Lecture 13

12 MARCH 2014

How can the quantum order finding algorithm fail?

1) phase estimation might produce a bad estimate to r.

But $\Pr\{\text{"}\} \leq \varepsilon$, so we can just increase the size of the circuit to reduce this probability.

2) But it could be that k & r have a common factor.

Simple way around this:

For a randomly chosen k, the chances that k & r are co-prime are pretty good, one can show that the # of primes less than r is $\geq \frac{r}{2\log r}$

so that the chance that s is prime

is $\geq \frac{1}{2\log r} \geq \frac{1}{2\log N}$ so repeating the algorithm $2\log N$ times gives k/r

w/ high probability such that they are co-prime, so that the continued fractions algorithm produces r.

Other methods work also...

Reduction of factoring to order finding

(i.e., a fast algorithm for order finding is automatically a fast algorithm for factoring)

Proceed in 2 steps:

1) Show that we can compute a factor of N if we can find a nontrivial solution $x \neq \pm 1 \bmod N$ to the equation $x^2 = 1 \bmod N$

2) a randomly chosen y co-prime to N is quite likely to have an order r which is even

& such that $y^{r/2} \neq \pm 1 \bmod N$

& so $x = y^{r/2} \bmod N$ is
a non trivial solution to

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

(b/c $y^r \bmod N = 1 \bmod N$
from definition of order)

We can appeal to the following theorems for this

Thm 1: Suppose N is an L bit composite number & x is a non-trivial solution to

$$x^2 = 1 \bmod N$$ in the range

$1 \leq x \leq N$ such that neither

$x = 1 \bmod N$ nor $x = N-1 = -1 \bmod N$

then at least one of
GCD$(x-1, N)$ and GCD$(x+1, N)$
is a nontrivial factor of N computable w/ $O(L^3)$ ops

Proof: Since $x^2 = 1 \bmod N$, we have

$$x^2 - 1 \bmod N = 0 \bmod N$$

so that N divides

$x^2 - 1 = (x+1)(x-1)$. This implies that N has a common factor w/ $x+1$ or $x-1$.

But by assumption $1 < x < N-1$,

So $x + 1 < N$

& $x - 1 < x + 1 < N$

so that N cannot be the common factor.

We can then compute $GCD(x-1, N)$ & $GCD(x+1, N)$ & get a non-trivial factor of N w/ $O(L^3)$ ops.

Another thm: Suppose $N = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$ is a prime factorization of an odd composite integer.

Let x be an integer chosen uniformly @ random subject to $1 \le x \le N-1$ & x is co-prime to N.

Let r be the order of $x \bmod N$. Then

$$\Pr\{r \text{ is even} \ \& \ x^{r/2} \not\equiv -1 \bmod N\} \ge 1 - \frac{1}{2^m}$$

(So when $m \ge 2$, $\Pr\{\cdot\} \ge 1/2$)

Full reduction:

Input: composite # N

output: nontrivial factor of N

Runtime: $O((\log N)^3)$ ops, constant success prob.

Alg.

1. If N even, return factor 2.
2. If $N = a^b$ for $a \geq 1$ & $b \geq 2$, return a (fast classical alg. for this special case)
3. choose $x \in [1, N-1]$ uniformly @ random. If $GCD(x,N) > 1$ then return the factor $GCD(x,N)$
4. If not, use quantum order finding to find order r of x mod N.
5. If r is even & $x^{r/2} \neq -1 \bmod N$ then compute $GCD(x^{r/2}-1, N)$ & $GCD(x^{r/2}+1, N)$ & test if factor

success prob. $\geq 1/2$