Continued Fractions Algorithm

$$[a_0, \ldots a_M] \equiv a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_M}}}}$$, a_i positive integers.

mth convergent $0 \le m \le M$ is $[a_0, \ldots a_m]$.

Algorithm determines continued fraction expansion of arbitrary real number.

Example:

$$\frac{31}{13} = 2 + \frac{5}{13} = 2 + \frac{1}{\left(\frac{13}{5}\right)} = 2 + \frac{1}{2+\frac{3}{5}} = 2 + \frac{1}{2+\frac{1}{\left(\frac{5}{3}\right)}} = 2 + \frac{1}{2+\frac{1}{1+\frac{2}{3}}}$$

$$\ldots 2 + \cfrac{1}{2 + \cfrac{1}{1 + 1/(1+\frac{1}{2})}} = [2, 2, 1, 1, 2].$$ Convergent.

How Quickly does Continued Fraction Algorithm Terminate?

If $\varphi = \frac{s}{r}$ is rational,

s and r L-bit integers.

Then φ computed in

$O(L^3)$ operations.

$O(L)$ "split and invert" steps,

each using $O(L^2)$ gates

for elementary arithmetic.

Factoring

order-finding $\Rightarrow$ factoring

1. We can compute a factor of N if we can non-trivially solve, $x \neq \pm 1 \pmod N$, the equation

$$x^2 = 1 \pmod N$$

2. A random y, coprime to N, may have even order, r.

... so.. $y^{r/2} \neq \pm 1$,

$$\Rightarrow x = y^{r/2} \pmod N$$

is a non-trivial solution to $x^2 = 1 \pmod N$.

Let N be an L-bit composite.

x a non-trivial solution of $x^2 = 1$, $1 \leq x \leq N-1$.

Then,

$\gcd(x-1, N)$ and/or $\gcd(x+1, N)$

is a non-trivial factor of N,

computed using $O(L^3)$ operations.

Let,

$$N = p_1^{\alpha_1} \cdots p_m^{\alpha_m} \quad \text{be odd.}$$

x satisfy $1 \leq x \leq N-1$, $\gcd(x, N) = 1$.

$$\text{ord}_N(x) = r.$$

Then,

$$P(r \text{ even and } x^{r/2} \neq -1) \geq 1 - \frac{1}{2^m}.$$

Reduction of Factoring to Order-Finding

Input: N

Output: non-trivial factor of N.

Runtime: $O((\log N)^3)$ operations.

Success Probability: $O(1)$.

Procedure:

1. N even $\Rightarrow$ return 2.
2. Determine if $N = a^b$ for $a \geq 1, b \geq 2$.
   If so, return a.
3. Randomly choose x, $1 < x < N-1$.
   If $\gcd(x, N) > 1$, return $\gcd(x, N)$.
4. Use order-finding to find $r = \text{ord}_N(x)$.
5. If r even, $x^{r/2} \neq -1$, then return $\gcd(x^{r/2}-1, N)$ or $\gcd(x^{r/2}+1, N)$.
   Otherwise fail.

Example

- $N = 15$.
- Choose $x = 7$.
- Prepare $|0\rangle|0\rangle$ then create

$$\frac{1}{\sqrt{2^t}} \sum_{k=0}^{2^t-1} |k\rangle|0\rangle = \frac{1}{\sqrt{2^t}} \left[|0\rangle + |1\rangle + |2\rangle + \ldots + |2^t - 1\rangle \right] |0\rangle.$$

by applying $\otimes H$ to first register, where $t = 11$ to ensure $\varepsilon \leq \frac{1}{4}$.

- Compute $f(k) = x^k \bmod N$. Then second register is,

$$\frac{1}{\sqrt{2^t}} \sum_{k=0}^{2^t-1} |k\rangle |x^k \bmod N\rangle = \frac{1}{\sqrt{2^t}} \Big[|0\rangle|1\rangle + |1\rangle|7\rangle + |2\rangle|4\rangle + |3\rangle|13\rangle + |4\rangle|1\rangle + |5\rangle|7\rangle + |6\rangle|4\rangle + \ldots \Big]$$

- Apply IQFT to first register and measure.

