Chapter 2

Shor’s quantum factoring algorithm

Shor’s idea:

• There exists an efficient quantum algorithm for finding the period of a function.

• Factoring can be reduced to period finding i.e., an efficient algorithm for period finding ⇒ an efficient algorithm for factoring.

Period finding problem

Input: a function \( f : \mathbb{N} \rightarrow \{0, \ldots, N-1\} \) such that \( \exists r \in \{0, \ldots, N-1\} \) (unknown) such that \( f(a) = f(b) \iff a = b \mod r. \)

Goal: output \( r. \)

2.1 From factoring to period finding

2.1.1 Classical algorithm for factoring a number \( N \) using period finding

Equivalent to finding a non trivial factor of \( N. \)

1. Pick a random \( x \in \{2, \ldots, N-1\}. \)

2. Calculate \( x \land N \) (efficient, use Euclid’s algorithm).

   • if \( x \land N = c \neq 1 \rightarrow c \) divides \( N. \)
   
   • if \( x \land N = 1 \rightarrow \) continue.

3. Consider the smallest \( r \in \{0, \ldots, N-1\} \) such that \( x^r = 1 \mod N. \) Since \( x \land N = 1, \) such an \( r \) exists.

4. \( r \) is the period of the function \( f(k) = x^k \mod N. \) Use the period finding algorithm to find \( r. \) If \( r \) is odd, go back to step 1.

5. Calculate \( (x^{r/2} + 1) \land N \) and \( (x^{r/2} - 1) \land N. \) If one of those values is different than 1 or \( N \) then this value is a non trivial factor of \( n. \) If both of those values are equal to 1 or \( N, \) start again from step 1.
2.1.2 Proof that the algorithm works

The main part of the proof will be the following lemma from number theory. The proof will be omitted.

**Lemma 1.** For any odd \( N \), for a randomly chosen \( x \) such that \( x \wedge N = 1 \) and \( r \) begin the smallest element in \( \{0, \ldots, n - 1\} \) satisfying \( x^r = 1 \mod N \), the event

\[
E : \ r \text{ is even} \quad \land \quad (x^{r/2} + 1) \neq 0 \mod N \\
\land \quad (x^{r/2} - 1) \neq 0 \mod N
\]

occurs with probability \( \geq \frac{1}{2} \).

If \( r \) is even, we have

\[
x^r = 1 \mod N \Leftrightarrow (x^{r/2} + 1)(x^{r/2} - 1) = 0 \mod N \\
\Leftrightarrow \exists k \in \mathbb{N}^*, \ (x^{r/2} + 1)(x^{r/2} - 1) = kN.
\]

Notice first that \( (x^{r/2} + 1) > 0 \) and we also have \( (x^{r/2} - 1) > 0 \) because \( x \geq 2 \) and \( r \geq 2 \).

If \( E \) holds, both \( x^{r/2} + 1 \) and \( x^{r/2} - 1 \) are not multiples of \( N \). Therefore, they will both have a non trivial factor of \( N \) and we actually have \( (x^{r/2} - 1) \wedge N \neq 1 \) and \( (x^{r/2} + 1) \wedge N \neq 1 \).

Conclusion: if \( E \) holds then step 5 outputs a non trivial factor of \( N \). Since \( \Pr[E] \geq \frac{1}{2} \), we require \( O(1) \) calls to the period finding algorithm for the algorithm to succeed with a high (constant) probability.

2.2 Shor’s period finding algorithm

Our goal here is to present Shor’s quantum algorithm for period finding. Let \( n := \lceil \log(N) \rceil \), \( q := \lceil \log(N^2) \rceil \) and \( Q := 2^q \in [2N^2, 2N^2] \). We have a quantum access to \( f : \mathbb{N} \rightarrow \{0, \ldots, N - 1\} \). We restrict the input space to \( q \) input bits and consider the quantum unitary

\[
O_f : |x\rangle_q|0\rangle_n \rightarrow |x\rangle_q|f(x)\rangle_n.
\]

The subscripts represent the number of qubits in each register. This means for example that register \( |x\rangle_q \) contains \( q \) qubits and register \( |0\rangle_n \) contains \( n \) qubits.

