\[
H_{\text{Heff}} \ket{x} = \frac{1}{2^n/2} \sum_y (-1)^{x \cdot y} \ket{y}
\]

\[
\left( H_{\text{Heff}} \right)^2 = \frac{1}{2^n} \mathbb{Z}_2 \quad \text{Fourier transform}
\]

\[-1 \rightarrow e^{2\pi i/N} \quad \mathbb{Z}_N \quad \text{Fourier transform}\]
Simon's problem

Exponential speed-up

$f: n \rightarrow n-1$ bits

$f(x) = f(y)$ iff $x = y \oplus a$

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

Classically, how to determine $a$?

Try $x_0, x_1, x_2, \ldots$

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

$x_i = x_j \oplus a \iff a = x_j \oplus x_i$

but if not lucky, then we know $a \neq x_i \oplus x_j$ for any pair so far
\[ f(x) = f(y) \quad \text{iff} \quad x = y \oplus \alpha \]

\[
\begin{align*}
  f(000) &= 5 \\
  f(001) &= 0 \\
  f(011) &= 6 \\
  f(111) &= 6
\end{align*}
\]

\[
\begin{align*}
  f(011 \oplus 100) &= f(111) \\
  f(111 \oplus 100) &= f(011)
\end{align*}
\]

in the real setting,

\[ f(x) = f(x + r) \]
period a has $n$ bits.
Classically, in the worst case would take $2^{n-1} + 1$ calls to $f(x)$ (if very very unlucky...)

But recall "birthday paradox" if each pair has a $\frac{1}{2^{n-1}}$ probability of colliding, so the probability of at least one collision after $m$ values is $\binom{m}{2}$. For a appreciable probability, need:

\[
\frac{m(m-1)}{2} \sim m^2 \sim 2^n,
\]

so $m \sim 2^{n/2}$.
Equivalently if we try m values $X_0, X_{m-1}$ then at most 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?

need $m(m-1) \leq 2^{n \frac{\log n}{2}}$  \( \Rightarrow m \sim 2^{\frac{n}{2}} \)

*unless “carelessly” choose $x_e \oplus X_i$, then $x_e \oplus x_j, x_e \oplus x_k$ don't exclude any new pairs
So classically to determine a $n$ bit $a$, we need $\sim 2^{n/2}$ invocations $f$. Quantumly: need $O(n + \alpha)$

E.g. For $n = 100$, $2^{n/2} = 2^{50} \approx 10^{15}$ at $10M/\text{sec}$ $\Rightarrow 3$ yrs

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

\[
U_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle
\]

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

\[0 \leq x < 2^n\]

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 \(f\) 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.
\[ H^n \frac{1}{\sqrt{2^n}} \left( \left| x_0 \right> + \left| x_0 \oplus a \right> \right) \]

\[ \frac{1}{\sqrt{2^n}} \sum_{y} (-1)^{x_0 \cdot y} \left| y \right> + \sum_{y} (-1)^{x_0 \cdot y + (x_0 \oplus a) \cdot y} \left| y \right> \]

\[ \frac{1}{\sqrt{2^{n+1}}} \sum_{y} (-1)^{x_0 \cdot y} \left| y \right> \]

\[ \begin{align*}
    &a \cdot y = 0 \quad \text{then} \quad 1 + (-1)^{a \cdot y} = 2 \\
    &a \cdot y = 1 \quad \text{then} \quad 1 + (-1)^{a \cdot y} = 0
\end{align*} \]

\[ = \frac{1}{2^{(n-1)/2}} \sum_{y} (-1)^{x_0 \cdot y} \left| y \right> \]

\[ y \left| y \cdot a = 0 \right. \]
(sum is over only y with y.a = 0)
Measure: gives some y s.t. y.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

\[ \vec{a} \quad \vec{y}_0 \quad \vec{y}_1 \]

but for binary valued vectors,
there's a \(1/2^n\) chance of \(y = (0, \ldots, 0)\),
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 \( \alpha = (a_2, a_1, a_0) \)

measure \( y = 101 \quad a_0 + a_2 = 0 \)

\( y = 010 \quad a_1 = 0 \)

since \( a \neq 0 \), constrains \( \alpha = 101 \)

classically \( f \) once gives no info on \( \alpha \)

\( f \) twice excludes one value of \( \alpha \)

quantumly \( f \) once excludes half the possible values, \( f \) again excludes half again, so twice excludes \( \frac{3}{4} \) of possible values

if really lucky can get first \( n-1 \) linearly independent (and non-zero) values of \( y \),

and hence determine \( \alpha \).

in general, need \( n+\alpha \) values of \( y \) to have

\( > 1 - \frac{1}{2^{\alpha+1}} \) probability of \( n-1 \) linearly independent
\[ a = (0,0,1) \]

\[ y = \begin{pmatrix} 0,0,0 \end{pmatrix} \\
    \begin{pmatrix} 0 \end{pmatrix} \\
    \begin{pmatrix} 0,0,1 \end{pmatrix} \\
    \begin{pmatrix} 1,1,0 \end{pmatrix} \]

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

\( n-1 \) columns \( S = \text{basis for } (n-1)-\text{dim orthog space} \)

\[ \begin{pmatrix} \vdots \\ \vdots \\ \vdots \end{pmatrix} \]

\( n+d \) rows

A value of \( y \) in each row.

Row rank = Column rank
probability they’re not linearly dependent

\[ \left( 1 - \frac{1}{2} n^x \right) \leq \text{probability that 1st column not all zero} \]

\[ \left( 1 - \frac{1}{2} n^x - 1 \right) \leq \text{probability that 2nd column \neq 0 and also not first column} \]

\[ \left( 1 - \frac{1}{2} \alpha + 1 \right) \leq \text{also not lin. comb. of first } n \alpha + 1 \text{ columns} \]

product \( \geq 1 - \frac{1}{2} \alpha + 1 \)

\( \alpha = 20 \geq 1 - 10^{-6} \)

i.e., high probability of enough linearly independent y values to determine a
Period Finding (real setting)

Consider $f(x) = b^x \mod n$

"discrete exponential"

Suppose $f(x+r) = f(x)$
has period $r$, $b^r \mod n = 1$ easy?

But: $f$

try $m$ times $(m) = \frac{m(m-1)}{2}$ pairs

$f$ is an $n$-bit function

so $x$ has $2^n$ values

$(m) \sim m^2 \sim 2^n$ $m \sim 2^{n/2}$