Classical vs Quantum Computation

Information: bit $\{0,1\}$ → random bit / coin → quantum bit

$|0\rangle = \begin{bmatrix}1\\0\end{bmatrix}$, $|1\rangle = \begin{bmatrix}0\\1\end{bmatrix}$

amplitudes

$|\psi\rangle = a_0|0\rangle + a_1|1\rangle = \begin{bmatrix}a_0\\a_1\end{bmatrix} \in \mathbb{C}^2$

$|a_0|^2 + |a_1|^2 = 1$

coin flip $= \begin{cases} 0 & \text{with probability } p \\ 1 & \text{with probability } 1-p \end{cases}$ $\quad p + (1-p) = 1$

Operation: Boolean gates: NOT, AND, OR; NAND

Retrieve (read-out): ?

$\mathbb{C}^2 \ni |\psi\rangle \longleftrightarrow \boxed{U} \longrightarrow |\psi'\rangle \in \mathbb{C}^2$

input qubit — invertible matrix (unitary) — output qubit

$U = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, $U^\dagger = \begin{bmatrix} \bar a & \bar c \\ \bar b & \bar d \end{bmatrix} = U^{-1}$

$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} \bar a & \bar c \\ \bar b & \bar d \end{bmatrix} = \begin{bmatrix} |a|^2+|b|^2 & a\bar c + b\bar d \\ \bar a c + \bar b d & |c|^2+|d|^2 \end{bmatrix}$ $\quad U^{-1} = \bar U^T \doteq U^\dagger$

$U \, U^\dagger = U U^{-1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \iff$ $|a|^2+|b|^2 = 1 = |c|^2+|d|^2$, $a\bar c + b\bar d = 0 = \bar a c + \bar b d$

examples: Pauli matrices

$X^{-1} = X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, $Y^{-1} = Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$, $Z^{-1} = Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ (nop)

$|\psi\rangle = \begin{bmatrix}a_0\\a_1\end{bmatrix} \xrightarrow[\text{Not}]{X} \begin{bmatrix}a_1\\a_0\end{bmatrix}$ $\qquad \begin{bmatrix}a_0\\a_1\end{bmatrix} \xrightarrow{Y} \begin{bmatrix}-ia_1\\ia_0\end{bmatrix}$ $\qquad \begin{bmatrix}a_0\\a_1\end{bmatrix} \xrightarrow{Z} \begin{bmatrix}a_0\\-a_1\end{bmatrix}$

$\{|0\rangle \to |1\rangle, \; |1\rangle \to |0\rangle\}$ $\qquad \{|0\rangle \to |0\rangle, \; |1\rangle \to -|1\rangle\}$

$|0\rangle \overset{H}{\longleftrightarrow} |+\rangle$, $|1\rangle \overset{H}{\longleftrightarrow} |-\rangle$; $X: |0\rangle \leftrightarrow |1\rangle$; $Z: |+\rangle \leftrightarrow |-\rangle$

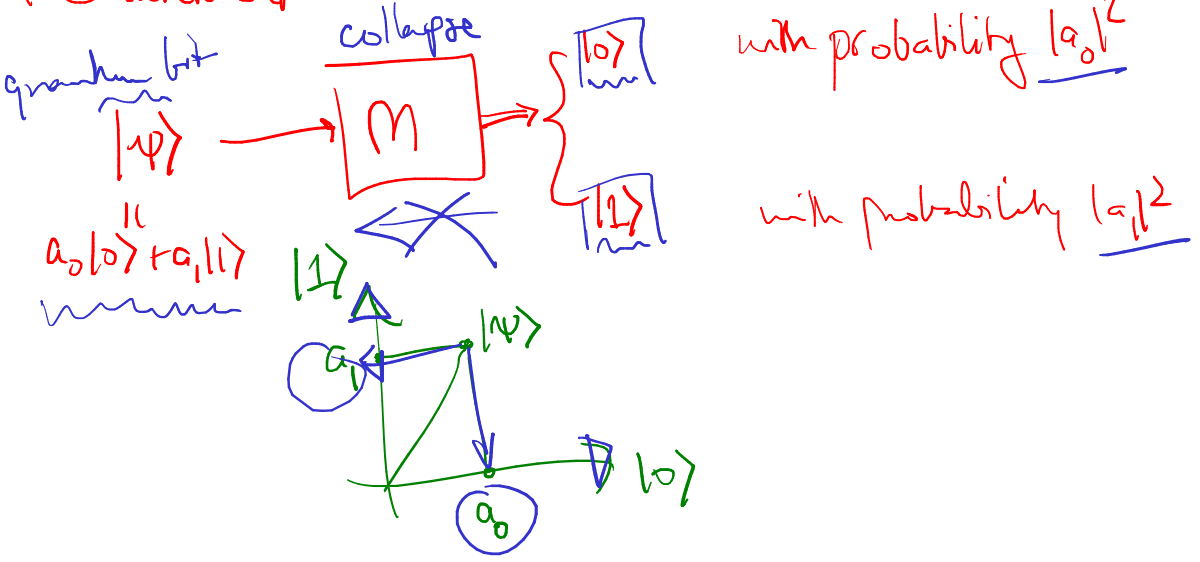
Hadamard: $H = \frac{1}{\sqrt2}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ $\qquad |+\rangle \overset{Z}{\longleftrightarrow} |-\rangle$

