Part I: Classical Computing

PROBLEM 1: **20 Points**

Suppose your research team requires 100% certainty before making a conclusion about the machine. For parts a, b, c, answer in a format similar to the one seen in the example above using lists of $f(...) = 0/1$

(a) **[5 pts]** For $n = 3$, list a set queried inputs and outputs for a machine $f(x)$ such that the team can conclude the machine is balanced, and compute the units of time used.

(b) **[5 pts]** For $n = 4$, list a set queried inputs and outputs for a machine $f(x)$ such that the team can conclude the machine is constant, and compute the units of time used.

(c) **[5 pts]** For $n = 7$, list a set of queried inputs and outputs for a function $f(x)$ such that would NOT allow the team to make a conclusion about the machine.

(d) **[5 pts]** Let $n = 2$ (so $N = 4$). Suppose you make two classical queries: $f(00)$ and $f(01)$. Both queries return 0. Determine whether the machine is constant, balanced, or unknown.

Solution:

(a) A machine can be concluded to be balanced the moment we see two different outputs (since a constant machine only outputs entirely 0s or entirely 1s).
Example list: $f(000) = 0, f(001) = 1$.
Time used: 2 units.

(b) For $n = 4$, there are $N = 16$ inputs. A balanced machine has exactly half its outputs as 0s (which is 8). To prove the machine is constant, we must query 9 inputs and receive the same output for all 9 (making it impossible to be balanced).
Example list: $f(0000) = 0, f(0001) = 0, f(0010) = 0, f(0011) = 0, f(0100) = 0, f(0101) = 0, f(0110) = 0, f(0111) = 0, f(1000) = 0$.
Time used: 9 units.

(c) For $n = 7$, $N = 128$. A balanced machine has 64 zeros and 64 ones. To NOT make a conclusion, we could query up to 64 inputs and receive the exact same output (since it could be a constant machine, or it could be a balanced machine where we just happened to pick all 64 of the zeros).
Example list: Any list of $k \leq 64$ distinct queries all returning 0, such as $f(0000000) = 0, \ldots, f(0111111) = 0$ (64 queries).

(d) For $n = 2$, a balanced machine has two 0s and two 1s. We have found two 0s. The remaining two untested inputs might both be 1 (meaning the machine is balanced) or both be 0 (meaning the machine is constant). Thus, the machine is **unknown**.

Scoring Rubric

- **(a) [5 pts]:** Award 5 points for providing a list with at least one 0 and one 1, and stating the corresponding correct units of time (e.g., 2 units). No partial credit is awarded.
- **(b) [5 pts]:** Award 5 points for listing 9 distinct queries with identical outputs and stating 9 units of time. No partial credit is awarded.
- **(c) [5 pts]:** Award 5 points for listing anywhere from 1 to 64 distinct queries with identical outputs. No partial credit is awarded.
- **(d) [5 pts]:** Award 5 points for correctly stating "unknown". No partial credit is awarded.

PROBLEM 2: **15 Points**

(a) **[5 pts]** For a general n-bit machine, suppose you query it k times, and every single query returns 0. Determine the minimum number of units of time k you must spend to absolutely guarantee the machine is constant, expressed in terms of n.

(b) **[10 pts]** Imagine the machine is not pre-programmed, but is instead controlled by a malicious adversary who decides the outputs on every turn you query to force you to make as many queries as possible, while still abiding by the Constant/Balanced rules. Justify your bound from part (a) for a worst-case scenario and describe how the adversary would respond.

Solution:

(a) $k = 2^{n-1} + 1$.

(b) An adversary wanting to maximize queries will try to delay your certainty for as long as possible. Certainty happens when you either see two different outputs (proves balanced) or you see more than 2^{n-1} identical outputs (proves constant).

The adversary will choose to return the exact same output (e.g., 0) for every query you make. By doing this, for the first 2^{n-1} queries, you cannot make a conclusion because the machine could still be balanced (you just happened to find all its 0s). Only on the query $2^{n-1} + 1$ does the adversary run out of 0s if they are pretending to be balanced. At this step, whatever they answer will guarantee the machine's identity, meaning the absolute worst-case scenario forces exactly $2^{n-1} + 1$ queries.

