

Simon's problem

exponential speed-up

$f: n \rightarrow n-1$ bits

$$f(x) = f(y) \text{ iff } x = y \oplus a$$

[precursor to $f(x) = f(x+r)$]

Classically, how to determine a ?

Try x_0, x_1, x_2, \dots

if get lucky: $f(x_i) = f(x_j)$

$$x_i = x_j \oplus a \Leftrightarrow a = x_j \oplus x_i$$

but if not lucky, then we

know $a \neq x_i \oplus x_j$ for any

pair so far

$$f(x) = f(y) \text{ iff } x = y \oplus a$$

$$f(000) = 5$$

$$f(001) = 0$$

$$f(011) = 6$$

$$f(111) = 6$$

$$f(x) = f(y)$$

$$a = x \oplus y$$

$$f(011 \oplus 100) = f(111)$$

$$f(111 \oplus 100) = f(011)$$

$$a = (100)$$

in the real setting,

$$f(x) = f(x + r)$$

period a has n bits.

Classically, in the worst case would take

$$2^{n-1} + 1 \text{ calls to } f(x)$$

(if very very unlucky...)

But recall "birthday ^(non-)paradox"
each pair has a $1/2^{n-1}$ probability
of colliding, so the
probability of at least one collision
after m values is $\frac{\binom{m}{2}}{2^{n-1}}$.

For a appreciable probability, need:

$$\frac{m(m-1)}{2} \sim m^2 \sim 2^n, \text{ so } m \sim 2^{n/2}$$

Equivalently if we try m values $x_0 \dots x_{m-1}$
 then at most $\frac{m(m-1)}{2}$ we've excluded
 $\binom{m}{2} = \frac{m(m-1)}{2}$ values of a .

In order to exclude all
 but one value of a , how many
 values of $\{x_k\}$ necessary?

$$\text{need } \frac{m(m-1)}{2} \approx 2^n$$

$$\Rightarrow m \sim 2^{n/2}$$

* unless "carelessly" choose $x_\ell = x_i \oplus x_j \oplus x_k$
 then $x_\ell \oplus x_i$, $x_\ell \oplus x_j$, $x_\ell \oplus x_k$ don't exclude any new
 pairs

$\begin{matrix} \text{previously chosen} \\ \swarrow \quad \downarrow \quad \searrow \\ x_i \quad x_j \quad x_k \end{matrix}$

So classically to determine n bit a ,
need $\sim 2^{n/2}$ invocations of f .

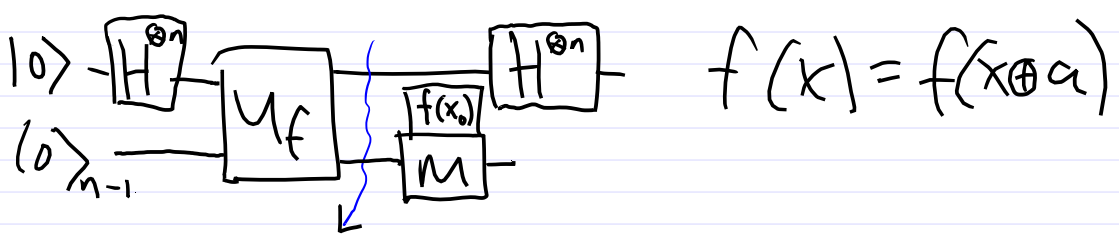
Quantumly: need $O(n)$

E.g. For $n=100$ $2^{n/2} = 2^{50} \sim 10^{15}$
at $10M/sec \rightarrow 3$ yrs

with QM take only 120 invocations
to get a (with probability
 $> 1 - 10^{-6}$)

$$U_f |x\rangle_n |y\rangle_{n-1} = |x\rangle_n |y \oplus f(x)\rangle_{n-1}$$

$$U_f H^{\otimes n} |x\rangle |0\rangle = \frac{1}{\sqrt{2^n}} \sum_{0 \leq x < 2^n} |x\rangle |f(x)\rangle$$



$$\frac{1}{\sqrt{2}} \sum_{0 \leq x < 2^n} |x\rangle |f(x)\rangle$$

measure output, collapses to

$$\frac{1}{\sqrt{2}} (|x_0\rangle + |x_0 \oplus a\rangle) |f(x_0)\rangle$$

but only get one of two
by measuring input (can't clone above state)

But we can apply an operator
before measuring inputs.

