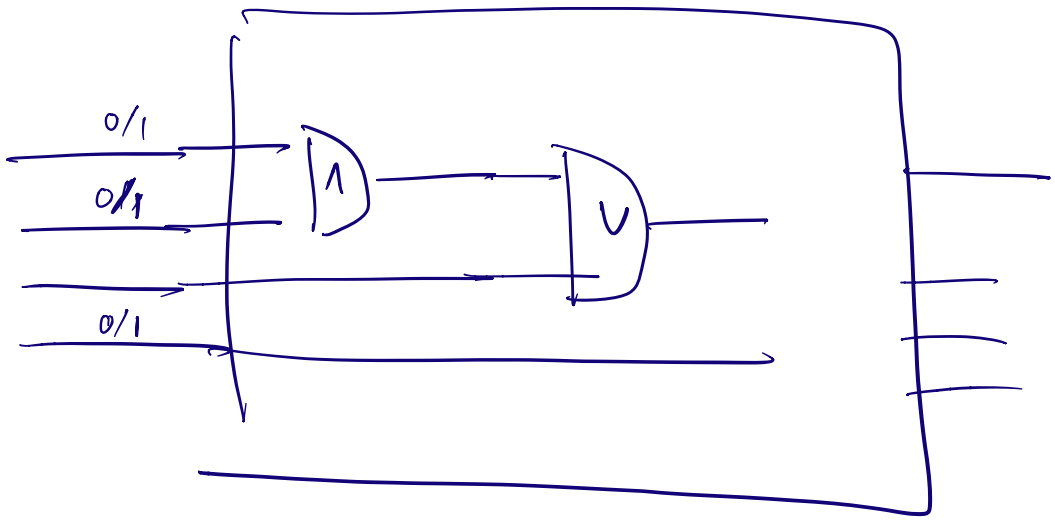


Deterministic ckts

Maps from $\{0,1\}^n \to \{0,1\}^m$

- Allowed operations:

  low-arity Boolean fns.

Randomized ckt

Wires carrying a distribution.

n wires.

Contents are specified by a

2^n-dimensional vector p

s.t. $\sum_{x \in \{0,1\}^n} p(x) = 1.$

Suppose we look at the first b wires. Then we get a sample $y \in \{0,1\}^b$ with pr of seeing y equal to

$$\sum_{z \in \{0,1\}^{n-b}} p(yz),$$

and the contents of the remaining $n-b$ wires now carry the distribution $q(z) = \frac{p(yz)}{\sum_{\tilde{z} \in \{0,1\}^{n-b}} p(y\tilde{z})}$

2e30,13

Again can apply low arity gates.

Quantum Ckts

n wires, each with 2 basic states 0 and 1.

Contents of a wire are

$$\alpha|0\rangle + \beta\cdot|1\rangle$$

where $\alpha, \beta \in \mathbb{C}$, $|\alpha|^2 + |\beta|^2 = 1$.

(instead of

$$p_0\cdot|0\rangle + p_1|1\rangle$$

where $p_0, p_1 \in [0,1]$)

$p_0 + p_1 = 1$.

Contents of 2 wires described by:

$$\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}\cdot|10\rangle + \alpha_{11}\cdot|11\rangle$$

where $\alpha_{ij} \in \mathbb{C}$.

$$\sum |\alpha_{ij}|^2 = 1.$$

Allowed operations:

all operations are low-arity Unitary matrices:

① U Unitary s.t. $U^* U = I$

$(\Leftrightarrow \quad \|Ux\|_2 = \|x\|_2)$

(2) Operates on only $O(1)$ many wires.

(arity $r \Rightarrow$ U is a $2^r \times 2^r$ matrix).

As an operation on n-qubit states, it looks like $U \otimes I$.

(U: 4×4, small; I: $2^{n-2} \times 2^{n-2}$, huge)

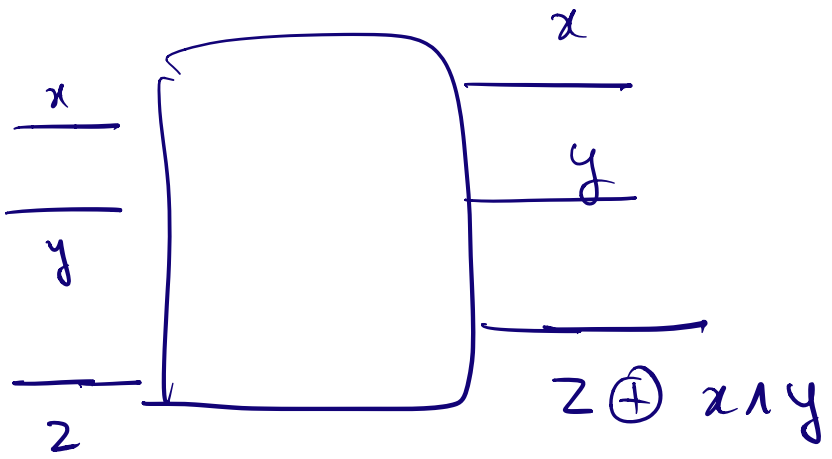
1-qubit Hadamard gate.

