\psi\rangle = c_1 |w_0\rangle + \left(\frac{2}{\sqrt{N}} c_1 + c_2\right) \cdot \left(|x_0\rangle - \frac{2}{\sqrt{N}} |w_0\rangle\right) \in S$$

Q leaves S invariant

initial state is $|w_0\rangle$ so

$Q^m |w_0\rangle \in S$

All the action of the algorithm takes place in S. S is two-dimensional

$Q^m |w_0\rangle = c_1 |w_0\rangle + c_2 |x_0\rangle$

where c_1 and c_2 are real.

Define $S' = \{c_1 |w_0\rangle + c_2 |x_0\rangle \mid c_1 \text{ and } c_2 \text{ real}\}$

All action is in S'.

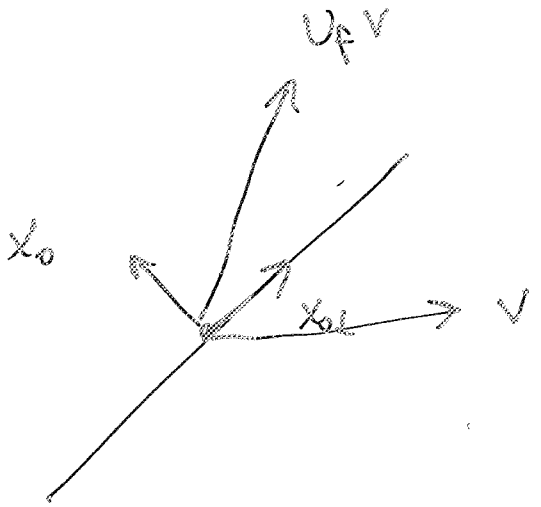
Look at action of Q in S'.

Define $|x_{0\perp}\rangle = (|w_0\rangle - |x_0\rangle\langle x_0|w_0\rangle) / (1 - |\langle x_0|w_0\rangle|^2)^{1/2}$

$|w_{0\perp}\rangle = (|x_0\rangle - |w_0\rangle\langle w_0|x_0\rangle) / (1 - |\langle x_0|w_0\rangle|^2)^{1/2}$

so $\langle x_{0\perp}|x_0\rangle = 0$ $\quad \langle w_{0\perp}|w_0\rangle = 0$

Claim: U_f is reflection about the line through $|x_{0\perp}\rangle$ in S'.



Also have in S'

$$|w_0\rangle\langle w_0| + |w_{0\perp}\rangle\langle w_{0\perp}| = I$$

$$\Rightarrow \quad -U_{w_0} = \underbrace{I - 2|w_{0\perp}\rangle\langle w_{0\perp}|}_{U_{w_{0\perp}}}$$

This is a reflection through the line through w_0.

$$Q = U_{w_{0\perp}} U_f = (\text{reflection about } w_0) \cdot (\text{reflection about } x_{0\perp})$$

Theorem: Let m_1 and m_2 be two mirror lines intersecting at O in the Euclidean plane. α = angle between them. Reflection through m_1 followed by reflection through m_2 is a rotation by 2α about O.

Proof by pictures

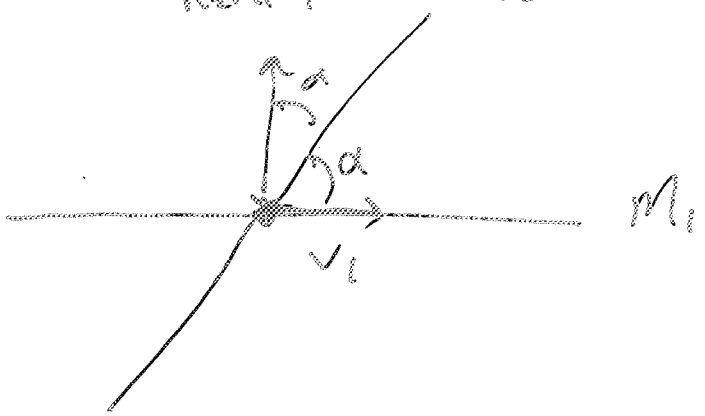
Let $\vec{v}_1$ parallel to m_1

$\vec{v}_2$ parallel to m_2

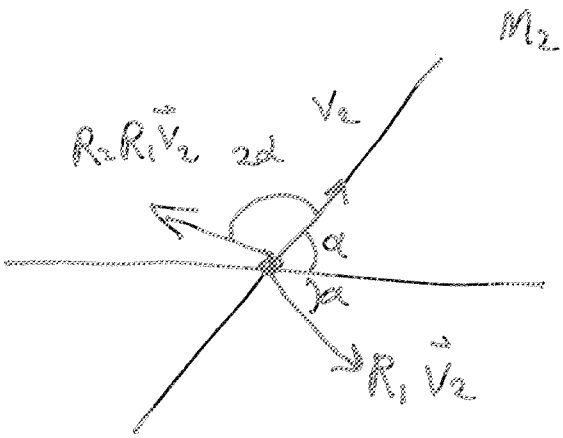
If theorem holds for $\vec{v}_1$ and $\vec{v}_2$ it holds for any superposition of them.

Show for $\vec{v}_1$

$R_2R_1\vec{v}_1$ m_2 $\vec{v}_1$ rotated by 2α



For $\vec{v}_2$



$\vec{v}_2$ is rotated by 2α

Conclusion: Q is a rotation in S' by 2α where α = angle between w_0 and x_{02}

$\cos\alpha = \langle w_0 | x_{0\perp} \rangle = (1 - \frac{1}{N})^{1/2}$

$\sin\alpha = \frac{1}{\sqrt{N}} = \langle w_0 | x_0 \rangle$.

