Exercise Sheet 11: Quantum Phase Estimation and Gottesman-Knill

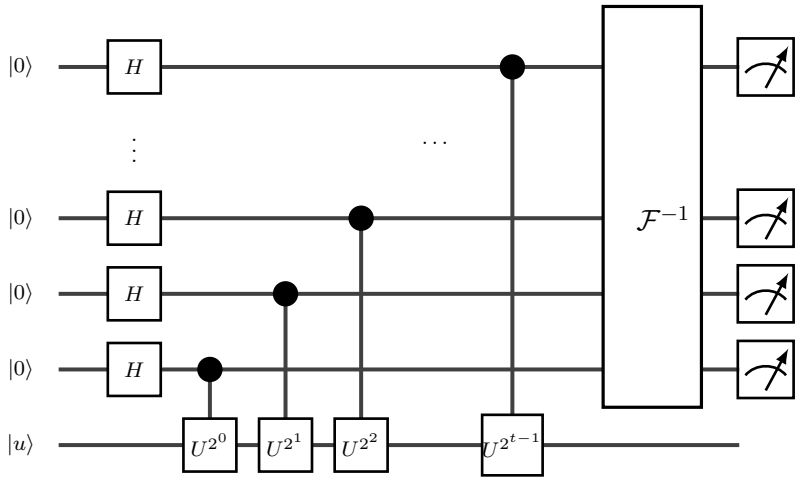
Quantum Phase Estimation

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).

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.

2 P. (c) Assume that ϕ 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 $|\phi_1 \dots \phi_t\rangle$ 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.

If the phase ϕ does not happen to have an exact t-bits representation, it is possible to show that a measurement outcome close to ϕ 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.

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

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.

2 P. (g) Show that U has eigenvalues of the form $e^{2\pi i k/r}$ 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?

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?

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 $G_n \coloneqq \{\bigotimes_{i=1}^n P_i \mid P_i \in G_1\}$ 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.

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.

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

1 P. (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

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

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 $CNOT(X \otimes \mathbb{I})CNOT^\dagger$.

[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.

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.

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 $|\psi\rangle$.

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.

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

$$|\psi\rangle \xrightarrow{\text{LOCC}} |\phi\rangle \;\Leftrightarrow\; \mathrm{Tr}_B[|\psi\rangle\langle\psi|] \prec \mathrm{Tr}_B[|\phi\rangle\langle\phi|]. \tag{2}$$

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

$$\rho \succ \sigma \;\Leftrightarrow\; \boldsymbol{\lambda}(\rho) \succ \boldsymbol{\lambda}(\sigma) \;\Leftrightarrow\; \sum_{j=1}^{k} \lambda_j(\rho) \geq \sum_{j=1}^{k} \lambda_j(\sigma) \text{ for all } 1 \leq k \leq n, \tag{3}$$

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. (2). Are the states entangled?

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?

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?

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?

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.

Total Points: 24 (+6)