Scoring Rubric

- **(a) [5 pts]:** Award 5 points for the correct expression $2^{n-1} + 1$. No partial credit is awarded.
- **(b) [10 pts]:** Award 5 points for identifying that the adversary's optimal strategy is to return the same value repeatedly. Award 5 points for explaining that this strategy maintains ambiguity until exactly the $(2^{n-1} + 1)$-th query.

PROBLEM 3: **25 Points**

For a modern 64-bit input ($n = 64$), the total number of inputs N can be treated as infinite. Reaching the deterministic bound from Problem 1 is not reasonable. Instead, your team decides to select inputs uniformly at random. If you query the machine k times and get the same output every time, you will guess "Constant."

(a) **[5 pts]** Let $n = 10$. You pick 3 distinct inputs entirely at random. If the machine is actually balanced, determine the probability that all 3 of your queries will return 0. (Leave your answer as a fraction).

(b) **[10 pts]** Find the general, closed-form expression for the probability that k distinct random queries all return 0, assuming the machine is actually balanced (for an arbitrary n).

(c) **[10 pts]** As N approaches infinity ($N \to \infty$), the probability of being "fooled" by a balanced machine after k identical outputs approaches a simple limit. Find this limit in terms of k. Using this limit, what is the minimum number of random queries k needed to be at least 99.9% confident that the machine is Constant?

Solution:

(a) For $n = 10$, $N = 1024$. A balanced machine has 512 zeros. The probability of picking 3 zeros without replacement is:

$$\frac{512}{1024} \times \frac{511}{1023} \times \frac{510}{1022} = \frac{1}{2} \times \frac{511}{1023} \times \frac{255}{511} = \frac{255}{2046} = \frac{85}{682}$$

(b) Let $N = 2^n$. The closed form is given by combinations or a falling factorial:

$$\frac{\binom{N/2}{k}}{\binom{N}{k}} \quad \text{or} \quad \prod_{i=0}^{k-1} \frac{N/2 - i}{N - i}$$

(c) As $N \to \infty$, sampling without replacement approaches sampling with replacement. The limit of the probability is $(1/2)^k$. To be 99.9% confident, the probability of being fooled must be less than 0.001:

$$(1/2)^k < 0.001 \implies 2^k > 1000 \implies k = 10$$

Scoring Rubric

- **(a) [5 pts]:** Award 5 points for the correct unsimplified equivalent or fully simplified fraction 85/682. No partial credit is awarded.
- **(b) [10 pts]:** Award 10 points for the correct expression (either combinations or product notation is accepted). No partial credit is awarded.
- **(c) [10 pts]:** Award 5 points for the correct limit $(1/2)^k$. Award 5 points for finding $k = 10$.

PROBLEM 4:

20 Points

Real-world classical computers suffer from thermal noise. Suppose the wire connecting your computer to the machine is degraded. Every time a bit travels down the wire, there is a probability $p = 0.1$ that the bit flips (a 0 becomes a 1, or a 1 becomes a 0).

(a) **[5 pts]** You query the *exact same* input x three times in a row to check for errors. The wire gives you the sequence: $[0, 0, 1]$. Assuming the true value of $f(x)$ is equally likely to be 0 or 1 before you started, compute the probability that the true output is actually 0 given the earlier sequence.

(b) **[15 pts]** Let $n = 3$. Assume the machine is equally likely to be Constant or Balanced. You query all distinct inputs exactly once. The wire gives you seven 0s and one 1.
Show that the machine is more likely to be constant than balanced by comparing specific values.

Solution:

(a) Let T be the true value. $P(T = 0) = P(T = 1) = 0.5$. By Bayes' Theorem:

$$P(\text{Data}|T = 0) = (0.9)(0.9)(0.1) = 0.081$$

$$P(\text{Data}|T = 1) = (0.1)(0.1)(0.9) = 0.009$$

$$P(T = 0|\text{Data}) = \frac{0.081}{0.081 + 0.009} = \frac{0.081}{0.090} = 0.9$$

The probability is 90% or 0.9.

