EXERCISES 11

Excercise 1. Find a decomposition of the controlled R_k gates, used in the circuit for the quantum Fourier transform, in terms of single qubit and CNOT gates.

Excercise 2. Find a quantum circuit for the inverse quantum Fourier transform, i.e., a quantum circuit implementing the inverse F_N^{-1} of the DFT matrix for $N = 2^n$.

Excercise 3. Consider the quantum circuit implementing the quantum Fourier transform (QFT) discussed in the lecture, and denote by $CR_k : (\mathbb{C}^2)^{\otimes 2} \to (\mathbb{C}^2)^{\otimes 2}$ the controlled R_k gates used in this circuit. In the following, we denote by $\|\cdot\|$ the operator norm (see lecture notes).

(1) Show that there is $k_{th} \in \mathbb{N}$ such that $\|CR_k - \mathbb{1}_4\| \leqslant 1/n^3$ for any $k \geqslant k_{th}$. Give an estimate for k_{th}.
(2) Let $V_n : (\mathbb{C}^2)^{\otimes n} \to (\mathbb{C}^2)^{\otimes n}$ denote the unitary obtained from the QFT circuit by replacing all CR_k with $k \geqslant k_{th}$ by identities. Show that $\|V_n - F_{2^n}\|$ scales as $\Theta(1/n)$. What is the complexity of V_n?

Excercise 4. For non-zero $d \in \mathbb{N}$ we say that integers n and m are *congruent modulo* d, written $n \equiv m \mod d$, if d divides $n - m$.

(1) Let $d \in \mathbb{N}$ be non-zero. Show that for every integer n there is a unique integer $q \in \mathbb{Z}$ and a unique $r \in \mathbb{N}$ such that $n = qd + r$ and $0 \leqslant r < d$.
(2) We say that integers n and m are co-prime if their greatest common divisor is 1. Show that for every pair of co-prime integers n and m there are integers $x, y \in \mathbb{Z}$ such that $nx + my = 1$. Conlclude that for any non-zero $d \in \mathbb{N}$ and any n co-prime to d there is a multiplicative inverse modulo d, i.e., a number $x \in \mathbb{Z}$ such that $nx \equiv 1 \mod d$.