Remember: First and second register in state

$$\frac{1}{\sqrt{2^t}}\left[|0\rangle|1\rangle + |1\rangle|7\rangle + |2\rangle|4\rangle + |3\rangle|13\rangle + |4\rangle|1\rangle + |5\rangle|7\rangle + |6\rangle|4\rangle + \ldots\right]$$

Assume implicit measurement of second register:

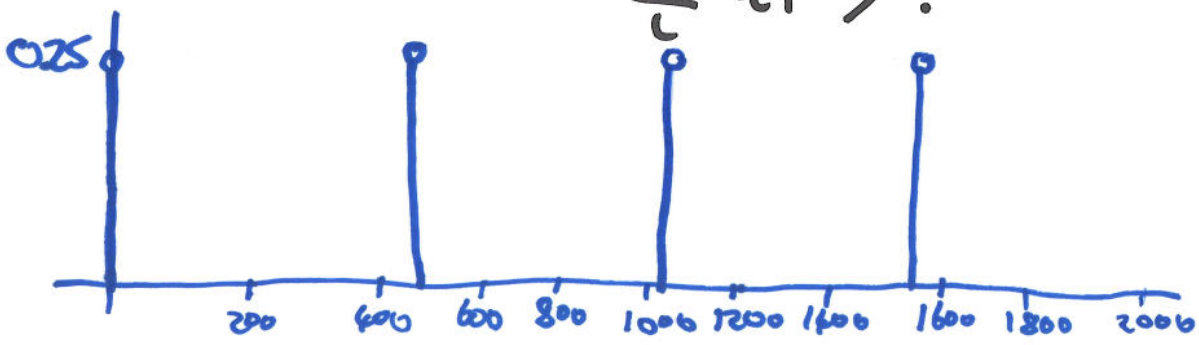
We obtain 1, 7, 4 or 13.

Suppose we measure 4.

Then, before IQFT on first register, first register is:

$$\frac{\sqrt{4}}{2^t}\left[|2\rangle + |6\rangle + |10\rangle + |14\rangle + \ldots\right].$$

After IQFT, we obtain $\sum_c \alpha_c |c\rangle$:



where $2^t = 2048$.

Measuring first register gives either 0, 512, 1024 or 1536. with pr ¼

Remember: Measure register one to get 0, 512, 1024 or 1536 with pr $\times \frac{1}{4}$ each.

e.g.

measure $l = 1536$.

- Compute cf. expansion of $1536/2048$

$= 1/(1+(1/3)) \Rightarrow \frac{3}{4}$ is a convergent.

- We postulate $r=4$ as the order of $x=7$.
- We test r is even and $x^{r/2} = 7^2 \neq -1$.

$\Rightarrow \gcd(x^2-1, 15) = 3$, and $\gcd(x^2+1, 15) = 5$ are factors.

General Applications of the QFT

Hidden Subgroup Problem:

Encompasses all known "exponentially fast" applications of the QFT.

.... a generalization of the task of finding the unknown period of a periodic function.

Period-Finding

Consider f periodic, where

$$f(x+r) = f(x), \quad 0 < r < 2^L,$$

r unknown.

Let U be a black box:

$$U|x\rangle|y\rangle \to |x\rangle|y \oplus f(x)\rangle.$$

How many black box queries and other operations are required to determine r?

Period-Finding Using one query and $O(L^2)$ operations

Inputs: Black box U, $U|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$.
State $|0\rangle$ to store result.
$t = O(L + \log(1/\epsilon))$ qubits initialized to $|0\rangle$.

Outputs: $r > 0$, (smallest r), such that $f(x+r) = f(x)$.

Runtime: One call to U + $O(L^2)$ operations. Success prob. $O(1)$.

Procedure:

1. $|0\rangle|0\rangle$
2. $\to \frac{1}{\sqrt{2^t}} \sum_{x=0}^{2^t-1} |x\rangle|0\rangle$ — init. superposition
3. $\to \frac{1}{\sqrt{2^t}} \sum_{x=0}^{2^t-1} |x\rangle|f(x)\rangle \approx \frac{1}{r\sqrt{2^t}} \sum_{\ell=0}^{r-1} \sum_{x=0}^{2^t-1} e^{2\pi i \ell x/r} |x\rangle|\hat{f}(\ell)\rangle$ — apply U
4. $\to \frac{1}{\sqrt{r}} \sum_{\ell=0}^{r-1} |\tilde{\ell/r}\rangle|\hat{f}(\ell)\rangle$ — IQFT
5. $\to \ell/r$ — measure
6. $\to r$. — continued fraction

Why Does This Work?