$X \begin{cases} |0\rangle \overset{H}{\longleftrightarrow} \frac{1}{\sqrt2}|0\rangle + \frac{1}{\sqrt2}|1\rangle \doteq |+\rangle \\ |1\rangle \overset{H}{\longleftrightarrow} \frac{1}{\sqrt2}|0\rangle - \frac{1}{\sqrt2}|1\rangle \doteq |-\rangle \end{cases} Z$

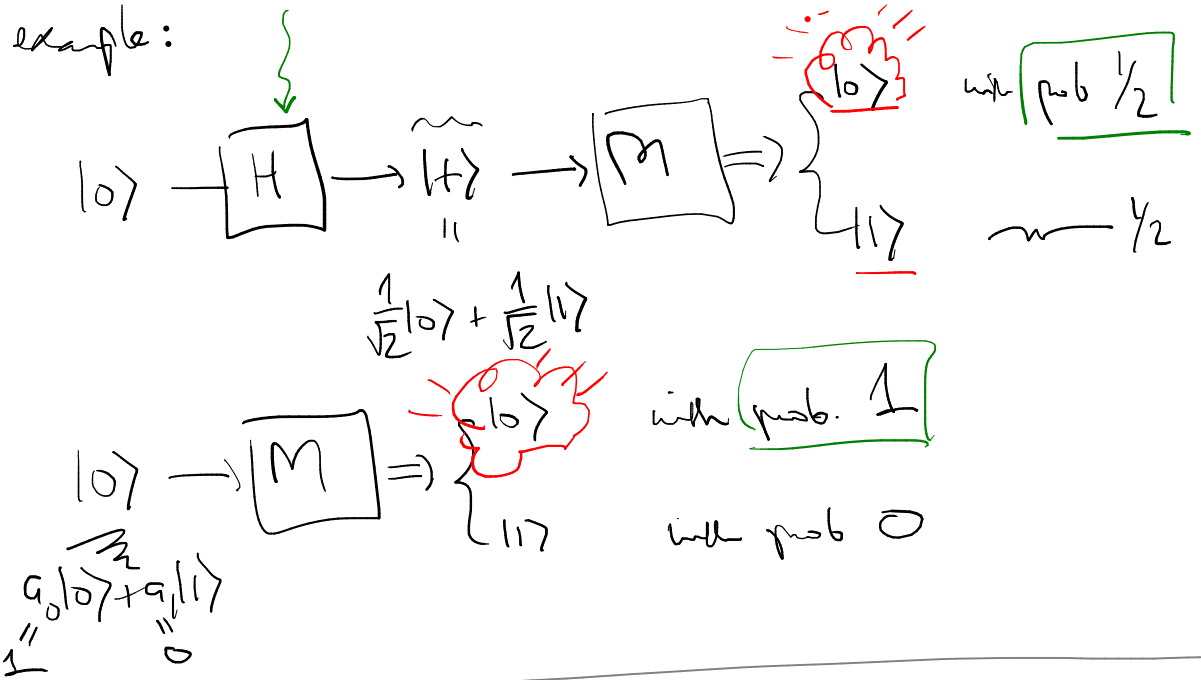
$Z|+\rangle = Z\left(\frac{1}{\sqrt2}|0\rangle + \frac{1}{\sqrt2}|1\rangle\right) = \frac{1}{\sqrt2}Z|0\rangle + \frac{1}{\sqrt2}Z|1\rangle$

$= \frac{1}{\sqrt2}|0\rangle - \frac{1}{\sqrt2}|1\rangle = |-\rangle$

Measurement:



example:



Bits $b \in \{0,1\}^n$ $\quad b = b_1 b_2 b_3 \dots b_n$ $\quad b_j \in \{0,1\}$

↳ concatenate individual bits

- 0 0
- 0 1
- 1 0
- 1 1

Quantum bits: 2-qubit state

$$|\psi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle$$

amplitudes $a_{00}, a_{01}, a_{10}, a_{11} \in \mathbb{C}$ $\quad |a_{00}|^2 + |a_{01}|^2 + |a_{10}|^2 + |a_{11}|^2 = 1$

$$|00\rangle = |0\rangle|0\rangle = |0\rangle \otimes |0\rangle = \begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix}$$

Tensor product or Kronecker product:

$$A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{bmatrix}$$

A: $m \times n$ $\quad$ B: $p \times q$ $\quad$ $A \otimes B$: $mp \times nq$

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & & & \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

$|00\rangle = |0\rangle \otimes |0\rangle = \begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} = \begin{matrix}00\\01\\10\\11\end{matrix}\begin{bmatrix}1\\0\\0\\0\end{bmatrix}$, $\quad \begin{bmatrix}0\\0\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}0\\0\\0\\0\end{bmatrix}$

