Homework # 5. Physics 265

Topic: *On quantum algorithms*

Due date: Thursday April 25, 2024. Choose a subset of about 6 problems to work on. You can also create and share your own problems or work on problems from previous problem sets.

1. **Quantum Fingerprinting**

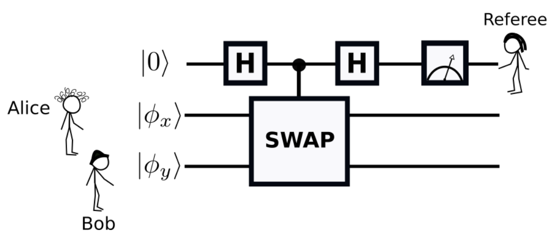


Figure 1: The referee performs a measurement to determine if Alice's state $|\phi_x\rangle$ is similar to Bob's state $|\phi_y\rangle$.

Alice holds an n-bit string x and Bob holds an n bit string y. A referee's goal is to find out if x is the same as y. Instead of sending the referee the strings themselves, Alice and Bob encode the information. Using x, Alice encodes an m qubit state $|\phi_x\rangle$ (with $m \sim \log(n)$) and Bob encodes an m qubit state $|\phi_y\rangle$. Alice and Bob have arranged to use the same encoding function and the states themselves are called *fingerprints*. The idea is that the number of qubits sent is much less than n. The two quantum states are not necessarily exactly the same nor are they necessarily orthogonal.

Alice and Bob send their quantum states (aka fingerprints) to the referee who performs the circuit in Figure 1. The initial state is

$$|\psi\rangle_{init} = |0\rangle \otimes |\phi_x\rangle \otimes |\phi_y\rangle .$$

The SWAP operation performs

$$|\phi_x\rangle \otimes |\phi_y\rangle \to |\phi_y\rangle \otimes |\phi_x\rangle$$

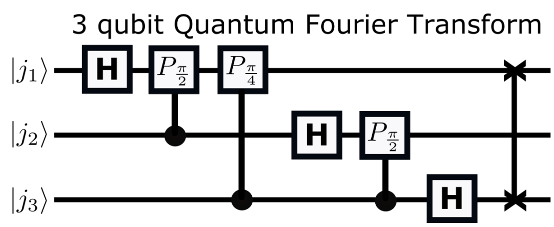
on Alice and Bob's quantum states. The SWAP operation is controlled by the referee's single qubit.

Show that the probability that the referee measures a 1 is

$$p_1 = \frac{1}{2}(1 - |\langle\phi_x|\phi_y\rangle|^2)$$

and is small if Alice and Bob's states are similar. The referee can accurately tell if the states are similar or not, particularly if a series of measurements are made. A paper on this topic here `https://arxiv.org/pdf/quant-ph/0102001.pdf`.

2. **On the Quantum Fourier Transform for 3 qubits**



In the above figure we show a circuit that computes the Quantum Fourier transform for three qubits.

The rightmost gate is a swap operation where the top and bottom bits are swapped. The single bit versions of the gates used in the transform are

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

$$P_{\frac{\pi}{2}} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

$$P_{\frac{\pi}{4}} = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{pmatrix}.$$

Create a circuit that does the inverse Fourier transform for 3 qubits.

I used the inverse of

$$P_{\frac{\pi}{4}}^{-1} = P_{-\frac{\pi}{4}} = Z P_{\frac{\pi}{2}} P_{\frac{\pi}{4}}$$

and a similar inverse for $P_{\frac{\pi}{2}}$.

3. **An eigenstate of the Quantum Fourier Transform**

Consider a finite dimensional Hilbert space with basis $|n\rangle$ and $n \in \mathbb{Z}_N$. We create a basis using a discrete Fourier transform via $|k\rangle_F = \frac{1}{\sqrt{N}} \sum_n \omega^{kn} |n\rangle$ where $\omega = e^{2\pi i/N}$ is a complex root of unity. The QFT operator

$$\hat{Q}_{FT} = \frac{1}{\sqrt{N}} \sum_{jk} \omega^{jk} |j\rangle \langle k| .$$

We construct operators that look like Pauli operators

$$\hat{X} = \sum_{n=0}^{N-1} |n+1\rangle \langle n| \tag{1}$$

$$\hat{Z} = \sum_{n=0}^{N-1} \omega^n |n\rangle \langle n| \tag{2}$$

In the above expression for $\hat{X}$, addition for $|n+1\rangle$ is modulo N.

a) Find expressions for $\hat{X}, \hat{Z}$ in the $|k\rangle_F$ basis.

