Introduction to Quantum Computing
Fall 2023, Mathematical Institute, Leiden University

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

Exercise Set 3

Exercise 3.1 Work out $CNOT(H|x\rangle \otimes H|y\rangle)$ for $x, y \in \{0,1\}$, and write the result again in terms of the Hadamard basis $\{H|0\rangle, H|1\rangle\}$.

Exercise 3.2 Show that $V := (1-i)(\mathbb{I} + iX)/2$ is in $\mathcal{U}(\mathbb{C}^2)$ and such that $V^2 = X$.

Exercise 3.3 Prove Proposition 2.6, i.e., show that the "circuit equality" in Figure 2.4 holds (where the computation is performed from left to right).

Exercise 3.4 Prove that the following statement (Lemma 3.3 from the notes) holds for $n \in \mathbb{N}$. For any $x = (x_1, \ldots, x_n) \in \{0,1\}^n$:

$$H^{\otimes n}|x\rangle = \frac{1}{2^{n/2}} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle$$

where $x \cdot y = x_1 y_1 \oplus \ldots \oplus x_n y_n \in \{0,1\}$ and $|x\rangle = |x_1\rangle \cdots |x_n\rangle$ and $|y\rangle = |y_1\rangle \cdots |y_n\rangle$.
Hint: First do the case $n = 1$, and then the general case.

Exercise 3.5 Let $f : \mathcal{X} \to \{0,1\}$ be a binary-valued function, and consider its unitary representation $U_f \in \mathcal{U}(\mathcal{H}_X \otimes \mathbb{C}^2)$, given by $U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$ for $x \in \mathcal{X}$ and $y \in \{0,1\}$. Show that

$$U_f(|x\rangle \otimes H|z\rangle) = (-1)^{zf(x)}|x\rangle \otimes H|z\rangle$$

for all $x \in \mathcal{X}$ and $z \in \{0,1\}$. Vice versa, let now $V_f \in \mathcal{U}(\mathcal{H}_X \otimes \mathbb{C}^2)$ be the unitary given by $V_f|x\rangle|z\rangle = (-1)^{zf(x)}|x\rangle|z\rangle$, and work out $V_f(|x\rangle \otimes H|y\rangle)$.

Exercise 3.6 If two parties, Alice and Bob, are not entangled then by sending *one qubit* Alice can communicate at most *one bit* of information to Bob (this is known as Holevo's bound). However, they can do better if they share an entangled state; this is called *superdense coding.* Indeed, assume that Alice holds the first qubit and Bob the second qubit of an EPR pair $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$, and that Alice wants to communicate the two bits $x, z \in \{0,1\}$. Show that by applying $X^x Z^z$ to her qubit of the EPR, and then sending this qubit to Bob, Bob can recover x and z by means of a suitable measurement.