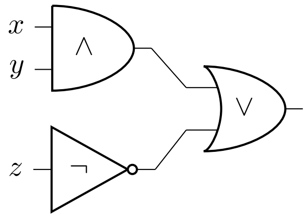
INTRODUCTION TO QUANTUM COMPUTING
Fall 2023, Mathematical Institute, Leiden University

Serge Fehr (lecturer)
Yu-Hsuan Huang (TA)

Exercise Set 4

Exercise 4.1 Consider the following classical binary circuit, using the logic *and*, *or* and *not* gates ($\wedge$, $\vee$ and $\neg$), which computes the function $f : \{0,1\}^3 \to \{0,1\}$, $(x,y,z) \mapsto (x \wedge y) \vee \neg z$.



Find a quantum circuit, with gate set consisting of the Toffoli gate and the Pauli X gate (only), that computes the unitary representation $U_f \in \mathcal{U}(\mathcal{H}^{\otimes 4})$ of the function f, i.e., the unitary that maps $|x\rangle|y\rangle|z\rangle|w\rangle$ to $|x\rangle|y\rangle|z\rangle|w \oplus f(x,y,z)\rangle$. Note that the quantum circuit may invoke addition "work qubits" that start off and must end up again in state $|0\rangle$.
Warning: This is *not* a direct application of Theorem 3.5, since the considered quantum gates (Toffoli and Pauli X) are not the ones obtained by applying Theorem 3.5.

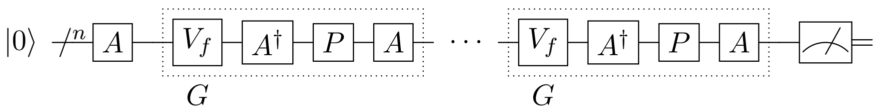
Exercise 4.2 Show that, up to an obvious adjustment in the classical post-processing, Simon's algorithm also works for the following generalization of the considered problem. Given a function $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ with the promise that $f(x) = f(x')$ if and only if $x' \oplus x \in V$, where V is a subspace of the $\mathbb{F}_2$-vector-space $\mathbb{F}^n$, find a basis of V.

Exercise 4.3 Show that in the context of Grover's algorithm for $f : \{0,1\}^n \to \{0,1\}$, if the number of x's with $f(x) = 1$ is $M = 2^n/4$ then Grover's algorithm finds a solution *with certainty* after just *one* Grover iteration (and thus just one query).

Exercise 4.4 Still in the context of the search problem addressed by Grover's algorithm, let us now assume that, next to (access to) $V_f \in \mathcal{U}(\mathcal{H}^{\otimes n})$, we we are given a unitary $A \in \mathcal{U}(\mathcal{H}^{\otimes n})$ with the property that $A|0\rangle = \sum_x \alpha_x |x\rangle$ with

$$\sum_{\substack{x \text{ s.t.} \\ f(x)=1}} |\alpha_x|^2 = p$$

for some known $p \geq M/2^n$. In other words, if $A|0\rangle$ is measured then an $x \in \{0,1\}^n$ is observed that satisfies $f(x) = 1$ with probability p. Note that $A = H^{\otimes n}$ achieves this with $p = M/2^n$. Consider now a variant of Grover's algorithm, where $H^{\otimes n}$ is replaced by A and $A^\dagger$ as follows (while P still is $P = 2|0\rangle\langle 0| - \mathbb{I}$):



Analyze in what way this improves upon the original Grover's algorithm.