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 $y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j \exp\left\{\frac{2\pi i j k}{N}\right\}$. The quantum Fourier transform is analogously defined as the unitary operation $\mathcal{F} : \mathbb{C}^{2^n} \to \mathbb{C}^{2^n}$, $|j\rangle \mapsto \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \exp\left\{\frac{2\pi i j k}{2^n}\right\} |k\rangle$. (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.

Solution

The fast-fourier transform uses $\mathcal{O}(N \log N) = \mathcal{O}(2^n \log 2^n)$ operations, compare `https://en.wikipedia.org/wiki/Fast_Fourier_transform`.

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

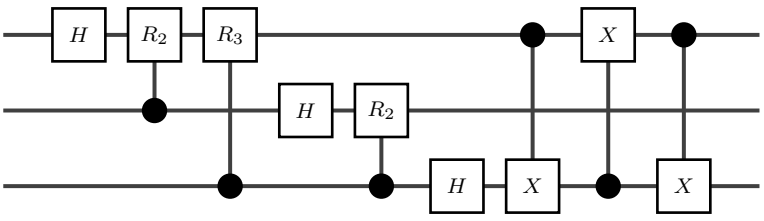
$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \tag{1}$$

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 $k = 2^{n-1}k_{n-1} + \ldots + 2k_1 + k_0$.

Solution

We will restrict our attention to inputs in the computational basis. This is justified by linearity and the fact that the computational basis is indeed a 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 implements a swap of the first and third qubits.
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 $H|x\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + \mathrm{e}^{2\pi i \frac{x}{2}}|1\rangle\right)$. The action of the phase gate on $|+\rangle$ controlled by the qubit $|y\rangle$ can analogously be written as $CR_k|y\rangle|+\rangle = |y\rangle\frac{1}{\sqrt{2}}\left(|0\rangle + \mathrm{e}^{2\pi i \frac{y}{2^k}}|1\rangle\right)$. This allows us to evaluate the output of the whole circuit (including the swap at the end) when acting on the input state $|xyz\rangle$ with $x, y, z \in \{0,1\}$ as

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

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

$$\begin{aligned}
\mathcal{F}|xyz\rangle &= \frac{1}{\sqrt{2}^3} \sum_{k_2,k_1,k_0\in\{1,0\}} \mathrm{e}^{2\pi i\left[\frac{x}{2}+\frac{y}{4}+\frac{z}{8}\right]\cdot(4k_2+2k_1+k_0)}|k_2k_1k_0\rangle \\
&= \frac{1}{\sqrt{2}^3}\left(\sum_{k_2\in\{0,1\}} \mathrm{e}^{2\pi i\left[\frac{x}{2}+\frac{y}{4}+\frac{z}{8}\right]4k_2}|k_2\rangle\right) \\
&\quad \otimes \left(\sum_{k_1\in\{0,1\}} \mathrm{e}^{2\pi i\left[\frac{x}{2}+\frac{y}{4}+\frac{z}{8}\right]2k_1}|k_1\rangle\right) \\
&\quad \otimes \left(\sum_{k_0\in\{0,1\}} \mathrm{e}^{2\pi i\left[\frac{x}{2}+\frac{y}{4}+\frac{z}{8}\right]k_0}|k_0\rangle\right) \\
&= \frac{1}{\sqrt{2}^3}\left(\sum_{k_2\in\{0,1\}} \mathrm{e}^{2\pi i\left[\frac{z}{2}\right]k_2}|k_2\rangle\right) \\
&\quad \otimes \left(\sum_{k_1\in\{0,1\}} \mathrm{e}^{2\pi i\left[\frac{y}{2}+\frac{z}{4}\right]k_1}|k_1\rangle\right) \\
&\quad \otimes \left(\sum_{k_0\in\{0,1\}} \mathrm{e}^{2\pi i\left[\frac{x}{2}+\frac{y}{4}+\frac{z}{8}\right]k_0}|k_0\rangle\right),
\end{aligned}$$

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

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.

Solution

For each additional register one adds a corresponding controlled phase gate to all the previous registers and a 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.

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.

