CS506: An Introduction to Quantum Computing

University of Illinois at Chicago

Class Notes

Student: Ameer Mustafa
Date: November 10, 2025

Shor's Factoring Problem

Input: An integer $N > 1$
Output: An integer (factor) $1 < p < N$ such that p divides N, or report that no such integer exists.

Step-By-Step Process

1. Check using a classical polynomial-time algorithm if N is prime. If so, report "no factor exists" and exit. **(a)**
2. If N is even, then $p = 2$, exit.
3. If $N = p^c$ for some prime p and integer $c \geq 1$, then using a classical algorithm find and report p, exit. **(a)**
4. Pick uniformly at random an integer $1 < a < N$.
5. If $\gcd(a, N) > 1$, then $p = \gcd(a, N)$, exit. **(b)**
6. Find the order r of a modulo N, i.e., the minimum r such that $a^r \equiv 1 \pmod{N}$ (**Quantum Part**)
7. If r is even and N does not divide $a^{r/2} + 1$, then $p = \gcd(a^{r/2} - 1, N)$.
   Else, report "Not successful." **(c)**

Expanding Part 6

6.1 Select an integer q such that q is a power of 2 and q is the minimum such integer that is at least $2N^2$. Let $t = \log_2 q$. **(e)**

6.2 Create the following

$$|\psi_1\rangle = \frac{1}{\sqrt{q}} \sum_{x=0}^{q-1} |x\rangle = \frac{1}{\sqrt{2^t}} \sum_{x_1,\ldots,x_t \in \{0,1\}} |x_1, \ldots, x_t\rangle$$

$$q \left\{ \begin{array}{cccc} |0\rangle & \longrightarrow & H & \longrightarrow \\ |0\rangle & \longrightarrow & H & \longrightarrow \\ \vdots & & \vdots & \\ |0\rangle & \longrightarrow & H & \longrightarrow \end{array} \right. \quad |\psi_1\rangle$$

6.3 (a) Let f be the function given by $f(i) = x^i \bmod N$. **(d)**

(b) Use modular exponential to compute $f(i)$ using $O\big((\log_2 N)^3\big)$ AND/OR/NOT gates with fan-in and fan-out at most 2.

(c) Replace each AND/OR/NOT gate by reversible 2- or 3-qubit gates, and replace each 3-qubit gate by $O(1)$ 2-qubit gates.

(d) This gives a U_f gate using $O\big((\log_2 N)^3\big)$ reversible 1- and 2-qubit gates.

$$U_f \,|g\rangle\,|h\rangle = |g\rangle\,|\,h \oplus f(g)\,\rangle$$

6.4 Apply U_f

$$U_f\,|\psi_1\rangle\,|0\rangle = \frac{1}{\sqrt{q}}\sum_{x=0}^{q-1}|x\rangle\,|f(x)\rangle$$

$$= \left(\frac{1}{\sqrt{\lfloor q/r\rfloor}}\sum_{z=0}^{\lfloor q/r\rfloor-1}|zr+x_0\rangle\right)|f(x_0)\rangle \qquad\qquad x_0\in\{0,1,\ldots,q-1\}$$

$$= |\psi_2\rangle\,|f(x_0)\rangle$$

$$\text{where }\ |\psi_2\rangle = \frac{1}{\sqrt{\lfloor q/r\rfloor}}\sum_{z=0}^{\lfloor q/r\rfloor-1}|zr+x_0\rangle$$

6.5 Let $|\psi_3\rangle = QFT_{2^t}\,|\psi_2\rangle$. This uses $O(t^2) = O(\log^3 N)$. Hadamard and controlled-rotation gates.

6.6 Measure $|\psi_3\rangle$ on a standard computational basis giving an integer.

$$m = k\tfrac{2^t}{r} + \delta,\ \text{for some } \delta < \tfrac{1}{2},\ \text{with probability} \geq \tfrac{4}{\pi^2}.$$

6.7 Use continued fraction expansion of $\frac{m}{2^t}$ to obtain r using $O(\log_2 N)$ operations. **(f)**

Comments

(a) Not necessary but may save computation time.

(b) $O(\log N)$ time.

(c) Probability of this $\geq \dfrac{1}{2}$.

(d) Output of f is an integer from $\{0,1,\ldots,N-1\}$ of $\lceil \log_2 N\rceil$ bits.

(e) Clearly, $q \leq 4N^2$, and $\log_2 q = t < 3\log_2 N$.

(f) We have to perform the QFT twice to obtain r with probability $\geq \dfrac{6}{\pi^2}$.

Total Success Probability:

$$\frac{1}{2}\times\frac{4}{\pi^2}\times\frac{4}{\pi^2}\times\frac{6}{\pi^2}\approx 0.05$$

Total Complexity: $O(\log_2 N)$ Classical + $O\big((\log_2 N)^3\big)$ Quantum gates.