Hints: use the identity $\mathbf{I} = \sum_k |k\rangle_F \langle k|_F$, the relations $\langle n|k\rangle_F = \frac{\omega^{nk}}{\sqrt{N}}$, ${}_F\langle k|n\rangle = \frac{\omega^{-nk}}{\sqrt{N}}$ and $\sum_j \omega^{jk} = N\delta_{k0}$. Sums are from 0 to $N-1$.

b) Show that

$$\hat{Q}_{FT} \hat{X} Q_{FT}^\dagger = \hat{Z} \qquad \text{and} \qquad \hat{Q}_{FT}^\dagger \hat{Z} Q_{FT} = \hat{X}.$$

Suppose you have a state vector $|\tilde{\eta}\rangle$ that is an eigenfunction of the discrete Fourier transform with eigenvalue 1. It satisfies $\hat{Q}_{FT} |\tilde{\eta}\rangle = |\tilde{\eta}\rangle$.

c) Show that $|\tilde{\eta}\rangle$ is also an eigenfunction of $Q_{FT}^\dagger$.

Given a particular state, $|\psi\rangle$, let a variance σ of an operator $\hat{f}$ be

$$\sigma(\hat{f}) = \left\langle \hat{f}^2 \right\rangle - \left\langle \hat{f} \right\rangle^2 = \langle\psi| \hat{f}^2 |\psi\rangle - (\langle\psi| \hat{f} |\psi\rangle)^2.$$

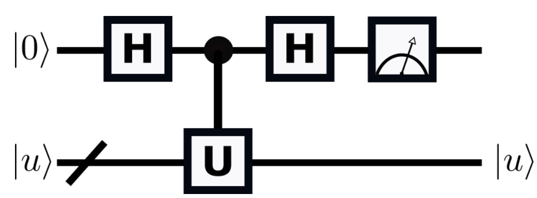
d) Show that $\sigma(\hat{X} + \hat{X}^\dagger) = \sigma(\hat{Z} + \hat{Z}^\dagger)$ and that $\sigma(\hat{X} - \hat{X}^\dagger) = \sigma(\hat{Z} - \hat{Z}^\dagger)$ where the expectation values are computed for the state $|\tilde{\eta}\rangle$.

The state $|\tilde{\eta}\rangle$ can be considered a state of minimum uncertainty. This discrete setting is relevant for computing discrete versions of Wigner or Husimi functions which are phase space analogs for quantum systems.

4. **Kitaev's phase estimation algorithm**

Suppose we can prepare $|u\rangle$, an eigenstate of the unitary operation U with eigenvalue $e^{2\pi i\phi}$. Our goal is to estimate the phase ϕ.

Consider the circuit in the following figure:



The eigenstate $|u\rangle$ could be in a multiple qubit space (that's what the slanted bar in the figure means).

a) Show that the probability of measuring 0 is $p_0 = \cos^2(\pi\phi)$.

b) Suppose that instead of applying the controlled U once, it is applied k times. What is the probability of measuring a zero?

Notes:

By repeating the measurements, it is possible to accurately measure the phase ϕ using the fraction of measurements that is measured 0 and 1.

If you remove the second Hadamard and insert a quantum Fourier transform operation on the lower bits, then you can directly measure the phase by measuring the lower bits.

5. **Accuracy of measurement in phase estimation**

In the previous problem, the probability of measuring 1 after running the circuit 1 time is

$$p_1 = 1 - p_0 = \sin^2(\pi\phi). \tag{3}$$

Suppose you run the circuit k times and make k measurements of the top qubit. The i-th measurement gives you z_i where $z_i \in \{0, 1\}$ as either 0 or 1 is measured.

You estimate the probability p_1 of measuring a 1 by computing the mean value of your measurements

$$\mu \sim \frac{1}{k} \sum_{i=1}^{k} z_i. \tag{4}$$

The error of each individual measurement is about the difference between a measurement of 0 and 1 which is about $\sigma_i \sim 1$ (where σ_i is the standard deviation of the i-th measurement).

a) Show that the uncertainty (or standard deviation) in your estimate for p_1 after running the circuit k times is

$$\sigma_{p1} \sim \frac{1}{\sqrt{k}}.$$

(Hint: propagate the error in equation 4.)