Solution

The circuit described in (c) consists of n Hadamard gates as well as $(n-1)+(n-2)+\ldots+1+0=\sum_{i=0}^{n-1}=\frac{n(n-1)}{2}$ many controlled phase gates, plus the final reversion circuit. The reversion can be performed with at most $n/2$ swaps, thus adding at most $3n/2$ CNOT gates to the circuit. Thus, we end up with a total quantum circuit complexity of $n+\frac{n(n-1)}{2}+3n/2=\mathcal{O}(n^2)$. 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.

Note: As here we allowed arbitrary 2-qubit gates in the definition of circuit complexity, we can improve the upper bound from above a little bit. Namely, we can absorb the Hadamard gates into the controlled phase gates, and we can immediately consider swap gates instead of decomposing them into CNOTs. This then gives us the quantum circuit complexity upper bound $\frac{n(n-1)}{2}+\frac{n}{2}=\frac{n^2}{2}$.

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

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

[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.

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.

Solution

Let $U = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. The rows and columns must be normalized, so $|a|^2 + |b|^2 = 1$, $|a|^2 + |c|^2 = 1$, $|c|^2 + |d|^2 = 1$, and $|b|^2 + |d|^2 = 1$ So we can write

$$a = e^{i\phi_a} \cos z,\ b = -e^{i\phi_b} \sin z,\ c = e^{i\phi_c} \sin z,\ d = e^{i\phi_d} \cos z\,.$$

Note that the choice of signs is arbitrary since we could include it in the phases ϕ, but it will come handy later. Additionally, the rows must be orthogonal w.r.t. the standard inner product. This orthogonality condition is then

$$(e^{i(\phi_a - \phi_c)} - e^{i(\phi_b - \phi_d)}) \sin z \cos z = 0\,.$$

If any of the entries are 0, then it is easy to see that we can find suitable values for x, y, z, t. (First pick z such that either $\sin z = 0$ or $\cos z = 0$, then adjust the phases of the non-zero entries with x, y, t.) In the general case, where $\sin z \cos z \neq 0$, the orthogonality condition implies that $\phi_a = \phi_b + \phi_c - \phi_d \mod 2\pi$. Thus, we can write

$$U = \begin{pmatrix} e^{i(\phi_b + \phi_c - \phi_d)} \cos z & -e^{i\phi_b} \sin z \\ e^{i\phi_c} \sin z & e^{i\phi_d} \cos z \end{pmatrix} .$$

Now, the linear system of equations

$$\begin{aligned} \phi_b &= x - y + t \\ \phi_c &= x + y - t \\ \phi_d &= x + y + t \end{aligned}$$

can be used to define x, y, t because the coefficient matrix $\begin{pmatrix} 1 & -1 & 1 \\ 1 & 1 & -1 \\ 1 & 1 & 1 \end{pmatrix}$ has a non-zero determinant and is thus invertible. Notice that then in particular $\phi_b + \phi_c - \phi_d = x - y - t$, which is what we claimed for the phase of the first entry. Thus, we have shown that for an arbitrary unitary $U \in U(2)$, we can find suitable real numbers x, y, z, t such that Eq. (4) holds.

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.

Solution

One can verify (by direct computation, multiplying the matrices) that

$$e^{i\alpha}R_z(\beta)R_y(\gamma)R_z(\delta) = \begin{pmatrix} e^{i(2\alpha-\beta-\delta)/2}\cos\gamma/2 & -e^{i(2\alpha-\beta+\delta)/2}\sin\gamma/2 \\ e^{i(2\alpha+\beta-\delta)/2}\sin\gamma/2 & e^{i(2\alpha+\beta+\delta)/2}\cos\gamma/2 \end{pmatrix} .$$

If we can find a choice of parameters $\alpha, \beta, \gamma, \delta$ such that this corresponds to Equation (4), we can use the result that that form is universal for 2-qubit unitaries. Comparing the two, one can choose

$$\alpha = x,\ \beta = 2y,\ \gamma = 2z,\ \delta = 2t\,.$$

With this choice, one gets

$$e^{ix}R_z(-2y)R_y(2z)R_z(-2t) = \begin{pmatrix} e^{i(x-y-t)}\cos z & -e^{i(x-y+t)}\sin z \\ e^{i(x+y-t)}\sin z & e^{i(x+y+t)}\cos z \end{pmatrix} .$$

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 $\overrightarrow{n}$ can be written as $R_{\overrightarrow{n}}(\theta) \equiv \exp(-i\theta\overrightarrow{n}\cdot\overrightarrow{\sigma}/2) = \cos(\theta/2)\mathbb{I} - i\sin(\theta/2)(n_xX + n_yY + n_zZ)$, and any single-qubit gate can be written as a rotation around some axis.

