Science Coffee House, IIT Kanpur

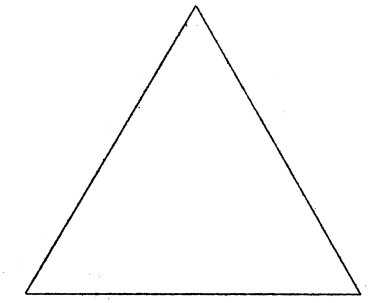
Group Theory and Quantum Error Correction
Task 0

INSTRUCTIONS

- *Questions are made to build up your understanding; referring is fine, but copying is discouraged*
- *You are strongly encouraged to do this task alone, but if you do collaborate with someone else, both should mention their collaborator's name in the submitted document*
- *You may resort to any (classical) computation when needed*
- *Everything not forbidden is allowed!* [1]

A Group of Questions

Consider an equilateral triangle,



[1] A certain physics professor (based) in IITK

Let F be the set of all functions (transformations in 3D) such that the triangle's shape, size, position, and orientation remains the same. (Hint: Rotation by 120° about the center is one such transformation, while rotation by 180° is not).

Question 1: Find all such transformations/functions (i.e., all elements of F). Also, show that all of them can only be rotations or reflections (flipping about an axis). Simple arguments will suffice for the second part.
Hint: Doing nothing is also a transformation (identity transformation). Also, rotation by θ and rotation by $2\pi + \theta$ are the same transformation.

Motivated by these symmetries of an object, we define the notion of a group; a group G is a non-empty set along with a binary operation ($\circ$) defined on the set such that it satisfies the following axioms:

1. $\forall a, b \in G, a \circ b \in G$ (Closure)
2. $\forall a, b, c \in G, (a \circ b) \circ c = a \circ (b \circ c)$ (Associativity)
3. $\exists\ e \in G$ s.t. $a \circ e = e \circ a = a\ \forall a \in G$ (Identity)
4. $\forall a \in G\ \exists\ a^{-1}$ s.t. $a \circ a^{-1} = a^{-1} \circ a = e$ (Inverse)

A simple example would be the set of integers under addition, $(\mathbb{Z}, +)$. One can easily see all the axioms are satisfied,

1. Sum of two integers is an integer
2. Addition is associative
3. Addition of 0 gives the same integer, so 0 is the identity
4. For any integer a, addition of $-a$ gives us 0

To make this idea more lucid, you can look at the symmetries of the equilateral triangle from the perspective of these axioms:

Question 2: Taking the set F and the group operation as composition $f \circ g$ (apply g then apply f) of the functions/transformations, show that it forms a group. How many elements does the group have? (order of a group denoted by $|F|$)
Hint: Show that all the axioms are obeyed

Sometimes, a subset of a group G with the same binary operation also turns out to be a group, i.e., it satisfies all the group axioms. These groups are naturally called subgroups of G. Ex: Even integers along with 0 form a subgroup $(2\mathbb{Z}, +)$ of $(\mathbb{Z}, +)$.

Question 3: Check the above example.

Question 4: Find any one non-trivial (neither $\{e\}$ nor G itself) subgroup of $(F, \circ)$ ($\circ$ is composition) and show it satisfies the necessary conditions.

A coset of a subgroup H of G using an element $g \in G$ is the set of elements $gH = \{g \circ h : \forall h \in H\}$. Ex: Cosets of $2Z$ using 1 gives the set of odd integers.

Question 5: Find all cosets of the subgroup you found in Question 4. Also, show that any two of these cosets are either the same or disjoint.

Notice that the cardinality (number of elements) of all cosets of a subgroup H is equal to the order of H.

Question 6: Show that no two elements of a coset can be equal, and using this, prove the above statement.

Question 7: Show that the union of all cosets from Question 5 gives us the entire group F.

Notice from Questions 5, 6, and 7 that the order of our group, $|F|$, is equal to the order of a subgroup $|H|$ multiplied by the number of distinct cosets of H. This turns out to be true for any finite group and gives us an astonishing result; the order of a subgroup of a group has to divide the order of the group perfectly. This is known as **Lagrange's Theorem**.

