EXERCISES 6

Excercise 1. Consider the classical NAND-gate, which transforms two bits $x, y \in \{0,1\}$ as follows

$$\mathrm{NAND}(x,y) = \mathrm{NOT}(\mathrm{AND}(x,y)) = \begin{cases} 0, & \text{if } x = y = 1 \\ 1, & \text{otherwise.} \end{cases}$$

Show that the gate set $\{\mathrm{NAND}, \mathrm{FANOUT}\}$ is universal (provided that ancillas are available).

Excercise 2. Consider the rotation unitaries

$$R_x(\theta) = \exp(-i\theta X/2),$$
$$R_y(\theta) = \exp(-i\theta Y/2),$$
$$R_z(\theta) = \exp(-i\theta Z/2).$$

(1) Express the Hadamard gate as a product of $R_x(\theta_1)$ and $R_z(\theta_2)$ and a phase $e^{i\phi}$ for some $\theta_1, \theta_2, \phi \in [0, 2\pi)$.
(2) Show that $XR_y(\theta)X = R_y(-\theta)$.
(3) Visualize the rotation operators $R_x(\theta), R_y(\theta)$ and $R_z(\theta)$ acting on the Bloch sphere (from an earlier exercise). Justify the name "rotation operators".

Excercise 3. Consider the swap gate $SWAP : \mathbb{C}^2 \otimes \mathbb{C}^2 \to \mathbb{C}^2 \otimes \mathbb{C}^2$ given by $SWAP(|a\rangle \otimes |b\rangle) = |b\rangle \otimes |a\rangle$ for $a, b \in \{0,1\}$ extended linearily. Implement the swap gate using only CNOT gates (you are allowed to use either of the two qubits as control, but write an explicit circuit).

Excercise 4. Show that we need at least $O(2^n)$ many gates are needed to implement all Boolean functions $f : \{0,1\}^n \to \{0,1\}$ by a circuit. The common way of stating this result is: There exist Boolean functions that are hard to compute! Follow the steps:

(1) Let A and B denote two finite sets. Show that there are $|B|^{|A|}$ many functions $f : A \to B$. Conclude that there are 2^{2^n} different Boolean functions $f : \{0,1\}^n \to \{0,1\}$.
(2) Consider boxes connected by wires (not necessarily forming circuits). Assume that we have k boxes each with 3 inputs and 3 outputs. Show that there are at most $(3k)^{3k}$ many wirings of the boxes where outputs of one box are connected to inputs of another (not necessarily different) box. **Hint:** Use the first sub-exercise.
(3) Consider now the case of circuits with n input bits computing some Boolean function $f : \{0,1\}^n \to \{0,1\}$. Assume that the circuit uses k Toffoli gates and some number of ancilla bits initially set to 0. Argue first that we may restrict the number of ancilla bits to $3k$ without changing the performance of any such circuit.
(4) To upper bound the number of circuits defined in the previous sub-exercise, we think of input and ancilla bits as grouped together in triples and each of these triples we think of as a box with 3 output wires and 3 (fictional) input wires. For simplicity, we may increase the number of ancilla bits to $3k+2n$ so that there are $(3n+3k)/3 = n+k$ such additional boxes. Show that there are at most $(3(n+2k))^{3(n+2k)}$ circuits of the described form. Conclude that

k has to grow exponentially fast in n if all functions $f : \{0,1\}^n \to \{0,1\}$ should be implementable by such circuits using k Toffoli gates.

(5) Argue that the conclusion from the previous subexercise does not change if we replace the Tofolli gate with any other universal set of gates with bounded number of input and output bits.