Hidden Subgroup

Simon's $Z_k$ $a_i = 0, ... , k-1$

$f(x) = f(x \Theta a_c)$

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

Abelian Subgroups $ab = ba$

Non-abelian Hidden Subgroups "Post-quantum"
Easy case, factor 15

"Cheats": if pick b s.t. \( b \mod n = 1 \)

\(^r U^4 = U^8 = \ldots = 1\)

"precompiled" knowing \( r \) in advance

\( G_{15} = (1, 2, 4, 7, 8, 11, 13, 14) \)

\( f(x) = 7^x \mod 15 \quad r = 4 \quad n_0 = 4 \)

\( U_f H^\otimes n |0\rangle_n |10\rangle_n = \frac{1}{2^{n/2}} \sum_{0 \leq x < 2^n} 1^x \rangle_n |f(x)\rangle_{n_0} \)

For \((2^1 + 1)(2^2 + 1)\), can use \( n = n_0 = 4 \)
Then for \( f(x) = \overline{x} \mod 15 \) wave function is

\[
\frac{1}{4} \left( |10\rangle |11\rangle + |11\rangle |17\rangle + |12\rangle |4\rangle + \ldots + |15\rangle |13\rangle \right)
\]

\[\text{Measure output as } |113\rangle = |f(x_0)\rangle\]

Then wave function collapses to

\[\frac{1}{2} \left( |13\rangle + |17\rangle + |111\rangle + |115\rangle \right) |113\rangle\]

(of the form \( \frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} |x_0 + k \langle r\rangle\rangle \) with \( \frac{r}{m} = 4 \))

\[|\Psi\rangle = \sum_x (\delta_x \langle x \rangle) |113\rangle\]

where

\[\delta_x = \frac{1}{2} \delta_{x, 4k + 3}\]

\[\delta_x\]

\[
\begin{array}{c}
3 \quad 7 \quad 11 \quad 15 \\
\end{array}
\]

Want period of \( x_0 \)
\[ \sum_{y} \leq e^{\frac{2\pi i xy}{2^n}} y_x = \frac{1}{4} \leq e^{\frac{2\pi i xy}{4^n}} y_x \]

\[ x = 3 \mod 4 \]

\[ y_x = \frac{1}{2} \delta_{x, 4k+3} \]

\[ = \sum_{\gamma_x} 2\pi i^{3y/16} \frac{3}{8} e^{2\pi i 4ky/16} e^{k=0} \]

Non-zero only when \( 4y/16 = j \)

\( y/4 = j \) or \( y = 0, 4, 8, 12 \)

Suppose measure \( y = 12 \)

\( 12 = j \frac{16}{r} \)

\( r \) is an (integer) multiple of \( 4/3 \) so

First possibility is \( r = 4 \)

To factor 15, use (see next page)

\[ (7^4 - 1) = (7^2 - 1)(7^2 + 1) = 0 \mod 15 \]

Then run Euclidean alg. \( (48, 15) \rightarrow 3 \) on the two factors \( (50, 15) \rightarrow 5 \)
how to factor $N$ knowing $b^r \mod N = 1$

Two conditions: need $r$ even

\[ b^{r/2} \mod N \neq -1 \]

\[ (b^{r/2} - 1)(b^{r/2} + 1) = 0 \mod N \]

$p$ must be a factor of one, and $q$ of the other

run Euclidean algorithm on $\left( b^{r/2}, N \right)$

Simple example, factor $5 \cdot 7 = 35$

Use $4^6 = 1 \mod 35$

\[ (4^3 - 1)(4^3 + 1) = 0 \mod 35 \]

(63, 35) ↦ (35, 28) ↦ (28, 7) ↦ (7, 0)

(65, 35) ↦ (35, 30) ↦ (30, 5) ↦ (5, 0)
Thm: If \( x \) estimates \( \frac{1}{r} \) and \( |x - \frac{1}{r}| < \frac{1}{2r^2} \), then \( \frac{1}{r} \) appears as one of the partial sums of \( X \).

Example: \( r < 2^7 \), measure \( y = 11490 \) within \( 1/2 \) of \( 2^{14} \cdot \frac{1}{r} \) \((n=14)\).

\[
\left| \frac{11490}{2^{14}} - \frac{1}{r} \right| < \frac{1}{2 \cdot 2^{14}}
\]

\[
\frac{11490}{2^{14}} = 0.7012939453 \ldots = \frac{1}{1 + \frac{1}{2} + \frac{1}{2^2} + \ldots}
\]

\[
= [0; 1, 2, 1, 7, 35, \ldots]
\]

\[
\Rightarrow \frac{54}{77} = \frac{1}{r} \Rightarrow r = 77
\]

(Confirm: \( 2^{14} \cdot \frac{54}{77} = 11490.079 \ldots \) within \( 1/2 \) of \( y = 11490 \))
Small phases?

\[ V_n = e^{i\pi/2n} \]

If factoring number with hundreds of digits, then \( 2^k \geq 10^{100} \)

Not experimentally feasible.

