N.3 Quantum vs. classical computation

$|x) := |x\rangle_1$

A, The lore of "quantum parallelism"

Hadamard gate $\quad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

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

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

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

$$= \frac{1}{2}\left(|0)\otimes|0) + |0)\otimes|1) + |1)\otimes|0) + |1)\otimes|1)\right)$$

$$= \frac{1}{2}\left(|00\rangle_2 + |01\rangle_2 + |10\rangle_2 + |11\rangle_2\right)$$

$$= \frac{1}{2}\left(|0\rangle_2 + |1\rangle_2 + |2\rangle_2 + |3\rangle_2\right)$$

in genera

given f

unitar

U

then

(

but: ne

(H

$|x) := |x\rangle_1$

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

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

$= (|0\rangle + |1\rangle)$

$+ |1\rangle) \otimes |1\rangle)$

in general: $$H^{\otimes m}|0\rangle_m = \frac{1}{2^{m/2}} \sum_{x=0}^{2^m-1} |x\rangle_m$$

given $f: \mathbb{N} \to \mathbb{N}$, assume to have f implemented by a unitary operation U_f, as follows

$$U_f(|x\rangle_m \otimes |y\rangle_m) = |x\rangle_m \otimes |f(x) +_2 y\rangle_m$$

then

$$U_f(H^{\otimes m}|0\rangle_m \otimes |0\rangle_m) = \frac{1}{2^{m/2}} \sum_{x=0}^{2^m-1} |x\rangle_m \otimes |f(x)\rangle_m$$

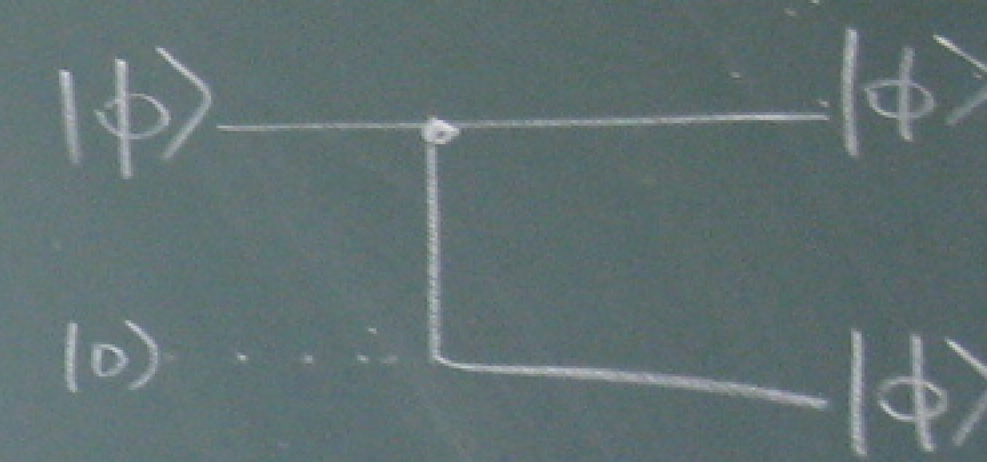
"quantum parallelism"

but: need to measure to read out the result. $\Rightarrow$ get $(x, f(x))$, with probability (that x occurs) of 2^{-m}

B) The "no-cloning" theorem.

There is no unitary operation K so that for all $|\phi\rangle \in \mathbb{C}^D$:

$$K\,|\phi\rangle \otimes |0\rangle = |\phi\rangle \otimes |\phi\rangle$$



<u>Proof.</u>

$$K(|\phi\rangle \otimes |0\rangle) = |\phi\rangle \otimes |\phi\rangle$$

$$K(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle$$

K linear $\Rightarrow$ $K((|\phi\rangle + |\psi\rangle) \otimes |0\rangle) = K(|\phi\rangle \otimes |0\rangle) + K(|\psi\rangle \otimes |0\rangle)$

$$(|\phi\rangle + |\psi\rangle) \otimes (|\phi\rangle + |\psi\rangle) = |\phi\rangle \otimes |\phi\rangle + |\psi\rangle \otimes |\psi\rangle$$

$$|\phi\rangle \otimes |\phi\rangle + |\phi\rangle \otimes |\psi\rangle + |\psi\rangle \otimes |\phi\rangle + |\psi\rangle \otimes |\psi\rangle$$

C) Deutsch's riddle.

U_f is given ("oracle"), calculates one of f_1, f_2, f_3, f_4

$f_i : B \to B$ $\quad f_0 = 0,\ f_1 = \neg,\ f_2 = id,\ f_3 = 1.$ we don't know which one

How often do we need to ask, to determine i?

classically, twice. Deutsch: quantum, once.

$$U_f (H \otimes H)(|0\rangle \otimes |0\rangle) = U_f \tfrac{1}{2}\big(|00\rangle + \overset{|0\rangle\otimes|1\rangle}{|01\rangle} + |10\rangle + |11\rangle\big)$$

$$= \tfrac{1}{2}\big(|0\, f(0)\rangle + |0\, \underbrace{(1+f(0))}_{f'(0)}\rangle + |1\, f(1)\rangle + |1\, \underbrace{(1+f(1))}_{f'(1)}\rangle\big)$$

$$= \frac{1}{2}\begin{cases} (|0\rangle + |1\rangle) \otimes (|f(0)\rangle + |f'(0)\rangle) & f(0) = f(1) \\ (|0\rangle + |1\rangle) \otimes (|f(0)\rangle + |f'(0)\rangle) & f(0) \neq f(1) \end{cases}$$

$U_f (H \otimes H)(|1\rangle \otimes$

... one of f_1, f_2, f_3, f_4

$\ldots_1, f_3 = 1$. we don't know which one

... i ?

... once.

