Solutions to the Practice Problems for Midterm 2

C191 Introduction to Quantum Computing, Fall 2025

1 Mixed States

1.1

Consider the quantum states $\rho = |+\rangle\langle+|$ and $\sigma = I/2$. Construct a (projective) measurement that produces different outcomes on ρ and σ.

Solution

One set of projectors that will give different outcome probabilities for ρ and σ is $\{|+\rangle\langle+|, |-\rangle\langle-|\}$. This solution is non-unique.

In fact, the only complete set of single-qubit projectors that does NOT work for this would be that of measurement in the standard basis, $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$.

1.2

Construct a purification for the mixed state $\rho = \frac{1}{14}|00\rangle\langle 00| + \frac{5}{14}|01\rangle\langle 01| + \frac{4}{7}|11\rangle\langle 11|$. That is, construct a pure state $|\psi\rangle_{AB}$ such that

$$\mathrm{Tr}_B\left[|\psi\rangle\langle\psi|\right] = \rho.$$

Solution

$$|\psi\rangle_{AB} = \sqrt{\frac{1}{14}}|00\rangle \otimes |00\rangle + \sqrt{\frac{5}{14}}|01\rangle \otimes |01\rangle + \sqrt{\frac{4}{7}}|11\rangle \otimes |11\rangle$$

Note that this solution is non-unique. Any orthonormal set of vectors can be used in the subspace B of the constructed pure state $|\psi\rangle_{AB}$.

2 Decoherence and the Density Matrix.

Consider a qubit in the state $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$. Suppose that some external physical process can apply a single Z gate at some time $t > 0$, but does so in a probabilistic manner. The probability distribution for having applied the Z gate by time t is given by $p(t) = \frac{1}{2} - \frac{1}{2}e^{-t/\tau}$.

2.1

Write down the density matrix $\rho(t)$ for the qubit at time $t \geq 0$, specifying all elements of the matrix.

Solution

We have $\rho(t) = (1 - p(t))\, |+\rangle\langle+| + p(t)Z\, |+\rangle\langle+|\, Z$. Writing this out in full gives

$$\rho(t) = \frac{1}{2}\,|0\rangle\langle 0| + \frac{1}{2}e^{-t/\tau}\,|0\rangle\langle 1| + \frac{1}{2}e^{-t/\tau}\,|1\rangle\langle 0| + \frac{1}{2}\,|1\rangle\langle 1|\,.$$

2.2

Write down the expectation values $\langle X\rangle$ and $\langle Z\rangle$ for all times t.

Solution

We have

$$\langle X\rangle = \mathrm{tr}(X\rho(t)) = \mathrm{tr}\left[\frac{1}{2}\,|1\rangle\langle 0| + \frac{1}{2}e^{-t/\tau}\,|1\rangle\langle 1| + \frac{1}{2}e^{-t/\tau}\,|0\rangle\langle 0| + \frac{1}{2}\,|0\rangle\langle 1|\right] = e^{-t/\tau}$$

and

$$\langle Z\rangle = \mathrm{tr}(X\rho(t)) = \mathrm{tr}\left[\frac{1}{2}\,|0\rangle\langle 0| + \frac{1}{2}e^{-t/\tau}\,|0\rangle\langle 1| - \frac{1}{2}e^{-t/\tau}\,|1\rangle\langle 0| - \frac{1}{2}\,|1\rangle\langle 1|\right] = 0.$$

3 The SWAP test.

The swap gate S on two qubits is defined first on product vectors, $S : |a\rangle \otimes |b\rangle \mapsto |b\rangle \otimes |a\rangle$ and then extended to sums of product vectors by linearity.

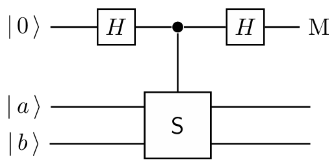
3.1

Show that $P_{\pm} = \frac{1}{2}(\mathbb{1} \pm S)$ are two orthogonal projectors (i.e. $P_+^2 = P_+$, $P_-^2 = P_-$ and $P_+P_- = 0$.

