**Quantum Algorithms and Cryptography**

NPTEL Questions- Practice Set 2

Instructor: *Shweta Agrawal*

**Instructions.**

- Note that this is an ungraded practice set question.
- Either use discussion forums to ask doubts or send direct email to TAs (noc25-cs61@nptel.iitm.ac.in).
- Please do not discuss/post the entire solution on the discussion forum.

---

1. What kind of function is given in Simon's problem, and what is the goal? Suppose we run Simon's algorithm once and obtain a string $j \in \{0,1\}^n$ upon measuring the first register. It is known that this $j$ satisfies the constraint $s \cdot j = 0 \bmod 2$. Is this sufficient to recover the hidden string $s$? Justify your answer.
2. Analyze the different steps of Simon's algorithm in the special case where $s = 0^n$ (so all $x_i$ values are distinct), and show that the final output $j$ is uniformly distributed over $\{0,1\}^n$.
3. Suppose Grover's algorithm is run on a search space of size $N = 2^n$.
   (a) Suppose $n = 2$, and the input string is $x = x_{00}x_{01}x_{10}x_{11} = 0001$. Give the specific initial state, three intermediate states, and the final state after one iteration ($k = 1$). Also, compute the success probability of measuring the marked item.
   (b) Repeat the above but for $k = 2$ iterations. What is the final state now, and what is the success probability?
4. Consider the character on $\mathbb{Z}_N$, $\chi_\gamma : \mathbb{Z}_N \to \mathbb{C}$ defined as $\chi_\gamma(x) = \omega^{\gamma \cdot x}$ where $\omega = e^{2\pi i/N}$. Prove the following.
   (a) $\mathbb{E}_{x \sim \mathbb{Z}_N}[\chi_\gamma(x)] = 0 \quad$ for $\gamma \neq 0$.
   (b) $\chi_\gamma(x)^* = \chi_{-\gamma}(x) = \chi_\gamma(-x)$.
   (c) $\{\chi_\gamma\}_{\gamma \in \mathbb{Z}_N}$ form an orthonormal basis.
5. Prove that if $s \neq 000\ldots0$

$$\implies \hat{f}(s) = \frac{1}{2}\left(\mathbb{E}_{\mathbf{x} \sim \{0,1\}^n}[f(\mathbf{x}) \mid \chi_s(\mathbf{x}) = +1] - \mathbb{E}_{\mathbf{x} \sim \{0,1\}^n}[f(\mathbf{x}) \mid \chi_s(\mathbf{x}) = -1]\right),$$

   where the $\mid$ notation denotes "conditional expectation" and $\mathbb{E}_{\mathbf{x} \sim \{0,1\}^n}[\cdot]$ denotes "the expected value, when $\mathbf{x}$ is chosen uniformly at random from $\{0,1\}^n$".
6. Let $f : \{0,1\}^n \to \mathbb{C}$. Now for $y \in \{0,1\}^n$, define the function $f^{+y} : \{0,1\}^n \to \mathbb{C}$ by $f^{+y}(x) = f(x+y)$. (Here the addition is in $\mathbb{F}_2^n$; i.e., coordinate-wise mod 2.) Compute $\widehat{f^{+y}}(s)$ in terms of $\hat{f}(s)$. How does performing Fourier sampling of $f^{+y}$ compare to performing Fourier sampling on $f$?

7. Consider the function $f(a) = 7^a \mod 10$.
   a) What is the period $r$ of $f$?
   b) Show how Shor's algorithm finds the period of $f$, using a Fourier transform over $Q = 128$ elements. Write down all intermediate superpositions of the algorithm for this case. You may assume you're lucky, meaning the first run of the algorithm already gives a measurement outcome $b = \frac{cQ}{r}$ with $c$ coprime to $r$.
8. What is the Hidden Subgroup Problem (HSP)? Explain how the discrete logarithm problem and the period-finding problem (as used in Shor's algorithm) can be viewed as an HSP instance.
9. Prove that two bases $B_1, B_2 \in \mathbb{R}^{m \times n}$ generate the same lattice, i.e. $\mathcal{L}(B_1) = \mathcal{L}(B_2)$ if and only if $B_2 = B_1 U$ for some unimodular matrix $U$.
10. In class we saw the random lattices used in cryptography, as well as hard problems on lattices such as shortest vector and closest vector problem. Express the SIS and LWE problems that we saw in class as lattice problems.
11. Recall the Gentry-Sahai-Waters FHE scheme we saw in class. To prove the semantic security (IND-CPA) of the scheme, we go via the following sequence of hybrid games:
    1. In $\mathsf{Game}_0$, the public key is sampled as in the real encryption scheme and the ciphertext is honestly computed.
    2. In $\mathsf{Game}_1$, the public key is replaced with a uniformly random matrix.
    3. In $\mathsf{Game}_2$, the ciphertext is replaced with a uniformly random matrix independent of the message.

    (a) Show that $\mathsf{Game}_0$ and $\mathsf{Game}_1$ are computationally indistinguishable via a reduction to the LWE assumption.
    (b) Show that $\mathsf{Game}_1$ and $\mathsf{Game}_2$ are statistically indistinguishable by invoking the Leftover Hash Lemma (LHL).
12. Recall the quantum key distribution protocol we saw in class.
    (a) Rewrite the protocol using EPR pairs. Argue that this protocol is equivalent to the one we saw in class.
    (b) What is the best strategy by Eve in this scenario? Argue that even the best strategy by Eve will be detected by the honest players with nonzero probability.
    (c) Why doesn't the following attack work? After the set S is announced, Eve changes the theta corresponding to the indices in S that she tampered with.
    (d) What aspect of this protocol is superior to the DDH based key exchange protocol that we saw in class?
13. Prove that a classical one time pad satisfies information theoretic security.
14. Prove that a quantum one-time pad results in a maximally mixed state.
15. Define a trapdoor claw-free function (TCF). List it's properties.