We renounce learning $x_0, x_0 \oplus a$ values
but we can learn a relation between
them: their mod 2 sum

$$H^{\otimes n} \frac{1}{\sqrt{2}} (|x_0\rangle + |x_0 \oplus a\rangle)$$

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

$$= \frac{1}{2^{\frac{n+1}{2}}} \sum_y (-1)^{x_0 \cdot y} (1 + (-1)^{a \cdot y}) |y\rangle$$

$a \cdot y = 0$ then $1 + (-1)^{a \cdot y} = 2$

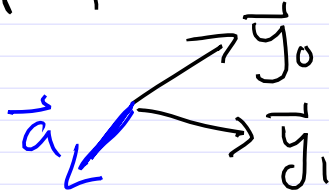
$a \cdot y = 1$ then $1 + (-1)^{a \cdot y} = 0$

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

(sum is over only y with $y \cdot a = 0$)
measure: gives some y s.t. $y \cdot a = 0$
Each such y constrains value of a
to live in orthogonal subspace.

In a real vector space, would be
easy: orthogonal to $n-1$ vectors
generically determines a single
vector (up to scale factor).

E.g. $3d$



but for binary valued vectors,
there's a $1/2^n$ chance of $y = (0, \dots, 0)$,
and an increasing probability that the
 k th y will be a linear combination
of the earlier ones. So need more than
 $n-1$ to be highly likely to pin down a

e.g. $n=3$, need to find $a = (a_2, a_1, a_0)$

measure $y = 101$ $a_0 + a_2 = 0$

$y = 010$ $a_1 = 0$

since $a \neq 0$, constrains $a = 101$

classically f once gives no info on a
 f twice excludes one value of a

quantumly f once excludes half the possible values,
 f again excludes half again, so twice excludes $3/4$ of possible values

if really lucky can get first $n-1$ linearly independent (and non-zero) values of y , and hence determine a .

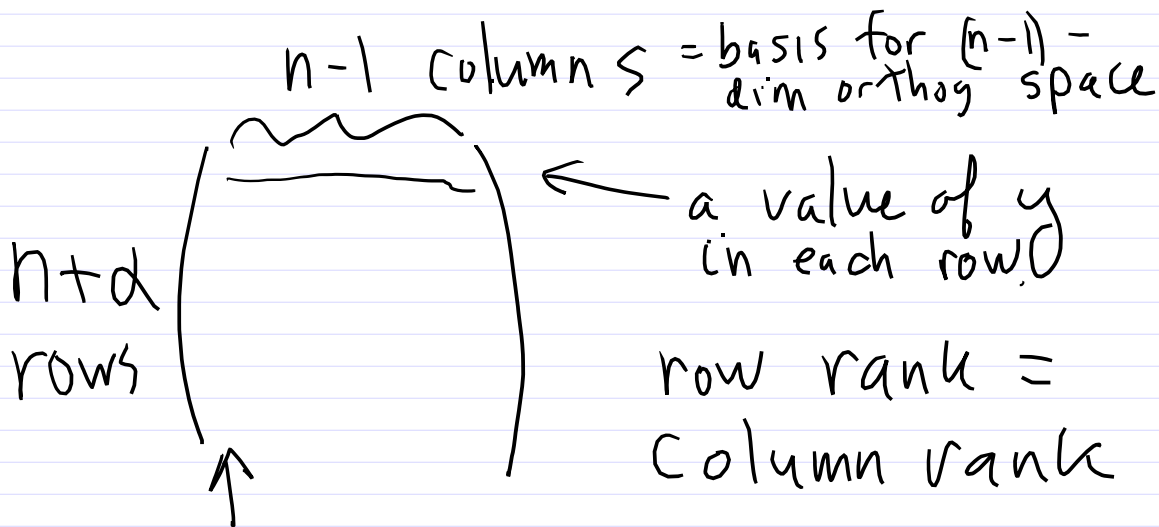
in general, need $n+d$ values of y to have

$> 1 - \frac{1}{2^{n+1}}$ probability of $n-1$ linearly independent

$$a = (0 \ 0 \ 1)$$

$$y = \left. \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix} \right\}$$

See Mermin Appendix G
for details of argument for why $n+d$
values of y have probability $> 1 - \frac{1}{2^{d+1}}$
of having $n-1$ linearly independent



probability they're not linearly dependent

$$\left(1 - \frac{1}{2^{n+d}}\right)$$

← probability that
1st column not
all zero

$$\left(1 - \frac{1}{2^{n+d-1}}\right)$$

← probability that 2nd
column $\neq 0$ and
also not
first column

$$\left(1 - \frac{1}{2^{d-1}}\right)$$

← also not lin. comb. of
first $n+d-1$
columns

product $> 1 - \frac{1}{2^{d+1}}$

$$d=20 > 1 - 10^{-6}$$

i.e. high probability of enough linearly independent y values to determine a