# Exercise Sheet 11: Quantum Phase Estimation and Gottesman-Knill

## Quantum Phase Estimation

Perhaps at the heart of the majority of modern quantum algorithms lies the *phase estimation algorithm*. The problem of phase estimation is the following: Given a unitary operator $U$ and one of its eigenvectors $|u\rangle$ with eigenvalue $\mathrm{e}^{2\pi i\phi}$, output (an approximation to) the phase $\phi \in [0,1]$.

**12 P.** **Exercise 1.** In this exercise, we will investigate the standard quantum algorithm for solving the phase estimation problem.

1 P. (a) On Sheet 9, the definition and the circuit of the quantum Fourier transform were discussed. Show that the Quantum Fourier transform is invertible and give its inverse (by specifying its effect on computational basis states, just as we did for the QFT).

*Solution*

On Sheet 9, we gave a quantum circuit consisting of unitary gates that implemented the Quantum Fourier transform. Thus, the Quantum Fourier transform $\mathcal{F}$, which acts on computational basis states as $\mathcal{F}|j\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{\frac{2\pi i k j}{N}} |k\rangle$, is unitary and in particular invertible, with the inverse $\mathcal{F}^{-1} = \mathcal{F}^\dagger$ acting on computational basis states as

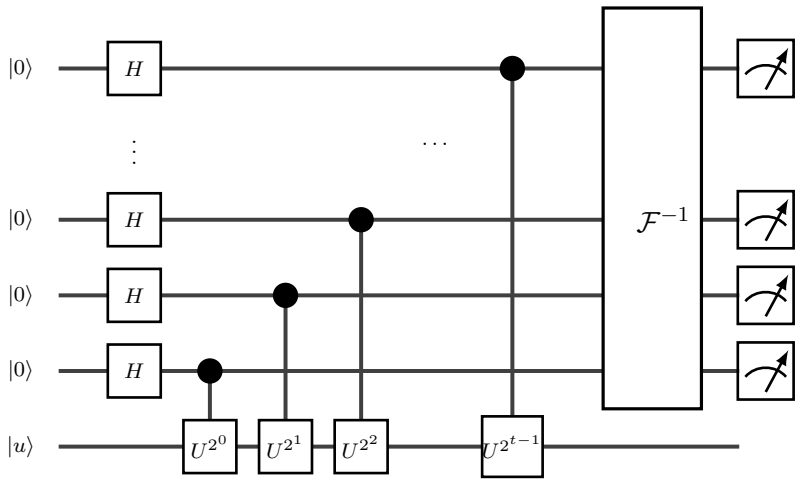
$$\mathcal{F}^{-1}|k\rangle = \mathcal{F}^\dagger|k\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{-\frac{2\pi i k j}{N}} |j\rangle\,.$$

With $\mathcal{F}|j\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{\frac{2\pi i k j}{N}} |k\rangle$ you can double-check that

$$\mathcal{F}^{-1}\mathcal{F}|j\rangle = \frac{1}{N} \sum_{k=0}^{N-1} \sum_{j'=0}^{N-1} e^{\frac{2\pi i k (j-j')}{N}} |j'\rangle = \frac{1}{N} \sum_{j'=0}^{N-1} N\delta_{j,j'} |j'\rangle = |j\rangle$$

and similarly for $\mathcal{F}\mathcal{F}^{-1}|j\rangle$.

The phase estimation algorithm is implemented via the following quantum circuit:




The circuit consists of $H$, the Hadamard gate; controlled-$U^{2^k}$-gates, that apply the unitary operator $U$ for $2^k$ times if the control qubit is $|1\rangle$; and $\mathcal{F}^{-1}$, the inverse of the quantum Fourier

transform. At the beginning, the first register comprising $t$ qubits is initialized as $|0\rangle^{\otimes t}$ and the second register is prepared in the state $|u\rangle$. This is then followed by a computational basis measurement on the first $t$ qubits.

2 P. (b) Express the state of the $t$ qubits in the first register before the inverse Fourier transform is applied in the computational basis $\{|x\rangle\}_{x\in\{0,1\}^t}$.