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

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

Solution

Together, $T = e^{-i\pi/8Z}$ and $HZH = X$ imply $HTH = e^{-i\pi/8X}$. For this specific case, one can write the exponentiated Z in its eigenbasis

$$e^{i\theta Z} = e^{i\theta}|0\rangle\langle 0| + e^{-i\theta}|1\rangle\langle 1|$$

and then applying the Haddamard gate.

$$He^{i\theta Z}H = e^{i\theta}H|0\rangle\langle 0|H + e^{-i\theta}H|1\rangle\langle 1|H = e^{i\theta}|+\rangle\langle +| + e^{-i\theta}|-\rangle\langle -| = e^{i\theta X}\,.$$

In the more general case, this can either be seen by expanding the exponential series or via functional calculus. Thus, we get.

$$\begin{aligned} THTH &= e^{-i\pi/8Z}e^{-i\pi/8X} \\ &= (\cos(\pi/8)I - i\sin(\pi/8)Z)(\cos(\pi/8)I - i\sin(\pi/8)X) \\ &= \cos^2(\pi/8)I - i(\cos(\pi/8)(X+Z) + \sin(\pi/8)Y)\sin(\pi/8)\,. \end{aligned}$$

So, we want θ to satisfy $\cos(\theta/2) = \cos^2(\pi/8)$, i.e., $\theta = 2\arccos\left(\cos^2(\pi/8)\right)$, and $\overrightarrow{n} = (\cos(\pi/8), \sin(\pi/8), \cos(\pi/8))$.

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 $\overrightarrow{n}$ in the previous point by some product of the operators H and T.

Solution

Because $\frac{\theta}{2\pi}$ is irrational, for every $\alpha \in [0, 2\pi)$ there is some $m \in \mathbb{N}$ such that $|(m\theta) \mod 2\pi - \alpha| \leq \delta$. This can be seen as follows: Take N to be an integer greater than $2\pi/\delta$ and define $\theta_k = (k\theta) \mod 2\pi$ for $k = 0, \ldots, N$. Now, by pigeonhole principle – i.e., when distributing $I > C$ items into C containers, at least one container has at least 2 items (see `https://en.wikipedia.org/wiki/Pigeonhole_principle`) –, there exist i, j such that $|\theta_i - \theta_j| \leq \delta$. Let's w.l.o.g. assume $i > j$ and $\theta_i > \theta_j$. Then, note that $R_{\vec{n}}(\theta_i - \theta_j) = R_{\vec{n}}(\theta_{i-j})$. As $|\theta_i - \theta_j| \leq \delta$, there exists $\ell \in \mathbb{N}$ such that $|\alpha - \ell|\theta_i - \theta_j|| \leq \delta$. So, if we pick $m = \ell(i - j)$, then we have the desired δ-approximation to α via $m\theta \mod 2\pi$. As rotations around a fixed axis depend continuously on the rotation angle, by picking δ small enough, we can ensure that $R_{\vec{n}}(m\theta) = (R_{\vec{n}}(\theta))^m = (THTH)^m$ approximates $R_{\vec{n}}(\alpha)$ to a desired accuracy.

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).

(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 $\mathcal{H} = \mathcal{H}_{\text{sys}} \otimes \mathcal{H}_{\text{pro}}$ 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 $\{V_i\}_{i=1}^n \subseteq \mathcal{U}(\mathcal{H}_{\text{sys}})$ if for every $1 \leq i \leq n$ there exists a pure quantum state $|\pi_{V_i}\rangle \in \mathcal{H}_{\text{pro}}$ such that