Solution

Using $S^2 = \mathbb{I}$, we get: $P_+P_- = 0$ and $P_{\pm}^2 = P_{\pm}$, which confirms that $P_{\pm}$are orthogonal projectors.

Consider the following "swap-test" quantum circuit composed of two Hadamard gates, one controlled S operation and the measurement M in the computational basis,



The state vectors $|a\rangle$ and $|b\rangle$ of the target qubits are normalised but not orthogonal to each other.

3.2

Step through the execution of this circuit, writing down quantum states of the three qubits after each computational step. What are the probabilities of observing 0 or 1 when the measurement M is performed?

Solution

Stepping through the circuit

$$\begin{aligned}
|0\rangle|a\rangle|b\rangle &\mapsto \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|a\rangle|b\rangle && (2)\\
&\mapsto \frac{1}{\sqrt{2}}(|0\rangle|a\rangle|b\rangle + |1\rangle|b\rangle|a\rangle) && (3)\\
&\mapsto \frac{1}{2}((|0\rangle + |1\rangle)|a\rangle|b\rangle + (|0\rangle - |1\rangle)|b\rangle|a\rangle) && (4)\\
&= |0\rangle\frac{1}{2}(|a\rangle|b\rangle + |b\rangle|a\rangle) + |1\rangle\frac{1}{2}(|a\rangle|b\rangle - |b\rangle|a\rangle). && (5)
\end{aligned}$$

From the last expression we can see that the outcomes 0 and 1 are observed with probabilities

$$\text{Probability of } 0 = \left|\frac{1}{2}(|a\rangle|b\rangle + |b\rangle|a\rangle)\right|^2 = \frac{1}{2}\left(1 + |\langle a \mid b\rangle|^2\right) \tag{1}$$

$$\text{Probability of } 1 = \left|\frac{1}{2}(|a\rangle|b\rangle - |b\rangle|a\rangle)\right|^2 = \frac{1}{2}\left(1 - |\langle a \mid b\rangle|^2\right) \tag{2}$$

3.3

As the orthogonal projectors P_+ and P_- add to the identity, any vector decomposes into a sum of two vectors in the two subspaces V_+ and V_- onto which P_+ and P_- project. Verify that after the whole circuit above and measuring the first qubit as 0 or 1, the second and third register collapse to the normalized components of $|a\rangle \otimes |b\rangle$ in the two subspaces V_+ and V_-.

Solution

Applying the projectors onto $|a\rangle|b\rangle$ gives the components:

$$P_+(|a\rangle|b\rangle) = \frac{1}{2}\left(|a\rangle|b\rangle) + |b\rangle|a\rangle\right) \tag{3}$$

$$P_-(|a\rangle|b\rangle) = \frac{1}{2}\left(|a\rangle|b\rangle) - |b\rangle|a\rangle\right). \tag{4}$$

The output state $|0\rangle \otimes 1/2(|a\rangle|b\rangle + |b\rangle|a\rangle) + |1\rangle \otimes 1/2(|a\rangle|b\rangle - |b\rangle|a\rangle)$ shows clearly that the second and third register collapse to the normalized components of $|a\rangle \otimes |b\rangle$ in the two subspaces V_+ and V_-.

3.4

Does the measurement result $M = 0$ imply that $|a\rangle$ and $|b\rangle$ are identical? Does the measurement result $M = 1$ imply that $|a\rangle$ and $|b\rangle$ are not identical?

Solution

Outcome $M = 0$ occurs with probability $\frac{1}{2}\left(1 + |\langle a \mid b\rangle|^2\right)$ even when the two states are different. Outcome $M = 1$ can only occur if the two states are not identical.

3.5

Suppose an efficient quantum algorithm encodes information about a complicated graph into a pure state of a qubit. Graphs which are isomorphic are mapped into the same state of the qubit. Given two complicated graphs your task is to check if they are isomorphic. You can run the algorithm as many times as you want and you can use the "swap-test" circuit. How would you accomplish this task?