*Hint: Make use of the tensor product structure of $(H|0\rangle)^{\otimes t}$. Also, you might find it helpful to first show that $CU^k_{1\to 2}(|+\rangle\otimes|u\rangle) = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\phi k}|1\rangle\right)\otimes|u\rangle$. Here, $CU^k_{1\to 2}$ denotes the controlled unitary in which $U^k$ is applied to the second register controlled on the first register being active.*

*Solution*

Before applying the inverse Fourier transform, the first register will be in the state

$$\begin{aligned}&\frac{1}{\sqrt{2^t}}\left(|0\rangle + \mathrm{e}^{2\pi i 2^{t-1}\phi}|1\rangle\right)\left(|0\rangle + \mathrm{e}^{2\pi i 2^{t-2}\phi}|1\rangle\right)\cdots\left(|0\rangle + \mathrm{e}^{2\pi i 2^{0}\phi}|1\rangle\right)\\ &= \frac{1}{\sqrt{2^t}}\sum_{k=0}^{2^t-1}\mathrm{e}^{2\pi i\phi k}|k\rangle\,.\end{aligned}$$

This can be seen as follows: Written in terms of gates, the state of all qubits before the inverse Fourier transform is

$$\begin{aligned}&CU^{2^{t-1}}_{1\to t}\ldots CU^{2^0}_{(t-1)\to t}(H|0\rangle)^{\otimes t}\otimes|u\rangle\\ &= CU^{2^{t-1}}_{1\to t}\ldots CU^{2^0}_{(t-1)\to t}\left(\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\right)^{\otimes t}\otimes|u\rangle\\ &= CU^{2^{t-1}}_{1\to t}\ldots CU^{2^1}_{(t-2)\to t}\left(\left(\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\right)^{\otimes(t-1)}\otimes\left(CU^{2^0}_{(t-1)\to t}\left(\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\right)\otimes|u\rangle\right)\right)\\ &= CU^{2^{t-1}}_{1\to t}\ldots CU^{2^1}_{(t-2)\to t}\left(\left(\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\right)^{\otimes(t-1)}\otimes\left(\frac{1}{\sqrt{2}}\left(|0\rangle|u\rangle+|1\rangle e^{2\pi i\phi\cdot 2^0}|u\rangle\right)\right)\right)\\ &= CU^{2^{t-1}}_{1\to t}\ldots CU^{2^1}_{(t-2)\to t}\left(\left(\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\right)^{\otimes(t-1)}\otimes\frac{1}{\sqrt{2}}\left(|0\rangle+e^{2\pi i\phi\cdot 2^0}|1\rangle\right)\otimes|u\rangle\right)\\ &= \ldots\\ &= \left(\frac{1}{\sqrt{2^t}}\left(|0\rangle+\mathrm{e}^{2\pi i 2^{t-1}\phi}|1\rangle\right)\left(|0\rangle+\mathrm{e}^{2\pi i 2^{t-2}\phi}|1\rangle\right)\cdots\left(|0\rangle+\mathrm{e}^{2\pi i 2^{0}\phi}|1\rangle\right)\right)\otimes|u\rangle\,.\end{aligned}$$

2 P. (c) Assume that $\phi$ can be written with exactly $t$ bits, i.e. $\phi = \sum_{k=1}^{t} 2^{-k}\phi_k$. Show that the measurement result at the end of the above circuit is $|\phi_1\ldots\phi_t\rangle$ with probability 1.

*Hint: First compute the effect of the inverse quantum Fourier transform on the state obtained in (b). Then observe that $|l\rangle = |2^t\phi\rangle$ is one valid contribution in the obtained superposition. Find its amplitude using the definition of the delta function as a complex sum over the unit circle.*

*Solution*

Apply the inverse Fourier transform to get the output state (before the measurement)

$$|\psi\rangle = \frac{1}{2^t}\sum_{k,l=0}^{2^t-1} e^{\frac{2\pi i k}{2^t}(2^t\phi - l)}|l\rangle = \sum_l \omega(l)|l\rangle$$

with

$$\omega(l) := \frac{1}{2^t}\sum_{k=0}^{2^{t-1}} e^{\frac{2\pi i k}{2^t}(2^t\phi - l)}\,.$$

Notice that by assumption $2^t\phi = \sum_{k=1}^{t} 2^{t-k}\phi_k$ is an integer with $0 \leq 2^t\phi \leq 2^t - 1$, hence we can consider $l = 2^t\phi$ and see that $\omega(2^t\phi_t) = 1$. This already implies that $|\psi\rangle = |2^t\phi\rangle$, since the total weight of all amplitudes is 1.

