3.4 Shor's Quantum Factoring Algorithm

Shor's factoring algorithm utilizes the quantum period-finding algorithm (also due to Shor) of the previous section to find a factor of a given integer N. It has been known long before quantum computing that factoring an integer N can be reduced to finding the multiplicative order of integers modulo N. Shor's algorithm is also based on this fact.

We state some definitions and basic facts from algebra and number theory. Proofs can be found in Nielsen and Chuang Appendix 4. Throughout we assume N is an n bit integer, $1 \ll N \leq 2^n$. We also assume that N is odd, because otherwise we simply have 2 as a factor.

In the following $\mathrm{GCD}(a,b)$ denotes the greatest common divisor of integers a and b. There is an efficient algorithm dating back to Euclid that computes GCD in polynomial time. If $\mathrm{GCD}(a,b) = 1$ we say that a and b are coprime or relatively prime.

Proposition 1 *Given an arbitrary integer $N \geq 1$, let Z_N^* denote the set of integers $1 \leq a \leq N-1$ that are coprime to N. The set Z_N^* forms a cyclic group under multiplication modulo N. If $N = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$ is the prime factorization of N, then the order (number of elements) of Z_N^* is given by the Euler-phi function*

$$\phi(N) = \prod_{i=1}^{k} p_i^{n_i - 1}(p_i - 1).$$

For any element $a \in Z_N^*$ of the group,

$$a^{\phi(N)} \equiv 1 \ \ mod\ N$$

The order of an element $a \in Z_N^*$ is defined as the smallest integer $r \geq 1$ such that

$$a^r \equiv 1 \ \ mod\ N.$$

Each element has a finite order that divides $\phi(N)$.

Now observe that for any $a \in Z_N^*$, the function

$$f_{N,a}(x) = a \cdot a^x \bmod N$$

is a periodic function on integers $x = 0, 1, \ldots,$ with a period equal to the order of a. So, we may apply the quantum period finding algorithm of the previous section with x in the range $0 \leq x \leq N^2 - 1$. Notice that the period is bounded by $\phi(N)$ which in turn is bounded by $N - 1 \leq \sqrt{N^2 - 1}$. The order of a can be found in $\mathrm{poly}(n)$ time using the quantum period-finding algorithm. The oracle in the algorithm is implemented by a subroutine that computes the function $f_{N,a}$, which can be done in complexity $O(n^3)$ using classical circuits.

We are now ready to give Shor's algorithm. The input to the algorithm is an odd composite integer N with at least two distinct prime factors. For N a prime power, there are efficient classical algorithms for finding the prime factor of N, so there is no essential loss of generality here. The output of the algorithm is one of the prime factors of N. Clearly, by recursive application of the algorithm, all prime factors can be found.

1. Select an integer $a \in [2, N-1]$ at random and compute $\mathrm{GCD}(a,N)$. If $\mathrm{GCD}(a,N) \neq 1$, exit. We have found a factor of N. Otherwise go to next step.

2. Call the quantum algorithm to find the order r of a.

3. If r is odd, go back to step 1 and start over. Otherwise, check if N divides $a^{r/2}+1$; if yes, go to step 1. If N does not divide $a^{r/2}+1$, output $\mathrm{GCD}(N, a^{r/2}+1)$ as a factor of N.

The justification of the algorithm is as follows. In step 3, if the order r is even, then we can write

$$a^r - 1 = (a^{r/2}-1)(a^{r/2}+1);$$

hence

$$(a^{r/2}-1)(a^{r/2}+1) \equiv 0 \mod N.$$

So N divides $(a^{r/2}-1)(a^{r/2}+1)$. We know that N does not divide $(a^{r/2}-1)$ because then we would have $a^{r/2} \equiv 1 \mod N$, contrary to the assumption that r is the order of a. It follows that $\mathrm{GCD}(N, a^{r/2}+1) \neq 1$. If N does not divide $a^{r/2}+1$, then $1 < \mathrm{GCD}(N, a^{r/2}+1) < N$, and $\mathrm{GCD}(N, a^{r/2}+1)$ is a non-trivial factor of N. (In this case $\mathrm{GCD}(N, a^{r/2}-1)$ is also a non-trivial factor of N.)

To summarize, we succeed unless (i) the order r is odd, or (ii) r is even but

$$a^{r/2} \equiv -1 \mod N.$$

How likely is success? By a well-known result from algebra, this probability is at least $1-2^{-k}$ where k is the number of distinct odd prime factors of N. The assumption that N has at least two distinct prime factors is made to ensure that $k \geq 2$ so that the probability of success is at least $1/2$. Otherwise, it has no significance.