The accuracy of the measurement is usually written as $O(1/\sqrt{k})$ where k is the number of queries of the unitary transformation or equivalently the number of times the circuit is run.

b) Equation 3 can be used to estimate ϕ from p_1. Explain why the accuracy of the estimated value for ϕ is also $O(1/\sqrt{k})$.

6. **On the order of an integer modulo another integer**

Consider positive integers a, M, r such that

$$a^r = 1 \mod M$$

Show that $a^{kr} = 1 \bmod M$ for any positive integer k.

This problem is relevant for the Shor factoring algorithm that relates period finding to order finding.

7. **Quantum circuits for modular multiplication**

Consider the operation

$$f(x) = ax \mod M$$

where x, a, M are integers; $0 \le x < 2^n$ and $0 < M < 2^n$ and $0 < a < M$.

a) Show that if a, M are relatively prime,

$$|x\rangle \to \begin{cases} |f(x)\rangle & \text{for} \quad 0 \le x < M \\ |x\rangle & \text{for} \quad x \ge M \end{cases}$$

gives a permutation of basis states and so can be implemented with a set of NOT and CNOT gates.

b) What is the set of values $\{f(x)\}$, if a, M are not relatively prime?

This is relevant for the Shor factoring algorithm.

Hints: If a, M are relatively prime, their greatest common divisor is 1. In part a) you can show that $f(x) = f(y)$ implies that $x = y$. Then via the pigeon-hole principle the different $f(x)$ values are unique and you have a permutation. In part b), the set generated by $f(x)$ depends on the greatest common divisor of a, M.

Some examples.

$a = 2, M = 4$. We compute the sequence $ia \mod M$ for $i = 0, 1, ...$ The sequence $ia = 0, 2, 0, ...$ period $= 2$. Here a is prime.

$a = 3, M = 4$. $ia = 0, 3, 2, 1, 0...$ period $=4$ $= M$. Here a is prime.

$a = 3, M = 5$. $ia = 0, 3, 1, 4, 2, 0..$ period $=5$ $= M$. Here a, M are prime.

$a = 6, M = 15$. $ia = 0, 6, 12, 3, 9, 0, ...$ period $=5$.

$a = 10, M = 15$. $ia = 0, 10, 5, 0, ...$ period $=3$.

8. **On bit-wise phase shifts**

A phase gate on a single qubit is defined as

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

Consider a system with n qubits and the accompanying quantum circuit in Figure 2.

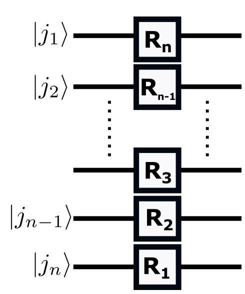


Figure 2: A circuit with phase gates applied to each qubit.

a) Show that this circuit performs a phase shift on the basis states

$$|x\rangle \to e^{2\pi i x/2^n} |x\rangle$$

where natural number x is treated as an integer in the exponential and labels the quantum state via a bit string.

b) What transformation occurs if the circuit is repeated?

9. **Quantum circuit for modular addition**

Consider the task of constructing a quantum circuit to compute

$$|x\rangle \to |(x + y) \mod 2^n\rangle$$

where y is a fixed integer constant, $0 \leq x < 2^n$ and $1 \leq y < 2^n$.

a) Show that an efficient way to do this, for a value of $y = 1$, is to first perform a quantum Fourier transform, then to apply single qubit phase shifts (as in the previous problem), then apply an inverse Fourier transform.

b) How many operations are required?

c) What values of y can be implemented this way?

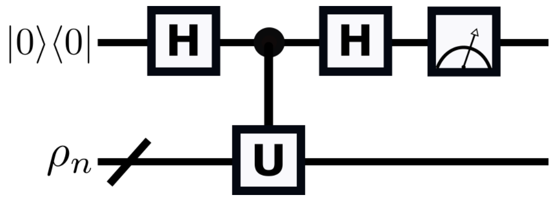
This is Problem 5.6 by Nielson and Chuang.

Hints: Order n^2 operations are required for the QFT.

I am not 100% sure about c, guessing that the operation in the previous problem at best works for $n - 1$ iterations.