As a sanity check, let us also prove by hand that the other summands vanish: If $l \neq 2^t\phi$ we have for $m = 2^t\phi - l \neq 0$

$$\omega(l) = \frac{1}{2^t}\sum_{k=0}^{2^{t-1}} e^{\frac{2\pi i k}{2^t}m} = 0\,.$$

In summary, $|\psi\rangle = |2^t\phi\rangle$. Clearly, measuring $|\psi\rangle$ in the computational basis gives the measurement result $|\phi_1 \ldots \phi_t\rangle$ with probability 1.

If the phase $\phi$ does not happen to have an exact $t$-bits representation, it is possible to show that a measurement outcome close to $\phi$ occurs with high probability. For the rest of the exercise, we will assume for simplicity that all phases mentioned have exact $t$-bits representations.

1 P. (d) Suppose now that, instead of applying the unitaries to a single eigenstate $|u\rangle$, we apply them to some superposition $|\psi\rangle = \sum_i c_i|u_i\rangle$, where each $|u\rangle_i$ is an eigenvector of $U$ with eigenvalue $e^{2\pi i\phi_i}$. What does the quantum phase algorithm now output?

*Hint: No need for any calculations.*

*Solution*

By linearity, the procedure outputs $\phi_i$ with probability $|c_i|^2$.

1 P. (e) How many queries to the unitary operator $U$ are used in the algorithm?

*Solution*

We use $1 + 2 + 4 + \ldots + 2^{t-1} = \sum_{k=0}^{t-1} 2^k = \frac{2^t-1}{2-1} = 2^t - 1 \in \mathcal{O}(2^t)$ queries to the unitary $U$.

In the lecture, you saw how the problem of finding prime factors of an integer $N$ can be reduced to finding the period of a certain function defined as

$$f(x) = a^x \mod N.$$

If $f(x+r) = f(x)$, where $r$ is even and $a^{r/2} \neq -1 \mod N$, then $a^r - 1 = (a^{r/2}+1)(a^{r/2}-1) = 0 \mod N$. This implies that $a^{r/2} \pm 1$ and $N$ have nontrivial common divisors, which can be found using Euclid's algorithm, hence finding a nontrivial factor of $N$. An $a$ such that $r$ has the right properties can be guessed with high probability. Here, the smallest integer $r$ such that $a^r \mod N = 1$, is called the *order* of $a$ in $\mathbb{Z}_N$.

The crucial point of Shor's algorithm is then to find the period of $f$. We want to elaborate how this can be done through period finding. Consider the operator

$$U|x\rangle = \begin{cases} |xa \mod N\rangle & \text{if } x < N \\ |x\rangle & \text{otherwise} \end{cases} .$$

Notice that, by definition,

$$U^k|x\rangle = \begin{cases} |xa^k \mod N\rangle = |xf(k) \mod N\rangle & \text{if } x < N \\ |x\rangle & \text{otherwise} \end{cases} .$$

2 P. (f) Using that $a$ and $N$ are coprime, show that $U$ is a unitary.

*Hint: Look at the action of $U$ on the computational basis.*

*Solution*

$U$ is a unitary if $xa \mod N = ya \mod N$ implies $x = y$. (Why? If that is the case, then $U$ acts bijectively on the computational ONB.) So, let's show that. If $xa \mod N = ya \mod N$, then there are integers $k$ and $l$ s.t. $xa + kN = ya + lN$, or $a(x-y) = N(l-k)$ Thus, either $x = y$ and $l = k$, or $a$ and $N$ have common factors. As we assumed $a$ and $N$ to be coprime, we get $x = y$ (and $l = k$).

2 P. (g) Show that $U$ has eigenvalues of the form $e^{2\pi ik/r}$ for integers $0 \leq k < r$. Find the corresponding eigenvectors, knowing that they are of the form

$$|v_s\rangle = \sum_{\ell=0}^{r-1} \alpha_{\ell,s} |a^\ell \mod N\rangle ,$$

with integers $0 \leq s < r$.

