Assignment 4
Due date: 11:59pm, November 10, 2022

1. **Strictly periodic functions on $\mathbb{Z}_m$: a few warm-up questions [12 points; 4 each].** Define a function $f : \mathbb{Z}_m \to \mathbb{Z}_m$ to be *strictly r-periodic* if it has this property:

   $f(a) = f(b)$ if and only if $a - b$ is a multiple of r (for any $a, b \in \mathbb{Z}_m$).

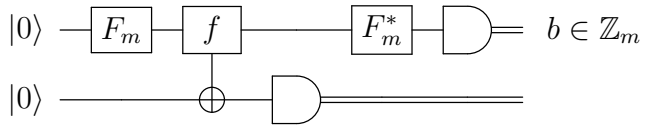
   Consider the case where $m = 35$, $r = 7$, and $s = 5$.

   (a) Give an example of a function $f : \mathbb{Z}_{35} \to \mathbb{Z}_{35}$ that is strictly 7-periodic. You may give the truth table or you may give a list of 35 numbers, that we'll interpret as $f(0), f(1), f(2), \ldots, f(34)$. Although any strictly 7-periodic function will get full marks here, please try to make your function look as irregular as you can subject to the condition of being strictly 7-periodic.

   (b) What are the *colliding sets* of your function in part (a)? List these sets. Also, each of colliding sets for your example satisfies the property that it of the form $\{a, a + 7, a + 2{\cdot}7, \ldots, a + (s - 1){\cdot}7\}$ for some $a \in \mathbb{Z}_{35}$.

   (c) List all $b \in \mathbb{Z}_{35}$ such that $b{\cdot}7 = 0$ (in mod 35 arithmetic).

2. **Strictly periodic functions on $\mathbb{Z}_m$: behavior of a quantum circuit [12 points].** Suppose that $m = r \cdot s$ where r and s are distinct primes and $f : \mathbb{Z}_m \to \mathbb{Z}_m$ is *strictly r-periodic* (as defined in question 1). Consider this quantum circuit, which acts on two m-dimensional registers, and where F_m is the Fourier transform.



   Show that the output of this circuit (more specifically, the outcome of the top measurement) is a uniformly-distributed random element of the set $\{b \in \mathbb{Z}_m : \text{such that } b{\cdot}r = 0\}$.

   (Although you are not asked to show it here, this is one approach for determining the periodicity r of f: compute the greatest common divisor of b and m. It turns out that, for at least half of the possible values of b, $\gcd(b, m) = r$.)

   Hint: You may assume the fact that, for any $k \geq 2$ and $a \in \{1, 2, \ldots, k-1\}$, it holds that

$$\sum_{j=0}^{k-1} \left(e^{2\pi i/k}\right)^{a \cdot j} = 0. \tag{1}$$

3. **Some basic questions about density matrices [12 points; 4 each].**

   (a) Show that for any $d \times d$ matrix ρ that is normal, positive, and for which $\mathrm{Tr}(\rho) = 1$ there exist d-dimensional state vectors $|\psi_0\rangle, |\psi_1\rangle, \ldots, |\psi_{d-1}\rangle$ and a probability vector $(p_0, p_1, \ldots, p_{d-1})$ such that

$$\rho = \sum_{k=0}^{d-1} p_k |\psi_k\rangle\langle\psi_k|. \tag{2}$$

   (b) Suppose that ρ_1 and ρ_2 are 2×2 density matrices with the property that, if measured in the computational basis, their outcome probabilities are exactly the same. Does that imply that $\rho_1 = \rho_2$? Show that the answer is no, by giving two different density matrices for which these outcome probabilities are nevertheless the same.

   (c) Now suppose that ρ_1 and ρ_2 are 2×2 density matrices with the property that, if measured in the computational basis, the outcome probabilities are the same *and* if measured in the Hadamard basis the outcome probabilities also are the same. Does this imply that $\rho_1 = \rho_2$? Either state that the answer is no and give a counterexample, or state that the answer is yes, and prove it.

4. **Kraus operators for two channels [12 points; 6 each].**

   (a) Consider the quantum channel that takes a qubit as input and produces as output a qubit in state $\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$ (regardless of what the input state is). Give a description of this channel in the Kraus form. That is, give Kraus operators for this channel.

   (b) Consider the quantum channel that takes a qubit as input and produces as output a qubit in state $|0\rangle\langle 0|$ (regardless of what the input state is). Give a description of this channel in the Kraus form. That is, give Kraus operators for this channel.

5. **Applying a qubit channel to one qubit of a 2-qubit system [12 points].**
   Let $\chi : \mathbb{C}^{2\times 2} \to \mathbb{C}^{2\times 2}$ be a quantum channel that maps qubits to qubits, with Kraus operators $A_1, A_2, \ldots, A_k$. Applying χ to the *second* qubit of a 2-qubit system is defined as $I \otimes \chi : \mathbb{C}^{4\times 4} \to \mathbb{C}^{4\times 4}$ with Kraus operators $I \otimes A_1, I \otimes A_2, \ldots, I \otimes A_k$. Show that applying $I \otimes \chi$ to $\rho \in \mathbb{C}^{4\times 4}$ results in

$$\begin{pmatrix} \chi(\rho_{00}) & \chi(\rho_{01}) \\ \chi(\rho_{10}) & \chi(\rho_{11}) \end{pmatrix}, \qquad \text{where} \qquad \rho = \begin{pmatrix} \rho_{00} & \rho_{01} \\ \rho_{10} & \rho_{11} \end{pmatrix} \tag{3}$$

   is the decomposition of ρ into four 2×2 blocks (i.e., ρ_{00}, ρ_{01}, ρ_{10}, $\rho_{11} \in \mathbb{C}^{2\times 2}$).

6. **(This is an optional question for bonus credit)**
   Expressing a qutrit as an equally weighted mixture of pure states [6 points].
   Let ρ be an arbitrary 3×3 matrix that is the density matrix of the mixed state of a qutrit. Show that there exist three normalized vectors $|\psi_1\rangle, |\psi_2\rangle, |\psi_3\rangle \in \mathbb{C}^3$, representing pure states, such that $\rho = \frac{1}{3}|\psi_1\rangle\langle\psi_1| + \frac{1}{3}|\psi_2\rangle\langle\psi_2| + \frac{1}{3}|\psi_3\rangle\langle\psi_3|$. Note that $|\psi_1\rangle, |\psi_2\rangle, |\psi_3\rangle$ are not required to be orthogonal here.

   There is a solution that can be explained in less than one page. If you submit a solution to this question, please do not exceed two pages.