$|01\rangle = |0\rangle \otimes |1\rangle = \begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}0\\1\end{bmatrix} = \begin{matrix}00\\01\\10\\11\end{matrix}\begin{bmatrix}0\\1\\0\\0\end{bmatrix}$

$|10\rangle = |1\rangle \otimes |0\rangle = \begin{bmatrix}0\\1\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} = \begin{matrix}00\\01\\10\\11\end{matrix}\begin{bmatrix}0\\0\\1\\0\end{bmatrix}$

$|11\rangle = |1\rangle \otimes |1\rangle = \begin{bmatrix}0\\1\end{bmatrix} \otimes \begin{bmatrix}0\\1\end{bmatrix} = \begin{matrix}00\\01\\10\\11\end{matrix}\begin{bmatrix}0\\0\\0\\1\end{bmatrix}$

$|01101\rangle = |0\rangle \otimes |1\rangle \otimes |1\rangle \otimes |0\rangle \otimes |1\rangle$

$2\times1 \quad 2\times1 \quad 2\times1 \quad 2\times1 \quad 2\times1$

$32 \times 1 = \begin{bmatrix}0\\1\\0\end{bmatrix} \begin{matrix}00000\\\vdots\\01101\\\vdots\\11111\end{matrix}$

Dirac notation: ket $|u\rangle = \begin{bmatrix}a_1\\a_2\\\vdots\\a_n\end{bmatrix}$ column vector

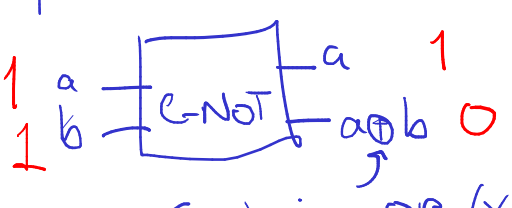
dot/inner product: bra $\langle u| = |u\rangle^\dagger = \begin{bmatrix}\bar{a}_1 & \bar{a}_2 & \cdots & \bar{a}_n\end{bmatrix}$

$\langle u|v\rangle = \begin{bmatrix}\cdots\end{bmatrix}\begin{bmatrix}\vdots\end{bmatrix}$ bracket = scalar (bra, ket)

$|u\rangle\langle v| = \begin{bmatrix}\cdot\\\cdot\\\cdot\end{bmatrix}\begin{bmatrix}\cdot & \cdot & \cdot\end{bmatrix} = \begin{bmatrix}\cdot & \cdot & \cdot\\\cdot & \cdot & \cdot\\\cdot & \cdot & \cdot\end{bmatrix}$ outer product

$C^2 = I \Rightarrow C^{-1} = C$

Operator on 2-qubit: Controlled NOT

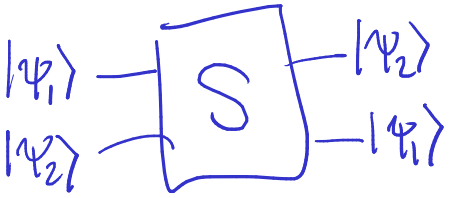


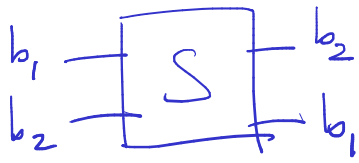
Exclusive OR (XOR)

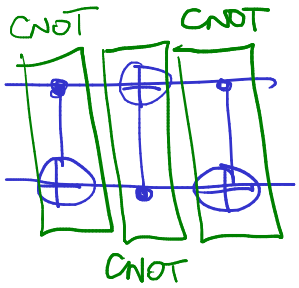
$C = \begin{matrix}00\\01\\10\\11\end{matrix}\begin{bmatrix}1 & & & \\ & 1 & & \\ & & & 1 \\ & & 1 & \end{bmatrix}$ (columns 00 01 10 11)

$= \begin{bmatrix}I_2 & 0\\0 & X\end{bmatrix}\begin{bmatrix}I_2 & 0\\0 & X\end{bmatrix} = \begin{bmatrix}I_2 & 0\\0 & I_2\end{bmatrix}$

Swap



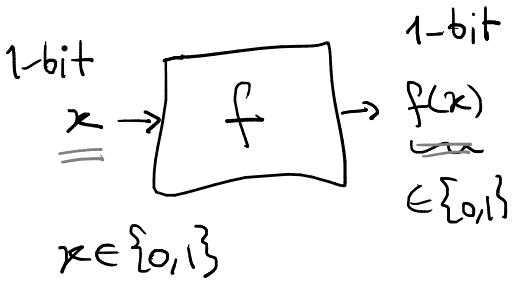




$$S = \begin{array}{c} \\ 00 \\ 01 \\ 10 \\ 11 \end{array} \begin{array}{c} \begin{array}{cccc} 00 & 01 & 10 & 11 \end{array} \\ \begin{bmatrix} 1 & & & \\ & & 1 & \\ & 1 & & \\ & & & 1 \end{bmatrix} \end{array}$$