*Hint: By assumption, $r$ is the order of $a$ in $\mathbb{Z}_N$. What does that imply for $U^r$?*

*Solution*

By definition of the order of $a$ in $\mathbb{Z}_N$, we have $U^r = \mathbb{I}$. That is, for the case $x < N$ (the other one is trivial),

$$xa^r \mod N = xf(r) \mod N = xf(0) \mod N = x \mod N = x .$$

This implies that the eigenvalues of $U$ are $r$-th roots of unity. That is, the eigenvalues are of the form $e^{2\pi ik/r}$, with integer $0 \leq k < r$.
Now, let's consider the action of $U$ on vectors $|v_s\rangle$ of the given form:

$$U|v_s\rangle = \sum_{\ell=0}^{r-1} \alpha_{\ell,s} |a^{\ell+1} \mod N\rangle = \sum_{\ell=0}^{r-1} \alpha_{(\ell-1) \bmod r,s} |a^\ell \mod N\rangle$$

where we used that $a^r \mod N = 1$. If $|v_s\rangle$ is an eigenvector of $U$ with eigenvalue $e^{2\pi ik/r}$, then – using our above form for the eigenvalues, we also have $U|v_s\rangle = e^{2\pi ik/r}|v_s\rangle$ for some $0 \leq k < r$. Then the coefficients must satisfy $\alpha_{(\ell-1) \bmod r,s} = e^{2\pi ik/r}\alpha_{\ell,s}$. Staring at this a bit, we see that $k = s$ and $\alpha_{\ell,s} = \frac{1}{\sqrt{r}} e^{-2\pi i\ell s/r}$ works. (Here, the $1/\sqrt{r}$ is for normalization.)

So, using phase estimation (recall our result from (d)) with (a superposition over) the eigenstates $|v_s\rangle$, we are able to get $q = k/r$ for some random $0 \leq k < r$. We could use this to

find a guess of $r$ by simply finding a fraction representation of $q$, but if $k$ and $r$ have a common divisor $d$, this will yield $r' = r/d$, as $q = k'/r' = (k/d)/(r/d)$. This can be dealt with by running the algorithm multiple times for different eigenvectors and get $k_1/r = k_1'/r_1', k_2/r = k_2'/r_2', \ldots$ With high probability, $r$ is the least common multiple of the $r_i'$.

We are almost done, the only element we're missing is that in general we do not know how to prepare the eigenvectors of $U$. We adress this in the final part of the exercise:

1 P. (h) What is the output of the phase estimation algorithm for the unitary $U$ if we input the vector $|1\rangle$ (instead of $|u\rangle$ in our circuit diagram)? Why does this solve the problem of not knowing how to prepare the eigenvectors of $U$?

*Solution*

We have $|1\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |v_s\rangle$. This can be seen via

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |v_s\rangle = \sum_{k=0}^{r-1} \left( \frac{1}{r} \sum_{s=0}^{r-1} \exp\left(-\frac{2\pi i s k}{r}\right) \right) |x^k \mod N\rangle = |1\rangle ,$$

where we used $\frac{1}{r} \sum_{s=0}^{r-1} \exp\left(-\frac{2\pi i s k}{r}\right) = \delta_{k,0}$. So, recalling our result from (d), the phase estimation algorithm when inputting $|1\rangle$ in the eigenstate register outputs $k/r$, where $k$ is a random integer from 0 to $r-1$. This is exactly what we had after (g), so with the same reasoning as above one can find $r$ (with high probability).

## Stabilizer formalism for Clifford circuits

A celebrated result 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 and a final measurement in the computational basis can be classically simulated in the sense that there exists a classical algorithm with polynomial runtime that can sample from the output distribution of such a computation. Furthermore, the so-called stabilizer formalism plays an important role in the development of quantum error correction.

In this exercise we will retrace the reasoning underlying the Gottesman-Knill theorem. 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 $G_1 = \{\pm\mathbb{I}, \pm X, \pm Y, \pm Z, \pm i\mathbb{I}, \pm iX, \pm iY, \pm iZ\}$ be the single-qubit *Pauli group* where multiplication is the group operation.[1]

(ii) Let $G_n := \{\bigotimes_{i=1}^n P_i \mid P_i \in G_1\}$ 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 $\mathcal{S}_{|\psi\rangle} = \{S_1, \ldots, S_n\} \subset G_n$ satisfying $S_i|\psi\rangle = |\psi\rangle$. We call the generalized Pauli operators $S_i$ the stabilizer generators of $|\psi\rangle$.[2] We note that such $S_1, \ldots, S_n$ are independent (in the sense that neither of these $n$ operators can be written as a non-trivial product of the others) and mutually commute.

