CSE 291 / Math 277 - Quantum Complexity Theory (Fall 2024)
Homework 3
Due Thursday, October 24, 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. **Two-level gates are exactly universal**

   One of the more remarkable aspects of quantum computation is that a few types of elementary operations suffice for universality. In the last homework, we explored universality in a computational sense—we can simulate any BQP computation using gates with only real amplitudes. In this problem, we will prove a more straightforward type of universality—any complex unitary can be decomposed as a product of gates from a simple gate set.

   Let's call a unitary *two-level* if it only acts nontrivially on two or fewer vector elements. So, for example, the following are examples of two-level 3×3 unitaries:

$$\begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} a & 0 & b \\ 0 & 1 & 0 \\ c & 0 & d \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & a & b \\ 0 & c & d \end{pmatrix}$$

   where $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is a 2×2 complex unitary matrix. Show that an arbitrary $d \times d$ unitary matrix can be decomposed as a product of two-level unitaries. Note that for the most part in this class we've focused on n-qubit unitaries, which act only the Hilbert space $(\mathbb{C}^2)^{\otimes n}$. For this problem (and often other applications), it helps to forget about that structure and just think about $d \times d$ matrices U such that $UU^\dagger = I$. (Hint: Starting with an arbitrary unitary matrix, can you apply a two-level unitary and simplify some small part of it?)

   Extra Remark: The decomposition of U into two-level unitaries is one way to show that U can be decomposed into 1- and 2-qubit gates since we now only need to show how to decompose an arbitrary two-level unitary. While you're not being asked to show this, the proof leverages the fact that any a two-level qubit can be thought of as a controlled single-qubit operation conjugated by a permutation.

2. **What if we just add more quantum to our quantum complexity class?**

   Recall that in the formal definition of BQP, the quantum circuit descriptions are generated by a poly-time classical Turing machine. Consider a variant BQQP (Bounded Error Quantum Quantum Polynomial Time) where the quantum circuit descriptions are themselves generated by a quantum circuit. That is, if we measure all qubits in the output of a quantum circuit, we get a (probability distribution over) encodings of another quantum circuit. You may assume the encodings are of some reasonable form (e.g., a list of gates and the qubits they act on).

In summary, a language is in BQQP if there exists a poly-time uniform family of quantum circuits whose output is an encoding of another quantum circuit that decides the language (i.e., for an input in the language, the probability the encoded circuit accepts the input is at least $2/3$; and for inputs outside the language, the probability the encoded circuit accepts the input is at most $1/3$.)

Prove that $\mathsf{BQQP} = \mathsf{BQP}$.

3. **Getting familiar with the Pauli matrices**

An important class of unitary operations that we will encounter later are the *Pauli matrices*:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

They have many nice properties:

- Hermitian: $X = X^\dagger$, $Y = Y^\dagger$, $Z = Z^\dagger$
- Square to the identity: $X^2 = Y^2 = Z^2 = I$
- Traceless: $\mathrm{tr}(X) = \mathrm{tr}(Y) = \mathrm{tr}(Z) = 0$
- Same determinant: $\det(X) = \det(Y) = \det(Z) = -1$
- Cyclic structure:

$$\begin{array}{lll} XY = iZ & YZ = iX & ZX = iY \\ YZ = -iX & ZY = -iX & XZ = -iY \end{array}$$

In fact, these properties imply that they form as basis for all complex matrices. In this problem, you will prove this and show that it implies a particularly nice form for single-qubit density matrices.

(a) Show that every 2×2 complex matrix $A \in \mathbb{C}^{2\times 2}$ is a linear combination of the identity matrix and Pauli matrices. That is,

$$A = \alpha_I I + \alpha_X X + \alpha_Y Y + \alpha_Z Z$$

for complex numbers $\alpha_I, \alpha_X, \alpha_Y, \alpha_Z \in \mathbb{C}$.

(b) Show that any single-qubit density matrix ρ can be written as

$$\rho = \frac{I + r_X X + r_Y Y + r_Z Z}{2}$$

where $r := (r_X, r_Y, r_Z)$ is a real vector with ℓ_2-norm bounded by 1. This is called the *Bloch* representation of ρ.