Lehr- und Forschungsgebiet
Mathematische Grundlagen der Informatik
RWTH Aachen
Prof. Dr. E. Grädel, F. Abu-Zaid, S. Schalthöfer

SS 2015

Quantum Computing — Assignment 8

Due: Wednesday, 01.07., 14:15

Exercise 1 15 Points

(a) Give a decomposition of the controlled-R_j gate presented in the lecture into single qubit and CNOT gates.

(b) Consider a black box U_f that computes a function $f : \{0,1\}^n \to \{0,1\}^n$ as usual: $U_f : |x\rangle|y \oplus f(x)\rangle$. Construct a quantum circuit which implements the following operation $\{0,1\}^n \to \{0,1\}^n$ using the black box, some other gates and, if needed, some extra qubits.

$$|x\rangle \mapsto e^{\frac{2\pi i \overline{f(x)}}{2^n}}|x\rangle$$

where for $x \in \{0,1\}^n$ we define $\overline{x} = \sum_{i=0}^{n-1} x_i \cdot 2^i$.
Hint: Use the gates R_j.

(c) Implement the following transformation $\{0,1\}^n \to \{0,1\}^n$ using only the transformation from (b) and the quantum Fourier transformation QFT over $\mathbb{Z}_{2^n}$.

$$|x\rangle \mapsto |\operatorname{bin}((\overline{x}+1) \bmod 2^n)\rangle$$

where for a natural number k, $\operatorname{bin}(k)$ denotes the binary representation of k.
Hint: Use the transformation from (b) where f is the identity.

Exercise 2 15 Points

(a) Describe a classical algorithm which decides in polynomial time for a given natural number n whether there exist a, k such that $n = a^k$.

(b) Show that an efficient classical factoring algorithm would also yield a classical algorithm to efficiently find the order modulo n of any x co-prime to n.
Hint: Show that the order of g in $\mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k}$ is the least common multiple of the orders of g in $\mathbb{Z}_{n_1}, \ldots, \mathbb{Z}_{n_k}$.

(c) The RSA crypto system uses a public key (e, n) and a private key d such that $d \equiv e^{-1} (\operatorname{mod} \varphi(n))$, where $n = p \cdot q$ for distinct primes p, q, φ denotes the Euler function, and $\gcd(e, \varphi(n)) = 1$.

For any message (integer) m with $\gcd(m, n) = 1$, the ciphertext is defined as $c = m^e \mod n$, and the ciphertext is decrypted with the private key using the identity $m = c^d \mod n$.

Show that, assuming there is an efficient polynomial-time algorithm that, given integers a and k, determines the order of a in $\mathbb{Z}_k^*$, there is a classical polynomial-time algorithm that can decrypt any RSA-encrypted ciphertext without factorizing n.