$\ldots \otimes |1\rangle$

$\ldots 01\rangle + |10\rangle + |11\rangle)$

$\ldots \underbrace{(1+f(0))}_{f'(0)}\rangle + |1\, f(1)\rangle + |1\, \underbrace{(1+f(1))}_{f'(1)}\rangle)$

$\ldots (|f(0)\rangle + |f'(0)\rangle) \quad f(0) = f(1)$

$\ldots \otimes (|f(0)\rangle + |f'(0)\rangle) \quad f(0) \neq f(1)$

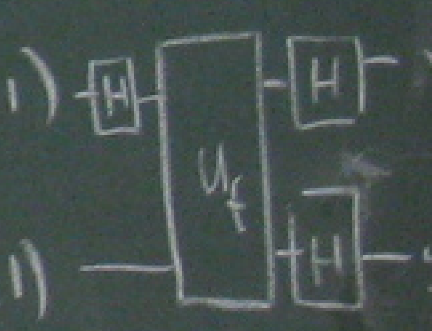
$$U_f (H \otimes H)(|1\rangle \otimes |1\rangle) = U_f \tfrac{1}{2} (|0\rangle - |1\rangle) \otimes (|0\rangle - |1\rangle)$$

$$= \tfrac{1}{2} U_f (|00\rangle - |01\rangle - |10\rangle + |11\rangle)$$

$$= \tfrac{1}{2} (|0 f(0)\rangle - |0 f'(0)\rangle - |1 f(1)\rangle + |1 f'(1)\rangle)$$

$$= \tfrac{1}{2} \begin{cases} (|0\rangle - |1\rangle) \otimes \overbrace{[\,|f(0)\rangle - |f(1)\rangle\,]}^{\sqrt{2}|\varphi\rangle} & f(0) = f(1) \\ (|0\rangle + |1\rangle) \otimes [\,|f(0)\rangle - |f(1)\rangle\,] & f(0) \neq f(1). \end{cases}$$

$$(H \otimes \mathbb{1}) U_f (H \otimes H) |1\rangle \otimes |1\rangle = \begin{cases} |1\rangle \otimes |\varphi\rangle & f(0) = f(1) \\ |0\rangle \otimes |\varphi\rangle & f(0) \neq f(1) \end{cases}$$



D) The problem of Bernstein and Vazirani

oracle: $U_f |x\rangle_m \otimes |y\rangle_1 = |x\rangle_m \otimes |y + a\cdot x\rangle_1$

$a \in \{0,1\}^m$ unknown.

$$a\cdot x = a_0 x_0 + a_1 x_1 + \dots + a_{m-1} x_{m-1}$$

How often do we need to call f to know a?

classically: m times

quantum: once.

$$f(x) = a\cdot x$$

$$\left(H^{\otimes m} \otimes H\right) U_f \left(H^{\otimes m} \otimes H\right)\left(|0\rangle_m \otimes |1\rangle_1\right)$$

$$= \text{——}\,\|\,\text{——}\; U_f \frac{1}{2^{m/2}} \sum_{x=0}^{2^m-1} |x\rangle_m \otimes \frac{1}{\sqrt{2}}\left(|0\rangle_1 - |1\rangle_1\right)$$

$$= \text{——}\,\|\,\text{——}\; 2^{-\frac{m+1}{2}} \sum_x U_f |x\rangle_m \otimes \left(|0\rangle_1 - |1\rangle_1\right)$$

$$= (H^{\otimes m} \otimes H_1)\, 2^{-\frac{m}{2}} \sum \underbrace{\frac{1}{\sqrt{2}}\Big[|x\rangle_m \otimes |f(x)\rangle_1 - |x\rangle_m \otimes |1 + f(x)\rangle_1 \Big]}$$

$$= |x\rangle_m \otimes \frac{1}{\sqrt{2}} \Big(|f(x)\rangle_1 - |1 + f(x)\rangle_1 \Big)$$

$$H|x\rangle = \frac{1}{\sqrt{2}} \sum_{\eta=0}^{1} (-1)^{x\cdot\eta} |\eta\rangle$$

$$\underbrace{|a\cdot x\rangle_1 - |1 + a\cdot x\rangle_1} = \begin{cases} |0\rangle - |1\rangle & a\cdot x = 0 \\ -(|0\rangle - |1\rangle) & a\cdot x = 1 \end{cases}$$

n.

$$= |x\rangle_m \otimes (-1)^{a\cdot x} \underbrace{\frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)}_{H|1\rangle_1}$$

$$= (H^{\otimes m} \otimes H) \frac{1}{2^{m/2}} \sum_{x=0}^{2^m-1} (-1)^{a\cdot x} |x\rangle_m \otimes H|1\rangle.$$

$$|x_{m-1} \dots x_1 x_0\rangle$$

$$= \frac{1}{2^m} \cdot \sum_{x} \sum_{\xi=0}^{2^m-1} (-1)^{a\cdot x} \cdot (-1)^{x\cdot\xi} |\xi\rangle_m \otimes |1\rangle_1.$$

$$= \sum_{\xi=0}^{2^m-1} \left(2^{-m} \sum_{x=0}^{2^m-1} (-1)^{(a +_2 \xi)\cdot x} \right) |\xi\rangle_m \otimes |1\rangle_1 = |a\rangle_m \otimes |1\rangle_1$$

$$\xi + a = 0 \mod 2$$

$$\xi = a \mod 2$$

$$\frac{1}{2^m} \sum_{x=0}^{2^m-1} (-1)^{x\cdot b} = \begin{cases} 1 & b = 0 \\ 0 & \text{otherwise.} \end{cases}$$

$$U_f (H \otimes H) ($$

$$=$$

$$=$$

$$=$$

$$(H \otimes \mathbb{1}) U_f ($$