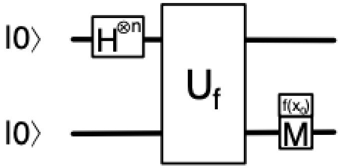
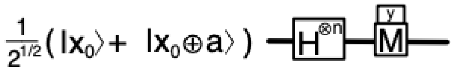
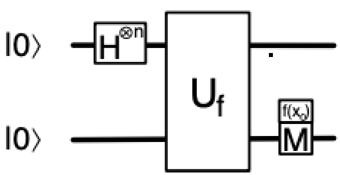
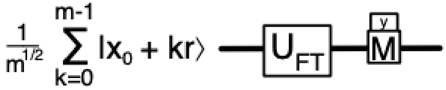
Lecture 18, 3 Nov 2020



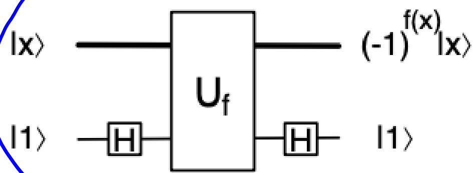


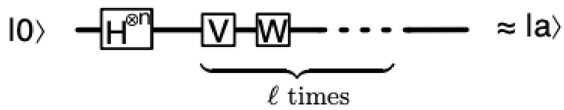
Simon '94 (p.56), $f(x) = f(x \oplus a)$, measured y has $a \cdot y = 0$ (equivalently $\sum_i a_i y_i = 0$ mod2), exponential speedup ($2^{n/2} \to O(n)$) to determine a