(b) For $n = 3$, $N = 8$. Data D is seven 0s, one 1.

If the machine is Constant: It is either all 0s (C_0) or all 1s (C_1).

$$P(D|C_0) = \binom{8}{1}(0.9)^7(0.1)^1 \approx 8(0.478)(0.1) \approx 0.3826$$

$$P(D|C_1) = \binom{8}{1}(0.1)^7(0.9)^1 = 8(0.0000001)(0.9) = 7.2 \times 10^{-7} \approx 0.00000072$$

So $P(D|\text{Constant}) \approx \frac{1}{2}(0.3826) + \frac{1}{2}(0.00000072) \approx 0.1913$.

If the machine is Balanced: True output has four 0s and four 1s. To get seven 0s and one 1, the single 1 could come from a true 0 flipping (and the true 1s all flipping to 0), or from a true 1 staying 1 (and the other three true 1s flipping, while true 0s stay 0).

$$P(D|\text{Balanced}) = \left[\binom{4}{3}(0.9)^3(0.1)^1 \times \binom{4}{4}(0.1)^4\right] + \left[\binom{4}{4}(0.9)^4 \times \binom{4}{3}(0.1)^3(0.9)^1\right]$$

$$= [4(0.729)(0.1) \times 0.0001] + [1(0.6561) \times 4(0.001)(0.9)] \approx 0.000029 + 0.002362 \approx 0.00239$$

Since $0.1913 > 0.00239$, the machine is much more likely to be constant.

Scoring Rubric

- **(a) [5 pts]:** Award 5 points for the correct probability 0.9 (or 9/10 or 90%). No partial credit is awarded.
- **(b) [15 pts]:**
  - Award 5 points for accurately calculating the probability of the data given a Constant machine (≈ 0.191).
  - Award 5 points for accurately calculating the probability of the data given a Balanced machine (≈ 0.0024).
  - Award 5 points for concluding it is more likely constant based on a comparison of these specific computed values.

Part II: Quantum Computing

PROBLEM 5: **25 Points**

Consider a 2-bit system ($n = 2$). The inputs are $\{00, 01, 10, 11\}$.

(a) **[5 pts]** Compute the expression for the uniform superposition state $|\psi\rangle$.

(b) **[5 pts]** Suppose f is a balanced function defined by $f(00) = 0$, $f(01) = 1$, $f(10) = 0$, $f(11) = 1$. Compute $U_f|\psi\rangle$.

(c) **[5 pts]** Suppose f is a constant function defined by $f(00) = 0$, $f(01) = 0$, $f(10) = 0$, $f(11) = 0$. Compute $U_f|\psi\rangle$.

(d) **[5 pts]** Define the **Total Phase** of a superposition as the sum of its coefficients (e.g., for $a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$, the Total Phase is $a + b + c + d$). Calculate the Total Phase for your results in (b) and (c).

(e) **[5 pts]** Based on your answer in (d), propose a rule a team could use to identify the machine type.

Solution:

(a) $|\psi\rangle = |00\rangle + |01\rangle + |10\rangle + |11\rangle$.

(b) The operator maps to $(-1)^{f(x)}$.
$U_f|\psi\rangle = |00\rangle - |01\rangle + |10\rangle - |11\rangle$.

(c) $U_f|\psi\rangle = |00\rangle + |01\rangle + |10\rangle + |11\rangle$.

(d) For (b): $1 - 1 + 1 - 1 = 0$.
For (c): $1 + 1 + 1 + 1 = 4$.

(e) **Proposed rule:** Calculate the Total Phase of the system. If it is 0, the machine is balanced. If its absolute value is 4 (or 2^n), the machine is constant.

Scoring Rubric

- **(a) [5 pts]:** Award 5 points for the correct un-normalized sum of the four states. No partial credit is awarded.
- **(b) [5 pts]:** Award 5 points for the correct final state with alternating signs. No partial credit is awarded.
- **(c) [5 pts]:** Award 5 points for the correct final state with all positive signs. No partial credit is awarded.
- **(d) [5 pts]:** Award 5 points for providing the values 0 and 4. No partial credit is awarded.
- **(e) [5 pts]:** Award 5 points for formulating a general distinguishing rule based on checking if Total Phase equals 0 or $\pm 2^n$.