Deutsch-Josza problem:

classical



x	f(x)
0	0/1
1	0/1

non-constant

0 0 1 1

0 1 0 1

Constant function

Question: determine if f is constant or not

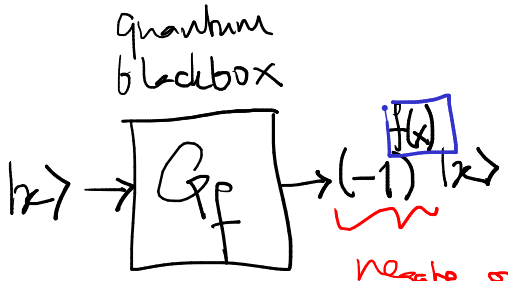
Cost: # queries to the blackbox

classical: need 2 queries

quantum: 1 query is enough

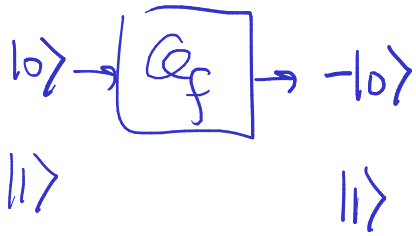
ex:

x	f
0	1
1	0



negate or not

$f=1$ $f=0$



$f(x)\in\{0,1\}$

Deutsch-Josza circuit

$$|0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \xrightarrow{\text{query } U_f} \frac{1}{\sqrt{2}}(-1)^{f(0)}|0\rangle + \frac{1}{\sqrt{2}}(-1)^{f(1)}|1\rangle$$

$$= \frac{1}{\sqrt{2}}(-1)^{f(0)}\left[|0\rangle + (-1)^{f(0)+f(1)}|1\rangle\right]$$

$(-1)^{f(0)+f(0)} = 1$ (even)

if $f(0)=f(1)$:

$$= (-1)^{f(0)}|+\rangle$$

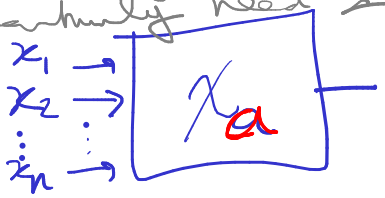
if $f(0)\neq f(1)$:

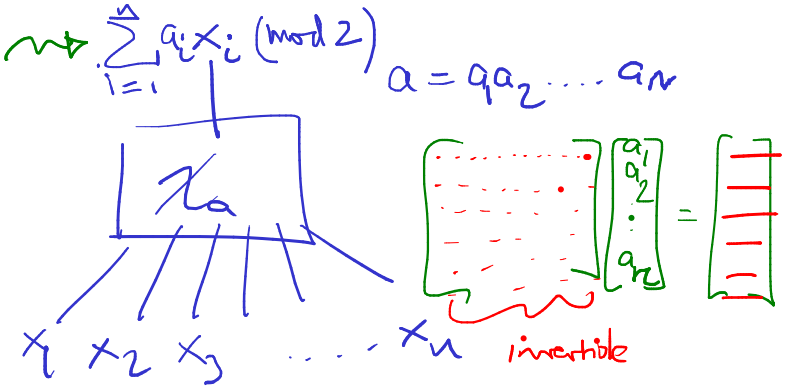
$$= (-1)^{f}|-\rangle$$

$$\xrightarrow{H} \begin{cases} (-1)^{f(0)}|0\rangle \\ (-1)^{f(0)}|1\rangle \end{cases} \xrightarrow{M} \Rightarrow$$

Bernstein-Vazirani:

classically need n queries
quantumly need 1 query





parity on n bits

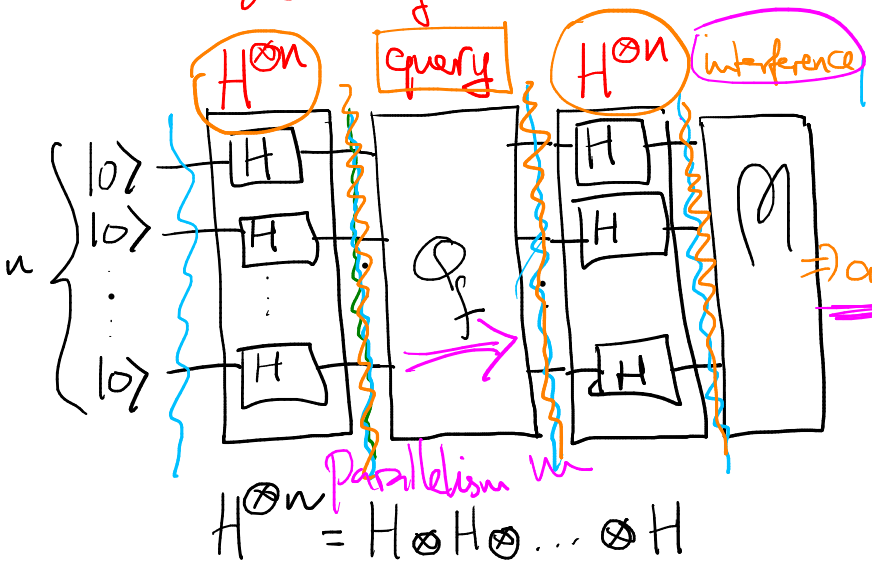
$a \in \{0,1\}^n$

ex: $a = 10110$ mask

$x = 10101$

$1+1+0 = 2 \pmod 2$ → even, odd

2^n many such a's



Parallelism in

$H^{\otimes n} = H \otimes H \otimes \dots \otimes H$

$|0^n\rangle \xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle$

$\xrightarrow{Q_f} \frac{1}{\sqrt{2^n}} \sum_x (-1)^{f(x)} |x\rangle$

parity indexed by a

$\chi_a(x) \in \{\pm 1\}$

$\xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{2^n}} \sum_x \chi_a(x) \frac{1}{\sqrt{2^n}} \sum_y \chi_y(x) |y\rangle$

$= \sum_y \left[\frac{1}{2^n} \sum_x \chi_{a \oplus y}(x) \right] |y\rangle$

average of $\chi_{a \oplus y}$

$a \oplus y = 0^n \Leftrightarrow y = a$

$= |a\rangle$

$\xrightarrow{M}$

Claim

$|x\rangle \xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} \chi_y(x) |y\rangle$

3-bit

x	$\chi_{101}(x)$	$\chi_{000}(x)$
000	1	1
001	-1	1
010	1	1
011	-1	1
100	-1	1
101	1	1
110	-1	1
111	1	1
	0	2^3

$a = 101$

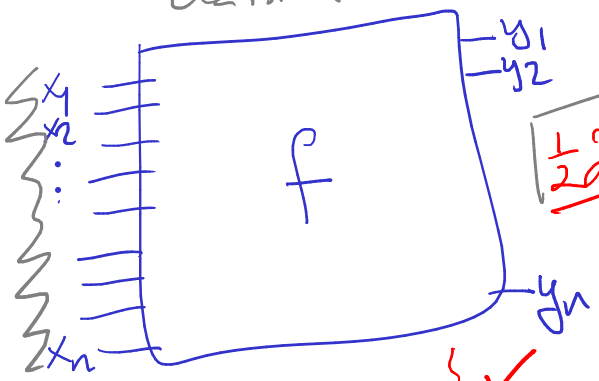
$a \neq 000$

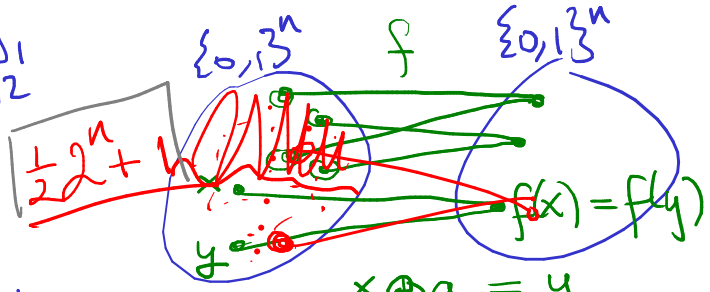
Simon's problem: promise

Quantumly n^c

Classical

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





$x \oplus a = y$

Domain ↑ Range

Shift

f is either 1:1 or 2:1 with period $a \in \{0,1\}^n$

bijective

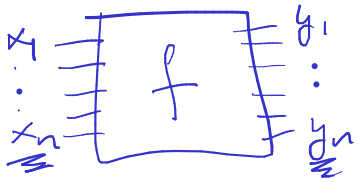
unknown

⇓

Shor's Factoring

Simon's algorithm:

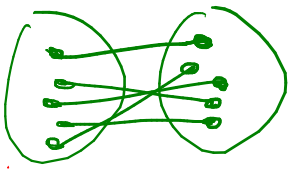
$f: \{0,1\}^n \to \{0,1\}^n$ — which case are we in?



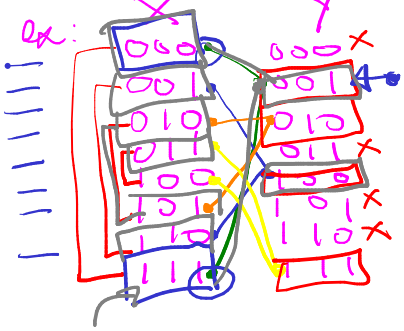
Promise: f is either **1:1** or

f is **2:1 with period s, $s \in \{0,1\}^n$**

$y = f(x)$, $x = x_1 x_2 \dots x_n$, $y = y_1 y_2 \dots y_n$



$\frac{1}{2}2^n + 1$ queries



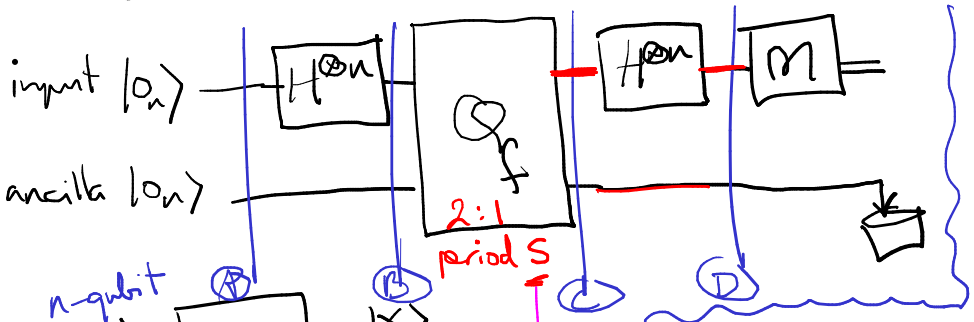
$s = 111$

$x = 000$

$x \oplus s = 000 \oplus 111 = 111$ (bitwise XOR)