(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 theory language, the Clifford group $\mathcal{C} \subset \mathcal{U}(2^n)$ is the normalizer of $G_n$.

[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.

**12 P. Exercise 2.**

2 P. (a) Show that the set $\mathcal{S} = \{Z_1, Z_2, \ldots, Z_n\}$ stabilizes the state $|0\rangle^{\otimes n}$ and that this is the unique state stabilized by $\mathcal{S}$. Here, we use the notation $Z_i = \mathbb{I} \otimes \cdots \otimes \mathbb{I} \otimes \underbrace{Z}_{i\text{-th qubit}} \otimes \mathbb{I} \otimes \cdots \otimes \mathbb{I}$ for the operator acting as $Z$ on the $i$-th qubit and as the identity on all other qubits.

*Solution*

For an arbitrary state $|\psi\rangle$ to be stabilized by $\mathcal{S}$, we have the $n$ conditions $Z_i|\psi\rangle = |\psi\rangle$ for all $1 \leq i \leq n$. 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

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

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

*Solution*

Suppose $|\psi\rangle = C|0\rangle^{\otimes n}$. According to (a), $|0\rangle^{\otimes n}$ is uniquely determined by the condition that it is stabilized by $Z_1, \ldots, Z_n$, i.e., by the $n$ relations $Z_i|0\rangle^{\otimes n} = |0\rangle^{\otimes n}$. Then $CZ_i|0\rangle^{\otimes n} = C|0\rangle^{\otimes n} = |\psi\rangle$. Inserting an identity we obtain $CZ_iC^\dagger C|0\rangle^{\otimes n} = CZ_iC^\dagger|\psi\rangle$. Defining $S_i = CZ_iC^\dagger$, we obtain

$$\begin{aligned} S_i|\psi\rangle &= CZ_iC^\dagger C|0\rangle^{\otimes n} \\ &= CZ_i|0\rangle^{\otimes n} \\ &= C|0\rangle^{\otimes n} \\ &= |\psi\rangle\,, \end{aligned}$$

so each $S_i$ stabilizes $|\psi\rangle$. As the the stabilizer $\{Z_1, \ldots, Z_n\}$ uniquely characterizes $|0\rangle^{\otimes n}$ and as $C$ is the unique Clifford operator with $|\psi\rangle = C|0\rangle^{\otimes n}$, we conclude that $\{S_1, \ldots, S_n\}$ uniquely characterizes $|\psi\rangle$.

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

*Solution*

We have that

$$\begin{aligned} (X \otimes \mathbb{I} \otimes \mathbb{I})(|+\rangle \otimes |0\rangle \otimes |-\rangle) &= |+\rangle \otimes |0\rangle \otimes |-\rangle\,, \\ (\mathbb{I} \otimes Z \otimes \mathbb{I})(|+\rangle \otimes |0\rangle \otimes |-\rangle) &= |+\rangle \otimes |0\rangle \otimes |-\rangle\,, \\ (\mathbb{I} \otimes \mathbb{I} \otimes -X)(|+\rangle \otimes |0\rangle \otimes |-\rangle) &= |+\rangle \otimes |0\rangle \otimes |-\rangle\,. \end{aligned}$$

Then, $\{X_1, Z_2, -X_3\}$ is 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

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

2 P. (d) Show that the gate set $\{CNOT, H, S\}$ is sufficient to generate all Pauli strings, that is, all elements of $\{\mathbb{I}, X, Y, Z\}^{\otimes n}$, starting from any non-trivial (non-identity) single-qubit Pauli matrix. Here, the allowed steps in generating an arbitrary Pauli matrix are of the form $P \mapsto GPG^\dagger$, where $P$ is a Pauli matrix that we can already reach, and where $G \in \{CNOT, H, S\}$.

*Hint: First show that is is true for a single qubit and then look at the case* $CNOT(X \otimes \mathbb{I})CNOT^\dagger$.