PROBLEM 6: **10 Points**

Suppose we have a 3-bit system ($n = 3$). The inputs are $\{000, 001, \ldots, 111\}$. The uniform superposition is $|\psi\rangle = \sum_{x \in \{0,1\}^3} |x\rangle$.

(a) **[5 pts]** If the machine is balanced, calculate how many states $|x\rangle$ will have a coefficient of $+1$ and how many will have a coefficient of -1 after applying U_f.

(b) **[5 pts]** Calculate the Total Phase of $U_f|\psi\rangle$ for this balanced machine.

Solution:

(a) For $n = 3$, there are $2^3 = 8$ possible states. Since the machine is balanced, exactly half of the outputs are 0 and half are 1. The 0s become $+1$ and 1s become -1. Thus, there are **four states with** $+1$ and

four states with -1.

(b) Total Phase $= 4(+1) + 4(-1) = 0$.

Scoring Rubric

- **(a) [5 pts]:** Award 5 points for stating four $+1$ and four -1. No partial credit is awarded.
- **(b) [5 pts]:** Award 5 points for calculating a Total Phase of 0. No partial credit is awarded.

PROBLEM 7: **10 Points**

[10 pts] Prove that the operator U_f is linear. That is, show that for any two superpositions $|\psi_1\rangle$ and $|\psi_2\rangle$ and constants a, b, the relation $U_f(a|\psi_1\rangle + b|\psi_2\rangle) = aU_f|\psi_1\rangle + bU_f|\psi_2\rangle$ holds.

Solution: Let $|\psi_1\rangle = \sum c_x|x\rangle$ and $|\psi_2\rangle = \sum d_x|x\rangle$. The linear combination is:

$$a|\psi_1\rangle + b|\psi_2\rangle = \sum_x (ac_x + bd_x)|x\rangle$$

Applying U_f by definition scales each basis state $|x\rangle$ by $(-1)^{f(x)}$:

$$U_f(a|\psi_1\rangle + b|\psi_2\rangle) = \sum_x (ac_x + bd_x)(-1)^{f(x)}|x\rangle$$

We can distribute this term algebraically:

$$= \sum_x \left[ac_x(-1)^{f(x)}|x\rangle + bd_x(-1)^{f(x)}|x\rangle\right]$$

$$= a\sum_x c_x(-1)^{f(x)}|x\rangle + b\sum_x d_x(-1)^{f(x)}|x\rangle$$

$$= aU_f|\psi_1\rangle + bU_f|\psi_2\rangle$$

This demonstrates perfect linearity.

Scoring Rubric

- **[10 pts]:**
  - Award 4 points for expressing the generic superpositions correctly as sums over basis states.
  - Award 4 points for properly applying U_f to the summed components algebraically.
  - Award 2 points for separating the result back into $aU_f|\psi_1\rangle + bU_f|\psi_2\rangle$.

PROBLEM 8: **15 Points**

Let $f : \{0,1\}^n \to \{0,1\}$ be an arbitrary function. We define the Total Phase of the resulting state $U_f|\psi\rangle$ (where $|\psi\rangle$ is the uniform superposition of all 2^n inputs) as S.

(a) **[5 pts]** For a general n, find the maximum possible absolute value of the Total Phase $|S|$. Determine the condition on f of which this maximum occurs.

(b) **[5 pts]** If f is balanced, prove that the Total Phase S must be 0 for any n.

(c) **[5 pts]** For $n = 2$, find all possible values the Total Phase S can take across all possible functions f.

Solution:

(a) The maximum absolute value $|S|$ is 2^n. This occurs when all terms in the sum have the exact same sign (all $+1$ or all -1), which means f is completely uniform: **it must be a Constant function**.

(b) A balanced function f means there are exactly 2^{n-1} inputs yielding $f(x) = 0$ (coefficient $+1$) and 2^{n-1} inputs yielding $f(x) = 1$ (coefficient -1). The Total Phase is their sum: $S = 2^{n-1}(+1) + 2^{n-1}(-1) = 0$.