Solution

You are essentially testing if the states of the two qubits are identical or not. Result $M = 0$ is inconclusive but $M = 1$ indicates that the two states are different. After many runs without $M = 1$ you can declare that the states are the same.

3.6

Show that $\mathrm{Tr}\left(S(\rho_a \otimes \rho_b)\right) = \mathrm{Tr}(\rho_a \rho_b)$.

Solution

We first use the diagonal forms of the density matrices: $\rho_a = \sum_i p_i |a_i\rangle \langle a_i|$ and $\rho_b = \sum_j q_j |b_j\rangle \langle b_j|$ to show that

$$\mathrm{Tr}\, S\left(\rho_a \otimes \rho_b\right) = \sum_{ij} p_i q_j \,\mathrm{Tr}\, S\left(|a_i\rangle \langle a_i| \otimes |b_j\rangle \langle b_j|\right) = \sum_{ij} p_i q_j \,\mathrm{Tr}\left(|b_j\rangle \langle a_i| \otimes |a_i\rangle \langle b_j|\right),$$

which can be written as

$$\begin{aligned}\sum_{ij} p_i q_j \left|\langle a_i \mid b_j\rangle\right|^2 &= \sum_{ij} p_i q_j \langle a_i \mid b_j\rangle \langle b_j \mid a_i\rangle \\ &= \operatorname{Tr}\left(\mid a_i\rangle \langle a_i \mid\mid b_j\rangle \langle b_j \mid\right) \\ &= \operatorname{Tr}\left(\sum_i p_i \left|a_i\right\rangle \left\langle a_i\right|\right)\left(\sum_j q_j \left|b_j\right\rangle \left\langle b_j\right|\right) = \operatorname{Tr} \rho_a \rho_b\end{aligned}$$

3.7

Instead of the state $|a\rangle \otimes |b\rangle$ the two target qubits are prepared in some mixed state $\rho_a \otimes \rho_b$. Show that the probability of getting the measurement outcome 0 is:

$$\frac{1}{2}\left(1+\operatorname{Tr} \rho_a \rho_b\right)$$

Solution

The projector $\frac{1}{2}(\mathbb{I}+S)$ projects onto the subspace corresponding to the measurement outcome 0.

$$\operatorname{Pr}(0)=\operatorname{Tr}\left[\frac{1}{2}(\mathbb{I}+S)\left(\rho_a \otimes \rho_b\right)\right]=\frac{1}{2}\left[1+\operatorname{Tr} S\left(\rho_a \otimes \rho_b\right)\right]$$

And using the previous part this becomes:

$$\operatorname{Pr}(0)=\frac{1}{2}\left(1+\operatorname{Tr} \rho_a \rho_b\right).$$

3.8

Does the measurement result $M=1$ imply that ρ_a and ρ_b are not identical?

Solution

No, it does not. The density operator $\rho \otimes \rho$ is not symmetric, i.e. it is not supported on the symmetric subspace. Indeed, the result $M=1$, that is, a successful projection on the antisymmetric subspace, will occur with probability

$$\operatorname{Pr}(1)=\frac{1}{2}\left[1-\operatorname{Tr}\left(\rho_a \rho_b\right)\right]$$

Now assume ρ_a and ρ_b are identical: $\rho_a=\rho_b \equiv \rho$. For a mixed state ρ, we have that $\operatorname{Tr} \rho^2<1$, hence

$$\operatorname{Pr}(1)=\frac{1}{2}\left(1-\operatorname{Tr} \rho^2\right)>0$$

for any mixed state ρ, even if $\rho \otimes \rho$ is not a symmetric state, that is, it is not a density matrix supported on the symmetric subspace.

4 Quantum error correction I

4.1

What is the maximum number of (mutually) independent stabilizers one can find on n qubits? Why?

Solution

We can only find n. Each independent stabilizer divides our Hilbert space dimension by 2. On n qubits, the Hilbert space is 2^n dimensional, so we can only halve the dimension of our Hilbert n times. That is, we can only find n independent stabilizers. (Note that you can achieve this bound, e.g, $Z_1, Z_2, \ldots, Z_n$ work).

