Exercise Sheet 9: Quantum circuits for quantum computing

The Quantum Fourier Transform

9 P. **Exercise 1.** At the heart of many 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 $y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j \exp\left\{\frac{2\pi ijk}{N}\right\}$. The quantum Fourier transform is analogously defined as the unitary operation $\mathcal{F} : \mathbb{C}^{2^n} \to \mathbb{C}^{2^n}$, $|j\rangle \mapsto \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \exp\left\{\frac{2\pi ijk}{2^n}\right\} |k\rangle$. (Note the identification $N = 2^n$.)

1 P. (a) What is the computational complexity of the fastest classical algorithm for the DFT? Look it up online.

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

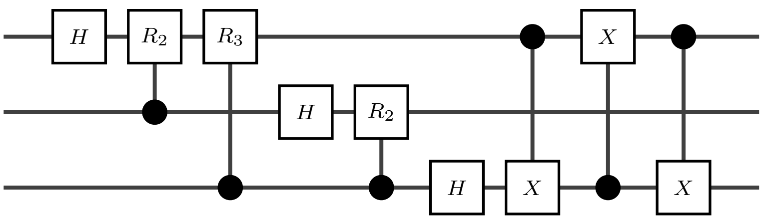
$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \tag{1}$$

the controlled phase gate that applies

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

on a *target* qubit if a *control* qubit is in the state $|1\rangle$ (and the identity if the control is in $|0\rangle$), and CNOT (aka controlled-X) gates. Note that in circuit diagrams controlled gates are conventionally represented by boxes on the target wires linked to dots on the control wires.

4 P. (b) Show that the following circuit implements the three-qubit quantum Fourier transform:



Hint: First argue that you can restrict your attention to computational basis states as inputs. To then show that the output state of the circuit on a computational basis state $|xyz\rangle$ coincides with $\mathcal{F}|xyz\rangle$, it will be helpful to use the binary representations of the integers involved. Our convention here is $k = 2^{n-1}k_{n-1} + \ldots + 2k_1 + k_0$.

2 P. (c) In (b), we fixed $n = 3$. Describe how to generalize the circuit given there to obtain a circuit for implementing the n-qubit quantum Fourier transform for a general n.

2 P. (d) Based on (c), give an upper bound on the quantum circuit complexity of the n-qubit quantum Fourier transform. How does it compare to the classical DFT algorithm from (a)?

Hint: Here, the quantum circuit complexity is defined as the smallest number of 2-qubit gates sufficient to implement a desired (unitary) operation. The gates do not necessarily have to act on neighbouring qubits.

We note that the quantum Fourier transform can in fact be approximately implemented with only $\mathcal{O}(n \log n)$ gates[1].

An Explicit Universal Gate Set

The aim of this exercise is to show that the gate set $\{CNOT, H, T\}$ is universal, i.e. we can approximate any unitary gate to an arbitrary accuracy just by using these three gates in a quantum circuit. Here, we only prove that we can use H and T to generate any single-qubit gate. The approximability of general n-qubit gates then follows from the known fact that $CNOT$ along with arbitrary one qubit gates is universal.

Recall that the T gate is given by $\begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$.

9 P. **Exercise 2.** We will start by showing that any single-qubit unitary U can be written as

$$U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta)\,, \tag{3}$$

where $R_z(\theta) = e^{-i\frac{\theta}{2}Z} = \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix}$, $R_y(\theta) = e^{-i\frac{\theta}{2}Y} = \begin{pmatrix} \cos\theta/2 & -\sin\theta/2 \\ \sin\theta/2 & \cos\theta/2 \end{pmatrix}$.

3 P. (a) Let $U \in U(2)$ be a one-qubit unitary. Show that there exist real numbers x, y, z, t such that

$$U = \begin{pmatrix} e^{i(x-y-t)}\cos z & -e^{i(x-y+t)}\sin z \\ e^{i(x+y-t)}\sin z & e^{i(x+y+t)}\cos z \end{pmatrix}. \tag{4}$$

Hint: To get started, think about which conditions for the rows and columns of U are equivalent to U being unitary.

1 P. (b) Show that any one-qubit unitary U can be expressed as

$$U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta) \tag{5}$$

for some real numbers $\alpha, \beta, \gamma, \delta$.

It is possible, but tedious, to show that we can find an analogous decomposition using any pair of linearly independent axes $\vec{n}$ and $\vec{m}$. You do not have to prove this here.

We will now see how to approximate an arbitrary single-qubit rotation around two linearly independent axes by using the Hadamard gate and the T gate. A single-qubit rotation with rotation axis $\vec{n}$ can be written as $R_{\vec{n}}(\theta) \equiv \exp(-i\theta\vec{n}\cdot\vec{\sigma}/2) = \cos(\theta/2)\mathbb{I} - i\sin(\theta/2)(n_x X + n_y Y + n_z Z)$, and any single-qubit gate can be written as a rotation around some axis.

