Freie Universität Berlin
**Tutorials on Quantum Information Theory**
Winter term 2020/21

**Problem Sheet 9**
**Quantum Fourier transform and stabilizers**

J. Eisert, J. Haferkamp, J. C. Magdalena De La Fuente

1. **Quantum Fourier transform.** Perhaps at the heart of the majority of modern quantum algorithms lies the *phase estimation algorithm*. For this reason, it is crucial in the field of quantum computation to be familiar with phase estimation. It relies on an efficient implementation of the *quantum Fourier transform*, to which we devote this excercise.

In classical numerics the discrete Fourier transform (DFT) is defined as the linear map $F : \mathbb{C}^N \to \mathbb{C}^N$, $x \mapsto y$ with $y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j \exp\left\{\frac{2\pi \mathrm{i} jk}{N}\right\}$. The quantum Fourier transform is analogously defined as the unitary operation $\mathcal{F} : \mathbb{C}^{2^n} \to \mathbb{C}^{2^n}$, $|j\rangle \mapsto \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \exp\left\{\frac{2\pi \mathrm{i} jk}{2^n}\right\} |k\rangle$.

a) Look-up the computational complexity of the fastest classical algorithm for the Fourier transform.

The quantum Fourier transform can be implemented using the Hadamard gates $H$,

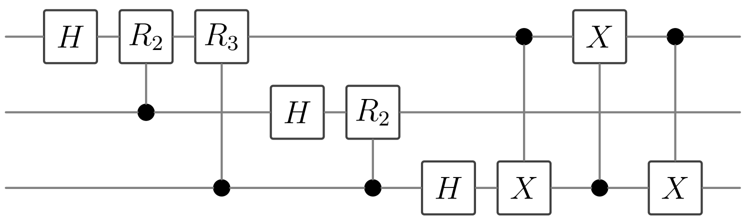
$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{1}$$

the controlled phase gate that applies

$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{e}^{2\pi \mathrm{i}/2^k} \end{pmatrix} \tag{2}$$

on a qubit if another qubit is $|1\rangle$ and CNOT gates that implement swap operations.

b) Show that the following circuit implements the three qubit quantum Fourier transform




c) How does this generalise to the $n$ qubit quantum Fourier transform?

d) What is the circuit complexity of the quantum Fourier transform and how does it compare to the classical DFT algorithms?

Note that the quantum Fourier transform can in fact be approximately implemented with only $\mathcal{O}(n \log n)$ gates.

2. **Stabilizer quantum computation.**

One of the most celebrated results in quantum computation is a statement about the resource costs of simulating quantum computations on a classical computers. The *Gottesman-Knill theorem* states that quantum computations composed of *Clifford gates* with *stabilizer states* as inputs can be classically simulated in the sense that there exists a classical algorithm with polynomial runtime which can sample from the output distribution of such a computation. Furthermore, the so-called stabilizer formalism plays an important rôle in the development of quantum error correction.

In this problem we will trace the train of thought underlying this result. Throughout, we will let $n$ be the number of qubits and hence $\mathcal{H} = (\mathbb{C}^2)^{\otimes n}$ be the Hilbert space. Let us start with some definitions

(i) Let $G_1 = \{\pm\mathbb{1}, \pm X, \pm Y, \pm Z, \pm\mathbb{1}, \pm iX, \pm iY, \pm iZ\}$ be the single-qubit *Pauli group* where multiplication is the group operation.[1].

(ii) Let $G_n := \{\bigotimes_{i=1}^n P_i, P_i \in G_1\}$ be the $n$-qubit Pauli group.

(iii) A *stabilizer state* is a quantum state $|\psi\rangle \in \mathcal{H}$ that is uniquely (up to a global phase) described by a set $\mathcal{S}_{|\psi\rangle} = \{S_1, \dots, S_m\} \subset G_n$ satisfying $S_i |\psi\rangle = +1 |\psi\rangle$. We call the generalised pauli-operators $S_i$ the stabilizers of $|\psi\rangle$.[2]

(iv) A Clifford operator $C$ is a unitary on $\mathcal{H}$ which leaves $G_n$ invariant, i.e. for all $g \in G_n$ it holds that $CgC^\dagger \in G_n$. In group theoretic slang the Clifford group $\mathcal{C} \subset U(2^n)$ is the normalizer of $G_n$.

Ok, now we are ready to begin.

a) Show that the set $\mathcal{S} = \{Z_1, Z_2, \dots, Z_n\}$ uniquely stabilizes the state $|0\rangle^{\otimes n}$, where we use the notation $Z_i = \mathbb{1} \otimes \cdots \otimes \mathbb{1} \otimes \underbrace{Z}_{i\text{-th qubit}} \otimes \mathbb{1} \otimes \cdots \otimes \mathbb{1}$ for the operator acting as $Z$ on the $i$-th qubit and as the identity on all other qubits.

b) Show that $n$ stabilizers suffice to uniquely characterize an arbitrary state in the *Clifford orbit* of $|0\rangle^{\otimes n}$, that is the states $|\psi\rangle$ for which there exists a (unique) Clifford operator $C$ such that $|\psi\rangle = C |0\rangle^{\otimes n}$.

c) Give a stabilizer representation of $|+\rangle \otimes |0\rangle \otimes |-\rangle$.

Any Clifford operator can be expressed as a product of single- and two-qubit Clifford operators, and indeed as a product from the generating set $\{CNOT, H, S\}$, where

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \quad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{3}$$

d) Show that this gate set is sufficient to generate all Pauli matrices starting from any single-qubit Pauli matrix.

e) Show that one can efficiently (in the number of qubits and gates) determine the stabilizer set of a state generated by a Clifford circuit (comprising $CNOT, H, S$ gates) applied to a stabilizer state

Now, let us assume that we measure the first qubit in the $Z$ basis.

f) Assume $Z_1$ commutes with all stabilizers. What is the probability of obtaining outcome $+1$?

One can show that in case $Z_1$ does not commute with all stabilizers, one can find an alternative set of stabilizers such that it anti-commutes with one of them but commutes with all remaining ones.

g) Use the existence of such a stabilizer to show that the measurement outcome is uniformly random. What is the post-measurement state?

In fact, this generalizes to the measurement of an arbitrary Pauli operator $g \in G_n$.

[1] Convince yourself that $G_1$ is closed under multiplication and the unsigned Pauli matrices are not.

[2] More generally, we can talk about subspaces stabilized by a set $\mathcal{S} \subset G_n$. This is a key insight in the theory of error correction codes.