Lecture "Quantum Information" WS 16/17 — Exercise Sheet #5

Problem 1: Grover's algorithm with multiple marked elements.
Consider the Grover search problem of finding x_0 such that $f(x_0) = 1$ for some function $f(x) \in \{0, 1\}$. In the lecture, we derived Grover's algorithm which finds x_0, given that it is unique. Now assume that there are $r > 1$ solutions to the equation $f(x) = 1$. In other words, suppose that we have N states and r of them are marked. The problem is to find one of the marked states with high probability.

Grover's algorithm with mulitple solutions is very similar to the unique solution one. First, the oracle is constructed the same way as before. Find the action of the oracle on a state $|x\rangle$. The remaining steps of the algorithm remain unchanged. Perform a step-by-step analysis of this modified Grover's algorithm, and estimate the number of iterations needed ot obtain one of the marked elements with high probability. How does the runtime of the algorithm scale in r and N? Compare this to the performance of a classical algorithm.

Problem 2: Phase estimation.
Consider a unitary U with an eigenvector $U|\phi\rangle = e^{2\pi i\phi}|\phi\rangle$. Assume that $\phi = 0.\phi_1\phi_2\dots\phi_n = \frac{1}{2}\phi_1 + \frac{1}{4}\phi_2 + \dots$. Our goal will be to study ways to determine ϕ as accurately as possible, given that we can implement U (and are given $|\phi\rangle$).

1. First, consider that we use controlled-U operations $CU|0\rangle|\phi\rangle = |0\rangle|\phi\rangle$, $CU|1\rangle|\phi\rangle = |1\rangle e^{2\pi i\phi}|\phi\rangle$. Describe a protocol where we apply CU to $|+\rangle|\phi\rangle$, followed by a measurement, to infer information about ϕ. Which information, and to which accuracy, can we obtain with N iterations?

2. Now consider a refined scheme. To this end, assume we can also apply controlled-$U^{(2^k)} \equiv CU_k$ operations for integer k efficiently.
   a) We start by applying CU_{n-1} to $|+\rangle|\phi\rangle$. Which information can we infer? What measurement do we have to make?
   b) In the next step, we apply CU_{n-2}, *knowing* the result of step a). What information can we infer? What measurement do we have to make? Rephrase the measurement as a unitary rotation followed by a measurement in the $|\pm\rangle$ basis.
   c) Iterating the preceding steps, describe a procedure (circuit) to obtain $|\phi\rangle$ exactly. How many times do we have to evaluate controlled-$U^{(2^k)}$'s?
   (*Note:* This procedure is known as *quantum phase estimation.*)

3. An alternative way to determine ϕ is to use the quantum Fourier transform. To this end, we apply a transformation $\sum_x |x\rangle|\phi\rangle \mapsto \sum_x |x\rangle U^x|\phi\rangle$, followed by a quantum Fourier transform and a measurement. Describe the resulting protocol, its outcome, and the number of $U^{(2^k)}$'s required.

4. Compare the two protocols derived in step 2 and 3.

5. What outcome will we obtain if we apply the phase estimation algorithm to a *superposition* of different eigenstates $\sum_k w_k|\phi^k\rangle$? (It might help to first consider the case where we measure the register with the $|\phi^k\rangle$'s.)

6. Let us now consider the factoring problem. For a coprime with N (such as it appears in the factoring problem, cf. lecture), the map $U : |x\rangle \mapsto |ax \bmod N\rangle$ is unitary (no proof required). This unitary has periodicity r (with $a^r \bmod N = 1$), i.e., its eigenvalues are r's roots of unity.
   What happens if we apply phase estimation to this U, given we are provided with an eigenvector $|\lambda\rangle$ of U?

7. Consider the form of the eigenvalues of U, and show that their equal weight superposition has a simple form. Discuss how this can be used to determine r without knowing an eigenvector $|\lambda\rangle$ of U. Discuss how this relates to Shor's factoring algorithm.

Problem 3: Syndrome measurement and correction for stabilizer codes.

1. We start by studying the error correction procedure for the 3-qubit bit flip code.

(a) Write down an explicit circuit for measuring the two syndromes Z_1Z_2 and Z_2Z_3 for the 3-qubit bit flip code, using two ancilla qubits. Show that this indeed implements the POVM measurement P_k given in the lecture.

(b) Write the correction circuit for each of the four outcomes of the error measurement. Express this in terms of operations controlled by the classical measurement outcomes of the syndrome measurement.

(c) Combine and modify step (a) and (b) to obtain a scheme which corrects the error without measurement, provided it has access to fresh ancillas.

(d) Discuss how we can implement effective Pauli operations on the *encoded* (logical) qubit $|\hat{0}\rangle$, $|\hat{1}\rangle$ by only acting with Paulis on the *encoding* (physical) qubits.

(e) Given two qubits encoded using the 3-qubit code, show that we can implement a CNOT between the logical qubits by acting with CNOTs only on the physical qubits.

2. Show that the syndrome measurement and the error correction for any stabilizer codes can be carried out using only CNOT, H, measurements in the Z basis, and ancillas (and possibly classical side processing).

3. Give the circuit for the syndrome measurement for the 5-qubit code.

4. Derive the error syndrome for each of the 15 single-qubit errors in the 5-qubit code. Verify that each error has its own syndrome, i.e., the code is non-degenerate.

Problem 4: Clifford circuits.

Clifford circuits are circuits which are built from $S = \left(\begin{smallmatrix} 1 & 0 \\ 0 & i \end{smallmatrix}\right)$, H, and CNOT. In this problem, we will show that a quantum computer which consists only of Clifford gates and Z measurements, and starting from the $|0\cdots 0\rangle$ state, can be simulated efficiently classically. The core idea is that at each state of the computation, the state of the system is a stabilizer state which can be kept described efficiently through its stabilizers (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 independent stabilizers to independent stabilizers.

3. In each step, we want to describe a unique state, i.e., for n qubits we have n independent stabilizers. Show that 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 $|0\cdots 0\rangle$.

5. Consider a quantum computation consisting of a sequence of Clifford gates $C_1, \ldots, C_\ell$, starting in the state $|\psi_0\rangle = |0\cdots 0\rangle$. 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.