4.2

Consider the stabilizers $\{Z_1Z_2, Z_2Z_3\}$ on 3 qubits. Construct a basis for the code subspace corresponding to these stabilizers.

Solution

$\{|000\rangle, |111\rangle\}$

4.3

Consider the stabilizer generators for a 7-qubit code

$$\begin{aligned} g_1 &= IIIXXXX \\ g_2 &= IXXIIXX \\ g_3 &= XIXIXIX \\ g_4 &= IIIZZZZ \\ g_5 &= IZZIIZZ \\ g_6 &= ZIZIZIZ \end{aligned}$$

What will the results of the syndrome measurements be if the error Z_1X_6 happens?

Solution

We need to check if $Z_1X_6 = ZIIIIXI$ commutes or anti-commutes with all of the syndromes. It is sufficient to only check for the first and sixth qubits.

$$\begin{aligned} g_1 &= +1, \quad g_3 = -1, \quad g_5 = -1 \\ g_2 &= +1, \quad g_4 = -1, \quad g_6 = +1 \end{aligned}$$

4.4

Construct two undetectable Pauli errors for the above 7-qubit code that mutually anticommute (i.e., construct a logical X and logical Z for the code subspace). (Hint: Every stabilizer has an even number of Paulis and there is an odd number of qubits).

Solution

$X_1X_2 \ldots X_7$ and $Z_1Z_2 \ldots Z_7$.

5 Quantum Error Correction II

5.1

Find a stabilizer for $|-\rangle$ and two independent stabilizers for $\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$.

Solution

Stabilizer for $|-\rangle$ is $-X$. Stabilizers for $\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$ are $-XX, ZZ$.

5.2

The 5-qubit code is defined via the following set of independent stabilizer generators:

$$g_1 = XZZXI, \quad g_2 = IXZZX, \quad g_3 = XIXZZ, \quad g_4 = ZXIXZ$$

Let $|\bar{\psi}\rangle$ be a state encoded in the 5-qubit code. What are the syndromes for the state $X_2 Z_3 |\bar{\psi}\rangle$?

Solution

The syndromes are $g_1 = -1, g_2 = +1, g_3 = -1, g_4 = +1$.

5.3

Find a set of 2 independent stabilizer generators for the following stabilizer code: $\{\alpha |000\rangle + \beta |111\rangle : \alpha, \beta \in \mathbb{C}\}$.

Solution

The stabilizer generators are Z_1Z_2, Z_2Z_3 (or any 2 different ones from $\{Z_1Z_2, Z_2Z_3, Z_1Z_3\}$).

5.4

Define a basis for the above code as $|\bar{0}\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$, $|\bar{1}\rangle = \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)$. Find a logical Z gate for this code, i.e. a 3-qubit gate G such that $G(\alpha |\bar{0}\rangle + \beta |\bar{1}\rangle) = \alpha |\bar{0}\rangle - \beta |\bar{1}\rangle$. Also find a logical X gate for this code.

Solution

Logical Z gate: XXX (or any one from $\{XXX, -YYX, -YXY, -XYY\}$). Logical X gate: ZZZ (or any one from $\{ZZZ, Z_1 = ZII, Z_2 = IZI, Z_3 = IIZ\}$).

6 Quantum Error Correction III

Consider the four-qubit code (the [[4, 1, 2]] code) defined by the stabilizer generators

$$g_1 = XXXX, \quad g_2 = ZIZI, \quad g_3 = IZIZ.$$

6.1

Show that $|0_L\rangle = \frac{1}{\sqrt{2}}(|0000\rangle + |1111\rangle)$ and $|1_L\rangle = \frac{1}{\sqrt{2}}(|1010\rangle + |0101\rangle)$ are in the codespace.

Solution

$$g_1|0_L\rangle = g_2|0_L\rangle = g_3|0_L\rangle = |0_L\rangle \tag{5}$$

and also

$$g_1|1_L\rangle = g_2|1_L\rangle = g_3|1_L\rangle = |1_L\rangle \tag{6}$$

so $|0_L\rangle$ and $|1_L\rangle$ are simultaneous +1 eigenstates of g_1, g_2, and g_3, which means they are codewords.