10. **Measuring the trace of a unitary transformation with a noisy quantum computer**

In a previous problem we showed how to estimate the phase of an eigenvalue of an $n \times n$ unitary matrix $\mathbf{U}$.



Instead of using an eigenstate as input, we give the circuit a density matrix

$$\rho_n = \frac{\mathbf{I}}{2^n}$$

which is that of a maximally noisy or mixed state. Here n is the number of bits in the bottom part of the circuit.

The input density matrix is

$$\begin{aligned}\rho_{n+1} &= |0\rangle\langle 0| \otimes \rho_n \\ &= |0\rangle\langle 0| \otimes \frac{1}{2^n}\sum_{x=0}^{2^n-1} |x\rangle\langle x|\end{aligned}$$

a) Show that if a 0 is measured the density matrix becomes

$$\rho'_{n+1,0} = |0\rangle\langle 0| \otimes \left[\frac{(\mathbf{I}+\mathbf{U})}{2}\rho_n\frac{(\mathbf{I}+\mathbf{U}^\dagger)}{2}\right]$$

b) Show that the probability that a 0 is measured is

$$p_0 = \frac{1}{2} + \frac{1}{2^{n+2}}\operatorname{tr}\big(\mathbf{U}+\mathbf{U}^\dagger\big)$$

If the circuit is repeated you will get an increasingly accurate estimate for p_0.

c) Find $\mathfrak{Re}(\operatorname{tr} U)$ (the real part of the trace of U) in terms of p_0.

Hint: $\operatorname{tr}(\mathbf{U}) = \sum_j u_{jj}$, $\operatorname{tr}\big(\mathbf{U}^\dagger\big) = \sum_j u^*_{jj}$. Compute $\operatorname{tr}\big(\mathbf{U}+\mathbf{U}^\dagger\big)$ and write it in terms of $\mathfrak{Re}(\operatorname{tr}\{\mathbf{U}\})$.

Based on the first problem in Preskill's 2020 problem set 4.

While the first bit in the circuit must be clean, the remaining n bits can be noisy. In this setting, noise may help the calculation!

11. **Estimating the trace of a unitary transformation – continued**

a) Modify the circuit in the previous problem so that you can measure the imaginary part of the trace of $\mathbf{U}$, which is $\mathfrak{Im}(\operatorname{tr}\mathbf{U})$.

Hint: I used a phase gate $\mathbf{S} = \operatorname{diag}(1, i)$.

b) Show that with k queries of $\mathbf{U}$ it is possible to estimate both real and complex parts of the normalized trace $\operatorname{tr}(U/2^n)$ to an accuracy of $O(1/\sqrt{k})$.

Hint: Use the previous problem in this problem set.

12. **Measuring trace of an operator**

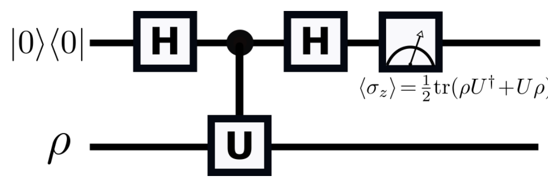


Figure 3: A series of measurements on average gives $p_0 - p_1 = \frac{1}{2}\operatorname{tr}\big(\rho(\mathbf{U}^\dagger + \mathbf{U})\big)$ where p_0 is the probability that the top qubit is in the $|0\rangle$ state and p_1 is the probability that the top qubit is in the $|1\rangle$ state. If $\mathbf{U}$ is Hermitian then the measurement gives $\operatorname{tr}(\rho\mathbf{U})$.

Assume that the measurement is done with measurement operator σ_z. A series of measurements $\langle\sigma_z\rangle$ on the top qubit gives $p_0 - p_1$ where p_0 is the probability that the first qubit is in the $|0\rangle$ state and p_1 is the probability that the first qubit is the in $|1\rangle$ state.

