Continued Fractions and Factoring

Note Title 4/25/2012

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

$$\left|\gamma - k/r\right| \leq \frac{1}{2Q} \qquad Q > 2r^2$$

γ 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 γ and show that one of the resulting rational approximations of γ will be k/r.

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

$$CF(\gamma) = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}} = \frac{P_n}{Q_n}$$

where P_n + Q_n are integers.

This is probably best illustrated by example: $\gamma = 7.27$

$$7 + \frac{27}{100} = 7 + \frac{1}{100/27} = 7 + \frac{1}{3 + 19/27} = 7 + \frac{1}{3 + 1/{27/19}}$$

$$= 7 + \cfrac{1}{3 + \cfrac{1}{1 + 8/19}} = 7 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{2 + 3/8}}}$$

$$= 7 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{2 + 2/3}}}} = \underset{a_0}{7} + \cfrac{1}{\underset{a_1}{3} + \cfrac{1}{\underset{a_2}{1} + \cfrac{1}{\underset{a_3}{2} + \cfrac{1}{\underset{a_4}{2} + \cfrac{1}{\underset{a_5}{1} + \frac{1}{2 = a_6}}}}}} = \frac{727}{100}$$

Could have stopped at a_3 to get:

$$7 + \cfrac{1}{3 + \cfrac{1}{1 + \frac{1}{2}}} = \frac{80}{11} \approx 7.27 \qquad 80 = P_3 \quad 11 = Q_3$$

Two important facts about continued fractions:

- if γ is rationale, eventually $P_n/Q_n = \gamma$ exactly.
- P_n/Q_n is the best approximation to γ by any fraction whose denominator is $\leq Q_n$.

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

In our case $\left| \frac{a}{N} - \frac{k}{r} \right| \leq \frac{1}{2M}$ $\qquad M \geq 2r^2$

Here (finally) is the algorithm for Order Finding:

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

Output: order(x) mod N.

Q is a large power of 2: $Q \gg N^2$ $\qquad Q = 2^q$

Will use 2 registers: $\underbrace{|\quad\rangle}_{\substack{\#\ \text{mod } Q \\ q \text{ qubits}}} \underbrace{|\quad\rangle}_{\substack{\#\ \text{mod } N. \\ \lceil \log N \rceil \text{ qubits.}}}$

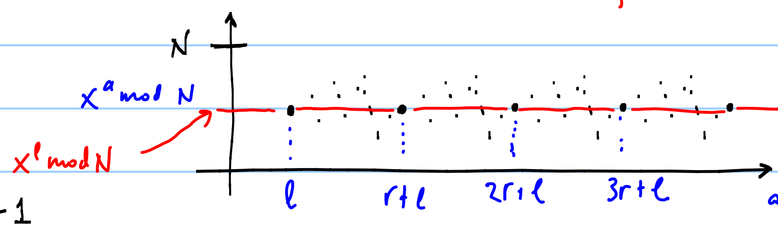
1. Start with $|0 \cdots 0\rangle \otimes |0 \cdots 0\rangle$

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

3. Compute $x^y \bmod N$ $\qquad \frac{1}{\sqrt{Q}} \sum_{a=0}^{Q-1} |y\rangle \, |x^y \bmod N\rangle$

this function has period r!

4. Measure 2nd register



get superposition of
$|jr+l\rangle \qquad 0 \le j \le \lfloor \frac{N}{r} \rfloor - 1$

l chosen at random from $\{0, \ldots, r-1\}$:

$$\frac{1}{\sqrt{s}} \sum_{j=0}^{s-1} |jr+l\rangle \, |x^l \bmod N\rangle \qquad s = \lfloor \frac{Q}{r} \rfloor$$

5. Now ignore the 2nd register and apply the QFT to the first register. As we have seen, with probability at least $1/c \log\log r$ for some constant c, we will get an a such that
$|ar - kN| \le r/2$ 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 + order finding. Period finding and the discrete log also fall under this category.

Period Finding: Given string x and black-box access to function $f: \{0,1\}^n \to \{0,1\}^m$
(unitary $U|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$)
Find least integer r such that $f(x+r) = f(x)$.

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

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 co-set. Given access to unitary $U|g\rangle|h\rangle = |g\rangle|h \oplus f(g)\rangle$ for $g \in G$, $h \in X$ and $\oplus$ appropriately chosen operation on X, find a generating set for K.

Simon: $G = \mathbb{Z}, +$. $\quad K = \{0, s\}$ $\quad f(x) = f(x \oplus s)$

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

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