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.

   Solution: The fast-fourier transform requires $\mathcal{O}(N \log N)$ operations.

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

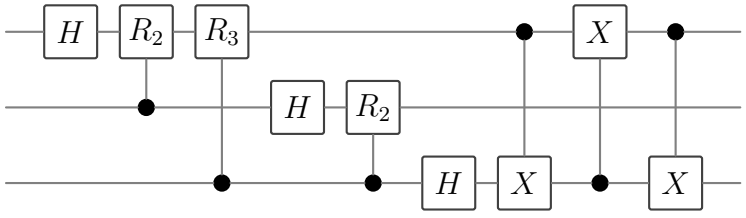
   $$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{1}$$

   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

   Solution: We will restrict our attention to inputs in the computational basis.

   We first look at the the three CNOT-gates at the end of the circuit. Evaluating the circuit on the computational basis shows that this group just implement a swap of the first and third qubit.

   Now, let us have a look at the remaning gates. Let $x, y \in \{0, 1\}$, we can cast the action of the Hadamard gate as $H|x\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + \mathrm{e}^{2\pi \mathrm{i} \frac{x}{2}} |1\rangle\right)$. The action of the phase gate on $|+\rangle$ controlled by the qubit $|y\rangle$ can analogously be written as

$R_k |+\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + \mathrm{e}^{2\pi \mathrm{i} \frac{y}{2^k}} |1\rangle \right)$. This allows us to evaluate the output of the circuit including the swap gate acting on the input state $|xyz\rangle$ with $x, y, z \in \{0, 1\}$ as

$$|\psi_{\text{out}}\rangle = \frac{1}{\sqrt{2}^3} \left(|0\rangle + \mathrm{e}^{2\pi \mathrm{i} \left[\frac{z}{2}\right]} |1\rangle \right) \otimes \left(|0\rangle + \mathrm{e}^{2\pi \mathrm{i} \left[\frac{y}{2} + \frac{z}{4}\right]} |1\rangle \right) \otimes \left(|0\rangle + \mathrm{e}^{2\pi \mathrm{i} \left[\frac{x}{2} + \frac{y}{4} + \frac{z}{8}\right]} |1\rangle \right). \tag{3}$$

It remains to to convince ourself that this actual a representation of the quantum Fourier transform. To this end, using the binary representation of $k = 4k_2 + 2k_1 + k_0$

$$\mathcal{F} |xyz\rangle = \frac{1}{\sqrt{2}^3} \sum_{k_2, k_1, k_0 \in \{1,0\}} \mathrm{e}^{2\pi \mathrm{i} \left[\frac{x}{2} + \frac{y}{4} + \frac{z}{8}\right] \cdot (4k_2 + 2k_1 + k_0)} |k_2 k_1 k_0\rangle \tag{4}$$

$$= \frac{1}{\sqrt{2}^3} \left(\sum_{k_2 \in \{0,1\}} \mathrm{e}^{2\pi \mathrm{i} \left[\frac{x}{2} + \frac{y}{4} + \frac{z}{8}\right] 4k_2} |k_2\rangle \right) \tag{5}$$

$$\otimes \left(\sum_{k_1 \in \{0,1\}} \mathrm{e}^{2\pi \mathrm{i} \left[\frac{x}{2} + \frac{y}{4} + \frac{z}{8}\right] 2k_1} |k_1\rangle \right) \tag{6}$$

$$\otimes \left(\sum_{k_0 \in \{0,1\}} \mathrm{e}^{2\pi \mathrm{i} \left[\frac{x}{2} + \frac{y}{4} + \frac{z}{8}\right] k_0} |k_0\rangle \right) \tag{7}$$

$$= \frac{1}{\sqrt{2}^3} \left(\sum_{k_2 \in \{0,1\}} \mathrm{e}^{2\pi \mathrm{i} \left[\frac{z}{2}\right] k_2} |k_2\rangle \right) \tag{8}$$

$$\otimes \left(\sum_{k_1 \in \{0,1\}} \mathrm{e}^{2\pi \mathrm{i} \left[\frac{y}{2} + \frac{z}{4}\right] k_1} |k_1\rangle \right) \tag{9}$$

$$\otimes \left(\sum_{k_0 \in \{0,1\}} \mathrm{e}^{2\pi \mathrm{i} \left[\frac{x}{2} + \frac{y}{4} + \frac{z}{8}\right] k_0} |k_0\rangle \right), \tag{10}$$

which is the expression we have derived for $|\psi_{\text{out}}\rangle$.

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

Solution: For each additional register one adds an corresponding controlled phase gate to all the previous registers and an Hadamard on the new one.

