Quantum Computing
Problem Set 5

Prof. Dr. Michael J. Hartmann

WiSe 2019-2020

Problem 1: Gate identities

Show that

$$
\begin{aligned}
Y =& iXZ && (1)\\
Z =& S^2 \quad \text{where} \quad S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} && (2)\\
X =& HZH && (3)
\end{aligned}
$$

Problem 2: Clifford Circuits

The Clifford group $\mathcal{C}$ is the set of quantum circuits generated using the gate set $\{X, Y, Z, H, S, CNOT\}$. Even though one can do many things with this set, it is not universal. In this problem you should show that all circuits in the Clifford group can be efficiently simulated classically. More precisely you should show that all circuits $C \in \mathcal{C}$, which are composed of a polynomial number of gates from the set $\{X, Y, Z, H, S, CNOT\}$ can be evaluated in a polynomial number of classical operations provided the initial state is a product state. Here polynomial means that the number is upper bounded by n^x, where n is the number of qubits and x a positive number.
In the following, we will denote by $\mathcal{C}$ the Clifford group and by $\mathcal{P}$ the Pauli group, which are all circuits generated using the gate set $\{X, Y, Z\}$. Pauli circuits $\mathcal{P}$ are very simple as they consist of single qubit gates only.

a) How many classical operations are needed to evaluate a Pauli circuit $P \in \mathcal{P}$.

The proof that the Clifford group can be efficiently simulated classically proceeds by showing that

$$\text{if} \quad C \in \mathcal{C} \quad \text{and} \quad P \in \mathcal{P}, \quad \text{then} \quad C^\dagger P C \in \mathcal{P}. \tag{4}$$

Before proving this statement we will consider it's implications.

b) Let $C \in \mathcal{C}$ and suppose the input state is $|0^{\otimes n}\rangle$ and that after running the circuit we measure the first qubit in the computational basis. The result will be 0 with probability

$$\Pr(0) = \langle 0^{\otimes n}| C^\dagger \left[|0_1\rangle \langle 0_1| \otimes \mathbb{1}_{2,\ldots,n}\right] |0^{\otimes n}\rangle \tag{5}$$

Show that this probability $\Pr(0)$ can be evaluated on a classical computer in a time polynomial in the number of gates of C. Hints: Use the identity $|0\rangle\langle 0| = (\mathbb{1} + Z)/2$ and equation (4).

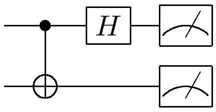
Next we are going to prove equation (4).

c) Show that to prove equation (4) it is sufficient to consider the cases $P \in \{X, Z\}$ and $C \in \{H, S, CNOT\}$. Hint: Use the algebraic relations from Problem 1.

d) Now prove that $C^\dagger P C \in \mathcal{P}$ by considering all combinations of $P \in \{X, Z\}$ and $C \in \{H, S, CNOT\}$.

Problem 3: Bell measurement

Show that the circuit

 (6)

Can be used to perform Bell measurements as discussed in problem set 4.