Contents

1. Hidden subgroup problem

1.1. Review of Shor's algorithm

Definition. The **factoring problem** is: given a positive integer N, find a non-trivial factor ($\neq 1, N$) in time polynomial in n (i.e. $O(\mathrm{poly}(n))$), where $n = O(\log N)$ is the length of the description of the problem input (memory/space used to store it).

Definition. An **efficient problem** is one that can be solved in polynomial time.

Remark. Clasically, the best known factoring algorithm runs in $e^{O\left(n^{1/3}(\log n)^{2/3}\right)}$. Shor's algorithm (quantum) runs in $O(n^3)$ by converting factoring into period finding:

- Given input N, choose $a < N$ which is coprime to N.
- Define $f : \mathbb{Z} \to \mathbb{Z}/N$, $f(x) = a^x \bmod N$. f is periodic with period r (the order of $a \bmod N$), i.e. $f(x + r) = f(x)$ for all $x \in \mathbb{Z}$. Finding r allows us to factor N.

1.2. Period finding

Problem (Periodicity Determination). Given an oracle for $f : \mathbb{Z}/M \to \mathbb{Z}/N$ with promises:

- f is periodic with period $r < M$ (i.e. $\forall x \in \mathbb{Z}/M$, $f(x + r) = f(x)$),
- f is one-to-one in each period (i.e. $\forall 0 \leq x < y < r$, $f(x) \neq f(y)$),

find r in time $O(\mathrm{poly}(m))$, where $m = O(\log M)$.

Clasically, this requires takes time $O(\sqrt{M})$.

Definition. Let $f : \mathbb{Z}/M \to \mathbb{Z}/N$. Let H_M and H_N be quantum state spaces with orthonormal state bases $\{|i\rangle : i \in \mathbb{Z}/N\}$ and $\{|j\rangle : j \in \mathbb{Z}/M\}$. Define the unitary **quantum oracle** for f by U_f by

$$U_f|x\rangle|z\rangle = |x\rangle|z + f(x)\rangle.$$

The first register $|x\rangle$ is the **input register**, the last register $|z\rangle$ is the **output register**.

Definition. The **quantum query complexity** of an algorithm is the number of times it queries f (i.e. uses U_f).

Definition. The **quantum Fourier transform** over $\mathbb{Z}/M$ is the unitary defined by its action on the computational basis:

$$U_{\mathrm{QFT}}|x\rangle = \frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} \omega^{xy}|y\rangle,$$

where $\omega = e^{2\pi i/M}$. Note that U_{QFT} requires only $O((\log M)^2)$ gates to implement, whereas a general unitary requires $O(4^n/n)$ elementary gates.

Lemma. Let $\alpha = e^{2\pi i y/M}$. Then

$$\sum_{j=0}^{k-1} \alpha^j = \begin{cases} \frac{1-\alpha^k}{1-\alpha} = 0 \text{ if } \alpha \neq 1 \text{ i.e. } M \nmid y \\ k \qquad\qquad \text{if } \alpha = 1 \text{ i.e. } M \mid y \end{cases}.$$

Lemma (Boosting success probability). If a process succeeds with probability p on one trial, then

$$\Pr(\text{at least one success in } t \text{ trials}) = 1 - (1-p)^t > 1 - \delta$$

for $t = \frac{\log(1/d)}{p}$.

Theorem (Co-primality Theorem). The number of integers less than r that are coprime to r is $O(r/\log\log r)$ for large r.

Algorithm (Quantum Period Finding). Let $f : \mathbb{Z}/M \to \mathbb{Z}/N$ be periodic with period $r < M$ and one-to-one in each period. Let $A = \frac{M}{r}$ be the number of periods. We work over the state space $H_M \otimes H_N$.