Remember: Step 3. $\rightarrow \frac{1}{\sqrt{2^t}} \sum_{x=0}^{2^t-1} |x\rangle |f(x)\rangle$

$\simeq \frac{1}{\sqrt{r 2^t}} \sum_{l=0}^{r-1} \sum_{x=0}^{2^t-1} e^{2\pi i l x / r} |x\rangle$ [illegible]

In step 3 we use,

$$|\hat{f}(l)\rangle = \frac{1}{\sqrt{r}} \sum_{x=0}^{r-1} e^{-2\pi i (x/r)} |f(x)\rangle.$$

Step 4. $\rightarrow \frac{1}{\sqrt{r}} \sum_{l=0}^{r-1} |\frac{\tilde{l}}{r}\rangle |\hat{f}(l)\rangle$

where $$|f(x)\rangle = \frac{1}{\sqrt{r}} \sum_{l=0}^{r-1} e^{2\pi i (x/r)} |\hat{f}(r)\rangle, \text{ and } \sum_{l=0}^{r-1} e^{2\pi i (x/r)} = r.$$

$|\hat{f}(l)\rangle$ is approximately the Fourier transform over $\{0, 1, \ldots 2^t - 1\}$ of $|f(x)\rangle$.

Order-finding finds the period of $f(k) = x^k$.

Shift-Invariance Property

> G is a group. H is a subgroup of G.
> If f on G is constant on cosets of H,
> then Fourier Transform of f is invariant over cosets of H.

QFT: $\sum_{h \in H} \alpha_h |h\rangle \rightarrow \sum_{g \in G} \tilde{\alpha}_g |g\rangle$,

where $\tilde{\alpha}_g = \sum_{h \in H} \alpha_h e^{2\pi i g h / |G|}$.

$H \subset G$, and G indexes orthonormal basis.

e.g.

$$U_k |g\rangle = |g+k\rangle$$

$$\Rightarrow U_k \sum_{h \in H} \alpha_h |h\rangle = \sum_{h \in H} \alpha_h |h+k\rangle \rightarrow \sum_{g \in G} e^{2\pi i g k / |G|} \tilde{\alpha}_g |g\rangle$$

Observe: $|e^{2\pi i g k / |G|} \tilde{\alpha}_g| = |\tilde{\alpha}_g|$ ... i.e. magnitudes unchanged.

Discrete Log

Period finding considered domain and range to be integers.

What about more general situations?

Consider $f(x_1, x_2) = a^{sx_1 + x_2} \bmod N$

$r = \text{ord}_N(a)$.

f is periodic as $f(x_1 + l, x_2 - ls) = f(x_1, x_2)$,

with period $(l, -ls)$.

Determining s allows one to solve discrete log problem.

Given a and $b = a^s$, what is s?

Discrete Log Solution Using One query and $O(\lceil \log r \rceil^2)$ operations

Query, U, performs,

$$U|x_1\rangle|x_2\rangle|y\rangle \to |x_1\rangle|x_2\rangle|y \oplus f(x)\rangle.$$

Assume knowledge of $r = \mathrm{ord}_N(a)$.

(... use order-finding algorithm)

Discrete Log

Inputs: Black box, $U|x_1\rangle|x_2\rangle|y\rangle = |x_1\rangle|x_2\rangle|y \oplus f(x_1,x_2)\rangle$,

where $f(x_1,x_2) = b^{x_1}a^{x_2}$

state $|0\rangle$ for result.

two $t = O(\lceil \log r \rceil + \log(\frac{1}{\epsilon}))$ qubit registers, $|0\rangle$ and $|0\rangle$.

Outputs: $s = \log_a(b)$, mod N (ie. $a^s = b$).

Runtime: One call to U and $O(\lceil \log r \rceil^2)$ operations

Success Probability: $O(1)$.

Discrete Log Procedure

1. $|0\rangle|0\rangle|0\rangle$ — init.