Show that

$$\langle\sigma_z\rangle = p_0 - p_1 = \frac{1}{2}\operatorname{tr}\big(\rho(\mathbf{U}+\mathbf{U}^\dagger)\big).$$

13. **Exponential error suppression**

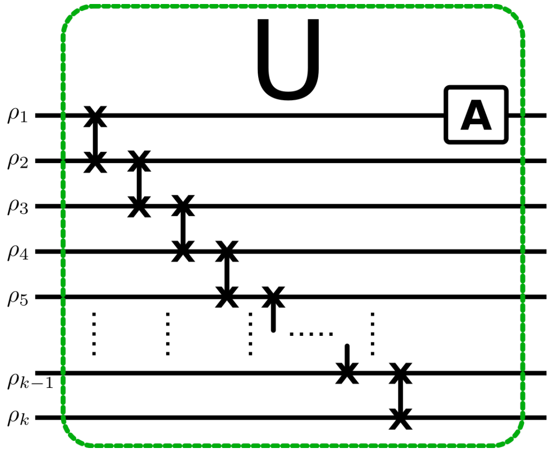


Figure 4: The unitary operator $\mathbf{U}$ operates on k systems. Input on the left are k copies of the same density operator ρ. They are swapped, then the Hermitian and unitary operator $\mathbf{A}$ is applied to the top system.

We consider a variant of the circuit in the previous problem with operator $\mathbf{U}$ shown in Figure 4.

The input on the left is

$$\rho_{\text{input}} = \rho_1 \otimes \rho_2 \otimes ... \otimes \rho_k$$

where each of the density operators ρ_i is a copy of the same density operator ρ.

a) Show that

$$\text{tr}(\mathbf{U}\rho_{\text{input}}) = \text{tr}\big(\rho^k \mathbf{A}\big)$$

Inserting the unitary operator shown in Figure 4 into Figure 3 gives a circuit shown in Figure 5.

This is known as **exponential error suppression**, as proposed by Bálint Koczor: `https://arxiv.org/pdf/2011.05942.pdf`.

As a density operator can be diagonalized, we can write

$$\rho = \sum_i p_i \left|\phi_i\right\rangle \left\langle\phi_i\right| . \tag{5}$$

where $|\phi_i\rangle$ is an orthogonal basis of ρ's eigenvectors. In this basis

$$\rho^k = \sum_i p_i^k \left|\phi_i\right\rangle \left\langle\phi_i\right| . \tag{6}$$

A setting is where

$$\rho = \lambda \left|\phi\right\rangle \left\langle\phi\right| + (1-\lambda) \left|\phi_N\right\rangle \left\langle\phi_N\right| \tag{7}$$

where $\lambda \sim 1$ corresponds to a desired computation output associated with state $|\phi\rangle$ and $(1-\lambda)$ is small and corresponds to noise giving an undesired state $|\phi_N\rangle$. The density matrix to the k-th power is

$$\rho^k = \lambda^k \left|\phi\right\rangle \left\langle\phi\right| + (1-\lambda)^k \left|\phi_N\right\rangle \left\langle\phi_N\right| . \tag{8}$$

If $\lambda \sim 1$ then $(1-\lambda)^k$ is really small. If $\text{tr}\big(\rho^k \mathbf{A}\big)$ is measured instead of $\text{tr}(\rho \mathbf{A})$, then the noise has been suppressed.

b) Does this circuit require the density operator ρ to be a single qubit system or could it describe a multi qubit system?

Hints: We illustrate how to calculate the system for $k = 2$, Consider a short version of $\mathbf{U}$ where $k = 2$ and only two density operators are swapped. The input density operator

$$\rho_{\text{input}} = \sum_i p_i \left|\phi_i\right\rangle \left\langle\phi_i\right| \otimes \sum_j p_j \left|\phi_j\right\rangle \left\langle\phi_j\right| .$$

The operation of the swap is

$$\begin{aligned} \text{SWAP}\rho_{\text{input}} &= \sum_{ij} p_i p_j \left|\phi_j\right\rangle_A \left\langle\phi_i\right|_A \left|\phi_i\right\rangle_B \left\langle\phi_j\right|_B \\ &= \sum_{ij} p_i p_j \left|\phi_j\right\rangle_A \left|\phi_i\right\rangle_B \left\langle\phi_i\right|_A \left\langle\phi_j\right|_B . \end{aligned}$$

Notice that the indices of the kets have flipped and the resulting state is entangled. We write operator

$$\mathbf{A} = \sum_{kl} a_{kl} \left|\phi_k\right\rangle_A \left\langle\phi_l\right|_A$$

in the basis of ρ's eigenvectors.