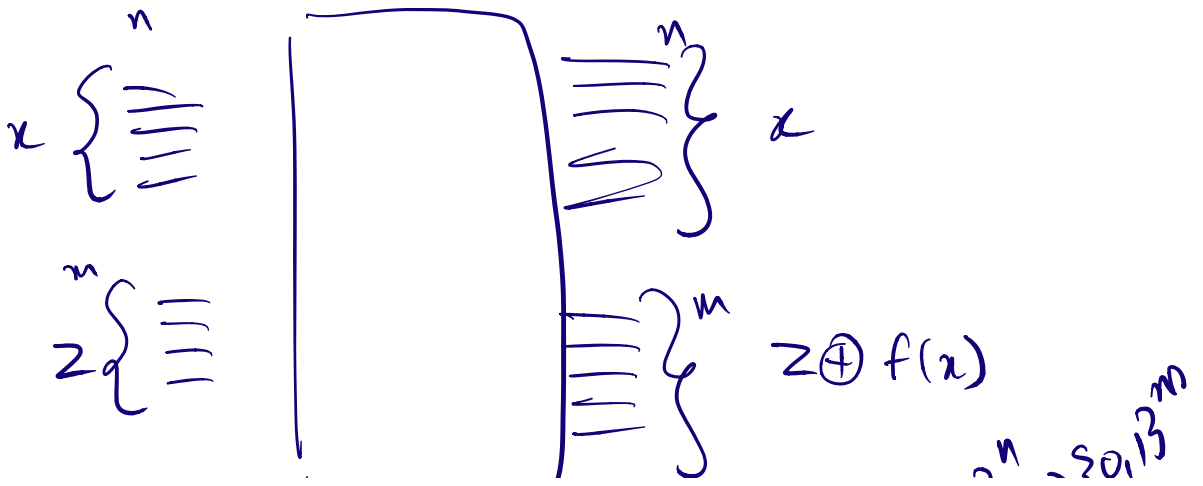
$$U = \begin{array}{c} \\ |0\rangle \\ |1\rangle \end{array} \begin{array}{c} \begin{array}{cc} |0\rangle & |1\rangle \end{array} \\ \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{bmatrix} \end{array}$$

$$U \cdot (|0\rangle) = \left(\frac{1}{\sqrt{2}}\right) \cdot |0\rangle + \sqrt{2}\,|1\rangle$$

$$U \cdot (|1\rangle) = \frac{1}{\sqrt{2}} \cdot |0\rangle + \left(\frac{-1}{\sqrt{2}}\right) \cdot |1\rangle$$

Reversible computation.





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

Factoring integers.

1. Factoring n reduces to finding the order of x in $\mathbb{Z}_n^*$.

2. Finding the order of x in $\mathbb{Z}_n^*$.

Quantum

(1) Quantum Fourier Transform.

(2) Classical computation of map $a \mapsto x^a \pmod n$

is possible

in reverse way.

Suppose n is not a prime power.

$n = \prod_i p_i^{e_i}$

Suppose x has even order $= r$.

Then $x^r \equiv 1 \pmod n$

and $x^{r/2} \not\equiv 1 \pmod n$.

$n \mid x^r - 1 = (x^{r/2} - 1)(x^{r/2} + 1)$

Consider $d = GCD(n, x^{r/2} - 1)$.

If it is 1 or n, we fail.

If r is the order, then

$x^{r/2} - 1 \not\equiv 0 \bmod n$

So $d \neq n$.

If $d=1$, then

$$n \mid x^{r/2}+1.$$

$$\Rightarrow x^{r/2} \equiv (-1) \mod n.$$

$$\Rightarrow x^{r/2} \equiv (-1) \pmod{p_i^{e_i}}.$$

Algorithm

Pick $x \in \mathbb{Z}_n^*$ at random.

Compute $r = \text{order}(x)$ in $\mathbb{Z}_n^*$ using quantum.

Compute $GCD(x^{r/2}-1, n)$.

This fails iff $x^{r/2} \equiv -1 \pmod{p_i^{e_i}}$ for all i.

Let r_i = order of x in $\mathbb{Z}_{p_i^{e_i}}^*$.

$r = \text{LCM}(r_1, r_2, \ldots)$.