Parts (b) - (d) of this question mainly focus on the analysis of Pauli X error, but similar arguments apply to other Pauli errors.

6.2

What are the resulting states starting from $|0_L\rangle$ and $|1_L\rangle$ if a Pauli X error occurred on the first qubit? What are the results of the syndrome measurements if this happened?

Solution

$X_1 = XIII$ on $|0_L\rangle$:

$$XIII|0_L\rangle = \frac{1}{\sqrt{2}}(|1000\rangle + |0111\rangle). \tag{7}$$

$X_1 = XIII$ on $|1_L\rangle$:

$$XIII|1_L\rangle = \frac{1}{\sqrt{2}}(|0010\rangle + |1101\rangle). \tag{8}$$

The results of syndrome measurements are $g_1 = +1$, $g_2 = -1$, $g_3 = +1$.

6.3

What are the resulting states starting from $|0_L\rangle$ and $|1_L\rangle$ if a Pauli X error occurred on the third qubit? What are the results of the syndrome measurements if this happened?

Solution

$X_3 = IIXI$ on $|0_L\rangle$:

$$IIXI|0_L\rangle = \frac{1}{\sqrt{2}}(|0010\rangle + |1101\rangle). \tag{9}$$

$X_3 = IIXI$ on $|1_L\rangle$:

$$IIXI|1_L\rangle = \frac{1}{\sqrt{2}}(|1000\rangle + |0111\rangle). \tag{10}$$

The results of syndrome measurements are $g_1 = +1$, $g_2 = -1$, $g_3 = +1$.

6.4

Write down a valid logical X (logical bitflip) operator for this code. Use this to show that the two pairs of states obtained from part (b) and (c) are related by a logical X error.

Solution

$X_L = XIXI$, but other operators such as $X_L' = gX_L$ with $g \in \{g_1^a g_2^b g_c^c | a, b, c \in \{0, 1\}\}$ are also valid.

With any valid X_L, we find that

$$X_L X_1 |0_L\rangle = X_3 |0_L\rangle \tag{11}$$

and also

$$X_L X_1 |1_L\rangle = X_3 |1_L\rangle \tag{12}$$

6.5

Argue why it is impossible for this four-qubit code to correct every possible single-qubit Pauli X error.

Solution

Pauli X on 1st qubit and Pauli X on 3rd qubit have the same syndrome outcomes and bring codewords in the same error subspaces. Therefore one cannot distinguish the location of the error. Furthermore, if a correction operation is applied to correct Pauli X on the 1st qubit, it would result in a logical bitflip error if the X error was on the 3rd qubit and vice versa.

Alternatively, one can directly use Knill-Laflamme to show it violate the error-correcting condition

$$\langle 0_L|X_1X_3|1_L\rangle = \langle 0_L|X_1X_LX_1|1_L\rangle = \langle 0_L|X_1X_1X_L|1_L\rangle = \langle 0_L|X_L|1_L\rangle = \langle 0_L|0_L\rangle = 1 \neq 0. \quad (13)$$

6.6

We have seen in class that at least five physical qubits are needed in order to have a quantum code that is able to correct every single-qubit Pauli error. Now let's prove this in a simpler situation, where the quantum code is non-degenerate, i.e. different noise operators in the set of correctable errors would bring the codewords to *orthogonal* error subspaces. In other words, $\langle i_L|E_l^\dagger E_k|i_L\rangle = 0$ for any different correctable error operators E_k and E_l, and any state $|i_L\rangle$ in the codespace. Now prove that in order for a quantum code encoding one logical qubit to be able to correct any single-qubit Pauli errors (X, Y, Z on any qubit), at least five physical qubits are needed.

(**Hint:** Use a dimension-counting argument to compare the dimensions available with n qubits and the dimensions needed to form orthogonal error subspaces.)