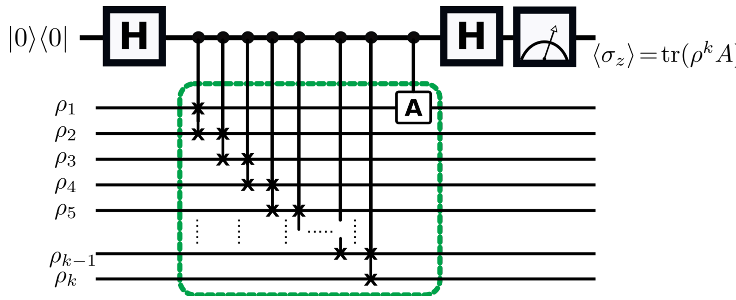


Figure 5: On the left we input k copies of a density operator ρ that includes some noise. The measurement $\langle\sigma_z\rangle = \mathrm{tr}\big(\rho^k \mathbf{A}\big)$ suppresses the noise. Here $\mathbf{A}$ is assumed to be Hermitian. The operator within the green box is the same as shown in Figure 4.

The operation of U

$$\begin{aligned}
U\rho_{\mathrm{input}} =& (A\otimes I)\mathrm{SWAP}\rho_{\mathrm{input}} \\
&= \sum_{kl} a_{kl} \left|\phi_k\right\rangle_A \left\langle\phi_l\right|_A \times \\
&\quad \sum_{ij} p_i p_j \left|\phi_j\right\rangle_A \left|\phi_i\right\rangle_B \left\langle\phi_i\right|_A \left\langle\phi_j\right|_B \\
=& \sum_{kl}\sum_{ij} a_{kl}\delta_{lj} p_i p_j \times \\
&\quad \left|\phi_k\right\rangle_A \left|\phi_i\right\rangle_B \left\langle\phi_i\right|_A \left\langle\phi_j\right|_B \\
=& \sum_{ijk} a_{kj} p_i p_j \left|\phi_k\right\rangle_A \left|\phi_i\right\rangle_B \left\langle\phi_i\right|_A \left\langle\phi_j\right|_B
\end{aligned}$$

We take the trace of both sub-systems

$$\begin{aligned}
\mathrm{tr}(U\rho_{\mathrm{input}}) &= \sum_{ijk} a_{kj} p_i p_j \left|\phi_k\right\rangle_A \left|\phi_i\right\rangle_B \left\langle\phi_i\right|_A \left\langle\phi_j\right|_B \\
&\quad \times \delta_{ki}\delta_{ij} \\
&= \sum_j a_{jj} p_j^2. \qquad (9)
\end{aligned}$$

We also compute

$$\begin{aligned}
\mathrm{tr}\big(A\rho^2\big) &= \mathrm{tr}\left(\sum_{ij} a_{ij} \left|\phi_i\right\rangle\left\langle\phi_j\right| \sum_k p_k^2 \left|\phi_k\right\rangle\left\langle\phi_k\right|\right) \\
&= \mathrm{tr}\left(\sum_{ijk} a_{ij} p_k^2 \left|\phi_i\right\rangle \delta_{jk} \left|\phi_k\right\rangle\right) \\
&= \mathrm{tr}\left(\sum_{ij} a_{ij} p_j^2 \left|\phi_i\right\rangle \left|\phi_j\right\rangle\right) \\
&= \sum_j a_{jj} p_j^2. \qquad (10)
\end{aligned}$$

Notice that equation 9 looks like equation 10. This implies that $\mathrm{tr}(U\rho) = \mathrm{tr}\big(A\rho^2\big)$ for the case with $k=2$. Your goal is to generalize this computation for $k>2$.

14. Using Grover's algorithm to solve a 3SAT problem

3SAT satisfiability problems are in the class of NP-Complete (P=can be verified in polynomial time; NP=nondeterministic polynomial time to solve; complete= other problems in NP can be reduced in polynomial time to 3SAT).

Let $\mathbf{x} = (x_1, x_2, x_3)$ where each $x_i \in \{0,1\}$ are Boolean variables. A function that returns either 0 or 1 is

$$\begin{aligned} f(\mathbf{x}) =& (x_1 \vee x_2 \vee x_3) \wedge (x_1 \vee x_2 \vee \bar{x}_3) \wedge \\ & (x_1 \vee \bar{x}_2 \vee x_3) \wedge (x_1 \vee \bar{x}_2 \vee \bar{x}_3) \end{aligned} \tag{11}$$

Our goal is use the Grover algorithm to find solutions to the above problem. That means we would like to use the Grover algorithm to help us find one or more strings for $\mathbf{x}$ that satisfy $f(\mathbf{x}) = 1$. This is a decision problem in 3-SAT.