2. $\to \frac{1}{2^\epsilon} \sum_{x_1=0}^{2^\epsilon-1} \sum_{x_2=0}^{2^\epsilon-1} |x_1\rangle|x_2\rangle|0\rangle$ — superposition

3. $\to \frac{1}{2^\epsilon} \sum_{x_1=0}^{2^\epsilon-1} \sum_{x_2=0}^{2^\epsilon-1} |x_1\rangle|x_2\rangle|f(x_1,x_2)\rangle$ — apply U

$$\approx \frac{1}{2^\epsilon \sqrt{r}} \sum_{\ell_2=0}^{r-1} \sum_{x_1=0}^{2^\epsilon-1} \sum_{x_2=0}^{2^\epsilon-1} e^{2\pi i (s\ell_2 x_1 + \ell_2 x_2)/r} |x_1\rangle|x_2\rangle|\hat{f}(s\ell_2, \ell_2)\rangle$$

$$= \frac{1}{2^\epsilon \sqrt{r}} \sum_{\ell_2=0}^{r-1} \left[\sum_{x_1=0}^{2^\epsilon-1} e^{2\pi i (s\ell_2 x_1)/r} |x_1\rangle\right]\left[\sum_{x_2=0}^{2^\epsilon-1} e^{2\pi i (\ell_2 x_2)/r} |x_2\rangle\right]|\hat{f}(s\ell_2, \ell_2)\rangle$$

4. $\to \frac{1}{\sqrt{r}} \sum_{\ell_2=0}^{r-1} |\widetilde{s\ell_2/r}\rangle|\widetilde{\ell_2/r}\rangle|\hat{f}(s\ell_2, \ell_2)\rangle$ — IQFT on first two regs.

5. $\to (\widetilde{s\ell_2/r}, \widetilde{\ell_2/r})$ — measure first two regs.

6. $\to s$. — generalised continued fractions.

Why?

Remember:

$$f(x_1, x_2) = b^{x_1} a^{x_2}.$$
$$a^s = b$$

Remember: Step 3: apply U

$$\to \frac{1}{2^t} \sum_{x_1=0}^{2^t-1} \sum_{x_2=0}^{2^t-1} |x_1\rangle |x_2\rangle |f(x_1, x_2)\rangle$$

$$\approx \frac{1}{2^t \sqrt{r}} \sum_{l_2=0}^{r-1} \sum_{x_1=0}^{2^t-1} \sum_{x_2=0}^{2^t-1} e^{2\pi i (s l_2 x_1 + l_2 x_2)/r} \times |x_1\rangle |x_2\rangle |\hat{f}(s l_2, l_2)\rangle$$

It can be shown that,

$$|\hat{f}(l_1, l_2)\rangle = \sum_{x_1=0}^{r-1} \sum_{x_2=0}^{r-1} e^{-2\pi i (l_1 x_1 + l_2 x_2)/r} |f(x_1, x_2)\rangle = \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} e^{-2\pi i l_2 j / r} |f(0, j)\rangle.$$

Moreover, this is because

$$|\hat{f}(l_1, l_2)\rangle \neq 0 \text{ only when } r | (l_1/s - l_2),$$

in which case

$$\sum_{k=0}^{r-1} e^{2\pi i k (l_1/s - l_2)/r} = r$$

Hidden Subgroup Problem

Efficiently determine period of periodic function.

However,

not all periods of periodic functions can be determined.

Let $f: G \to X$, G a finite group, X a finite set, where f is constant on the cosets of a subgroup K, and distinct on each coset.

Given $U: |g\rangle|h\rangle \to |g\rangle|h \oplus f(g)\rangle$, $g \in G$, $h \in X$, $\oplus$ an appropriate binary operation on X,

find a generating set for K.

Hidden Subgroup Problem

Order-finding, period-finding, discrete log

... etc.

are instances of the

hidden subgroup problem.

... for example. ...