Solution

For a non-degenerate code, different errors map a codeword to orthogonal states. In order for the errors to be correctable, Knill-Laflamme theorem further implies $E_k|i_L\rangle$ for different E_k and $|i_L\rangle$ should all be orthogonal. If the code consists of n physical qubits and can correct any single-qubit Pauli errors, there are then $3n$ correctable errors. The code should at least encode one logical qubit, so the codespace has dimension 2. It requires then a dimension of $2 \times 3n + 2$ in the Hilbert space to be able to have these orthogonal error subspaces and the codespace. However, the n-qubit system is of dimension 2^n. So we must have

$$2^n \geq 2(3n+1), \quad (14)$$

which means $n \geq 5$.

7 Quantum Fourier Transform

Recall that the Quantum Fourier Transform is an $N \times N$ matrix ($N = 2^n$ for n qubits) QFT_N where the entry at ith row and jth column ($i, j = 0, \ldots, N-1$) equals $\omega_N^{i \cdot j}/\sqrt{N}$ ($\omega_N = e^{2\pi i/N}$).

7.1

Show that $\mathrm{QFT}_2 = H$.

Solution

In matrix form,

$$\mathrm{QFT}_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = H.$$

7.2

Does $\mathrm{QFT}_{2^n} |0^n\rangle = H^{\otimes n} |0^n\rangle$ when $n > 1$?

Solution

Yes, $\mathrm{QFT}_{2^n} |0^n\rangle = H^{\otimes n} |0^n\rangle$:

$$\mathrm{QFT}_{2^n} |0^n\rangle = \sum_{x \in \{0,1\}^n} \frac{\omega_N^0}{\sqrt{N}} |x\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle = H^{\otimes n} |0^n\rangle .$$

7.3

Does $\mathrm{QFT}_{2^n} = H^{\otimes n}$ when $n > 1$?

Solution

No, $\mathrm{QFT}_{2^n} \neq H^{\otimes n}$ when $n > 1$. For example, QFT_{2^n} has complex entries whereas $H^{\otimes n}$ only has real entries.

7.4

Show that QFT_N is a unitary.

Solution

It suffices to show that the columns of QFT_N are orthonormal. We will use the following two facts about roots of unity:

1. $\sum_{j=0}^{N-1} \omega_N^{-kj} \omega_N^{kj} = N$ for any k
2. $\sum_{j=0}^{N-1} \omega_N^{kj} = 0$ for any integer $1 \leq k \leq N-1$.

Let's call the columns of QFT_n $|Q_0\rangle, \ldots, |Q_N\rangle$. First, the columns are normal (unit vectors):

$$\langle Q_k | Q_k \rangle = \frac{1}{N} \sum_j \omega_N^{-kj} \omega_N^{kj} = 1.$$

Next, we show that they are pairwise orthogonal: If $k_2 > k_1$,

$$\langle Q_{k_1} | Q_{k_2} \rangle = \frac{1}{N} \sum_j \omega_N^{-k_1 j} \omega_N^{k_2 j} = \frac{1}{N} \sum_j \omega_N^{(k_2 - k_1) j} = 0.$$

7.5

Let $|\psi\rangle = \sum_{k=0}^{N-1} \alpha_k |k\rangle$ be a state. Suppose $\mathrm{QFT}_N |\psi\rangle = \sum_{k=0}^{N-1} \beta_k |k\rangle$. Show that the coefficients satisfy

$$\beta_k = \sum_\ell \alpha_\ell \frac{\omega_N^{k\ell}}{\sqrt{N}}.$$

Solution

First, the action of QFT_N on $|k\rangle$ is

$$\mathrm{QFT}_N |k\rangle = \sum_\ell \frac{\omega_N^{\ell k}}{\sqrt{N}} |\ell\rangle$$

by the definition of matrix multiplication. So by linearity,

$$\mathrm{QFT}_N |\psi\rangle = \sum_k \alpha_k \left(\sum_\ell \frac{\omega_N^{\ell k}}{\sqrt{N}} |\ell\rangle \right) = \sum_\ell \left(\sum_k \alpha_k \frac{\omega_N^{\ell k}}{\sqrt{N}} \right) |\ell\rangle .$$

Switching just the names of the two variables ℓ and k, then we see that

$$\mathrm{QFT}_N |\psi\rangle = \sum_k \left(\sum_\ell \alpha_\ell \frac{\omega_N^{k\ell}}{\sqrt{N}} \right) |k\rangle$$

So β_k satisfies the given form.