3 P. (c) Calculate $THTH$, and find suitable θ and $\vec{n} = (n_x, n_y, n_z)$ for it.

Hint: Use that $T = e^{-i\pi/8Z}$ and $HZH = X$. First show $HTH = e^{-i\pi/8X}$.

2 P. (d) The rotation angle $\frac{\theta}{2\pi}$ in (c) is known to be an irrational number. Use this to explain that you can approximate an arbitrary rotation about the axis $\vec{n}$ in the previous point by some product of the operators H and T.

Let us define another rotation about an axis $\vec{m}$ as $R_{\vec{m}}(\theta) = HR_{\vec{n}}(\theta)H$. Because H is a rotation about $X+Z$ axis, the axis $\vec{m}$ is not equal to $\vec{n}$. Then from the comment in (b), we can generate an arbitrary single-qubit unitary by $R_{\vec{m}}$ and $R_{\vec{n}}$, and we can get the latter via (d).

[1] Cleve, Richard, and John Watrous. "Fast parallel circuits for the quantum Fourier transform." Proceedings 41st Annual Symposium on Foundations of Computer Science. IEEE, 2000.

(No-)Programming Quantum Computers

6 P. **Exercise 3.** In this exercise, you will prove the so-called *Quantum No-Programming Theorem.* Consider a bipartite Hilbert space $\mathcal{H} = \mathcal{H}_{\mathrm{sys}} \otimes \mathcal{H}_{\mathrm{pro}}$ given as a tensor product of a system Hilbert space and a program Hilbert space. A unitary $U \in \mathcal{U}(\mathcal{H})$ is *an (exact) programmable quantum processor* for a set of unitaries $\{V_i\}_{i=1}^n \subseteq \mathcal{U}(\mathcal{H}_{\mathrm{sys}})$ if for every $1 \leq i \leq n$ there exists a pure quantum state $|\pi_{V_i}\rangle \in \mathcal{H}_{\mathrm{pro}}$ such that

$$U(|\psi\rangle \otimes |\pi_{V_i}\rangle) = (V_i|\psi\rangle) \otimes |\pi'_{V_i}\rangle \; \forall |\psi\rangle \in \mathcal{H}_{\mathrm{sys}}\,, \tag{6}$$

with some state $|\pi'_{V_i}\rangle \in \mathcal{H}_{\mathrm{pro}}$.

2 P. (a) In Eq. (6), we implicitly assume that $|\pi'_{V_i}\rangle$ is independent of the input state $|\psi\rangle$ on the system register. Show that this can indeed be assumed without loss of generality.

Hint: Start from a version of Eq. (6) *with* $|\psi\rangle$*-dependent* $|\pi'_{V_i}(\psi)\rangle$ *and take inner products of two such equations for different input states* $|\psi\rangle$ *and* $|\phi\rangle$*.*

2 P. (b) Fix some $1 \leq i \neq j \leq n$. Suppose $V_i \neq e^{i\varphi} V_j$ holds for all $\varphi \in [0, 2\pi)$. Show that $\langle \pi_{V_i} | \pi_{V_j} \rangle = 0$.

Hint: Start from Eq. (6) *and take inner products of two such equations for* V_i *and* V_j*. You will want to exclude the case* $\langle \pi'_{V_i} | \pi'_{V_j} \rangle \neq 0$ *with a proof by contradiction.*

1 P. (c) Suppose that $V_i \neq e^{i\varphi} V_j$ holds for all $\varphi \in [0, 2\pi)$ and for all $1 \leq i \neq j \leq n$. Conclude from (b) that any any exact programmable quantum simulator for $\{V_i\}_{i=1}^n$ needs a program space $\mathcal{H}_{\mathrm{pro}}$ of dimension $\dim(\mathcal{H}_{\mathrm{pro}}) \geq n$.

1 P. (d) Conclude that there is no universal (exact) programmable quantum simulator with finite-dimensional program space. That is, if $\dim(\mathcal{H}_{\mathrm{sys}}) > 1$, then any (exact) programmable quantum simulator for $\mathcal{U}(\mathcal{H}_{\mathrm{sys}})$ requires a program space $\mathcal{H}_{\mathrm{pro}}$ of dimension $\dim(\mathcal{H}_{\mathrm{pro}}) = \infty$.

Recap

Now that the lecture has started to shift from sheer quantum information towards quantum computation, let us look back into how mixed states and non-unitary channels are related to pure states and unitary operations on a larger Hilbert space. In these exercises we again present you with a quantum state or channel acting on a given Hilbert space. Then, we ask you to enlarge the Hilbert space in a way that turns mixed into pure, and non-unitary into unitary. Although we have already formalized these concepts with theorems and definitions, our approach here is more direct: can you come up with direct ways to solve the following exercises, without invoking fancy math?

