COL863: Quantum Computation and Information

Ragesh Jaiswal, CSE, IIT Delhi

Order finding

Given co-prime integers $N > x > 0$, compute the order of x modulo N.

Quantum Order-finding

1. $|0\rangle |1\rangle$ (Initial state)
2. $\rightarrow \frac{1}{2^{t/2}} \sum_{j=0}^{2^t-1} |j\rangle |1\rangle$ (Create superposition)
3. $\rightarrow \frac{1}{2^{t/2}} \sum_{j=0}^{2^t-1} |j\rangle \left| x^j \ (mod\ N) \right\rangle$ (Apply $U_{x,N}$)
   $\approx \frac{1}{\sqrt{r}2^{t/2}} \sum_{s=0}^{r-1} \sum_{j=0}^{2^t-1} e^{(2\pi i)\frac{sj}{r}} |j\rangle |u_s\rangle$
4. $\rightarrow \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} \left| \widetilde{(s/r)} \right\rangle |u_s\rangle$ (Apply inverse FT to 1^{st} register)
5. $\rightarrow \widetilde{(s/r)}$ (Measure first register)
6. $\rightarrow r$ (Use continued fractions algorithm)

- What is the size of the circuit that computes the order with high probability? $O(L^3)$

Quantum Computation: Factoring

Factoring

Given a positive composite integer N, output a non-trivial factor of N.

- We will solve the factoring problem by reduction to the order finding problem.
- Theorem 1: Suppose N is an L bit composite number, and x is a non-trivial solution to the equation $x^2 = 1 \ (mod \ N)$ in the range $1 \leq x \leq N$, that is, neither $x = 1 \ (mod \ N)$ nor $x = -1 \ (mod \ N)$. Then at least one of $gcd(x-1, N)$ and $gcd(x+1, N)$ is a non-trivial factor of N that can be computed using $O(L^3)$ operations.
- Theorem 2: Suppose $N = p_1^{\alpha_1} ... p_m^{\alpha_m}$ is the prime factorisation of an odd composite positive integer. Let x be an integer chosen uniformly at random, subject to the requirement that $1 \leq x \leq N-1$ and x is co-prime to N. Let r be the order of x modulo N. Then

$$\mathbf{Pr}[r \text{ is even and } x^{r/2} \neq -1 \ (mod \ N)] \geq 1 - \frac{1}{2^m}.$$

Factoring

Given a positive composite integer N, output a non-trivial factor of N.

Quantum Factoring Algorithm

1. If N is even, return 2 as a factor.
2. Determine if $N = a^b$ for integers $a, b \geq 2$ and if so, return a.
3. Randomly choose $1 \leq x \leq N - 1$. If $gcd(x, N) > 1$, then return $gcd(x, N)$.
4. Use the Quantum order-finding algorithm to find the order r of x modulo N.
5. If r is even and $x^{r/2} \neq -1 \ (mod \ N)$, then compute $p = gcd(x^{r/2} - 1, N)$ and $q = gcd(x^{r/2} + 1, N)$. If either p or q is a non-trivial factor of N, then return that factor else return "Failure".

End