*Solution*

First, let's look at a single qubit. Here, $H$ allows us to switch between $X$ and $Z$ via $HXH^\dagger = Z$. Similarly, $S$ switches between $X$ and $Y$ via $SXS^\dagger = Y$. So, $\{H, S\}$ is sufficient to generate all single-qubit Pauli matrices on some qubit starting from any non-trivial single-qubit Pauli matrix on that qubit.
Now, how do we get to tensor products of Paulis? Here, the $CNOT$ can be used to couple to qubits. Explicitly, we have $CNOT_{12} X_1 CNOT_{12}^\dagger = X_1 \otimes X_2$. So, starting from any non-trivial single-qubit Pauli matrix on qubit $i$, we can, e.g., first use conjugation with $H$ and/or $S$ to get to $X_i$. Then we use conjugation with suitable $CNOT$s to get $X_j$ on all qubits $j$ that have non-trivial Pauli tensor factors. Finally, for each such $j$, we use conjugation with $H$ and/or $S$ to get to whichever among $X_j$, $Y_j$, or $Z_j$ we are aiming for on that qubit.

2 P. (e) Argue that one can efficiently (i.e., with a number of classical computation steps polynomial in the number of qubits and gates) determine the stabilizer set of a state generated by a (known) Clifford circuit (comprising $CNOT, H, S$ gates) applied to a stabilizer state.

*Solution*

Let $G$ be the number of gates, and we use $n$ for the number of qubits. The initial stabilizer state is described by $n$ stabilizer generators $S_1, \ldots, S_n$ according to (b). Let $S_1^{(g)}, \ldots, S_n^{(g)}$ denote the stabilizer generators after the $g$th Clifford gate, with $S_i^{(0)} = S_i$. For every Clifford gate $C_g$, $1 \leq g \leq G$, in the computation, we can update the stabilizer generators as $S_i^{(g)} = C_g S_i^{(g-1)} C_g^\dagger$. (That these are actually the stabilizer generators for the state after the action of the first $g$ gates can be proved as in (b).) As we are dealing with Pauli strings (with a phase) throughout, each update just involves changing one (for $H$ and $S$) or two (for $CNOT$) tensor factors, which can be done with a constant number of operations. Thus, overall, this procedure uses $\mathcal{O}(nG)$ operations, which is polynomial in $n$ and $G$.

From the above reasoning, we conclude that we can efficiently simulate the effect of a Clifford circuit applied to a stabilizer state by keeping track of the stabilizers.

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

1 P. (f) Assume $Z_1$ commutes with all stabilizers of $|\psi\rangle$. What is the probability of obtaining outcome $+1$ when measuring $Z_1$ on $|\psi\rangle$?

*Hint: Start from* $Z_1|\psi\rangle = Z_1 S_i |\psi\rangle$ *for an arbitrary stabilizer generator* $S_i$ *of* $|\psi\rangle$.

*Solution*

We have by assumption that $Z_1|\psi\rangle = Z_1 S_i|\psi\rangle = S_i(Z_1|\psi\rangle)$ for all $i$. $Z_1|\psi\rangle$ is, thus, stabilized by $\{S_1, ..., S_n\}$. Since states are uniquely defined (up to global phases) by the set of $n$ stabilizers (by (b)), this implies $Z_1|\psi\rangle = \mathrm{e}^{i\varphi}|\psi\rangle$ for some phase $\varphi \in [0, 2\pi)$. Since $Z_1$ has eigenvalues $-1$ and 1, we see that $\varphi \in \{0, \pi\}$ and the probability of measuring 1 is either 0 (if $\varphi = \pi$) or 1 (if $\varphi = 0$).

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.

2 P. (g) Use the existence of such a stabilizer representation to show: If $Z_1$ does not commute with all stabilizers of $|\psi\rangle$, then the measurement outcome when measuring $Z_1$ on $|\psi\rangle$ is uniformly random.