Name	G	X	K	Function
Deutsch	$\{0,1\}, \oplus$	$\{0,1\}$	$\{0\}$ or $\{0,1\}$	$K=\{0,1\}: \begin{cases} f(x)=0 \\ f(x)=1 \end{cases}$ $K=\{0\}: \begin{cases} f(x)=x \\ f(x)=1-x \end{cases}$
Simon	$\{0,1\}^n, \oplus$	any finite set	$\{0,s\}$ $s \in \{0,1\}^n$	$f(x \oplus s) = f(x)$
Period-Finding	$\mathbb{Z}, +$	any finite set	$\{0,r,2r,\dots\}$ $r \in G$	$f(x+r) = f(x)$
Order-Finding	$\mathbb{Z}, +$	$\{a^j\}$ $j \in \mathbb{Z}_r$ $a^r = 1$	$\{0,r,2r,\dots\}$ $r \in G$	$f(x) = a^x$ $f(x+r) = f(x)$

Name	G	X	K	Function
Discrete Log	$\mathbb{Z}_r \times \mathbb{Z}_r$ $+ \pmod r$	$\{a^j\}$ $j \in \mathbb{Z}_r$ $a^r = 1$	$(l, -l_s)$ $l, s \in \mathbb{Z}_r$	$f(x_1, x_2) = a^{kx_1 + x_2}$ $f(x_1 + l, x_2 - l_s) = f(x_1, x_2)$
Order of a permutation	$\mathbb{Z}_{2^m} \times \mathbb{Z}_{2^n}$ $+ \pmod{2^m}$	$\mathbb{Z}_{2^n}$	$\{0, r, 2r, \dots\}$ $r \in X$	$f(x, y) = \pi^x(y)$ $f(x + r, y) = f(x, y)$ π = permutation on X
Hidden Linear Function	$\mathbb{Z} \times \mathbb{Z}_N +$	$\mathbb{Z}_N$	$(l, -l_s)$ $l, s \in X$	$f(x_1, x_2)$ $= \pi(sx_1 + x_2 \bmod N)$ π = permutation on X
Abelian Stabilizer	(H, X) H = any Abelian group	any finite set	$\{s \in H \mid$ $f(s, x) = x,$ $\forall x \in X\}$	$f(gh, x) = f(g, f(h, x))$ $f(gs, x) = f(g, x)$

For G a finite Abelian group,

a QC can solve the hidden subgroup problem

using poly$(\log|G|)$ operations.

Finite Abelian groups are isomorphic to products of additive groups over the integers, mod N.

$\ldots \Rightarrow$ QFT of f over G

remains well-defined

and efficient.

Algorithm

Use QFT to create superposition over group.

Apply black box for f

$$\Rightarrow \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle |f(g)\rangle.$$

Rewrite $|f(g)\rangle$ in the Fourier basis:

$$\Rightarrow |f(g)\rangle = \frac{1}{\sqrt{|G|}} \sum_{l=0}^{|G|-1} e^{2\pi i lg/|G|} |\hat{f}(l)\rangle$$

can be simplified because f is constant and distinct on cosets of the subgroup, K,

.. so ..

$$|\hat{f}(l)\rangle = \frac{1}{\sqrt{|G|}} \sum_{g \in G} e^{-2\pi i lg/|G|} |f(g)\rangle \simeq 0$$

except when l is such that $\sum_{h \in K} e^{-2\pi i lh/|G|} = |K|$.

Remember: We are interested in when

$$\sum_{k \in K} e^{-2\pi i lk/|G|} = |K|.$$

... for which l?

Determining l allows one to determine elements of K. Since K is Abelian, one eventually determines whole hidden subgroup.

.... but...

period-finding and discrete log exploit continued fraction to obtain l from $l/|G|$.

For these cases $\gcd(l, |G|) = 1$ with high probability

But, in general $\Pr(\gcd(l, |G|) = 1)$ is not guaranteed to be high....

... but...

Any finite Abelian group G is isomorphic to a product of cyclic groups of prime power order:

$$G = \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \ldots \mathbb{Z}_{p_M},$$

So,

$$|f(g)\rangle = \frac{1}{\sqrt{|G|}} \sum_{l=0}^{|G|-1} e^{2\pi i (g/|G|} |\hat{f}(l)\rangle \equiv,$$

$$\text{and } e^{2\pi i (g/|G|} \equiv \prod_{i=1}^{M} e^{2\pi i l_i' g_i / p_i}, \; g_i \in \mathbb{Z}_{p_i}$$

Phase estimation gives l_i', from which we determine l, and thus, sample K, to solve the Hidden Subgroup problem.

Other Quantum Algorithms Exploiting Hidden Subgroup Problem?

More difficult problems might be solvable by considering various groups, G, and functions, f.

Non-Abelian groups?

e.g. problem of graph isomorphism

... permutations wrt symmetric group, S_n.

