1 Assignment 4: Grover with unknown number of solutions

In the lecture we discussed Grover’s algorithm in the case where there is exactly one \(x \in \{0, 1\}^n\) s.t. \(f(x) = 1\). Here we are going to go one step further and discuss the case where we don’t know the number of solutions. To that end, let \(m\) be a fixed integer and \(l\) be a uniformly random integer \(0 \leq l < m\). Furthermore, let \(\theta\) be the initial angle between the state \(|U\rangle = H^\otimes n|0^n\rangle\) and \(|B\rangle\) defined as

\[
|B\rangle = |f^{-1}(0)|^{-\frac{1}{2}} \sum_{x: f(x) = 0} |x\rangle.
\]

Suppose we run \(l\) iterations of Grover and then measure the output.

1.1 Success probability

Show that the probability of observing a string \(x\) s.t. \(f(x) = 1\) is given by

\[
P_m = \frac{1}{m} \sum_{l=0}^{m-1} \sin^2((2l + 1)\theta). \tag{1}
\]

1.2 Simplifying the expression

Show that

\[
P_m = \frac{1}{2} - \frac{\sin(4m\theta)}{4m \sin(2\theta)}. \tag{2}
\]

Hint: recall the trigonometric identities

\[
\sin^2 \left( \frac{\theta}{2} \right) = \frac{1 - \cos(\theta)}{2} \tag{3}
\]

and

\[
\sum_{j=0}^{m-1} \cos(\alpha + 2\beta j) = \frac{\sin(m\beta) \cos(\alpha + (m - 1)\beta)}{\sin(\beta)}. \tag{4}
\]

1.3 Expected number of steps

Show that if we pick \(m\) as \(2^n\), the probability of success is lower-bounded by a constant. Conclude from that that with probability \(\geq \frac{2}{3}\) we can find \(x\) s.t. \(f(x) = 1\) from \(O(2^n)\) queries.
2 From Order Finding to Factoring

Let \( N = p \cdot q \) (with \( p, q \) prime numbers of the order of magnitude \( 2^{\lambda/2} \)) be an RSA modulus. During the lecture, you saw a quantum algorithm SHOR which takes as input \( x \in \mathbb{Z}_N^\times \) and returns its order, that is to say the smallest \( r > 0 \) such that \( x^r = 1 \mod N \). We are going to see how to factor \( N \) using this algorithm. In the following, we will look at elements \( x \mod N \) which will be represented as elements in \([0, N - 1]\).

We are going to use the following classical results from algebra:

**Theorem 2.1** (Bezout’s theorem). For any \( x, y \in \mathbb{Z} \), there exists \( u, v \in \mathbb{Z} \) such that \( xu + yv = \gcd(x, y) \).

Reciprocally, if there exists \( u, v \in \mathbb{Z} \) such that \( xu + yv = d \), then \( \gcd(x, y) | d \).

**Theorem 2.2** (Chinese Remainder Theorem). If \( M = \prod_{i=1}^p n_i \), where the \( n_i \) are integers greater than 1 which are pairwise coprime, then \( \mathbb{Z}_M \simeq \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_p} \) via the ring isomorphism \((x \mod N) \mapsto (x \mod n_1, \ldots, x \mod n_p)\).

**Theorem 2.3.** Let \( G \) a finite commutative group, let \( x \in G \) with order \( w(x) \). If \( x^r = 1 \), then \( w(x) | r \).

1. Using the Bezout’s Theorem, compute \(|\mathbb{Z}_l^\times|\) for \( l \) a prime number.
2. Using the Chinese Remainder Theorem, compute \( \phi(N) = |\mathbb{Z}_N^\times| \).
3. Take \( x \) uniform in \( \mathbb{Z}_N \). What is the probability that \( x \in \mathbb{Z}_N^\times \)?
4. Let \( x \in \mathbb{Z}_N^\times \) of odd order. Show that \( -x \) has even order. Deduce that if \( x \) is uniformly sampled in \( \mathbb{Z}_N^\times \), what the probability for \( x \) to have even order is \( \geq 1/2 \).
5. Sample \( x \) uniform in \( \mathbb{Z}_N^\times \) of even order. Let \( r \) be its order. Assume that \( x^{r/2} \pm 1 \neq 1 \), \( N \) (it can be proven to happen with a small probability \( \varepsilon \)), propose a way to find a non-trivial factor of \( N \).
6. Deduce an algorithm making calls to SHOR which finds a non-trivial factor of \( N \) with high probability. Give its expected number of call to SHOR.

3 Modular Exponentiation

We are going to construct the gate \( \Lambda_m(M_a)|k\rangle|x\rangle \mapsto |k\rangle|a^k \cdot x \mod N\rangle \) for any \( a \in \mathbb{Z}_N \). In what is following, every quantum algorithm will be allowed to use ancillas and \( N \) can be represented over \( k \) qubits.

1. Let \( F \) and \( F^{-1} \) be computed by Boolean circuits of size \( \leq L \) and depth \( \leq d \). Show that \( F \) can be realized by a reversible circuit of size \( O(L + n) \) and depth \( O(d) \) using ancillas. (Recall that in those cases, we know how to construct a quantum circuit \( F^{\oplus} \) such that \( F^{\oplus}|x\rangle|y\rangle|0^m\rangle = |x\rangle|y \oplus F(x)\rangle|0^m\rangle \).
2. Show that for every \( a \in (\mathbb{Z}_N)^\times \) there exists an efficient quantum gate \( T_a|x\rangle \mapsto |ax \mod N\rangle \)
3. Propose a classical algorithm that on input \( x, k, N \) computes \( x^k \mod N \) by doing \( O(\log(k)) \) operations in \( \mathbb{Z}_N \).