Lecture & Proseminar 250120/250122
"Quantum Information, Quantum Computation, and Quantum Algorithms" WS 2020/21

— Exercise Sheet #10 —

Problem 1: Phase estimation

Consider a unitary U with an eigenvector $U|\phi\rangle = e^{2\pi i\phi}|\phi\rangle$. Assume that

$$\phi = 0.\phi_1\phi_2\ldots\phi_n = \tfrac{1}{2}\phi_1 + \tfrac{1}{4}\phi_2 + \ldots + \tfrac{1}{2^n}\phi_n \ ,$$

i.e. ϕ can be exactly specified with n binary digits. Our goal will be to study ways to determine ϕ as accurately as possible, given that we can implement U (and are given the state $|\phi\rangle$).

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 in the $|\pm\rangle$ basis, to infer information about ϕ. Which information, and to which accuracy, can we obtain with N iterations? (*Bonus question:* Could this scheme be refined by changing the measurement?)

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.*)

Problem 2: Factoring 15

Verify the factoring algorithm (i.e., the reduction to period finding described in the lecture – subection 3.c) 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: Controlled gates and measurements.

An n-qubit Toffoli gate is a Toffoli gate with $n-1$ controls; i.e., it flips the n'th bit if and only if the other $n-1$ bits are all one.

1. Show that the n-qubit Toffoli gate can be implemented using two $n-1$-qubit Toffoli gates and two regular 3-qubit Toffoli gates using one ancillary qubit.

2. Decomposing every gate into 3-qubit Toffoli gates, how many 3-qubit Toffoli gates do you need to construct the n-qubit Toffoli gate?

3. Find a construction which is more efficient in terms of the scaling of the number 3-qubit Toffoli gates used, at the cost of using more ancillas. (A linear number of 3-fold Toffoli gates should suffice.)

(*Hint:* Remember that the Toffoli gate can be used to build a logical AND gate using ancillas.)