Lehr- und Forschungsgebiet
Mathematische Grundlagen der Informatik
RWTH Aachen
Prof. Dr. E. Grädel, D. Fischer, T. Ganzow,
B. Puchala

WS 09/10

Complexity Theory and Quantum Computing — Assignment 12

Due: Monday, February 01, 12:00

Exercise 1

Let $G = \{g_1, \ldots, g_n\}$ be an abelian group and let $i \in \{1, \ldots, n\}$. Find the Fourier transform of $f : G \to \mathbb{C}$ defined by

$$f(g) = \begin{cases} 1, & \text{if } g = g_i \\ 0, & \text{otherwise.} \end{cases}$$

Exercise 2

Let $n = n_1 n_2$, where $\gcd(n_1, n_2) = 1$. Let also $f : \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \to \mathbb{Z}_n$ be the function given by $f(k_1, k_2) = a_1 n_2 k_1 + a_2 n_1 k_2$, where a_1 (respectively a_2) given by the Chinese Remainder Theorem, is the multiplicative inverse of n_2 (respectively n_1) modulo n_1 (respectively n_2). Show that f is an isomorphism.

Exercise 3

(a) We define the operator $S : \mathbb{C}^{\mathbb{Z}_{2^n}} \to \mathbb{C}^{\mathbb{Z}_{2^n}}$ as follows. For $f : \mathbb{Z}_{2^n} \to \mathbb{C}$, the function $S(f) : \mathbb{Z}_{2^n} \to \mathbb{C}$ is given by $S(f)(x) = f((x+1) \mod 2^n)$. Compute the Fourier coefficients of $S(f)$ in terms of the Fourier coefficients of f.

(b*) Consider a black-box U_f that computes a function $f : \{0,1\}^n \to \{0,1\}^n$ as usual: $U_f : |x\rangle|y\rangle \mapsto |x\rangle|y \oplus f(x)\rangle$. Construct a quantum circuit, which implements the following operation $\{0,1\}^n \to \{0,1\}^n$, using two applications of 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 as presented in the lecture.

(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 $\mathbb{Z}_{2^n}$.

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

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