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

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

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* $|\phi\rangle$*.*

Solution

Suppose $|\pi'_{V_i}\rangle = |\pi'_{V_i}(\psi)\rangle$ depends on the input state $|\psi\rangle$ on the system register. Take two different input states $|\psi\rangle, |\phi\rangle$ on the system register. Then, Eq. (6) says

$$U(|\psi\rangle \otimes |\pi_{V_i}\rangle) = (V_i|\psi\rangle) \otimes |\pi'_{V_i}(\psi)\rangle\,,$$
$$U(|\phi\rangle \otimes |\pi_{V_i}\rangle) = (V_i|\phi\rangle) \otimes |\pi'_{V_i}(\phi)\rangle\,.$$

Taking the inner products of these two equations, we get

$$\begin{aligned}\langle\psi|\phi\rangle &= (|\psi\rangle \otimes |\pi_{V_i}\rangle)^\dagger (|\phi\rangle \otimes |\pi_{V_i}\rangle) \\ &= (U(|\psi\rangle \otimes |\pi_{V_i}\rangle))^\dagger U(|\phi\rangle \otimes |\pi_{V_i}\rangle) \\ &= ((V_i|\psi\rangle) \otimes |\pi'_{V_i}(\psi)\rangle)^\dagger (V_i|\phi\rangle) \otimes |\pi'_{V_i}(\phi)\rangle \\ &= \langle\psi|\phi\rangle \cdot \langle\pi'_{V_i}(\psi)|\pi'_{V_i}(\phi)\rangle\,.\end{aligned}$$

Thus, whenever $\langle\psi|\phi\rangle \neq 0$, we conclude that $\langle\pi'_{V_i}(\psi)|\pi'_{V_i}(\phi)\rangle = 1$ and thus $|\pi'_{V_i}(\psi)\rangle = |\pi'_{V_i}(\phi)\rangle$. What about $\langle\psi|\phi\rangle = 0$? Just pick some third $|\varphi\rangle$ with $\langle\psi|\varphi\rangle \neq 0$ and $\langle\phi|\varphi\rangle \neq 0$ and use the above to conclude that $|\pi'_{V_i}(\psi)\rangle = |\pi'_{V_i}(\varphi)\rangle = |\pi'_{V_i}(\phi)\rangle$. This shows that $|\pi'_{V_i}(\psi)\rangle = |\pi'_{V_i}\rangle$ is actually independent of ψ.

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.*

Solution

By Eq. (6), we have

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

We can take an inner product of the two equations, we get

$$\langle\pi_{V_i}|\pi_{V_j}\rangle = \langle\psi|V_i^\dagger V_j|\psi\rangle \cdot \langle\pi'_{V_i}|\pi'_{V_j}\rangle \;\forall|\psi\rangle \in \mathcal{H}_{\text{sys}}\,. \tag{7}$$

Assume for contradiction that $\langle\pi'_{V_i}|\pi'_{V_j}\rangle \neq 0$, then we can divide both sides of the equation by it and get that $\langle\psi|V_i^\dagger V_j|\psi\rangle = \frac{\langle\pi_{V_i}|\pi_{V_j}\rangle}{\langle\pi'_{V_i}|\pi'_{V_j}\rangle}$ is actually independent of $|\psi\rangle$. This implies that $V_i^\dagger V_j \propto \mathbb{I}$, so V_i and V_j coincide up to a global phase. This contradicts our assumption, thus we get $\langle\pi'_{V_i}|\pi'_{V_j}\rangle = 0$ and, via Eq. (7), also $\langle\pi_{V_i}|\pi_{V_j}\rangle = 0$.

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 $\mathcal{H}_{\text{pro}}$ of dimension $\dim(\mathcal{H}_{\text{pro}}) \geq n$.

Solution

By (b), the states $|\pi_{V_i}\rangle \in \mathcal{H}_{\text{pro}}$, $1 \leq i \leq n$, are pairwise orthogonal. Therefore, $\dim(\mathcal{H}_{\text{pro}}) \geq n$.

1 P. (d) Conclude that there is no universal (exact) programmable quantum simulator with finite-dimensional program space. That is, if $\dim(\mathcal{H}_{\text{sys}}) > 1$, then any (exact) programmable

quantum simulator for $\mathcal{U}(\mathcal{H}_{\text{sys}})$ requires a program space $\mathcal{H}_{\text{pro}}$ of dimension $\dim(\mathcal{H}_{\text{pro}}) = \infty$.