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle|f(x)\rangle = [|000\rangle + |111\rangle]|001\rangle + [|001\rangle + |110\rangle]|100\rangle + [|010\rangle + |101\rangle]|010\rangle + [|011\rangle + |100\rangle]|111\rangle$$

Quantum circuit: measure

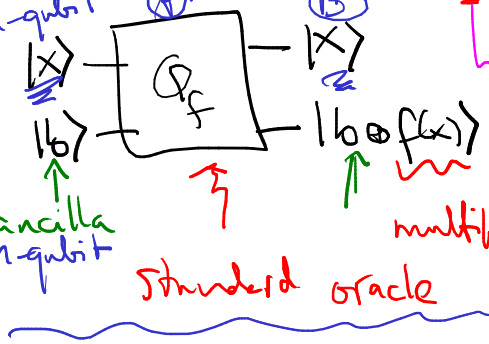


(A) $|0_n\rangle \otimes |0_n\rangle = |0_n\rangle|0_n\rangle$

(B) $\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle|0_n\rangle$

$0_n \oplus f(x) = f(x)$

2:1, $s \in \{0,1\}^n$



(C) $\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle|f(x)\rangle$ — $(\tilde{x}, \tilde{x} \oplus s)$

$$= \frac{1}{\sqrt{2^n}} \sum_{\tilde{x}} \left(|\tilde{x}\rangle + |\tilde{x} \oplus s\rangle\right)|f(\tilde{x})\rangle$$

(D) $$\frac{1}{\sqrt{2^n}} \sum_{\tilde{x}} \left[|\tilde{x}\rangle|f(\tilde{x})\rangle + |\tilde{x} \oplus s\rangle|f(\tilde{x})\rangle\right] \xrightarrow{H^{\otimes n} \otimes I}$$

$$\frac{1}{\sqrt{2^n}} \sum_{\tilde{x}} \left[\frac{1}{\sqrt{2^n}} \sum_y \chi_y(\tilde{x})|y\rangle + \frac{1}{\sqrt{2^n}} \sum_y \chi_y(\tilde{x} \oplus s)|y\rangle\right]|f(\tilde{x})\rangle \quad (*)$$

Last time: fact:

$$|x\rangle \xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{2^n}} \sum_y \chi_y(x)|y\rangle \quad \text{where} \quad \chi_y(\tilde{x}) = (-1)^{y \cdot \tilde{x}}$$

$$\chi_a(b) = (-1)^{a\cdot b} = (-1)^{\sum_{i=1}^{n} a_i b_i} \qquad a, b \in \{0,1\}^n$$

$$= \begin{cases} +1 & \text{if } \sum a_i b_i \text{ is even} \\ -1 & \text{if } \sum a_i b_i \text{ is odd} \end{cases}$$

$$\chi_a(b) = (-1)^{a_1 b_1} (-1)^{a_2 b_2} \cdots (-1)^{a_n b_n} = (-1)^{a_1 b_1 + a_2 b_2 + \cdots + a_n b_n}$$

mask

$a_1 = 1$: $(-1)^{b_1}$ — if $b_1 = 1$: -1; if $b_1 = 0$: $+1$

$a_2 = 0$: $+1$

a: mask 11111|0000

b: ##|####

#1's

---

① $$\frac{1}{2^n} \sum_x \sum_y \left[\chi_y(x) + \chi_y(x \oplus s) \right] |y\rangle |f(x)\rangle$$

$\chi_y(x \oplus s) = \chi_y(x)\chi_y(s)$

$$= \frac{1}{2^n} \sum_x \sum_y \chi_y(x) \left[1 + \chi_y(s) \right] |y\rangle |f(x)\rangle$$

