If there is a problem you can't solve, then there is an easier problem you can solve: find it.
– George Pólya

Problem Set 4

PCMI USS, Summer 2023

1. (**The Berstein-Vazirani problem**) Suppose $a \in \mathbb{Z}_2^n$ is a an unknown bitstring. The goal is to learn the entire string (all the bits). You can query any bitstring $x \in \mathbb{Z}_2^n$, to which the oracle will respond with $a \cdot x$, the dot product of a and x modulo 2.

   (a) Play the game classically with your groupmates, with one person assigned the role of teacher or oracle. What is the classical query complexity of the Bernstein-Vazirani question?

   (b) Now let's consider the quantum version. The oracle $\mathcal{O}_a$ will operate on the Hilbert space $\mathcal{H} = (\mathbf{C}^2)^{\otimes n} \otimes (\mathbf{C}^2)$, where the first factor is the query register and the second is the response register, and we define $\mathcal{O}_a$ on a basis by

   $$\mathcal{O}_a |x, r\rangle = |x, r \oplus a \cdot x\rangle,$$

   for any $a \in \mathbb{Z}_2^n$ and $r \in \mathbb{Z}_2$. We will be using the phase kickback trick; verify that for any $x \in \mathbb{Z}_2^n$, we have

   $$\mathcal{O}_a |x, -\rangle = (-1)^{a \cdot x} |x, -\rangle$$

   (c) Ok, now for the quantum algorithm. Explain how to create the state

   $$|\psi_0\rangle = \frac{1}{\sqrt{2^n}} \sum_{j \in \mathbb{Z}_2^n} |j\rangle |-\rangle$$

   (d) Now take $|\psi_0\rangle$ and apply $\mathcal{O}_a$ to the first register. Write down the resulting state.

   (e) Next apply $H^{\otimes n}$ to the first register. Again, write down the resulting state. Simplify your expression as much as possible.

   (f) Finally, measure the first register. With what probability can you now guess the value of a?

   (g) Compare the classical and quantum query complexites. What conclusion can you make about the Bernstein-Vazirani problem?

2. In Simon's Problem, suppose the hidden string s is allowed to be all zeros. Can you adapt the quantum algorithm so that it handles this case? [In terms of the hidden subgroup (HSP) problem, this is the case where the subgroup is $H = \{0\}$, which is an important subgroup!]

3. (a) Give an analysis of the classical query complexity of Simon's Problem. Assume the hidden string s is not all 0's. Analyze both the classical exact error complexity and the bounded error query complexity. Be as precise or as rigorous as you can.
   (b) Now allow the possibility that $s = 0$. How does this change your analysis of the classical query complexity? Again, analyze both the exact and bounded error cases.

4. In Simon's algorithm, we saw that each quantum query gives us a random value of $z \in \mathbb{Z}_2^n$ such that $z \cdot s = 0$. (Again, let's assume s is not all 0's for this problem.) Give an analysis of how many such z's must be chosen to have a high probability (more than 2/3, say) of being able to determine s uniquely. Be as precise or as rigorous as you can.

5. Further investigate the HSP for the group $\mathbb{Z}_2^n$. That is, suppose $f : \{0,1\}^n \to \{0,1\}^n$ is a function, and suppose there is a secret subgroup H of $\mathbb{Z}_2^n$ such that

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

(The condition $y = x \oplus h$ for some $h \in H$ is equivalent to saying that y and x lie in the same coset of H.) You wish to determine the hidden subgroup H, and you are allowed to query any $x \in \{0,1\}^n$, to which you are given the response $f(x)$.

   (a) Show that Simon's problem is exactly the same as HSP for $\mathbb{Z}_2^n$ in the case that you are promised that $|H| = 2$.
   (b) Suppose you are promised that the hidden subgroup H has 4 elements. Can you give a quantum algorithm to solve HSP under this assumption?
   (c) How about the case when your are promised that $|H| = 2^{n-1}$?
   (d) What about other special cases? Can you say anything about the general case?