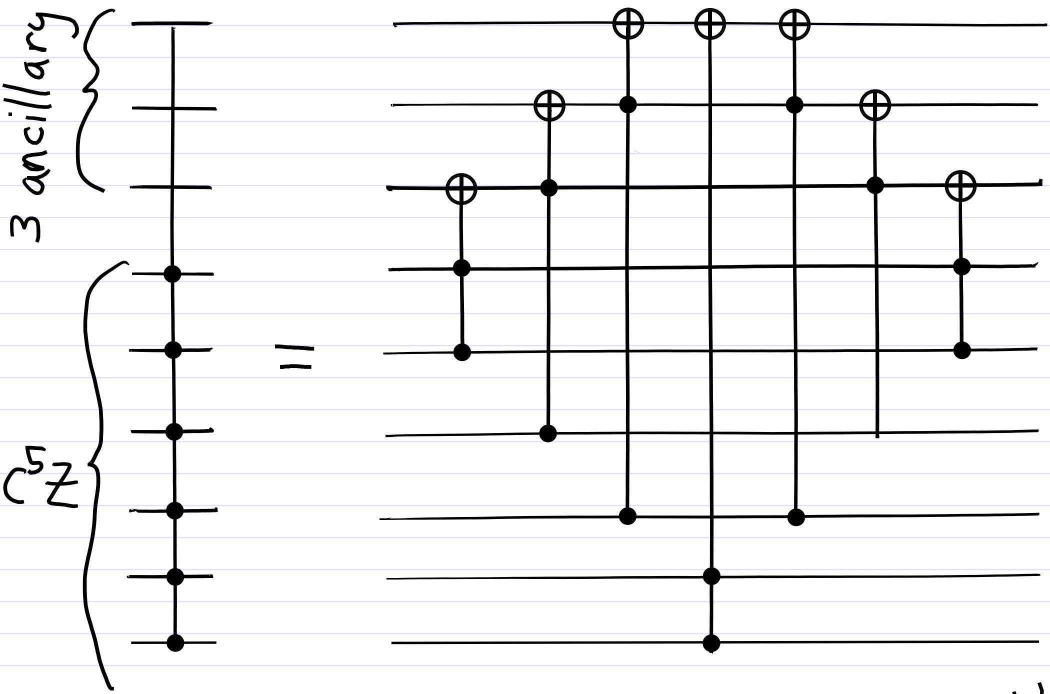


Shor '94 (p.70), $f(x) = f(x + r)$, resulting y is measured with probability $p(y) = \frac{1}{2^n m}\left|\sum_{k=0}^{m-1} \mathrm{e}^{2\pi i k r y/2^n}\right|^2$, gives $|y - 2^n/r| < 1/2$ with $p > .4$, sufficient to determine period r via partial fraction expansion, exponential speedup ($n2^n, \exp(n^{1/3}) \to O(n^3)$).
(Note: replaces $\mathbf{H}^{\otimes n}|x\rangle = \frac{1}{2^{n/2}}\sum_{0 \le y < 2^n} \mathrm{e}^{i\pi x \cdot y}|y\rangle$ with $\mathbf{U}_{\mathrm{FT}}|x\rangle = \frac{1}{2^{n/2}}\sum_{0 \le y < 2^n} \mathrm{e}^{2\pi i x y/2^n}|y\rangle$.)
Practical application is $f(x) \equiv b^x \bmod N$, where $b \equiv a^c \bmod N$ is an encrypted message, from which d', satisfying $cd' \equiv 1 \bmod r$, can be calculated, and d' recovers unencrypted message $a \equiv b^{d'} \bmod N$ (in contrast to using d, with $cd = 1 \bmod (p-1)(q-1)$, where $N = pq$ and r divides $(p-1)(q-1) = |G_{pq}|$).

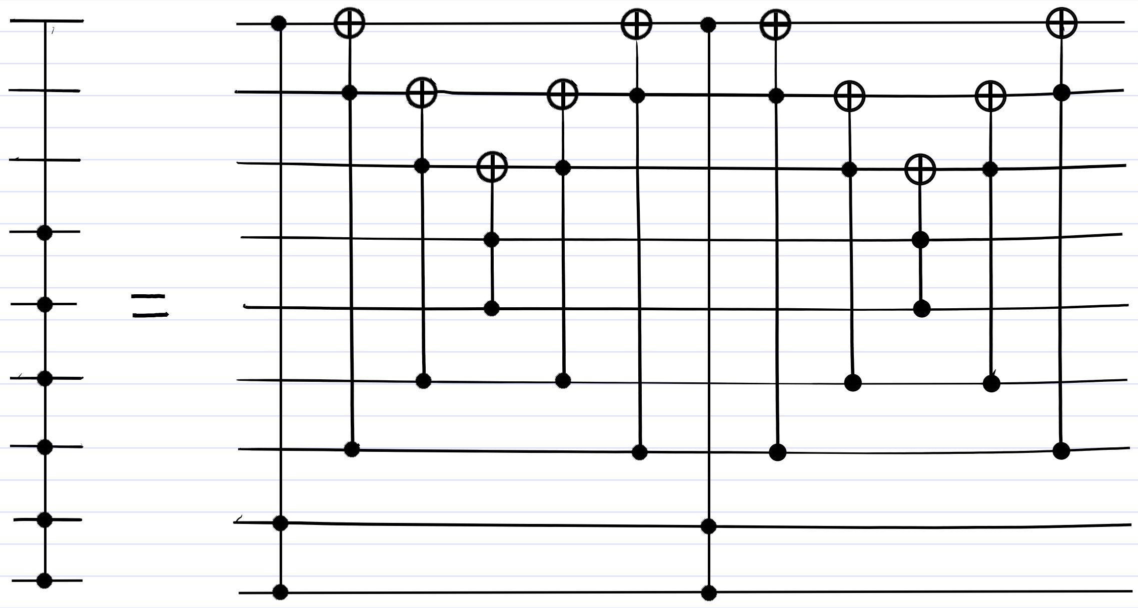




Grover '96 (p.90), $f(x) = 1$ only for (m) marked value(s) $x = a$, uses "phase kickback" to express $\mathbf{U}_f$ in terms of $\mathbf{V} = \mathbf{1} - 2|a\rangle\langle a|$, and $\mathbf{W} = 2|\phi\rangle\langle\phi| - \mathbf{1} = \mathbf{H}^{\otimes n}(2|0\rangle\langle 0| - \mathbf{1})\mathbf{H}^{\otimes n}$ is easily constructed. Applying $\ell \approx \frac{\pi}{4}\frac{2^{n/2}}{\sqrt{m}}$ times gives probability $p(a) \approx 1 - O(m/2^n)$, for square-root speedup ($2^n/m \to \sqrt{2^n/m}$).