7.6

Let $|\psi + t\rangle = \sum_{k=0}^{N-1} \alpha_k |(k+t) \mod N\rangle$ be a shifted version of $|\psi\rangle$ ($t > 0$ is an integer). Show that

$$\mathrm{QFT}_N |\psi + t\rangle = \sum_{k=0}^{N-1} \omega_N^{kt} \beta_k |k\rangle .$$

Conclude that $\mathrm{QFT}_N |\psi\rangle$ and $\mathrm{QFT}_N |\psi + t\rangle$ generate the same measurement outcome distribution when measuring in the standard basis $\{|0\rangle, |1\rangle, \ldots, |N-1\rangle\}$.

Solution

First, the action of QFT_N on $|(k+t) \mod N\rangle$ is

$$\mathrm{QFT}_N |k + t \mod N\rangle = \sum_\ell \frac{\omega_N^{\ell(k+t)}}{\sqrt{N}} |\ell\rangle$$

by the definition of matrix multiplication. So by linearity,

$$\mathrm{QFT}_N |\psi\rangle = \sum_k \alpha_k \left(\sum_\ell \frac{\omega_N^{\ell(k+t)}}{\sqrt{N}} |k\rangle \right) = \sum_\ell \omega_N^{\ell t} \left(\sum_k \alpha_k \frac{\omega_N^{\ell k}}{\sqrt{N}} \right) |\ell\rangle .$$

Switching just the names of the two variables ℓ and k, then we see that

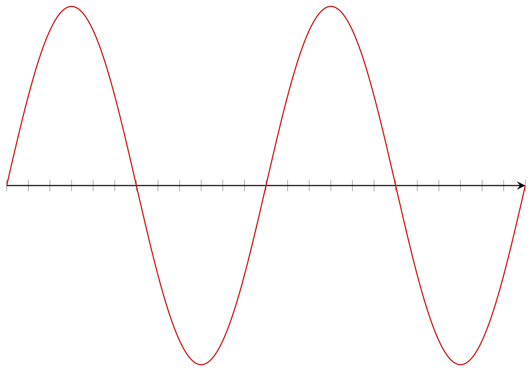
$$\mathrm{QFT}_N |\psi\rangle = \sum_k \omega_N^{kt} \left(\sum_\ell \alpha_\ell \frac{\omega_N^{k\ell}}{\sqrt{N}} \right) |k\rangle .$$

So indeed

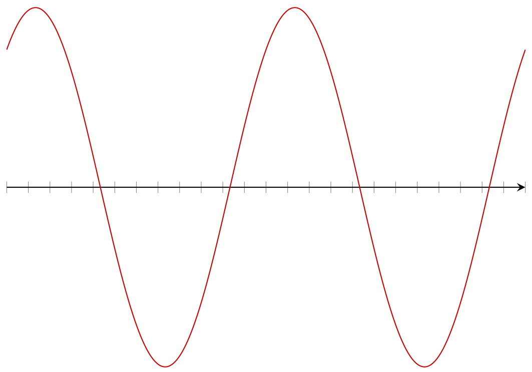
$$\mathrm{QFT}_N |\phi\rangle = \sum_k \omega_N^{kt} \beta_k |k\rangle .$$

Because the probability of measuring $|k\rangle$ is its amplitude's *absolute value* squared, then the additional ω_N^{kt} factor does not change this probability, i.e., both states give the same measurement outcome distribution.

The result above says that if the state $|\psi\rangle$ is like the following:



and the state $|\psi = t\rangle$ is a shifted version of $|\psi\rangle$:



then performing a Fourier transform on the two states and measuring in the computational basis will result in the same distribution of outcomes.