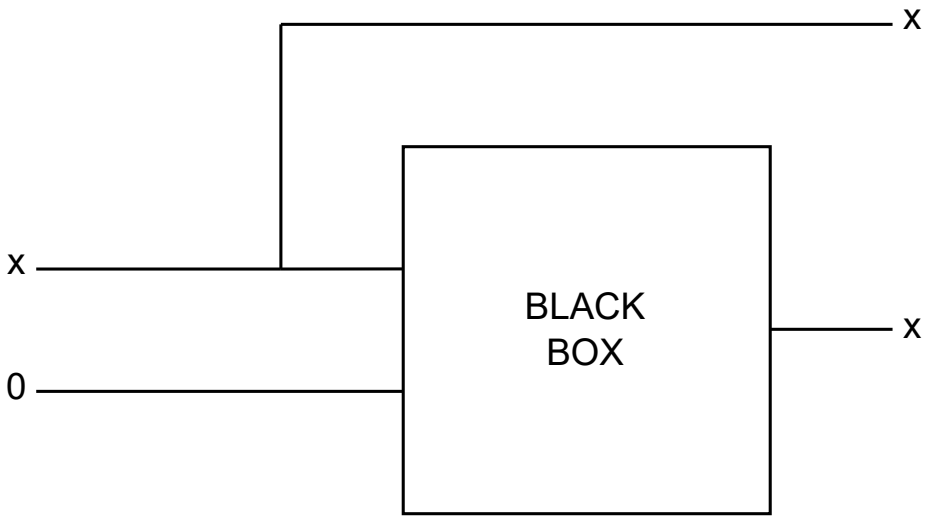
Question 8: Given a group G with $|G| = p$ where p is prime, how many subgroups will G have? What are their orders?

A bit of cloning

A 'bit' or a binary digit is the most basic unit of information used in classical computers. A bit can either be **OFF** (0) or **ON** (1).

Suppose one wants to clone or copy a bit; what must they do?

A circuit of the following form accomplishes our task,



Question 1: What must be the 'Black Box' for the cloning to be successful for any input bit x?
Hint: Think of the basic circuit gates

States in quantum mechanics are represented by norm (length) 1 vectors, written as $\vec{v} = |v\rangle = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$ (do note that the vector components can be complex). Like a classical bit, a 2-state quantum system is called a 'qubit'. The basis vectors of a qubit are the **OFF** ($|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$) and the **ON** ($|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$) states.

The remarkable property one can observe at first glance is that states which are neither **OFF** nor **ON** are allowed! For instance, $|v\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$ is a valid state in which our system is in a uniform mix of **OFF** and **ON** (this is the property of quantum superposition!).

Operations on qubits are done by linear transformations (particularly unitary transformations) on the vector space in which our states lie. So, our circuit gates are now linear transformations.

Like the gate you found in the classical case, we want a gate that acts on two qubits. To understand the working of such a gate, we first need to understand how to describe the state of 2 qubits. Suppose the first qubit is in state $|v\rangle$ and the second qubit is in state $|u\rangle$, so we write the combined state of both these qubits as $|v\rangle\,|u\rangle$ (order in which they are written matters).

Question 2: Given $|v\rangle = \begin{pmatrix} 1/2 \\ \sqrt{3}/2 \end{pmatrix}$, and $|u\rangle = \begin{pmatrix} \sqrt{3}/2 \\ 1/2 \end{pmatrix}$, explicitly write $|v\rangle\,|u\rangle$.
Hint: Expand both vectors in their basis using the ket ($|0\rangle, |1\rangle$) *notation. Also, refer to the next paragraph for an example.*

Let's say we want to clone $|\psi\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$ using $|0\rangle$ as the state being copied into. We can write our initial state as $|\psi\rangle\,|0\rangle = (a\,|0\rangle + b\,|1\rangle)\,|0\rangle = a\,|0\rangle\,|0\rangle + b\,|1\rangle\,|0\rangle$. Now, the quantum analog of the copying gate we will use is the controlled not (CNOT) gate. The CNOT gate acts as follows: if the first (control) qubit is in the $|0\rangle$ state, it does nothing; and if the first qubit is in the $|1\rangle$ state, it flips the second (target) qubit's state.