Solution

As $\dim(\mathcal{H}_{\text{sys}}) > 1$, the set $\mathcal{U}(\mathcal{H}_{\text{sys}})$ contains infinitely (even uncountably) many unitaries that are all mutually different even up to a global phase. Then, the result of (b) implies $\dim(\mathcal{H}_{\text{pro}}) = \infty$.

Note: This whole exercise is adapted from `https://arxiv.org/abs/quant-ph/9703032`.

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 $\{|0\rangle, \dots, |d-1\rangle\}$. 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:

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

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*, $\mathcal{B}$:

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

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

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

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.

Solution

If we pick p such that $p_1 = 1$ and $p_j = 0 \, \forall j > 1$ then we obtain the state $\rho_p = |\psi_1\rangle\langle\psi_1|$ which is pure and normalized. Since $|\psi_1\rangle$ is one element from the basis $\mathcal{B}$ defined above, we know that it is maximally entangled. Thus we have a pure, entangled state, as requested.
Let's compute the entanglement entropy explicitly. For $p = \delta_1$ we have $\rho_p = |\psi_1\rangle\langle\psi_1|$. Then,

$$\begin{aligned}
E(\rho_p) &= S\left(\mathrm{Tr}_B\left[|\psi_1\rangle\langle\psi_1|\right]\right) \\
&= S\left(\mathrm{Tr}_B\left[(\mathbb{I}\otimes U_1)|\omega\rangle\langle\omega|(\mathbb{I}\otimes U_1)^\dagger\right]\right) \\
&= S\left(\mathrm{Tr}_B\left[(\mathbb{I}\otimes U_1)\frac{1}{d}\sum_{i,i'=0}^{d-1}|ii\rangle\langle i'i'|(\mathbb{I}\otimes U_1)^\dagger\right]\right) \\
&= S\left(\frac{1}{d}\sum_{i,i'=0}^{d-1}\mathrm{Tr}_B\left[|i\rangle\langle i'|\otimes U_1|i\rangle\langle i'|U_1^\dagger\right]\right) \\
&= S\left(\frac{1}{d}\sum_{i,i'=0}^{d-1}|i\rangle\langle i'|\,\mathrm{Tr}\left[U_1|i\rangle\langle i'|U_1^\dagger\right]\right) \\
&= S\left(\frac{1}{d}\sum_{i,i'=0}^{d-1}|i\rangle\langle i'|\delta ii'\right) \\
&= S\left(\frac{1}{d}\sum_{i=0}^{d-1}|i\rangle\langle i|\right) \\
&= -\sum_{i=0}^{d-1}\frac{1}{d}\log\frac{1}{d} \\
&= \log d\,.
\end{aligned}$$

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)?

Solution

For the state to be pure, we need it's density matrix to have rank one. From the definition of ρ_p as a mixture of states from the ONB $\mathcal{B}$, it is already written in a diagonal form (it is already its eigendecomposition). Since the rank is the number of non-zero eigenvalues, ρ_p can only be a pure state if one and only one of the p_j is non-zero. That is, the distribution has to be a Kroenecker delta $p = \delta_k$ and $\rho_p = |\psi_k\rangle\langle\psi_k|$.

With that, we can see that all possible choices k result in a state with the same entanglement entropy. On the one hand, by definition, $|\psi_k\rangle = (\mathbb{I} \otimes U_j)|\omega\rangle$ is a local unitary transformation of the maximally entangled state. On the other hand, local unitary transformations do not change the entanglement entropy

$$E((U_A \otimes V_B)|\phi\rangle\langle\phi|_{AB}(U_A \otimes V_B)^\dagger) = E(|\phi\rangle\langle\phi|_{AB})\,,$$

where $E(|\phi\rangle\langle\phi|_{AB}) = S(\mathrm{Tr}_B[|\phi\rangle\langle\phi|_{AB}])$ and $S(\rho)$ is the von-Neumann entropy. You can check that by writing the Schmidt decomposition of $|\phi\rangle_{AB}$ and then applying the unitaries, resulting in a local change of basis but leaving the Schmidt coefficients unchanged.

Putting things together, the answer is no. There is no distribution p for which the resulting state is pure and entangled, but has a different entanglement entropy than the one from (a) (which is the one of the maximally entangled state).