To construct the Grover iterator we require a unitary transformation U_f that is a function of the Boolean function $f(\mathbf{x})$. The operator

$$U_f \left|\mathbf{x}, q\right\rangle \to \left|\mathbf{x}, f(\mathbf{x}) + q\right\rangle \tag{12}$$

where $\mathbf{x} \in \{0,1\}^n$ and $q \in \{0,1\}$. Equivalently

$$U_f \left|\mathbf{x}, -\right\rangle \to (-1)^{f(x)} \left|\mathbf{x}, -\right\rangle . \tag{13}$$

a) Design a circuit that performs U_f for the 3SAT problem with $f(\mathbf{x})$ given in equation 11.

Hint: It may be handy to use the relation

$$(a \vee b \vee c) = \overline{\bar{a} \wedge \bar{b} \wedge \bar{c}}$$

I found this relation helped to construct the logical function $f()$ with gates.

15. **On Fourier transforms for qutrits**

This problem is related to the hidden subgroup problem. We consider a problem similar to that of Simon's problem but with qutrits instead of qubits.

Consider a string of numbers $x = (x_1 x_2 x_3 ... x_n)$ with n digits and where each digit $x_i \in \{0,1,2\}$. With group operation $(+ \bmod 3)^n$ operating on each digit, the strings are the elements of the group $G = \mathbb{Z}_3^{\otimes n}$. For example the group operation is $\mathbf{x} + \mathbf{y} = \mathbf{z}$ and each digit individually satisfies $z_i = (x_i + y_i) \bmod 3$.

a) Characterize the group $\hat{G}$ of 1d representations of G.

b) What is a Fourier basis $\{|\chi_k\rangle\}$ for the group in terms of qutrit basis states $|x_1 x_2 ... x_n\rangle$?

Consider a subgroup $H \subset G$ generated by an n-bit string $\mathbf{s} = (s_1 s_2 ... s_n)$. The subgroup H has elements $\{\mathbf{0}, \mathbf{s}, 2\mathbf{s}\}$ where $\mathbf{0}$ refers to a string of zeros.

c) Consider the subgroup H generated by

$$\mathbf{s} = (1,0,2,1).$$

The element

$$\mathbf{s} + \mathbf{s} = (2,0,1,2)$$

is also in the subgroup. The subgroup H contains three elements,

$$H = \{(0,0,0,0), (1,0,2,1), (2,0,1,2)\}.$$

Find all the elements of $H^\perp$, the group of representations in $\hat{G}$ that act like the identity when restricted to members of H.

Hints: Show that you need to find values of $\mathbf{k} = (k_1 k_2 k_3 k_4)$ that satisfy

$$\mathbf{k} \cdot \mathbf{s} = 0 \bmod 3 \quad \text{and} \quad \mathbf{k} \cdot (\mathbf{s} + \mathbf{s}) = 0 \bmod 3.$$

Then find values of $\mathbf{k}$ that satisfy both relations. The order of $H^\perp$ should divide the order of the group G.

16. **On Quadratization of Boolean functions and the Ising model**

Consider the following optimization function

$$f(x_1, x_2, x_3, x_4, x_5) = \alpha x_1 x_3 x_4 x_5 - \beta x_1 x_2 x_3 x_4 x_5$$

with α, β positive real coefficients. The variables are Boolean $x_i \in \{0,1\}$ for $i = 1,2,3,4,5$.

a) With some extra variables, construct a **quadratic** optimization minimization function that has the same minima as $f()$.

b) Suppose your quadratic optimization function $g()$ has two minima $\mathbf{x}^*$ and $\mathbf{y}^*$ and they have the same value, $g(\mathbf{x}^*) = g(\mathbf{y}^*)$. Here $\mathbf{x}^*, \mathbf{y}^*$ are Boolean strings. Using your related Ising model Hamiltonian, you run an adiabatic algorithm to find the ground state. You perform a measurement of the final resulting ground state. You can run the algorithm multiple times and measure the resulting ground state multiple times. What are the results of these measurements?

Hints: The ground state would be degenerate. During the adiabatic evolution, the two lowest energy levels would approach each each until they are equal.

17. **Propose and solve your own problem**