Continued Fractions and Factoring

The last technical piece we need before we are ready to present Shor’s factoring algorithm is continued fractions. We have some value \( Y \) (real decimal number) which is a close approximation of a rational number \( \frac{k}{r} \) (with \( k \) relatively prime to \( r \)) and we would like to recover \( r \). Specifically we have that:

\[
|Y - \frac{k}{r}| \leq \frac{1}{2Q} \quad (Q > 2r^2)
\]

\( Y \) is actually obtained as a ratio of two numbers which are known to us, but this is not important at this point.

We will use the continued fraction representation of \( Y \) and show that one of the resulting rational approximations of \( Y \) will be \( \frac{k}{r} \).

Continued Fractions: A real number \( Y \) can be approximated by a sequence of integers \( a_0, a_1, a_2, \ldots, a_n \) as

\[
\text{CF}(y) = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\ddots + \frac{1}{a_n}}}} = \frac{P_n}{Q_n} \quad \text{where } P_n + Q_n \text{ are integers.}
\]

This is probably best illustrated by example: \( Y = 7.27 \)

\[
7 + \frac{27}{100} = 7 + \frac{1}{\frac{100}{27}} = 7 + \frac{1}{3 + \frac{19}{27}} = 7 + \frac{1}{3 + \frac{1}{1 + \frac{8}{27}}}
\]

\[
= 7 + \frac{1}{3 + \frac{1}{1 + \frac{1}{2 + \frac{1}{9}}} - 1 + \frac{1}{2 + \frac{1}{9}}}.
\]
\[
7 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{a_4 + \frac{1}{a_5 + \frac{1}{a_6}}}}}}}}}
= \frac{7}{a_0} + \frac{1}{a_1} + \frac{1}{a_2} + \frac{1}{a_3} + \frac{1}{a_4} + \frac{1}{a_5} + \frac{1}{a_6} = \frac{727}{100}
\]

Could have stopped at \(a_3\) to get:

\[
7 + \cfrac{1}{3 + \frac{1}{1 + \frac{1}{2}}} = \frac{80}{11} \approx 7.27
\]

\(80 = p_3\)

\(11 = q_3\)

Two important facts about continued fractions:

- if \(x\) is rational, eventually \(p_n/q_n = x\) exactly.
- \(p_n/q_n\) is the best approximation to \(x\) by any fraction whose denominator is \(\leq q_n\).

**Theorem:** If \(|x - k/r| \leq \frac{1}{2r^2}\), then \(k/r\) is a convergent of continued fraction \(q\) of \(x\). (proof in appendix of Nielsen + Chuang)

In our case:

\[
\left| \frac{a_n}{N} - \frac{k}{r} \right| \leq \frac{1}{2M}
\]

\(M \geq 2r^2\)

Here (finally) is the algorithm for Order Finding:

**Input:** \((x, N)\) s.t. \(\gcd(x, N) = 1\).

**Output:** \(\text{ord}_N(x) \mod N\).

\(Q\) is a large power of 2: \(Q \gg N^2\)

\(Q = 2^q\)

Will use 2 registers: \(\# \mod Q\) \(\rightarrow\) \(\# \mod N\).

\(|\text{qubits}| = \lceil \log_2 Q \rceil \text{ qubits}\).
1. Start with $|0\cdots0\rangle \otimes |0\cdots0\rangle$

2. QFT on register 1 to get:
   $$\frac{1}{\sqrt{q}} \sum_{y=0}^{q-1} |y\rangle |x^y \mod N\rangle$$

3. Compute $x^y \mod N$
   $$\frac{1}{\sqrt{q}} \sum_{y=0}^{q-1} |y\rangle |x^y \mod N\rangle$$
   (this function has period $r$)

4. Measure 2nd register
   $$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle |x^y \mod N\rangle$$
   $l$ chosen at random from $0, \ldots, r-1$:
   $$|\psi\rangle = \frac{1}{\sqrt{s}} \sum_{j=0}^{s-1} |j\rangle |x^j \mod N\rangle$$
   $$s = \left\lfloor \frac{N}{r} \right\rfloor$$

5. Now ignore the 2nd register and apply the QFT to the 1st register. As we have seen, with probability at least $1/c$ log $N$ for some constant $c$, we will get an $a$ such that
   $$|ar - kN| \leq r/2$$
   where $gcd(k, r) = 1$.

6. Use continued fractions to find $k/r$ an approximation to $a/N$.

---

The Quantum Fourier Transform is the basis of a number of efficient quantum algorithms for problems that have no efficient classical solution. We have already seen factoring and order finding. Period finding and the discrete log also fall under this category.
**Period Finding**: Given being $x$ and black-box access to function $f: \mathbb{Z}_p, \mathbb{Z}_p^n \to \mathbb{Z}_0, \mathbb{Z}_m^*$ (unitary $U|x\rangle|y\rangle = |x\rangle|y\rangle \otimes |f(x)\rangle$), find least integer $r$ such that $f(x+r) = f(x)$.

**Discrete Log**: Input: prime $p$ and generator $g \in \mathbb{Z}_p^*$, also some $x \in \mathbb{Z}_p^*$. Output: $y$ such that $g^y \equiv x \pmod{p}$.

All of these problems are instances of the hidden subgroup problem:

Let $f$ be a function from a finitely generated group $G$ to a finite set $X$. Suppose that $f$ is constant on the cosets of a subgroup $K$ and distinct on each coset. Given access to unitary $U|g\rangle|h\rangle = |g\rangle|h\otimes|f(g)\rangle$ for $g \in G$, $h \in X$ and $\otimes$ appropriately chosen operation on $X$, find a generating set for $K$.

**Simon**: $G = \mathbb{Z}_2, +$, $K = \{0, s\}$, $f(x) = f(x+s)$

**Order Finding**: $G = \mathbb{Z}_2, +$, range of $a^r \pmod{N}$ $j \in \mathbb{Z}$ for some $a$. $K = \{0, r, 2r, \ldots, \frac{N}{r}\}$, $r \in G$, $f(x) = a^x \pmod{N}$, $f(x+r) = f(x)$.

The hidden subgroup problem can be solved for an Abelian group in time $O(\log |G|)$. 