*Hint 1: It will be useful to establish that $S_1 = S_1^\dagger$ is Hermitian. To do so, argue that $-\mathbb{I}$ cannot be part of any stabilizer group.*

*Hint 2: compute the value of $\langle\psi|Z_1|\psi\rangle$ using the anticommutation relations with the one anticommuting stabiliser.*

*Solution*

Variant 1 for proving that the measurement outcome is uniformly random: Let $S_1$ be the anticommuting stabilizer. Using that the eigenprojector onto the $+1$ eigenspace of $Z_1$ is given by $\frac{\mathbb{I}+Z_1}{2}$, we then have

$$\Pr[Z_1 = +1] = \frac{1}{2}\mathrm{tr}[(\mathbb{I} + Z_1)|\psi\rangle\langle\psi|] = \frac{1}{2}\langle\psi|(\mathbb{I} + Z_1 S_1)|\psi\rangle \tag{2}$$

$$= \frac{1}{2}\langle\psi|(\mathbb{I} - S_1 Z_1)|\psi\rangle = \langle\psi|(\mathbb{I} - Z_1)/2|\psi\rangle \tag{3}$$

$$= \Pr[Z_1 = -1] \tag{4}$$

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

Variant 2 for proving that the measurement outcome is uniformly random: Consider $\langle Z_1\rangle_\psi = \langle\psi|Z_1|\psi\rangle = \Pr[1] - \Pr[-1]$. We have (using that $S_1$ and $Z_1$ are Hermitian)

$$\langle\psi|Z_1|\psi\rangle = \langle\psi|Z_1 S_1|\psi\rangle = -\langle\psi|S_1 Z_1|\psi\rangle = 0. \tag{5}$$

In fact, this generalizes beyond $Z_1$ to the measurement of an arbitrary Pauli operator $P \in G_n$. Therefore, we see that checking commutation with the stabilizers gives us a recipe for efficiently simulating samples resulting from computational basis measurements.

## Recap

In exercise sheet 6 we have seen the concept of majorization and one central result on LOCC that builds on it. We want to use this result to build some physical intuition on what can or cannot be done using LOCC operations.

**6 P. Bonus Exercise 1.** Remember the key result

$$|\psi\rangle \xrightarrow{\text{LOCC}} |\phi\rangle \;\Leftrightarrow\; \mathrm{Tr}_B[|\psi\rangle\langle\psi|] \prec \mathrm{Tr}_B[|\phi\rangle\langle\phi|]. \tag{6}$$

In words: conversion of $|\psi\rangle$ into $|\phi\rangle$ under LOCC is possible if and only if the reduced state $\mathrm{Tr}_B[|\phi\rangle\langle\phi|]$ majorizes the reduced state $\mathrm{Tr}_B[|\psi\rangle\langle\psi|]$. Here, majorization of density matrices is understood as the fact that the two sets of ordered eigenvalues fulfill the conditions

$$\rho \succ \sigma \;\Leftrightarrow\; \boldsymbol{\lambda}(\rho) \succ \boldsymbol{\lambda}(\sigma) \;\Leftrightarrow\; \sum_{j=1}^{k} \lambda_j(\rho) \geq \sum_{j=1}^{k} \lambda_j(\sigma) \text{ for all } 1 \leq k \leq n, \tag{7}$$

with, for all $j$, $\lambda_j(\rho) \geq \lambda_{j+1}(\rho)$ and $\lambda_j(\sigma) \geq \lambda_{j+1}(\sigma)$.

1 P. (a) Can the two states $|\psi\rangle_{AB} = |0\rangle_A \otimes |+\rangle_B$ and $|\phi\rangle_{AB} = \left(\sqrt{\frac{5}{8}}|0\rangle + \sqrt{\frac{3}{8}}|1\rangle\right)_A \otimes \left(\frac{1}{\sqrt{2}}|+\rangle + \frac{e^{i\pi/6}}{\sqrt{2}}|-\rangle\right)_B$ be transformed into each other (both ways) using LOCC operations? Justify your answer based on Eq. (6). Are the states entangled?

*Solution*

Yes, those are two product states (thus not entangled), so they can be converted into each other using LOCC operations. Observe that the definition given in the question is already a valid Schmidt decomposition, with a single coefficient of value 1. Both have pure-state reduced density matrices, with only one eigenvalue of value 1. Then,

$$\sum_{j=1}^{k} s_j^2(\psi) = \sum_{j=1}^{k} s_j^2(\phi) \text{ for all } 1 \leq k \leq 2\,,$$

where $s_j(\psi)$ are the singular values, or coefficients of the Schmidt decomposition. The majorization relations go both ways, so they can be transformed into each other using only LOCC operations.

1 P. (b) What about the states $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$? Can they be converted into each other (both ways) under LOCC? And are they entangled?