2.2.1 Algorithm for period finding

1. Initialize the protocol at the state

\[
|0\rangle_q|0\rangle_n.
\]

2. Apply \( QFT_Q \) on the first register. We get

\[
\frac{1}{\sqrt{Q}} \sum_{a=0}^{Q-1} |a\rangle_q|0\rangle_n.
\]

3. Apply \( O_f \) on the whole state to obtain

\[
\frac{1}{\sqrt{Q}} \sum_{a=0}^{Q-1} |a\rangle_q|f(a)\rangle_n.
\]
4. Measure the second register: it gives some value \( f(s) \) for some \( s < r \). Let \( m := \# \{ a \in \{0, \ldots, Q - 1 \} : f(a) = f(s) \} \). We have

\[
\{ a \in \{0, \ldots, Q - 1 \} : f(a) = f(s) \} = \{ s, s + r, \ldots, s + (m - 1)r \} = \{ jr + s \}_{0 \leq j < m}
\]

When measuring \( f(s) \) in the second register, the first register collapses to

\[
\frac{1}{\sqrt{m}} \sum_{j=0}^{m-1} |jr + s\rangle.
\]

5. Apply QFT\(_Q\) on this first register.

\[
\frac{1}{\sqrt{m}} \sum_{j=0}^{m-1} \frac{1}{\sqrt{Q}} \sum_{b=0}^{Q-1} e^{\frac{2\pi ib(jr+s)}{Q}} |b\rangle
\]

\[
= \frac{1}{\sqrt{mQ}} \sum_{b=0}^{Q-1} e^{\frac{2\pi ib}{Q}} \left( \sum_{j=0}^{m-1} e^{\frac{2\pi jrb}{Q}} \right) |b\rangle
\]

6. Measure the first register. What is the probability of outputting each specific \( b \)?

| Special case developed here : \( r \) divides \( Q \). |

In this case, we have \( m = \frac{Q}{r} \). We have

\( b \) is a multiple of \( \frac{Q}{r} \) \( \iff \) \( e^{\frac{2\pi ib}{Q}} = 1 \).

Any such \( b \) will therefore have squared amplitude

\[
\left| \frac{1}{\sqrt{mQ}} e^{\frac{2\pi ib}{Q}} \left( \sum_{j=0}^{m-1} e^{\frac{2\pi jrb}{Q}} \right) \right|^2
\]

\[
= \left| \frac{1}{\sqrt{mQ}} e^{\frac{2\pi ib}{Q}} \left( \sum_{j=0}^{m-1} 1 \right) \right|^2
\]

\[
= \frac{m}{Q} = \frac{1}{r}
\]

Each \( b \in \{0, \ldots, Q - 1\} \) which is a multiple of \( \frac{Q}{r} \) will be measured with probability exactly \( \frac{1}{r} \). Notice also that there are exactly \( r \) such multiples, which are the elements of \( \{0, \frac{Q}{r}, \ldots, (r-1)\frac{Q}{r}\} \). Therefore, the measurement will always output a multiple of \( \frac{Q}{r} \).

Output \( b \): a uniformly random multiple of \( \frac{Q}{r} \).

This means there exists a random (unknown) \( c \in \{0, \ldots, r - 1\} \) such that \( b = \frac{Q}{r} \cdot \) or equivalently \( \frac{b}{Q} = \frac{c}{r} \).

7. Find \( r \) from the above equality. How?
• $b, Q$ are known, $c, r$ are unknown. We can rewrite $\frac{b}{Q} = \frac{b'}{Q'}$ with $b' \land Q' = 1$.
• $c$ is a random number in $\{0, \ldots, r-1\}$. This implies that $c \land r = 1$ with probability greater than $\Omega(\frac{1}{\log(\log(r))})$. When this happens, we necessarily have $c = b'$ and $r = Q'$.
• Check that $Q'$ is a period of $f$. If yes: done. If no, go back to step 1.

General case (Sketch): $r$ does not divide $Q$.

If we measure the first register, we obtain $b$ such that $|\frac{b}{Q} - \frac{c}{r}| \leq \frac{1}{2Q}$ with high probability for some random $c$. If this is the case, $\frac{c}{r}$ is the only fraction with $c \land r = 1$ and $r \leq N$ such that $|\frac{b}{Q} - \frac{c}{r}| \leq \frac{1}{2Q}$ (proof omitted). This is because we chose $Q$ such that $Q \geq N^2$.

If we indeed have $c \land r = 1$, which still happens with probability greater than $\Omega(\frac{1}{\log(\log(r))})$, we can use the continuous fraction method to find the unique fraction $\frac{c}{r}$ satisfying $|\frac{b}{Q} - \frac{c}{r}| \leq \frac{1}{2Q}$ from which we can get $r$.

DONE :)