$\chi_y(s) \in \pm 1$

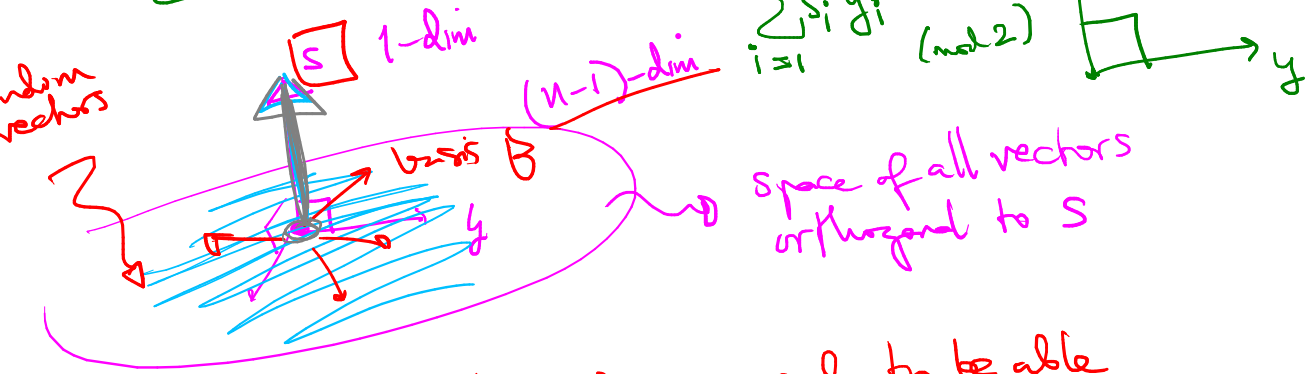
if $\chi_y(s) = -1$:

$$= \frac{2}{2^n} \sum_x \sum_{y:} \chi_y(x) |y\rangle |f(x)\rangle$$

$\chi_y(s) = 1$

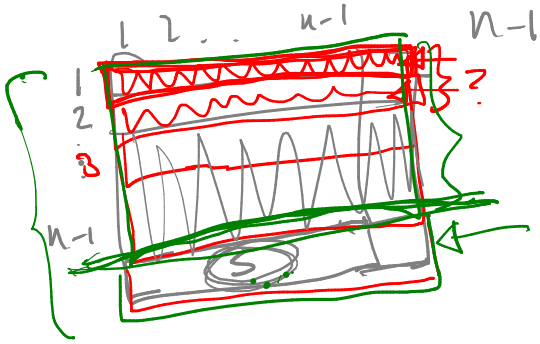
measure → random y so that $s \cdot y = 0$ "orthogonal"

$\sum_{i=1}^{n} s_i y_i \equiv 0 \pmod 2$



How many random vectors do we need to be able to build a basis? Polynomial in n rounds

$n-1$ linearly independent vectors $\perp$ s

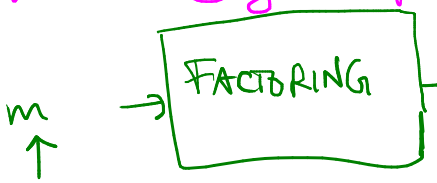


n rounds ⇒ discover s

$2^{n-1} + 1$ rounds

Shor's Factoring algorithm

Shor 1994: FACTORING is easy in a quantum world



m: positive composite integer

d: nontrivial divisor of m

Cost: try all divisors of m: 2, 3, 4, ..., m−1 ≈ 2^|m|

where r is smallest positive integer s.t.

$$a^r \equiv 1 \pmod m$$

$gcd(a,m)=1$

a, m are coprime (no shared divisors)

$gcd(2,15)=1$

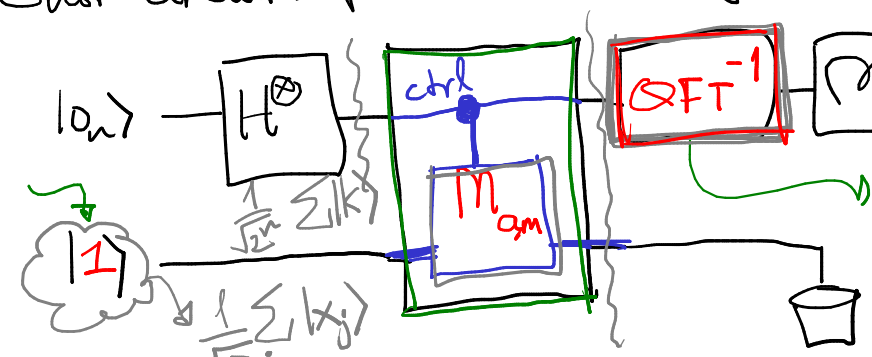
$a^1, a^2, a^3, \ldots, \equiv 1 \pmod m$ — Stop when we obtain 1

runningtime is wrt the binary lengths of m, a

There is no known efficient algorithm for FACTORING.

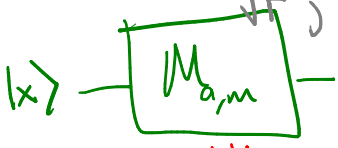
The hardness of FACTORING is used as a security guarantee for many crypto systems (RSA, SSL, ...)

