CSE 291 / Math 277 - Quantum Complexity Theory (Fall 2024)
Homework 5
Due Thursday, November 7, 3:00pm

Note: It is highly recommended (though not required) that you type your answers. It is your responsibility to make any handwriting clear and legible for grading. You may work with 1-2 other collaborators, but you must write the solutions separately and clearly mark the names of each person you worked with.

Problems:

1. **A majority of quantum query techniques**

   For any bitstring $x \in \{0,1\}^N$, we define its majority as the bit that occurs most often:

$$\mathsf{Maj}(x) = \begin{cases} 1 & \text{if } |x| \geq N/2 \\ 0 & \text{otherwise} \end{cases}$$

   where $|x|$ is the Hamming weight of x.

   Let's first establish that there are no efficient query algorithms for Majority by a reduction from the Or function:

   (a) Recall that $\mathsf{Or}(x) = x_1 \vee \cdots \vee x_N$ has quantum query complexity $\Omega(\sqrt{N})$ by the Grover lower bound. Show that a quantum query algorithm for Majority implies a query algorithm for Or, and therefore, conclude the quantum query complexity of Majority is $\Omega(\sqrt{N})$.

   In fact, Majority is even harder than Or. We will show this via both the polynomial and adversary methods.

   (b) Show that the quantum query complexity of Majority is $\Omega(N)$ by the polynomial method. You will probably want to use the following theorem:

   Theorem 1 ([Paturi 92]) *Let $p\colon \mathbb{R} \to R$ be a real polynomial. Suppose $p(z) \in [0,1]$ on all integer points $z \in \{0,1,\ldots,N\}$. Then, there exists a universal constant $C \in \mathbb{R}^+$ such that*

$$\deg(p) \geq \max_{z \in [0,N]} \left(\frac{|p'(z)|}{C(1+|p'(z)|)} \sqrt{z(N-z)} \right)$$

   (c) Show that the quantum complexity of Majority is $\Omega(N)$ by the adversary method.

2. **Sample complexity of learning stabilizer states**

   Let $|\psi\rangle$ be an unknown n-qubit stabilizer state (i.e., a state prepared by applying a Clifford circuit to $|0^n\rangle$). Suppose would like to make some measurements to determine $|\psi\rangle$ with high probability using as few copies of the state as possible. A single copy of $|\psi\rangle$ is clearly insufficient—consider the case where we're trying to distinguish $|0\rangle$

and $|+\rangle$. In fact, for *general* quantum states, $\Omega(2^n)$ copies of the state are needed. However, for stabilizer states, it turns out that $O(n)$ copies are sufficient!

We will use a measurement protocol called "Bell sampling". Let's try to derive some of its properties. First, define the two-qubit Bell basis:

$$|\sigma_{00}\rangle := \tfrac{|00\rangle+|11\rangle}{\sqrt{2}} \qquad |\sigma_{01}\rangle := \tfrac{|01\rangle+|10\rangle}{\sqrt{2}}$$
$$|\sigma_{10}\rangle := \tfrac{|00\rangle-|11\rangle}{\sqrt{2}} \qquad |\sigma_{11}\rangle := \tfrac{|01\rangle-|10\rangle}{\sqrt{2}}$$

One can check that this is indeed an orthonormal basis. For a two-qubit state $|\varphi\rangle$, measuring in this basis means you get the outcome $|\sigma_{ij}\rangle$ with probability $|\langle\sigma_{ij}|\varphi\rangle|^2$. To perform Bell sampling, we will measure pairs of qubits of the state $|\psi\rangle \otimes |\psi\rangle$ in the Bell basis. That is, for all $i \in \{1, \ldots, n\}$, we measure the ith qubits of the first and second copy of $|\psi\rangle$ in the Bell basis.

(a) Show that the probability of measuring the $|\sigma_{00}\rangle$ outcome for all the qubit pairs is equal to $\frac{1}{2^n}\left|\sum_{x\in\{0,1\}^n} \langle x|\psi\rangle^2\right|^2$.

Notice that we can rewrite this probability using the fact that

$$\sum_{x\in\{0,1\}^n} \langle x|\psi\rangle^2 = \sum_{x\in\{0,1\}^n} \langle x|\psi\rangle\,(\langle\psi|x\rangle)^* = \mathrm{tr}(|\psi\rangle\langle\psi^*|) = \langle\psi^*|\psi\rangle\,.$$

Of course, this is just the probability of a single outcome. We have to consider the remaining outcomes. We will use the following nice observation about the Bell basis—namely, every basis element is related to $|\sigma_{00}\rangle$ by a single-qubit Pauli operation:

$$|\sigma_{01}\rangle = (X \otimes I)\,|\sigma_{00}\rangle\,,\quad |\sigma_{10}\rangle = (Z \otimes I)\,|\sigma_{00}\rangle\,,\quad |\sigma_{11}\rangle = i(Y \otimes I)\,|\sigma_{00}\rangle$$

Since we can identify each Bell basis state with a Pauli operation (i.e, one of I, X, Y, or Z), we can identify a Bell sampling measurement with a Pauli string $P = P_1 \otimes P_2 \otimes \cdots \otimes P_n$. The Pauli P_i corresponds to the Bell basis measurement result on the ith qubit pair.

(b) Show that the probability of measuring the Pauli string $P \in \{I, X, Y, Z\}^{\otimes n}$ using Bell sampling is equal to $\frac{1}{2^n}\,|\langle\psi^*|\,P\,|\psi\rangle|^2$.

We'd like to say that the P we sample is a stabilizer of $|\psi\rangle$, but that's not quite right. Instead, we have the following fact:

(c) Show that $\langle\psi|\,P\,|\psi\rangle = 0$ for all Pauli strings P not in the stabilizer group of $|\psi\rangle$ (i.e., neither P nor $-P$ is in the stabilizer group).

Unfortunately, the Bell sampling outcome gives us the conjugate of $|\psi\rangle$ on one side. To continue, we'll need the following useful fact (proof left as an exercise):

Fact 1 *For every n-qubit stabilizer state $|\psi\rangle$, there exists a Pauli string $Q \in \{I, Z\}^{\otimes n}$ such that $Q\,|\psi^*\rangle = |\psi\rangle$.*

Note of warning: the Q used in the fact above need not be a stabilizer of $|\psi\rangle$. We now have all the tools we need to finish the stabilizer learning algorithm. You're only being asked to solve the first step.

(d) Prove that with high probability, $O(n)$ Bell samples suffice to construct a complete generating set for the stabilizer group of $|\psi\rangle$ *up to phase*.

To finish the algorithm, it suffices to determine the signs on the stabilizer group elements. To do this, for each stabilizer generator P measure a single copy of the state $|\psi\rangle$ in the eigenbasis of P. This will determine the sign. Once we have learned all the stabilizer generators and their phases, we have uniquely determined the state $|\psi\rangle$.