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* $(\rho_1 + \rho_2)^\Gamma = \rho_1^\Gamma + \rho_2^\Gamma$*.*

Solution

As discussed in the previous question, for ρ_p to be mixed, we need at least two elements of p to be non-zero. To look for a simple example, we will look at the case where p has only two non-zero values, that is p_1 and $p_2 = 1 - p_1$. Then, $\rho_p = p_1|\psi_1\rangle\langle\psi_1| + (1-p_1)|\psi_2\rangle\langle\psi_2|$. Again, this is a valid eigendecomposition with eigenvalues $\{p_1, 1-p_1\}$, so the purity is $\mathrm{Tr}[\rho_p^2] = (p_1)^2 + (1-p_1)^2 = 1 - 2p_1 + 2p_1^2$. This is smaller than 1 for any $0 < p_1 < 1$.

Now let us think about entanglement. We know from the lecture (Section 5.2.2), that the PPT criterion is necessary for separability, and even sufficient for pairs of qubits. We can without loss of generality consider the set of orthogonal unitaries to be $\{U_j\}_{j=1}^4 = \{\mathbb{I}, X, Z, XZ\}$ (any other choice of basis would have resulted in a local rotation of the basis, which has no effect on the entanglement properties). With this, the four possible states in the eigendecomposition are the four Bell states. Then for our choice of p, the state that we constructed is

$$\rho_p = p_1|\Phi^{x_1y_1}\rangle\langle\Phi^{x_1y_1}| + (1-p_1)|\Phi^{x_2y_2}\rangle\langle\Phi^{x_2y_2}|\,.$$

Now, let us apply the hint

$$\begin{aligned}
\Rightarrow \rho_p^\Gamma =& p_1\left(|\Phi^{x_1y_1}\rangle\langle\Phi^{x_1y_1}|\right)^\Gamma + (1-p_1)\left(|\Phi^{x_2y_2}\rangle\langle\Phi^{x_2y_2}|\right)^\Gamma \\
=& p_1\left(\frac{1}{2}\mathbb{I} - |\Phi^{\bar{x_1}\bar{y_1}}\rangle\langle\Phi^{\bar{x_1}\bar{y_1}}|\right) + (1-p_1)\left(\frac{1}{2}\mathbb{I} - |\Phi^{\bar{x_2}\bar{y_2}}\rangle\langle\Phi^{\bar{x_2}\bar{y_2}}|\right) \\
=& \frac{1}{2}\mathbb{I} - p_1|\Phi^{\bar{x_1}\bar{y_1}}\rangle\langle\Phi^{\bar{x_1}\bar{y_1}}| - (1-p_1)|\Phi^{\bar{x_2}\bar{y_2}}\rangle\langle\Phi^{\bar{x_2}\bar{y_2}}|\,.
\end{aligned}$$

Since the Bell states form a basis, we can write the identity as $\mathbb{I} = |\Phi^{00}\rangle\langle\Phi^{00}| + |\Phi^{01}\rangle\langle\Phi^{01}| + |\Phi^{10}\rangle\langle\Phi^{10}| + |\Phi^{11}\rangle\langle\Phi^{11}|$. Then, the eigenvalues of ρ_p^Γ can be read directly from the above decomposition: $\left\{\frac{1}{2}, \frac{1}{2}, \frac{1}{2} - p_1, \frac{1}{2} - (1-p_1)\right\}$. For any choice of $p_1 \neq 1/2$, one of the four eigenvalues is negative, so the state is entangled. As per the above, the state is mixed if $p_1 \notin \{0, 1\}$. So ρ_p is a mixed entangled state for $p_1 \in (0, 1/2) \cup (1/2, 1)$.

This argument could have been generalized to having not only two elements but four. In this case, naming the probabilities of the respective Bell states $p_{x,y}$, the condition for entanglement would be $\max_{x,y} p_{x,y} > 1/2$.

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.