1. Construct the state $\frac{1}{\sqrt{M}} \sum_{i=0}^{M-1} |i\rangle|0\rangle$.
2. Query U_f on the state, giving $\frac{1}{\sqrt{M}} \sum_{i=0}^{M-1} |i\rangle|f(i)\rangle$.
3. Measure second register in computational basis, giving outcome $y \in \mathbb{Z}/N$, and input state collapses to $|\text{per}\rangle = \frac{1}{\sqrt{A}} \sum_{j=0}^{A-1} |x_0 + jr\rangle$, where $f(x_0) = y$ and $0 \leq x_0 < r$. TODO: add diagram showing amplitudes for this state.
4. Apply the Quantum Fourier Transform to $|\text{per}\rangle$:

$$\begin{aligned} \text{QFT}|\text{per}\rangle &= \frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} \frac{1}{\sqrt{A}} \sum_{j=0}^{A-1} \omega^{(x_0+jr)y} |y\rangle \\ &= \frac{1}{\sqrt{MA}} \sum_{y=0}^{M-1} \omega^{x_0 y} \sum_{j=0}^{A-1} \omega^{jry} |y\rangle \\ &= \sqrt{\frac{A}{M}} \sum_{k=0}^{r-1} \omega^{x_0 kM/r} |kM/r\rangle \end{aligned}$$

   Note now the outcomes and probabilities are independent of x_0, so carry useful information about r. TODO add diagram showing amplitudes for this state.
5. Measure $\text{QFT}|\text{per}\rangle$, yielding outcome $c = k_0 M/r$ for some $0 \leq k_0 < r$. So $\frac{c}{M} = \frac{k_0}{r}$. If k_0 is corpime to r, then the denominator r_0 of the simplified fraction $\frac{c}{M}$ is equal to r.
6. By the coprimality theorem, the probability that k_0 is coprime to r is $O(1/\log\log r)$.
7. To check if the computed value r_0 of r is correct, compute/query U_f to check if $f(0) = f(r_0)$ (this works since f is periodic and one-to-one in each period, and $r_0 \leq r$).
8. Repeat the previous steps $O(\log\log r) = O(\log\log M) = O(\log m)$ times. This obtains the correct value of r with high probability.

Remark. Why is QFT helpful for period finding?

Let $R = \{0, r, ..., (A-1)r\} \in \mathbb{Z}/M$, so

$$|R\rangle = \frac{1}{\sqrt{A}}\sum_{k=0}^{A-1}|kr\rangle$$

$$|\mathrm{per}\rangle = |x_0 + R\rangle = \frac{1}{\sqrt{A}}\sum_{k=0}^{A-1}|x_0 + kr\rangle.$$

For each $x_0 \in \mathbb{Z}/M$, define the shift operator $k \to x_0 + k$ and the associated linear map $U(x_0) : H_M \to H_M$, $|k\rangle \mapsto |x_0 + k\rangle$. Since $(\mathbb{Z}/M, +)$ is abelian, all $U(x_i)$ commute: $U(x_1)U(x_2) = U(x_1 + x_2) = U(x_2)U(x_1)$. Hence, they have a simultaneous basis of eigenvectors $\{|\chi_k\rangle : k \in \mathbb{Z}/M\}$, i.e. for all $k, x_0 \in \mathbb{Z}/M$, $U(x_0)|\chi_k\rangle = w(x_0, k)|\chi_k\rangle$, where $|w(x_0, k)| = 1$. The $|\chi_k\rangle$ are called **shift-invariant states** and form an orthonormal basis for H_M.

Now

$$|R\rangle = \sum_{k=0}^{M-1} a_k|\chi_k\rangle, \quad a_k \text{ depend only on } r$$

$$|\mathrm{per}\rangle = U(x_0)|R\rangle = \sum_{k=0}^{M-1} a_k w(x_0, k)|\chi_k\rangle$$

So measurement in the $|\chi_k\rangle$ basis gives outcome k with $\Pr(k) = |a_k w(x_0, k)|^2 = |a_k|^2$. Suppose the unitary U maps from the shift-invariant basis to the computational basis: $U : |\chi_k\rangle \mapsto |k\rangle$.