The swap circuit at the end is replaced by a combination of swaps implementing a general reversion of the order of the registers.

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

Solution: Before the reversion, we act with n gates on the first register, $n-1$ gates on the second and so on. This adds up to a total number of $n(n-1)/2$ gates. The reversion can be performed with at most $n/2$ swaps adding $3n/2$ CNOT gates to the circuit. Thus, we end up with a circuit complexity of $\mathcal{O}(n^2)$. This is for gates that are not subject to geometric locality restriction, i.e. they can act on arbitrary pairs of qubits and not just on nearest neighbours.

In constrast, the classical computational complexity of the fast fourier transform is $\mathcal{O}(n2^n)$, i.e. exponentially worse.

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 $G_1 = \{\pm\mathbb{1}, \pm X, \pm Y, \pm Z, \pm\mathbb{1}, \pm\mathrm{i}X, \pm\mathrm{i}Y, \pm\mathrm{i}Z\}$ 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 $\mathcal{S}_{|\psi\rangle} = \{S_1, \ldots, S_m\} \subset G_n$ 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 $\mathcal{S} = \{Z_1, Z_2, \ldots, Z_n\}$ 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.

   Solution: For an arbitrary state $|\psi\rangle$ we have the n conditions $Z_i |\psi\rangle = |\psi\rangle$. Writing $|\psi\rangle = \sum_x \psi_x |x_1, \ldots, x_n\rangle$ the i-th condition reads

   $$Z_i |\psi\rangle = \sum_x \psi_x (-1)^{x_i} |x_1, \ldots, x_n\rangle = |\psi\rangle ,$$

   from which we conclude that

   $$|\psi\rangle = \sum_x \psi_x \delta_{x_i,0} |x\rangle .$$

   Putting all n conditions together we have

   $$|\psi\rangle = \sum_x \psi_x (\prod_{i=1}^n \delta_{x_i,0}) |x\rangle = \psi_{00\ldots0} |0\rangle^{\otimes n} .$$

   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 $|\psi\rangle = C |0\rangle^{\otimes n}$.

[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.

Solution: We have the n relations $Z_i |0\rangle = |0\rangle$. Inserting an identity we obtain $CZ_iC^\dagger C |0\rangle = CZ_iC^\dagger |\psi\rangle$. Defining $S_i = CZ_iC^\dagger$ and using the uniqueness of C the claim follows.

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

Solution: $\{X_1, Z_2, -X_3\}$

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

$$S = \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{i} \end{pmatrix}, \quad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{11}$$

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

Solution: H switches between Z and the $X - Y$ plane. S rotates in the $X - Y$ plane. $CNOT$ couples two qubits.

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

Solution: obvious. The algorithm updates the n stabilizers in every step of the computation and thus has runtime $O(nN)$, where N is the number of gates.

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 $+1$?

Solution: We have that $Z_1 |\psi\rangle = Z_1S_i |\psi\rangle = S_i(Z_1 |\psi\rangle)$ for all i. $Z_1 |\psi\rangle$ is, thus, stabilized by $\{S_1, ..., S_n\}$. This implies $Z_1 |\psi\rangle = \mathrm{e}^{\mathrm{i}\phi} |\psi\rangle$. Since Z_1 has eigenvalues -1 and 1, the probability of measuring 1 is either 0 or 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?

Solution: Let S_1 be the anticommuting stabilizer. We then have

$$\begin{aligned} \Pr[Z_1 = +1] &= \mathrm{Tr}[(\mathbb{1} + Z_1)/2 |\psi\rangle\langle\psi|] = \langle\psi| (\mathbb{1} + Z_1S_1)/2 |\psi\rangle & (12) \\ &= \langle\psi| (\mathbb{1} - S_1Z_1)/2 |\psi\rangle = \langle\psi| (\mathbb{1} - Z_1)/2 |\psi\rangle & (13) \\ &= \Pr[Z_1 = -1] & (14) \end{aligned}$$

Hence $\Pr[Z_1 = -1] = \Pr[Z_1 = +1] = 1/2$. In absorbing S_1 into $\langle\psi|$ we implicitely used that S_1 is hermitian. This is necessarily the case because $-\mathbb{1}$ cannot be part of the stabilizer group: $-\mathbb{1}$ stabilizes the trivial vector space only for obvious reasons. Since $|\psi\rangle$ is a state it must be non-zero. If $-\mathbb{1}$ is not in the stabilizer group, it must be $S_i^2 = \mathbb{1}$ for all i.

The post-measurement state is $(1 \pm Z_1)/2 |\psi\rangle$, i.e., the stabilizer S_1 is replaced by $(1 \pm Z_1)/2$.

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