

1. (10 points) Let U_f be the quantum oracle corresponding to the function $f : \{1, \dots, N\} \rightarrow \{0, 1\}$, i.e.,

$$U_f|x\rangle = (-1)^{f(x)}|x\rangle. \quad (1)$$

We start with the state $|+\rangle = \frac{1}{\sqrt{N}} \sum_{x=1}^N |x\rangle$ and repeatedly apply the Grover operator

$$R = -U_+U_f, \quad \text{where } U_+ = 1 - 2|+\rangle\langle+|. \quad (2)$$

Write an explicit expression for the quantum state after k iterations.

2. (10 points) Let p be a prime number. Suppose that we know the factorization of $p - 1$.

- a) Give an efficient (i.e., polynomial in $\log p$) algorithm to check whether a given element $x \in \mathbb{Z}_p^*$ is a primitive root.
- b) Give an efficient *probabilistic* algorithm to find a primitive root. The algorithm must produce a correct answer eventually, but the running time may fluctuate. Give an upper bound for the average running time (we average over the random bits used by the algorithm but not over p). **Hint:** Use the following lower bound for the Euler function

$$\phi(q) \geq c \frac{q}{\ln \ln q} \quad \text{for some positive constant } c. \quad (3)$$

The last two problems are concerned with the *non-Abelian hidden subgroup problem*. Let G be a finite group (which we know) and $H \subseteq G$ a subgroup (which we need to find). A *hidden subgroup oracle* is a function $f : G \rightarrow M$ (where M is an arbitrary set, e.g., $\{0, 1\}^n$) satisfying the following condition:

$$f(x) = f(y) \quad \text{if and only if} \quad y = xh \text{ for some } h \in H. \quad (4)$$

In other words, f is constant on right cosets of H and takes distinct values on distinct cosets. The goal is to find H using the oracle in a classical or quantum fashion.

The non-Abelian hidden subgroup problem arises naturally in many settings, for example, in connection with the graph isomorphism problem. Indeed, suppose we need to check whether two graphs, Γ_1 and Γ_2 are isomorphic. This question may be phrased as follows: Is there a permutation of vertices of the disjoint union, $\Gamma = \Gamma_1 \sqcup \Gamma_2$ that switches Γ_1 and Γ_2 ? Thus, the graph isomorphism problem is reduced to finding the automorphism group of Γ , which is a subgroup in the permutation group S_n . The corresponding oracle function $f : S_n \rightarrow \text{graphs}$ takes a vertex permutation σ to the graph $\sigma(\Gamma)$ obtained by applying σ to Γ .

It is known that sufficient information can be extracted from a quantum hidden subgroup oracle with polynomially many queries (see M. Ettinger, P. Hoyer, E. Knill, quant-ph/9901034). More exactly, given $k = \text{poly}(\log |G|)$ copies of the state

$$\rho = \frac{1}{|G|} \sum_{x^{-1}y \in H} |x\rangle\langle y|, \quad (5)$$

one can determine H with probability close to one.¹ However, no efficient algorithm is known to accomplish this task, which is considered one of the major challenges in quantum computation. . . Hopefully, this gives you enough context for the problems.

3. (15 points) The *dihedral* group D_N is the symmetry group of an N -sided regular polygon. Elements of this group can be conveniently designated as $g = (a, x)$, where $a \in \{+1, -1\}$, $x \in \mathbb{Z}_N$ (we will refer to a as *parity*). The element $(+1, x)$ is the rotation by angle $\frac{2\pi x}{N}$, whereas $(-1, x)$ is the reflection about some axis.² In this notation, the multiplication rule can be represented as follows:

$$(a, x) \cdot (b, y) = (ab, x + ay). \quad (6)$$

Consider the hidden subgroup problem for D_N . Let us assume that the hidden subgroup has the form $H = \{(+1, 0), (-1, \omega)\}$ (i.e. H consists of the identity element and the reflection about some unknown axis).

We create the state $|\psi\rangle = \frac{1}{\sqrt{2N}} \sum_{g \in D_N} |g\rangle$, let the oracle compute $f(g)$, and discard the computed value. Thus we obtain the mixed state ρ (see Eq. (5)).

a) Write the state ρ in the Fourier basis, i.e., represent it in the form

$$\rho = \sum_{q, q'} \gamma(q, q') \otimes (|\xi_q\rangle \langle \xi_{q'}|), \quad \text{where } |\xi_q\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \mathbb{Z}_N} e^{iqx} |x\rangle, \quad q = \frac{2\pi y}{N}, \quad y \in \mathbb{Z}_N. \quad (7)$$

(Here, $\gamma(q, q')$ is some operator on the parity qubit.)

b) Now we measure the parity qubit in the basis $\{|+\rangle, |-\rangle\}$, where $|\pm\rangle = \frac{1}{\sqrt{2}}(|+1\rangle \pm |-1\rangle)$. We also measure the momentum q . Show that the outcome (α, q) occurs with the following probability:

$$p(0, q) = \frac{1 + \cos q\omega}{2N}, \quad p(1, q) = \frac{1 - \cos q\omega}{2N}. \quad (8)$$

c) Let $n = \lceil \log_2 N \rceil$. Show that the unknown parameter ω can be found with $O(n)$ queries to the oracle and exponential *classical* postprocessing. (The algorithm must produce the correct result with probability at least $2/3$.) **Hint:** We sample $m = O(\log n)$ pairs according to the above distribution. Then we try every possible value of ω and find the best fit.

4. (10 points) An *action* of a group G on a set M is a function $u : G \times M \rightarrow M$ that satisfies the equation:

$$u(gh, a) = u(g, u(h, a)). \quad (9)$$

Suppose we have a quantum oracle corresponding to some action of \mathbb{Z} on a finite set M . We are given two elements $a, b \in M$, and we need to tell if they belong to the same orbit, i.e.,

¹Can you prove that without reading the paper? In addition to intellectual satisfaction, this will bring you 10 points of extra credit. **Hint:** Check *all* elements of the group G one after another, not disturbing the given state $\rho^{\otimes k}$ too much.

²The reflection about an arbitrary symmetry axis is represented as the rotation $(1, x)$ followed by the reflection about some fixed axis, which is denoted by $(-1, 0)$.

if $b = u(\omega, a)$ for some $\omega \in \mathbb{Z}$. Reduce this problem to the hidden subgroup problem for the dihedral group. The reduction may be quantum, but its total complexity must be polynomial in $\log |M|$. **Hint:** First, find the periods of a and b with respect to the group action. Show that if both periods are equal to N , then the following function f corresponds to a certain hidden subgroup $H \subseteq D_N$:

$$f(+1, x) = u(x, a), \quad f(-1, x) = u(x, b). \quad (10)$$