Lecture & Proseminar 250078/250042
"Quantum Information, Quantum Computation, and Quantum Algorithms" WS 2023/24

— Exercise Sheet #11 —

Problem 28: Clifford circuits.

Clifford circuits are circuits which are composed only of $S = \left(\begin{smallmatrix}1 & 0\\ 0 & i\end{smallmatrix}\right)$, H, and CNOT (Clifford gates). In this problem, we will show that a quantum computer which starts from the $|0\cdots0\rangle$ state and then only applies Clifford gates and measurements in the computational basis (in any order) can be simulated efficiently classically.
The core idea is that at each point of the computation (i.e., after each operation), the state of the system is a stabilizer state. It can thus be efficiently described through its stabilizers $S_1, \dots, S_n$, which can be updated efficiently in any step of the computation.

1. Show that the gate set above allows to obtain all Pauli matrices.
2. Show that Clifford circuits C map products of Paulis $P_1 \otimes \cdots \otimes P_n$ ($P_i = I, X, Y, Z$) to products of Paulis, $C(P_1 \otimes \cdots \otimes P_n)C^\dagger = P_1' \otimes \cdots \otimes P_n'$. Explain why this maps an independent (i.e., minimal) set of stabilizers to another independent set of stabilizers.
3. In each step, we want to describe a unique state, i.e., for n qubits we have n independent stabilizers. Show that this implies that for any Pauli product O which commutes with the stabilizers, O or $-O$ is in the stabilizer.
4. Write a (minimal) set of stabilizers for the state $|0\cdots0\rangle$.
5. Consider a quantum computation consisting of a sequence of Clifford gates $C_1, \dots, C_\ell$, starting in the state $|\psi_0\rangle = |0\cdots0\rangle$. Show that in each step of the computation, the state $|\psi_s\rangle = C_s|\psi_{s-1}\rangle$ of the quantum computer can be described by a set of stabilizers, and that the stabilizers for step s can be efficiently computed from those for step $s-1$ (given a C_s is a one- or two-qubit gate).
6. Finally, let us consider Z measurements. W.l.o.g., we will assume that we measure the first qubit.
   a) Show that after the measurement of the first qubit, we are in an eigenstate of $ZI\cdots I$.
   b) Show that if $\pm ZI\cdots I$ is contained in the stabilizer, there exists a minimal basis of stabilizers which contains $\pm ZI\cdots I$, while all other stabilizers are of the form $\pm I * \cdots *$ (where $*$ can be arbitrary Paulis.) Show that this implies that the state is a product state of the first (measured) qubit and the remaining ones, $|i\rangle|\psi'\rangle$, i.e., we can discard the first qubit. What are the new stabilizer for $|\psi'\rangle$?
   c) Consider first the case where $\pm ZI\cdots I$ is contained in the stabilizer *before* the measurement. What is the measurement outcome of a Z measurement on the first qubit? What is the new stabilizer?
   d) Second, consider the case where $\pm ZI\cdots I$ is not contained in the stabilizer.
   - Show that if $\pm ZI\cdots I$ is not contained in the stabilizer, it must anti-commute with at least one stabilizer, since we have n independent stabilizers.
   - Next, show that we can find a minimal basis of stabilizers which only contains a single stabilizer $\hat{S}$ which anti-commutes with $ZI\cdots I$ (i.e., which has a X or Y on the first qubit); in the following, we will work in that basis.
   - Use the existence of this $\hat{S}$ to show that $\langle\psi|ZI\dots I|\psi\rangle = 0$, i.e., the measurement outcome is completely random.
   - Given a the measurement outcome 0 or 1, we are in an eigenstate of $S_{\text{new}} = \pm ZI\cdots I$, respectively, i.e., S_{new} is a stabilizer for the post-measurement state. Furthermore, all other stabilizers except $\hat{S}$ are still stabilizers, since they commute with S_{new}. Explain how this allows us to obtain n independent stabilizers for the post-measurement state.
7. Put these steps together to explain how quantum computation with Clifford gates can be classically simulated.

It is worth noting that all we need to do in the classical simulation is arithmetics modulo 2, which is even much weaker than general polynomial-time classical computation; in fact, it is in a complexity class called $\oplus L$ ("parity L"). Thus, quantum computation with Clifford gates is even weaker than classical computation.