Let $\mathcal{H}_A, \mathcal{H}_B$ be two d-dimensional Hilbert spaces, with their computational bases $\{|0\rangle, \ldots, |d-1\rangle\}$. Now, we look back to Section *3.1.2 All teleportation schemes* in the lecture notes, and recover the concept of an *othonormal basis of unitaries* of a d-dimensional Hilbert space:

$$\{U_j \,|\, j \in \{1, \ldots, d^2\}\}.$$

Let $|\omega\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ be a maximally entangled state $|\omega\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |ii\rangle$. Then, as we saw in the context of general teleportation schemes, we can use the ONB of unitaries together with a maximally entangled state to reach an *orthonormal basis of maximally entangled states*, $\mathcal{B}$:

$$\mathcal{B} := \{(\mathbb{I} \otimes U_j)|\omega\rangle \,|\, j \in \{1, \ldots, d^2\}\}.$$

Just as a reminder, this ONB of maximally entangled states $\mathcal{B}$ spans exactly the same space as the computational basis of $\mathcal{H}_A \otimes \mathcal{H}_B$: $\{|ij\rangle \,|\, i,j \in \{0,\dots,d-1\}\}$. The only difference is that the basis elements themselves are *maximally* entangled in one case versus *minimally* entangled (product) in the other case.

We use $|\psi_j\rangle$ to denote the elements of the maximally entangled ONB: $\mathcal{B} = \{|\psi_j\rangle \,|\, j \in \{1,\dots,d^2\}\}$. Consider $p = (p_j)_{j=1}^{d^2}$ a discrete probability distribution: $p_j \in [0,1]$, $\sum_j p_j = 1$.

10 P. Bonus Exercise 1. For any given p as defined above, consider the quantum state

$$\rho_p := \sum_{j=1}^{d^2} p_j |\psi_j\rangle\langle\psi_j|.$$

1 P. (a) Find a p for which ρ_p is a pure, entangled state. Compute its entanglement entropy explicitly.

Hint: Pick the simplest p you can, so that you can prove each property in a few lines.

1 P. (b) Are there values of p for which ρ_p is again pure and entangled, but with a different entanglement entropy than the one you found in Exercise (a)?

3 P. (c) Find a p for which ρ_p is a mixed, entangled state. Compute the purity, and prove that it is an entangled state using the PPT criterium. For this question, assume that the dimension of the Hilbert space is $d = 2$, so we look at pairs of qubits, and you can choose a specific orthonormal basis of unitaries.

Hint: Remember the Bell states

$$\begin{aligned}
|\Phi^+\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) && = |\Phi^{00}\rangle \\
|\Phi^-\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = (\mathbb{I} \otimes Z)|\Phi^+\rangle && = |\Phi^{01}\rangle \\
|\Psi^+\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = (\mathbb{I} \otimes X)|\Phi^+\rangle && = |\Phi^{10}\rangle \\
|\Psi^-\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = (\mathbb{I} \otimes XZ)|\Phi^+\rangle && = |\Phi^{11}\rangle\,.
\end{aligned}$$

Use the fact that $|\Phi^{xy}\rangle\langle\Phi^{xy}|^\Gamma = \frac{1}{2}\mathbb{I} - |\Phi^{\bar{x}\bar{y}}\rangle\langle\Phi^{\bar{x}\bar{y}}|$ where $\bar{x}$ is the negation of the bit x. Here ρ^Γ is the partial transpose and it fulfills $(\rho_1 + \rho_2)^\Gamma = \rho_1^\Gamma + \rho_2^\Gamma$.

1 P. (d) Find a p for which ρ_p is a mixed, separable state. Compute the purity and give the expression as a convex combination of product states explicitly.

Hint: Pick the simplest p you can, so that the computation and the proof do not take more than a few lines.

3 P. (e) Let p be such that ρ_p is not pure. Give a third Hilbert space $\mathcal{H}_C$ and a *pure* quantum state $\tilde{\rho}_p = |\tilde{\Psi}_p\rangle\langle\tilde{\Psi}_p|$ living in $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$ such that

$$\mathrm{Tr}_C[|\tilde{\Psi}_p\rangle\langle\tilde{\Psi}_p|] = \rho_p.$$

For which dimension of $\mathcal{H}_C$ can we be sure that such a pure state exists?

Hint: Remember the Schmidt decomposition of a pure state $|\psi\rangle_{DE} = \sum_j \sqrt{\lambda_j}|b_j\rangle_D \otimes |\tilde{b}_j\rangle_E$ with $\sqrt{\lambda_j}$ the singular values and $\{|b_j\rangle\}_j$ and $\{|\tilde{b}_j\rangle\}_j$ some ONBs for $\mathcal{H}_D$ and $\mathcal{H}_E$ respectively. What is the reduced state $\mathrm{Tr}_E[|\psi\rangle\langle\psi|]$?

1 P. (f) Compute the entanglement entropy of $\tilde{\rho}_p$ from (e) w.r.t. the the bipartition $AB|C$.

Total Points: 24 (+10)