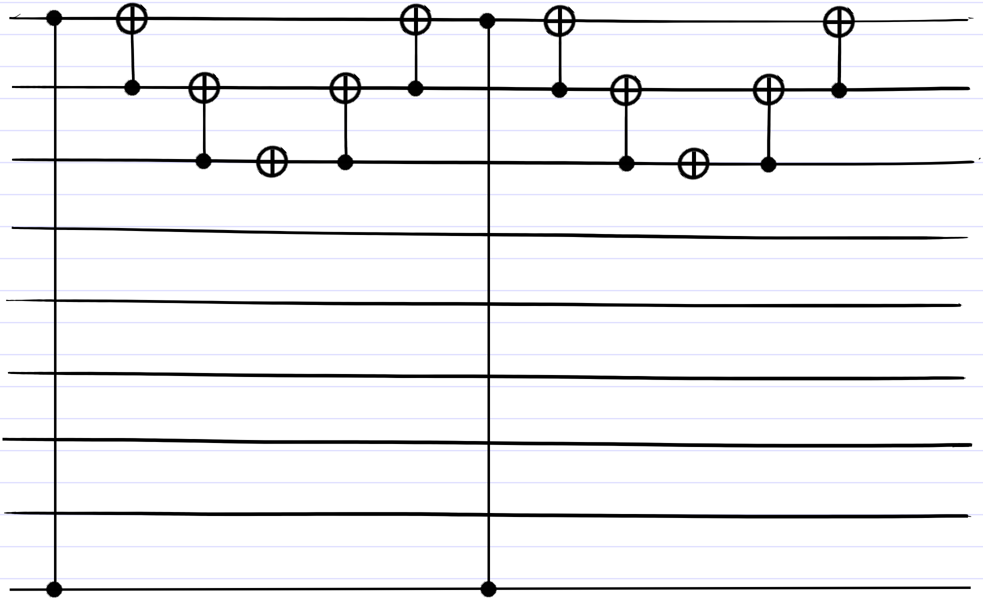


For n-fold $C^{n-1}Z$, needs n-3 ancillary initialized to $|0\rangle$

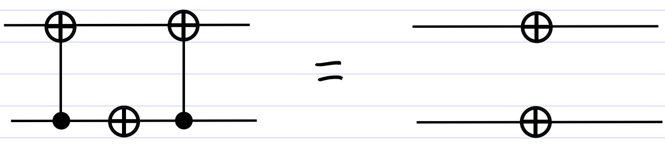


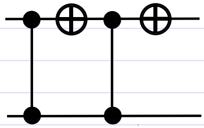
Now the ancillaries can have any states (or even be entangled with other qubits)

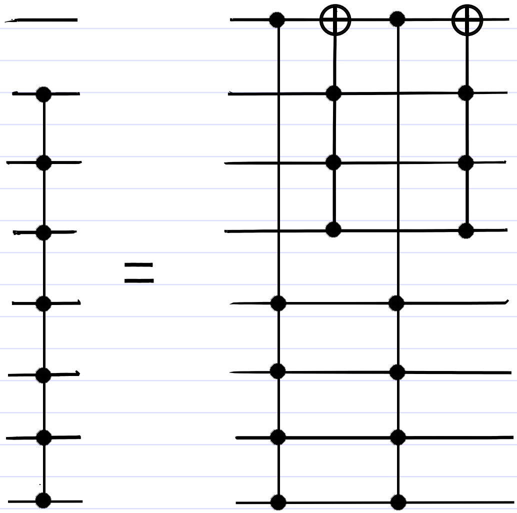
If any of the upper four (of six) are $|0\rangle$, then reduces to identity (pairwise cancellation)



If the upper five (of six) are all on, becomes the above.