We know $x^{r_i} \equiv 1 \pmod{p_i^{e_i}}$

So $x^{r_i/2} \equiv \pm 1 \pmod{p_i^{e_i}}$

Chance of this is $\leq \frac{1}{2}$.

Finding the order of x in $\mathbb{Z}_n^*$.

Let q be a power of 2.

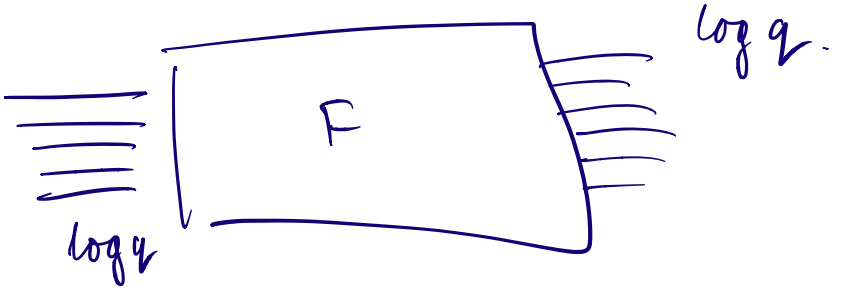
Consider $F = \begin{matrix} & & b & \\ & \cdots & \cdots & \cdots \\ a & \cdots & e^{2\pi i \frac{ab}{q}} & \cdots \end{matrix}$

$$\begin{bmatrix} & & & \\ & & & \\ & & & \\ & & & \end{bmatrix}$$

The Fourier transform matrix.

Unitary.

Fact: The unitary F can be computed in $\text{poly}(\log q)$ quantum operations.



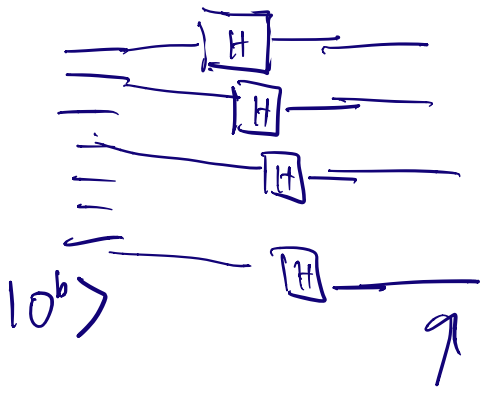
$$\sum_{a=0}^{q-1} \alpha_a |a\rangle \longmapsto \sum_{a=0}^{q-1} \alpha_a \cdot \sum_{b=0}^{q-1} \omega^{ab} \cdot |b\rangle$$

$$= \sum_{b=0}^{q-1} \left(\sum_a \alpha_a \omega^{ab} \right) |b\rangle$$

This is basically FFT.

The order finding algorithm.

~~First~~ (A) start with:



$$\sum_{y \in \{0,1\}^b} \left(\frac{1}{\sqrt{2}}\right)^b \cdot |y\rangle$$

$$= \frac{1}{2^{b/2}} \cdot \sum_{y \in \{0,1\}^b} |y\rangle$$

(B) Use a classical reversible computation (by repeated squaring mod n) to compute

$$\frac{1}{(\sqrt{2})^b} \sum_{y \in \{0,1\}^b} |y\rangle |0\rangle \mapsto$$

$$\frac{1}{\sqrt{2^b}} \sum_{y \in \{0,1\}^b} |y\rangle |(x^y \bmod n)\rangle$$

$|0\rangle|0\rangle = |00\rangle$

(c) Do Fourier Transform.

$$\frac{1}{2^{b/2}} \sum_{y \in \{0,1\}^b} |y\rangle |x^y \bmod n\rangle$$

$$\mapsto \frac{1}{2^{b/2} \cdot 2^{b/2}} \sum_{y \in \{0,1\}^b} \sum_{z=0}^{2^b-1} e^{\frac{2\pi i y z}{2^b}} |z\rangle |x^y \bmod n\rangle$$

y as an integer $< 2^b$

$$= \quad (q = 2^b)$$

$$\frac{1}{q} \sum_{y,z=0}^{q-1} \left(\omega^{yz} \right) |z\rangle |x^y \bmod n\rangle$$

z: $q = 2^b$ values

$x^y \bmod n$: takes r values $< n$

(1) Look at $z, (x^y \bmod n)$.

$$\sum \left(\sum_{y : x^y = h \bmod n} \omega^{yz} \right) |z\rangle |h\rangle$$

$h \in \langle x \rangle \leq \mathbb{Z}_n^*$

$z \in \{0, 1, \ldots q-1\}$

FINAL ANALYSIS

$\left(\sum_{y : x^y \equiv h \bmod n} \omega^{yz} \right)$ is big

for some special z's,

and those z's can tell

you the order of x.