Algorithms for FFTs over S_n exist.

... but a quantum algorithm for graph isomorphism is not known.

Promise Problems

Hidden subgroup problem is of type:

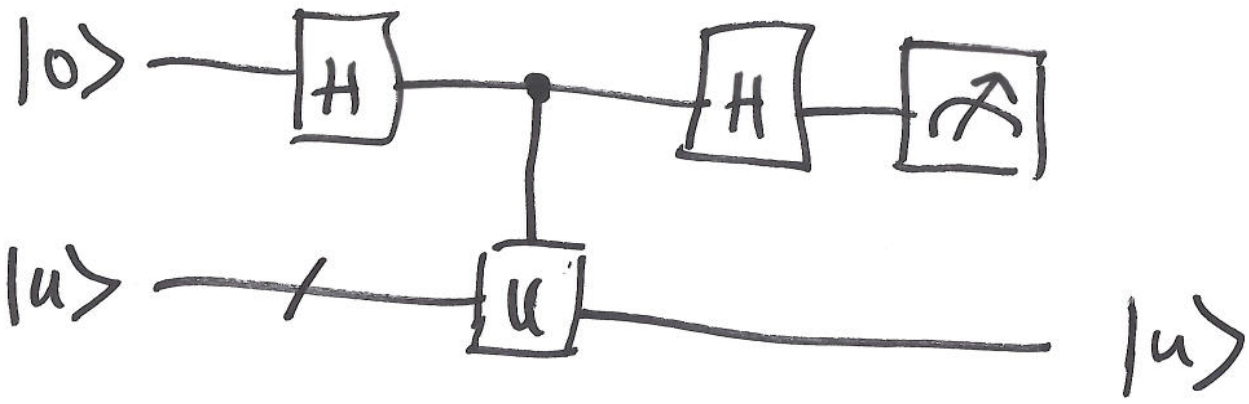
$F(x)$ is promised to have such and such a property:
characterize this property.

... but...

for problems without some sort of promise,
QCs cannot achieve exponential speed-up.

Kitaev's Algorithm

An alternative to the phase estimation algorithm:



$|u\rangle$ is an eigenstate of U with eigenvalue $e^{2\pi i \varphi}$

The top qubit is measured to be 0 with probability $p = \cos^2(\pi\varphi)$.

By replacing U with U^k and repeating, one can obtain as many bits of p, and thus of φ, as required.

Summary: QFT and applications

- When $N = 2^n$, QFT,

$$|j\rangle = |j_1, \ldots, j_n\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i j \frac{k}{N}} |k\rangle$$

may be written as,

$$|j\rangle \rightarrow \frac{1}{2^{n/2}} \left(|0\rangle + e^{2\pi i 0.j_n} |1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_{n-1} j_n} |1\rangle\right) \ldots \left(|0\rangle + e^{2\pi i 0.j_1 j_2 \ldots j_n} |1\rangle\right)$$

and may be implemented

using

$\Theta(n^2)$ gates.

Summary: Phase Estimation:

Let $|u\rangle$ be an eigenstate of U
with eigenvalue $e^{2\pi i \varphi}$.

Starting from $|0\rangle^{\otimes t}|u\rangle$, and using U^{2^k},

one can efficiently obtain

$$|\tilde{\varphi}\rangle|u\rangle,$$

where $\tilde{\varphi}$ approximates φ to
$t - \lceil \log(2 + \frac{1}{2\varepsilon}) \rceil$ bits
with probability $\geq 1 - \varepsilon$.

Order-Finding

$r = \mathrm{ord}_N(x)$ can be computed in $O(L^3)$ operations using phase estimation,

for L-bit integers, x and N.

.... a better upper bound is

$$O(L^2 \log L \log(\log L)).$$

Factoring

Prime factors of an L-bit integer, N,
can be determined in $O(L^3)$ operations,
by
finding the order of a random x
co-prime to N.

Hidden Subgroup Problem

Let $f : G \to X$,

where G is a finite Group

X is a finite set.

f is constant on the cosets of a subgroup, K,
and distinct on each coset.

Given U: $|g\rangle|h\rangle \to |g\rangle|h \oplus f(g)\rangle$, $g \in G$, $h \in X$,

find a generating set for K.