Resolution: accurate phases affect probability, but not precision of \( y \) once measured.

\[ \mathcal{P}_\varphi(y) = \frac{1}{2^nm} \sum_{k=0}^{m-1} e^{2\pi i k n / 2n} | \varphi_n(y) |^2 \]

to leading order in small \( \varphi \):

\[ | p(y) - \mathcal{P}_\varphi(y) | \lesssim 2\varphi \quad (\text{all } |m| < |y|) \]

\[ 2\varphi \lesssim \frac{1}{100} \quad (< 1\% \text{ effect}) \]

\[ \Rightarrow \varphi \lesssim \frac{1}{500} \]
Want $\max \mathcal{U} = n^{11/2} < \frac{1}{500}$
so can ignore phases $e^{i\pi/k}$
with $2^k > 500 n \pi$

For $n \approx 3000$ ($N \approx 10^{500}$, 500 digit number)

Can ignore all $k \geq 22$

QFI grows only linearly in $n$!
(to desired probability)
Grover's Algorithm
Search.
Given \( N \) items, I "marked" look at \( k \) of them prob = \( k/N \) & finding it, Quantum: "look" at \( \sqrt{N} \) e.g. Database

\[ \sqrt{\frac{m^2 + n^2}{2}}, \sqrt{p} \]
\[ f(x) = \begin{cases} 0 & x \neq a \\ 1 & x = a \end{cases} \] Marked item

\[ N = 2^n \]

\[ U_f |x\rangle_n |y\rangle_1 = |x\rangle_1 |y\rangle_1 \oplus f(x) \rangle_1 \]

"Phase Kibble"

\[ |x\rangle_1 - \sqrt{\frac{1}{N}} \sum_{x=0}^{2^n-1} |x\rangle_1 |E(x)\rangle_1 \]

\[ U_f (|x\rangle \otimes |H\rangle_1) = |E(x)\rangle \otimes (|x\rangle \otimes |H\rangle_1) \]

\[ V(|x\rangle_n) = (-1)^{f(x)} |x\rangle_n = \begin{cases} |x\rangle_n & x \neq a \\ -|a\rangle_n & x = a \end{cases} \]

\[ V |\psi\rangle = |\psi\rangle - 2 |a\rangle \langle a | \psi\rangle \]

\[ V_f = 1 - 2 |a\rangle \langle a | \]

\[ V_f \text{ embodies} \]
\[ a = 10110 \]

\[ |y\rangle \rightarrow |y + f(x)\rangle \]

\[ |\psi\rangle = H^{\otimes n} |0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0, 1\}^n} |x\rangle \]

Also need

\[ W = 2 |\psi\rangle \langle \psi | - 1 \]

Inverts states orthogonal to \(|\psi\rangle\)

\[ V = 1 - 2 |a\rangle \langle a | \]
work in 2d space generated by $|a\rangle, |\phi\rangle$

$|a\rangle$

$|\phi\rangle$

$|w\rangle$

$|\psi\rangle$

$\langle a | \phi \rangle = \cos\left(\frac{\pi}{2} - \theta\right) = \sin\theta = \frac{1}{2^{n/2}}$

$\sim \theta \sim \frac{1}{\sqrt{n}}$

$WV$ is a rotation (by what angle?) by $2\theta$

(or $V = (1 - i)$ $W = R_\theta VR - \theta$

$WV = R_\theta VR - \theta V = R_{2\theta}$)
Apply $(WV)^l \quad \theta = \frac{1}{2^{n/2}}$

with $(2\ell + 1) \frac{1}{2^{n/2}} = \frac{\pi}{2}$

gives closest possible to $|\alpha\rangle$

\[ l = \frac{\pi}{4} 2^{n/2} = \frac{\pi}{4} \sqrt{N} \]

\[ p(a) = |\langle a | (WV)^l | \phi\rangle|^2 \]

\[ = \sin^2 (2\ell + 1) \theta = \sin^2 \left( \frac{2\ell + 1}{2^{n/2}} \right) \]

\[ \begin{array}{c}
\text{p}(a) \\
\frac{1}{2^n} \\
0
\end{array} \quad \begin{array}{c}
l \\
\frac{\pi}{4} \sqrt{N}
\end{array} \]