Shor circuit: for Period Finding with inputs m & a with $gcd(a,m)=1$



$r \equiv 1 \pmod m$ (inverse)

Quantum Fourier Transform

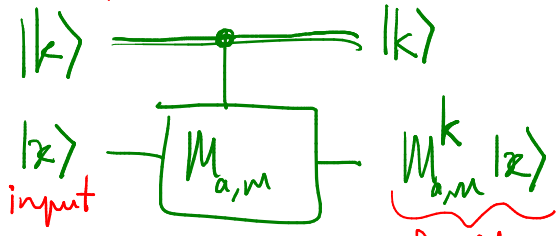


invertible since $gcd(a,m)=1$

reversible classical computing

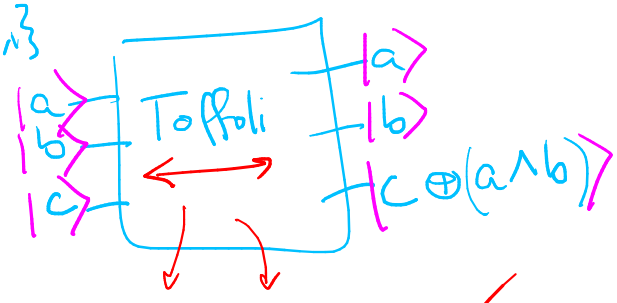
classical computing ⇒ quantum computing

Counter

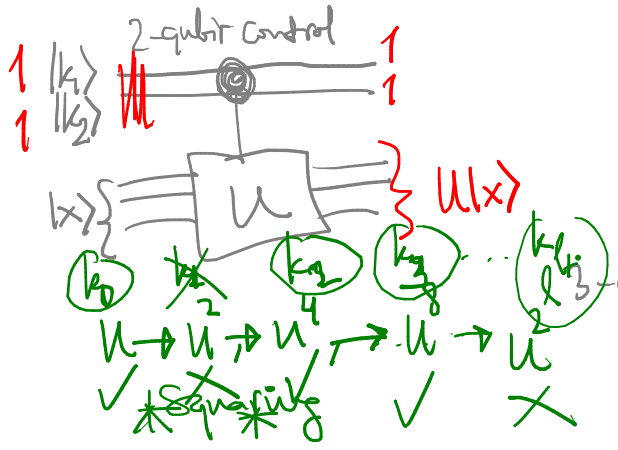


apply $M_{a,m}$ to $|x\rangle$ k times

$a,b,c \in \{0,1\}$



NOT AND ✓



$$U^k = U^{2k_2+k_1} = (U^2)^{k_2}(U^1)^{k_1}$$

$k = k_3k_2k_1$

$$U^k = U^{4k_3+2k_2+k_1} = (U^4)^{k_3} \times (U^2)^{k_2} \times U^{k_1}$$

$|k\rangle = |k_2k_1\rangle$ · product

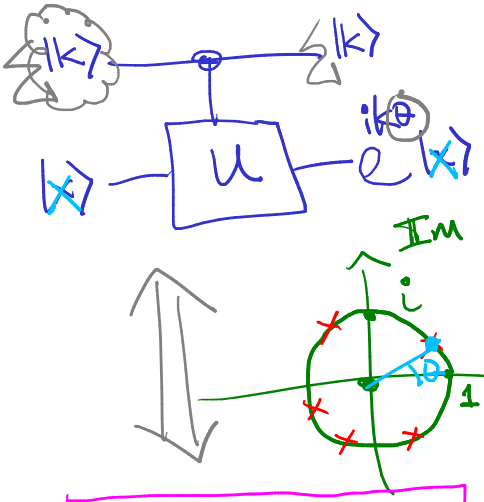
· squaring

high order bit — low order bit

4-qubit: $k = \boxed{k_3k_2k_1}$

$$U^k = (U^8)^{k_4} \times (U^4)^{k_3} \times (U^2)^{k_2} \times (U^1)^{k_1}$$

GRL-U



- unitary U: length preserving isometry
- eigenvalues of U are of the form
- eigenvectors

$$U^k|x\rangle = e^{ik\theta}|x\rangle$$

normalized

quantum state norm 1 $\quad \| |x\rangle \| = 1$

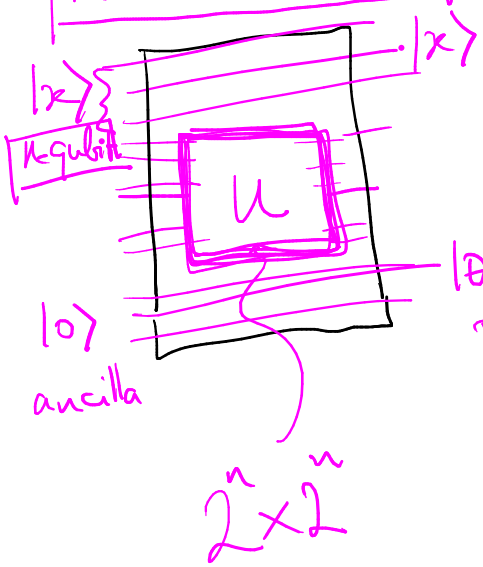
Phase Estimation

eigenvalue estimation assumption

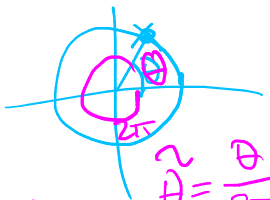
$$U|x\rangle = e^{i\theta}|x\rangle \qquad \theta \in \mathbb{R}$$

cycle

input



precision?



$$\tilde{\theta} = \frac{\theta}{2\pi} \in [0,1)$$

$2^n \times 2^n$

$$e^{i\theta} = e^{2\pi i\tilde{\theta}}$$