Exercise Sheet 8

Quantum Information

To be handed in by June 18th, 2015

Problem 1: Phase estimation. (35 points)

Consider a unitary U with an eigenvector $U|\phi\rangle = e^{2\pi i\phi}|\phi\rangle$. Assume that $\phi = 0.\phi_1\phi_2\ldots\phi_n = \frac{1}{2}\phi_1 + \frac{1}{4}\phi_2 + \ldots$. 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 sections 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 2: Factoring 15. (15 points)

Verify the factoring algorithm (i.e., the reduction to period finding described in the lecture) for $N = 15$ – i.e., consider all $a = 2, \ldots, N-1$, check wether $\gcd(a, N) = 1$, find r s.th. $a^r \bmod N = 1$ (you don't have to use a quantum computer), and check if this can be used to compute a non-trivial factor of N. How many different cases do you find? What possible periods r appear?

Problem 3: The 3-qubit bit flip code. (25 points)

1. 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.
2. 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.
3. Combine and modify step 1 and 2 to obtain a scheme which corrects the error without measurement, provided it has access to fresh ancillas.
4. 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.
5. 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.

Problem 4: Fast Fourier transform. (25 points)

In this problem, we will use the expression

$$|x_1, \ldots, x_n\rangle \mapsto \tfrac{1}{2^{n/2}}(|0\rangle + 2^{2\pi i 0.x_n}|1\rangle)(|0\rangle + 2^{2\pi i 0.x_{n-1}x_n}|1\rangle)(|0\rangle + 2^{2\pi i 0.x_1x_2\ldots x_n}|1\rangle) \qquad (1)$$

for the quantum Fourier transform $\mathcal{F}$ to derive a classical Fourier transformation (the fast Fourier transformation, FFT) on vectors of length 2^n which scales as $O(n2^n)$.

1. Show first that directly carrying out the sum in the classical Fourier transform requires $O(2^{2n})$ steps.
2. As shown in the lecture, $\mathcal{F}$ maps $\sum_x a_x |x\rangle$ to $\sum_y b_y |y\rangle$, where b_y is the classical Fourier transform of a_x. Use this, combined with Eq. (1), to derive an explicit expression of b_y in terms of the a_x (in the spirit of Eq. (1), of course).
3. Your expression should contain a sum over $x_1, \ldots, x_n$. Show that this sum can be carried out bit by bit. In each step, it takes e.g. an input vector $a_x \equiv f(x_1, \ldots, x_n)$ and replaces it by $g(x_1, \ldots, x_{n-1}, y_1)$, and so further, sequentially replacing x_i's by y_j's.
4. What is the number of elementary operations required for each of these transformations? What is the total computational cost of the algorithm?