Solution

The prime example of a mixed separable state is the maximally mixed state (the normalized identity). As our state ρ_p is a convex combination of states forming an ONB, if we choose all coefficients to be equal (so $p_j = 1/d^2$ for all j) we get

$$\rho_p = \frac{1}{d^2} \sum_{j=1}^{d^2} |\psi_j\rangle\langle\psi_j| = \frac{1}{d^2}\mathbb{I}\,.$$

The purity is then $\mathrm{Tr}[\rho_p^2] = \left(\frac{1}{d^2}\right)^2 \mathrm{Tr}[\mathbb{I}_{d^2\times d^2}] = \frac{1}{d^2}$. Considering the bipartition into $\mathcal{H}_A$ and $\mathcal{H}_B$, we have that $\mathbb{I}_{AB} = \mathbb{I}_A \otimes \mathbb{I}_B$. So for $p_j = 1/d^2$ we have that ρ_p is mixed and it is even more than separable, it is a product state. In particular, a valid expression as a convex combination of product states is simply $\rho_p = \frac{1}{d}\mathbb{I}_A \otimes \frac{1}{d}\mathbb{I}_B$.
For the special case of qubits, we know (from previous question) that any choice of p with $\max_j p_j \leq 1/2$ is separable.

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* $\mathrm{Tr}_E[|\psi\rangle\langle\psi|]$*?*

Solution

If ρ_p is not pure, than there are several non-zero p_j, so we can write without loss of generality

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

where $2 \leq K \leq d^2$ is the number of non-zero elements in p. Then, choosing $|\tilde{\Psi}_p\rangle = \sum_{j=1}^{K} \sqrt{p_j}|\psi_j\rangle_{AB} \otimes |j\rangle_C$ for some ONB $\{|j\rangle\}_{j=1}^{K}$ of $\mathcal{H}_C$ we get

$$\begin{aligned}
\mathrm{Tr}_C[|\tilde{\Psi}_p\rangle\langle\tilde{\Psi}_p|] &= \mathrm{Tr}_C\left[\sum_{j,j'=1}^{K} \sqrt{p_j p_{j'}}|\psi_j\rangle\langle\psi_{j'}|_{AB} \otimes |j\rangle\langle j'|_C\right] \\
&= \sum_{k=1}^{K} (\mathbb{I}_{AB} \otimes \langle k|)\left(\sum_{j,j'=1}^{K} \sqrt{p_j p_{j'}}|\psi_j\rangle\langle\psi_{j'}|_{AB} \otimes |j\rangle\langle j'|_C\right)(\mathbb{I}_{AB} \otimes |k\rangle) \\
&= \sum_{j,j',k=1}^{K} \sqrt{p_j p_{j'}}|\psi_j\rangle\langle\psi_{j'}|_{AB}\delta_{jk}\delta_{jk'} \\
&= \sum_{k=1}^{K} p_k |\psi_k\rangle\langle\psi_k|_{AB} \\
&= \rho_p.
\end{aligned}$$

The smallest possible dimension of $\mathcal{H}_C$ is given by the rank of the mixed state ρ_p. In our case, since the state is already written in its eigenbasis, the rank is K. In general, the dimension of the Hilbert space in which the state lives (in our case $\dim(\mathcal{H}_A \otimes \mathcal{H}_B) = d^2$) is sufficient for a purification to exist.

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

Solution

The entanglement entropy between AB and C is given by the Shannon entropy of the distribution p. This can be seen by relating it to the von Neumann entropy of the original state ρ_p.

$$\begin{aligned} E_{AB:C}\left(|\tilde{\Psi}_p\rangle\right) &= S\left(\mathrm{Tr}_C\left[|\tilde{\Psi}_p\rangle\langle\tilde{\Psi}_p|\right]\right) \\ &= S(\rho_p) \\ &= \mathrm{Tr}[\rho_p \log \rho_p] \\ &= \sum_{j=1}^{K} p_j \log p_j \\ &= H(p)\,. \end{aligned}$$

Alternatively, one could trace out the original two subsystems A and B.

$$\begin{aligned} E_{AB:C}\left(|\tilde{\Psi}_p\rangle\right) &= S\left(\mathrm{Tr}_{AB}\left[|\tilde{\Psi}_p\rangle\langle\tilde{\Psi}_p|\right]\right) \\ &= S\left(\sum_{j=1}^{K} p_j |j\rangle\langle j|\right) \\ &= \sum_{j=1}^{K} p_j \log p_j \\ &= H(p)\,. \end{aligned}$$

The second equality here is only straightforward since the states $|\psi_j\rangle$ are orthonormal.

Total Points: 24 (+10)