Then use 

(twice) to reduce to 



Above a construction where the ancillaries of some can be the control bits of others

Collision problem

N items, classically check m

$N \sim \frac{1}{2} m(m-1)$ so need $m \sim N^{1/2}$

Quantum: look at some fraction

$m \sim N^a$, call them marked

Grover $\sqrt{N/m} \sim \left(N/N^a\right)^{1/2}$

optimum $N^a \sim N^{(1-a)/2}$

$a = \frac{1-a}{2} \Rightarrow \boxed{a = 1/3}$

So both $N^{1/3}$

Parity of n bits QM $n/2$ (barely speedup)

OR (any one is on) no speedup

Why $N^{1/2}$?

Classically work with probabilities

$$\frac{1}{N}, \frac{2}{N}, \ldots \frac{m}{N} \sim 1$$

QM: work with amplitudes

$$\frac{1}{\sqrt{N}}, \frac{2}{\sqrt{N}}, \frac{3}{\sqrt{N}}, \ldots, \frac{T}{\sqrt{N}} \quad \frac{T^2}{N} \sim 1$$

Quantum Key Distribution

100% provably secure encryption

One-time pad

m = message, n bits

r = n random bits

$c = m \oplus r$ encoded message

never reuse r

[Careful $m_0 \oplus r = c_0$ $m_1 \oplus r = c_1$

Then $c_0 \oplus c_1 = m_0 \oplus m_1$

has direct info on m_0, m_1

(r cancels if reused)

QKD is a secure way of transmitting a onetime pad

Alice & Bob can agree on a one-time pad and they know if intercepted by Eve

I		H	
$\|0\rangle$	$\|1\rangle$	$H\|0\rangle$	$H\|1\rangle$
$\rightarrow$	$\uparrow$	$\nearrow$	$\searrow$

Alice sends photons to Bob and each chooses independently H, I.
If they choose same + measure then get same result.
But if e.g. Alice $H|0\rangle$ and Bob measures w/o H
-- only 50% agreement

Alice	I	H	H	H	I	I	H	I	H
prepares	0	1	0	1	1	0	1	0	0
Bob	H	H	H	I	I	H	I	I	I
measures	1	1	0	0	1	1	1	0	0

By classical channel, communicate sequence of H, I, identify the roughly 50% same choice

Discard the rest!

How do they know if intercepted by Eve? she has to guess I, H and measure. But if she guesses wrong, e.g., doesn't apply H, measures, then forwards to Bob, he applies H and half the time his measurement will disagree with Alice.

$$H|0\rangle \underset{E}{\rightrightarrows} \begin{matrix}|0\rangle \\ |1\rangle\end{matrix}$$

Alice and Bob sacrifice some of their good bits and exchange via public channel.

Eve guesses H, I correctly 50% of time. If guesses wrong, then Bob's measurement corrupted half of those times.

so $\frac{1}{2} \cdot \frac{1}{2} = 1/4$ of the sacrificed bits will disagree if eavesdrop:

$$P_{\substack{\text{detect}\\ \text{Eve}}} = 1 - \underbrace{\left(3/4\right)^n}_{\text{(all agree)}}$$

For $n=72$ sacrificed,

$$\simeq .999999999 \simeq 1-10^{-9}$$

Vienna


HEDY LAMARR
QUANTUM COMMUNICATION TELESCOPE
Hedy Lamarr
born Hedwig Eva Maria Kiesler
*11/09/1914 – † 01/19/2000
was an Austrian and American actress and inventor (Frequency-hopping spread spectrum)
Frequency-hopping spread spectrum