7.7

Show that if $|\psi\rangle$'s amplitudes are periodic with period t (i.e., $\alpha_k = \alpha_{(k+t) \mod N}$), then it is equal to the state $|\psi + t\rangle$:

$$|\psi + t\rangle = \sum_{k=0}^{N-1} \alpha_k \left|(k+t) \mod N\right\rangle .$$

Solution

Using the fact that the amplitudes are periodic $\left(\alpha_k = \alpha_{(k+t) \bmod N}\right)$, we can express $|\psi + t\rangle$ as

$$|\psi + t\rangle = \sum_{k=0}^{N-1} \alpha_{(k+t) \bmod N} |(k+t) \mod N\rangle$$

In order, the summation sums the states $|t\rangle, |t+1\rangle, \ldots |N-1\rangle, |0\rangle, |1\rangle, \ldots |t-1\rangle$ with the appropriate amplitudes. But the order in which we sum them up does not matter, so we can take the summation from $|0\rangle$ to $|N-1\rangle$ instead of $|t\rangle$ to $|N-1\rangle$ followed by $|0\rangle$ to $|t-1\rangle$. That is, we can write the state as

$$|\psi + t\rangle = \sum_{k'=0}^{N-1} \alpha_{k'} \left|k'\right\rangle$$

But this is the same as $|\psi\rangle$, so we are done.

7.8

Recall the N'th root of unity $\omega_N = e^{i\frac{2\pi}{N}}$. Show that $\omega_N^r = 1$ if and only if r is an integer multiple of N.

Solution

If $r = \ell N$ for some integer ℓ, then

$$\omega_N^r = \omega_N^{\ell N} = \left(\omega_N^N\right)^\ell = 1^\ell = 1.$$

If $r = \ell N + k$ for some integer ℓ and $0 < k < N$, then

$$\omega_N^r = \omega_N^{\ell N + k} = \omega_N^{\ell N}\omega_N^k = \omega_N^k \neq 1.$$

7.9

Recall (from part 7.6) that the quantum Fourier transforms of $|\psi\rangle$ and $|\psi + t\rangle$ are related in the following way. If

$$\mathrm{QFT}_N |\psi\rangle = \sum_{k=0}^{N-1} \beta_k |k\rangle\,,$$

then

$$\mathrm{QFT}_N |\psi + t\rangle = \sum_{k=0}^{N-1} \omega_N^{kt}\beta_k |k\rangle\,.$$

Show that if $|\psi\rangle = |\psi + t\rangle$, then $\mathrm{QFT}_N |\psi\rangle$ has nonzero amplitudes only on integer multiples of N/t. That is, show that if $\beta_k \neq 0$, then $k = \ell(N/t)$ for some integer ℓ.

Solution

Because $|\psi\rangle = |\psi + t\rangle$, then their quantum Fourier transforms are also equal. That is,

$$\sum_{k=0}^{N-1} \beta_k|k\rangle = \sum_{k=0}^{N-1} \omega_N^{kt}\beta_k|k\rangle$$

But this means that if $\beta_k \neq 0$, then ω_N^{kt} must be 1 , otherwise the two states would be different. So in this case, $kt = \ell N$ for some integer ℓ.

7.10

Argue how the previous parts imply the following fact about the quantum Fourier transform applied to quantum states with *periodic* amplitudes:

Suppose that you have a quantum state

$$|\psi\rangle = \sum_{k=0}^{N-1} \alpha_k |k\rangle$$

with periodic amplitudes ($\alpha_k = \alpha_{(k+t) \bmod N}$ for some $1 \leq t \leq N-1$). Note that periodicity requires that t divides N.

Then

$$\mathrm{QFT}_N |\psi\rangle = \sum_{k=0}^{N-1} \beta_k |k\rangle$$

where $\beta_k \neq 0$ only if k is an integer multiple of N/t.

Solution

By part 7 the t-periodicity gives $|\psi\rangle = |\psi + t\rangle$, and part 9 then immediately implies that $\mathrm{QFT}_N |\psi\rangle$ has non-zero amplitudes only at integers $k = \ell \frac{N}{t}$.