Work in $|x_0\rangle, |x_{0\perp}\rangle$ basis. Start in state

$|w_0\rangle = |x_0\rangle\langle x_0|w_0\rangle + |x_{0\perp}\rangle\langle x_{0\perp}|w_0\rangle$

$= \sin\alpha\,|x_0\rangle + \cos\alpha\,|x_{0\perp}\rangle$

Apply Q^m

$Q^m|w_0\rangle = \sin\alpha_m\,|x_0\rangle + \cos\alpha_m\,|x_{0\perp}\rangle$

$\alpha_m = (2m+1)\alpha$

Choose m so that $\alpha_m \cong \frac{\pi}{2}$

For large N, $\alpha \cong \frac{1}{\sqrt{N}}$

$(2m+1)\frac{1}{\sqrt{N}} = \frac{\pi}{2} \Rightarrow m =$ closest integer to $\frac{\pi}{4}\sqrt{N} - \frac{1}{2}$

call this $\bar{m}$

Measure state in computational basis

prob. of $x_0 = |\langle x_0|Q^{\bar{m}}|w_0\rangle|^2 = \sin^2\alpha_{\bar{m}}$ close to 1

prob. of $x \neq x_0 = |\langle x|Q^{\bar{m}}|w_0\rangle|^2 = \cos^2\alpha_{\bar{m}}\,|\langle x|x_{0\perp}\rangle|^2$

$= O(\frac{1}{N})$.

Can we do better? This is the best we can do.

To show this we assume any algorithm works by alternating function calls with other unitary evolution.

$U_f = I - 2|x_0\rangle\langle x_0|$ function call

State after k steps of algorithm

$$|\psi_k'\rangle = U_k U_f U_{k-1} U_f \cdots U_1 U_f |\psi_{in}\rangle$$

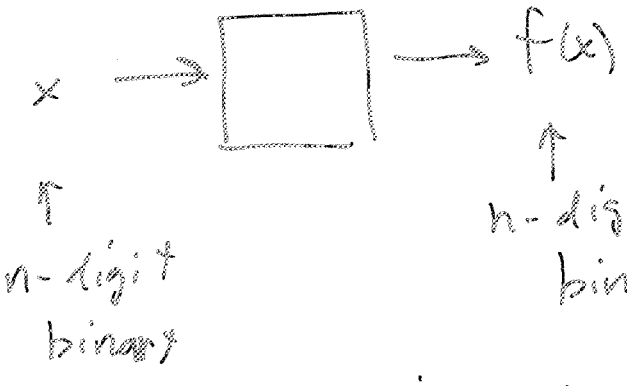
Compare this to

$$|\psi_k\rangle = U_k U_{k-1} \cdots U_1 |\psi_{in}\rangle$$

Show that if prob. of find x_0 is greater than $\frac{1}{2}$ i.e. $|\langle x_0|\psi_k'\rangle|^2 > \frac{1}{2}$) then k must be $\Theta(\sqrt{N})$.

Simon's algorithm

This is a period-finding algorithm which is a precursor to Shor.



This function is a 2 to 1 mapping

In particular

$f(x) = f(y)$ iff $y = x \oplus \xi$

(ξ: n-digit binary)

$$x \oplus \xi = (x_n + \xi_n \bmod 2)(x_{n-1} + \xi_{n-1} \bmod 2) \ldots (x_1 + \xi_1 \bmod 2)$$

Note: $y = x \oplus \xi$

$\Rightarrow y \oplus \xi = x$

$x = x_n x_{n-1} \cdots x_1$

$\xi = \xi_n \xi_{n-1} \cdots \xi_1$

ξ is fixed and unknown

Find ξ in poly(n) steps

Start in state

$$|\psi_{in}\rangle = \frac{1}{2^{n/2}} \sum_x |x\rangle$$

Apply U_f

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

(x: n-digit binaries)

$$U_f \left(\frac{1}{2^{n/2}} \sum_x |x\rangle|0\rangle \right) = \frac{1}{2^{n/2}} \sum_x |x\rangle|f(x)\rangle$$

Measure second register. Result is $f(x_0)$ for some random x_0. Resulting state

$$\frac{1}{\sqrt{2}} \left(|x_0\rangle + |x_0 \oplus \xi\rangle \right)$$

Fact that x_0 is random makes this state useless for finding ξ if we just measure it.

Apply H^n this gives us

$$\frac{1}{2^{(n+1)/2}} \sum_y \left[(-1)^{x_0 \cdot y} + (-1)^{(x_0 \oplus \xi)\cdot y} \right] |y\rangle$$

$$= \frac{1}{2^{(n+1)/2}} \sum_y (-1)^{x_0 \cdot y} \left[1 + (-1)^{\xi \cdot y} \right] |y\rangle$$

$$= \frac{1}{2^{(n-1)/2}} \sum_{\{y \mid y \cdot \xi = 0\}} (-1)^{x_0 \cdot y} |y\rangle$$

Measure state

result: value of y such that $y \cdot \xi = 0$

Do this approximately n times

Get n independent values of y, y_i such that $\xi \cdot y_i = 0$

linear equations, solve for ξ.

Found ξ with approximately n function calls.