Question 3: Find the action of CNOT on $|v\rangle\,|u\rangle$ that you found in the last question.
Hint: The first vector represents the first qubit, and the second vector represents the second qubit. Also, remember that quantum gates are linear.

Now, let's try and clone our qubit.

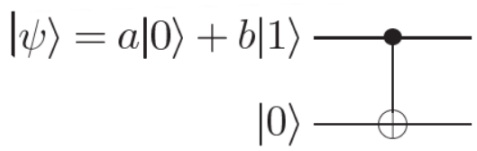


Figure 1: The upper line represents the first qubit, and the lower line represents the second qubit. The symbol in the middle is the CNOT gate, where the upper line is the control qubit and the lower line is the target qubit.

Question 4: As shown in the above circuit, we try to clone $|\psi\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$ to another qubit $|0\rangle$ using the CNOT gate. Find the output of the circuit (final state of both the qubits). Is our cloning successful?
Hint: For our cloning to be successful, the final state has to be $|\psi\rangle\,|\psi\rangle$.

If you solve the above question correctly, you would notice that it is impossible to clone a general state! This is the remarkable **Quantum No Cloning Theorem**. Notice this has a prominent effect on quantum error correction; think classical redundancy codes. These are now obsolete because making copies of our state is now impossible.

Quantum State Tomography

So we can't clone a general state; what a bummer :((But is all lost? No, suppose we have N identical qubits, and we want to make a lot of its copies. Clearly, we can't clone it. Instead, we can perform measurements to find the (close to) exact state of the qubit, then simply make as many such qubits as we need.

Let us first understand how measurements work in quantum mechanics. Given an 'equally mixed' qubit $|\psi\rangle = \frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle$, if we want to measure whether the qubit is **OFF** or **ON**, what can we expect? Since it is 'equally mixed', we get either **OFF** or **ON** with equal probabilities. In quite the contrast with our classical world, measurements in quantum mechanics are probabilistic! This means that even if we know our state accurately, it is impossible to be certain what the measurement outcome will be; we only know the probability of a particular outcome.

In general, for a state $|\psi\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$, the probability of **OFF** is $|a|^2$, and the probability of **ON** is $|b|^2$. This is where the restriction of the norm of a vector being 1 comes from.

Now, suppose we have N identical qubits in the state $|\psi\rangle = \begin{pmatrix} a \\ be^{i\phi} \end{pmatrix}$ where a and b are non-negative reals. How do we estimate a, b, ϕ?

Question 1: Using $N/2$ qubits and measurements in **OFF** and **ON** basis, estimate a and b.
Hint: Take n_0 *to be the number of* ***OFF*** *outcomes.*

There is nothing inherently special about the **OFF** and **ON** basis (this is also called the **computational basis**); another basis widely used in quantum computing is the **Hadamard basis**, where $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, and $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$ are the basis vectors.

Question 2: Write $|\psi\rangle$ explicitly in the Hadamard basis.

Once we have our wavefunction in the Hadamard basis, we can easily find the probability of our qubit being in the $|+\rangle$ or $|-\rangle$ state.

Question 3: Using the remaining $N/2$ qubits and measurements in Hadamard basis, estimate ϕ. Use values of a and b obtained from Question 1.
Hint: Take n_+ to be the number of + outcomes.

Congratulations! You have found all the parameters of the state $|\psi\rangle$ and can now make as many qubits initialized to this state as you want.

BONUS: Find confidence interval: We have estimated the state, but how good is our estimate? Find 95% confidence intervals for the parameters we estimated in Questions 1 and 3. Comment on the scaling with N.
Hint: Use Bayes' Theorem. Assume uniform prior and make any necessary approximations.