*Solution*

Both states are maximally entangled, with singular values $\{1/\sqrt{2}, 1/\sqrt{2}\}$. The reduced density matrices then both have eigenvalues $\{1/2, 1/2\}$ (actually, both are the normalized single qubit identity). Again, the majorization conditions are fulfilled with equality, so both states can be converted into each other through LOCC operations.

Note that we even already know from previous exercise sheets which operation gives the desired transformation, as

$$|\Psi^-\rangle = (\mathbb{I} \otimes XZ)|\Phi^+\rangle\,.$$

1 P. (c) What about $|\Phi^+\rangle$ from (b) and $|\psi\rangle$ from (a)? Can they be converted into each other (both ways) under LOCC?

*Solution*

We have a maximally entangled state $|\Phi^+\rangle$ and a product state $|\psi\rangle$, with

$$\mathrm{Tr}_B\left[|\Phi^+\rangle\langle\Phi^+|\right] = \frac{1}{2}\mathbb{I}_2 \qquad \text{and} \qquad \mathrm{Tr}_B\left[|\psi\rangle\langle\psi|\right] = |0\rangle\langle 0|$$

with respective eigenvalues $\{1/2, 1/2\}$ and $\{1\}$. Since $1/2 < 1$ and $1/2+1/2 = 1+0$, $\mathrm{Tr}_B\left[|\Phi^+\rangle\langle\Phi^+|\right] \prec \mathrm{Tr}_B\left[|\psi\rangle\langle\psi|\right]$ but $\mathrm{Tr}_B\left[|\psi\rangle\langle\psi|\right] \not\prec \mathrm{Tr}_B\left[|\Phi^+\rangle\langle\Phi^+|\right]$. So, $|\Phi^+\rangle$ can be transformed into $|\psi\rangle$ using LOCC but not the other way around.

1 P. (d) What about $|\Phi^+\rangle$ from (b) and $|\eta\rangle = \frac{1}{\sqrt{3}}|++\rangle + \sqrt{\frac{2}{3}}|--\rangle$? Can they be converted into each other (both ways) under LOCC?

*Solution*

Both states are entangled, and

$$\mathrm{Tr}_B\left[|\Phi^+\rangle\langle\Phi^+|\right] = \frac{1}{2}\mathbb{I}_2 \qquad \text{and} \qquad \mathrm{Tr}_B\left[|\eta\rangle\langle\eta|\right] = \frac{1}{3}|+\rangle\langle+| + \frac{2}{3}|-\rangle\langle-|$$

The eigenvalues are $\{1/2, 1/2\}$ and $\{2/3, 1/3\}$ respectively, so $\mathrm{Tr}_B\left[|\Phi^+\rangle\langle\Phi^+|\right] \prec \mathrm{Tr}_B\left[|\eta\rangle\langle\eta|\right]$ but $\mathrm{Tr}_B\left[|\eta\rangle\langle\eta|\right] \not\prec \mathrm{Tr}_B\left[|\Phi^+\rangle\langle\Phi^+|\right]$. So, $|\Phi^+\rangle$ can be transformed into $|\eta\rangle$ but not the other way around.

2 P. (e) Compute the entanglement entropy of all states above (you can give an approximate numerical value if necessary). Conclude on the role of entanglement in the allowed transformations using LOCC operations.

*Solution*

Remember the definition of entanglement entropy:

$$E(|\psi\rangle_{AB}) = -\rho_A \log_2 \rho_A = -\sum_{j=1}^{d} \lambda_j \log_2 \lambda_j, \quad \text{with } \rho_A = \mathrm{Tr}_B[|\psi\rangle\langle\psi|]\,.$$

Then, for all the states considered above:

$$E(|\psi\rangle) = E(|\phi\rangle) = -1\log_2 1 = 0$$
$$E(|\Phi^+\rangle) = E(|\Psi^-\rangle) = -2\left(\frac{1}{2}\log_2\frac{1}{2}\right) = 1$$
$$E(|\eta\rangle) = -\frac{1}{3}\log_2\frac{1}{3} - \frac{2}{3}\log_2\frac{2}{3} \approx 0.918296$$

In all the cases, states can be transformed into other states with equal or less entanglement entropy, but not into states with more.

***Total Points: 24 (+6)***