Introduction to Quantum Computing — Serge Fehr (lecturer)
Fall 2023, Mathematical Institute, Leiden University — Yu-Hsuan Huang (TA)

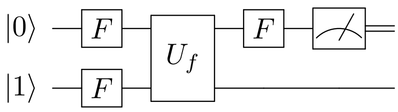
Exercise Set 5

Exercise 5.1 For integer $N \geq 2$, let $f : \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$ be an arbitrary function. For a fixed orthonormal basis $\{|0\rangle, \ldots, |N-1\rangle\}$ of $\mathcal{H}_N = \mathbb{C}^N$, consider the unitary $U_f \in \mathcal{U}(\mathcal{H}_N \otimes \mathcal{H}_N)$ given by $U_f|x\rangle|y\rangle = |x\rangle|y+f(x)\rangle$ for $x, y \in \mathbb{Z}/N\mathbb{Z}$, where "+" is the addition mod N. As usual, we have $\omega_N := e^{2\pi i/N}$. Show that for any $x \in \mathbb{Z}/N\mathbb{Z}$, the vector

$$|x\rangle \otimes \sum_y \omega_N^y |y\rangle ,$$

with the sum over all $y \in \mathbb{Z}/N\mathbb{Z}$, is an eigenvector of U_f. What is the corresponding eigenvalue?

Exercise 5.2 For any integer $N \geq 2$, consider the generalization of Deutsch's algorithm for a function $f : \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$, given by the circuit



where F is the quantum Fourier transform on $\mathcal{H}_N = \mathbb{C}^N$ (w.r.t. basis $\{|0\rangle, \ldots, |N-1\rangle\}$) as given in Def. 4.2, U_f is given as above, and the measurement is in the basis $\{|0\rangle, \ldots, |N-1\rangle\}$. Note that the wires here represent states in $\mathcal{H}_N$ (and thus not qubits, unless $N = 2$).

Show that if f is either *constant* or *surjective*, then from the output of the algorithm one can determine with certainty which one it is.

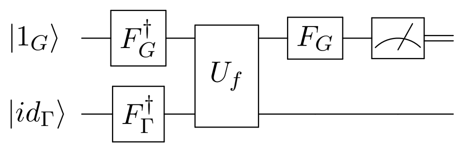
Exercise 5.3 Let G be an arbitrary finite Abelian group, and let $\hat{G}$ be the dual group. Take it for given (or convince yourself) that $\Gamma := \{\chi(g) \,|\, g \in G, \chi \in \hat{G}\}$ is a finite subgroup of the multiplicative group $\mathcal{S}(\mathbb{C})$. Note that we may then consider the dual group $\hat{\Gamma}$ of Γ.

Consider fixed orthonormal bases $\{|g\rangle\}_{g\in G}$ and $\{|\chi\rangle\}_{\chi\in\hat{G}}$ of the Hilbert space $\mathcal{H} := \mathbb{C}^{|G|}$, and let F_G be the corresponding generalized quantum Fourier transform, i.e.,

$$F_G = \frac{1}{\sqrt{|G|}} \sum_{g,\chi} \chi(g)|\chi\rangle\langle g|$$

where the sum is over $g \in G$ and $\chi \in \hat{G}$. Similarly, we let $\{|\gamma\rangle\}_{\gamma\in\Gamma}$ and $\{|\xi\rangle\}_{\xi\in\hat{\Gamma}}$ be orthonormal bases of $\mathcal{H}' := \mathbb{C}^{|\Gamma|}$ and F_Γ the corresponding generalized quantum Fourier transform.

Let $f : G \to \Gamma$ be a character, i.e., an element of $\hat{G}$, and let $U_f \in \mathcal{U}(\mathcal{H} \otimes \mathcal{H}')$ be given by $U_f|g\rangle|\gamma\rangle = |g\rangle|\gamma \cdot f(g)\rangle$ for $g \in G$ and $\gamma \in \Gamma$. Then, show that the following generalization of the Bernstein-Vazirani algorithm recovers the inverse character $f^{-1} = \bar{f}$, and thus f:

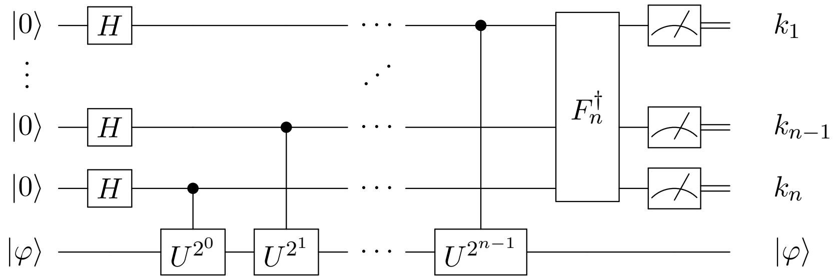


where $1_G \in \hat{G}$ is the trivial character $1_G : g \mapsto 1$, $id_\Gamma \in \hat{\Gamma}$ is the identity map $id_\Gamma : z \mapsto z$ on Γ, and the measurement is in the basis $\{|\chi\rangle\}_{\chi\in\hat{G}}$.

Note: The original Bernstein-Vazirani algorithm considers a function $f : x \mapsto s \cdot x$, which we can identify with the character $\chi_s : x \mapsto \omega_N^{s \cdot x}$ in $\widehat{\mathbb{Z}/N\mathbb{Z}}$. The above is then indeed a generalization.

(Turn page)

Exercise 5.4 ☺ Let U be a unitary operator, acting on an arbitrary Hilbert space, and let $|\varphi\rangle$ be an eigenvector of U with eigenvalue $e^{2\pi i\mu}$ for $\mu \in [0, 1)$. For the purpose of this exercise, we assume that μ has a binary representation of length (at most) n for some positive $n \in \mathbb{Z}$, meaning that $2^n\mu \in \mathbb{Z}$ so that we can write $\mu = [0.m_1 \cdots m_n]$ using the notation from Section 4.5. Consider now the following quantum circuit, which makes use of Hadamards, of control unitaries $C\big(U^{2^j}\big)$ for $j \in \{0, \ldots, 2^{n-1}\}$ and of the (inverse of the) quantum Fourier transform F_n on $\mathcal{H}^{\otimes n}$ as considered in Sect. 4.5, applied to n qubits in state $|0\rangle$ and to $|\varphi\rangle$.



What is the resulting output $(k_1, \ldots, k_n) \in \{0, 1\}^n$, obtained by measuring the n qubits in the computational basis?