(c) For $n = 2$, the sum S is composed of 4 signs from $\{+1, -1\}$. The possible combinations of signs and their sums are:

- Four $+1$: sum is 4
- Three $+1$, one -1: sum is 2
- Two $+1$, two -1: sum is 0
- One $+1$, three -1: sum is -2
- Four -1: sum is -4

The possible values are $\{-4, -2, 0, 2, 4\}$.

Scoring Rubric

- **(a) [5 pts]:** Award 5 points for the correct value 2^n and condition that f is constant. No partial credit is awarded.
- **(b) [5 pts]:** Award 3 points for stating there are an equal number (2^{n-1}) of 0s and 1s. Award 2 points for showing their sums algebraically cancel to 0.
- **(c) [5 pts]:** Award 5 points for the correct set $\{-4, -2, 0, 2, 4\}$. No partial credit is awarded.

PROBLEM 9:

15 Points

Often in quantum computing, we do not want to measure the "Total Phase" of a giant superposition because it is hard to calculate for large n. Instead, we use a technique called **Phase Kickback**, where we encode the result of $f(x)$ into the phase of a single bit.

(a) **[5 pts]** Consider the input state $|\phi\rangle = |0\rangle - |1\rangle$. Apply the operator U_f to this state (treating it as an operation on the single bit x). Expand and simplify $U_f(|0\rangle - |1\rangle)$, and compute the result.

(b) **[5 pts]** Prove that if $f(x) = 0$, the state remains $|\phi\rangle$. Prove that if $f(x) = 1$, the state becomes $-|\phi\rangle$.

(c) **[5 pts]** Justify why this is more powerful than the Total Phase sum: why is it better to have a single state change its global sign ($\pm$) rather than having to sum up 2^n different coefficients?

Solution:

(a) By linearity, $U_f(|0\rangle - |1\rangle) = U_f|0\rangle - U_f|1\rangle = (-1)^{f(0)}|0\rangle - (-1)^{f(1)}|1\rangle$.

(b) If $f(x) = 0$, the operator applies $(-1)^0 = +1$ to the system.
State becomes $+1(|0\rangle - |1\rangle) = |\phi\rangle$.
If $f(x) = 1$, the operator applies $(-1)^1 = -1$ to the system.
State becomes $-1(|0\rangle - |1\rangle) = -|\phi\rangle$.

(c) Phase kickback translates a local calculation (the binary answer 0 or 1) into a global shift (a positive or negative sign on the entire state vector). This is computationally more powerful because global phase can be easily manipulated through matrix interference natively in hardware (like applying Hadamard), rather than requiring an observer to physically sum an exponentially large string of 2^n individual superposition amplitudes.

Scoring Rubric

- **(a) [5 pts]:** Award 5 points for the correct linear expansion. No partial credit is awarded.
- **(b) [5 pts]:** Award 5 points for providing correct algebraic steps showing multiplication by $(-1)^0$ and $(-1)^1$ and properly distributing.
- **(c) [5 pts]:** Award 5 points for providing logical reasoning referencing the ability to measure/interfere a single state globally versus summing exponential 2^n terms.

Part III: Deutsch's Algorithm

PROBLEM 10: **15 Points**

A classical computer can query only one input at a time.

(a) **[5 pts]** List one example of a constant function and one example of a balanced function that have the *exact same* value for $f(0)$.

(b) **[5 pts]** List one example of a constant function and one example of a balanced function that have the *exact same* value for $f(1)$.

(c) **[5 pts]** Show that no classical method using only a single query can ever determine whether f is constant or balanced.

Solution:

(a) **Constant:** $f(0) = 0, f(1) = 0$. **Balanced:** $f(0) = 0, f(1) = 1$. Both output $f(0) = 0$.

(b) **Constant:** $f(0) = 1, f(1) = 1$. **Balanced:** $f(0) = 0, f(1) = 1$. Both output $f(1) = 1$.

(c) A classical method limited to one single query can only ever read a 0 or a 1. If it reads a 0, as shown in (a), it could still be Constant or Balanced. If it reads a 1, as shown in (b), it could still be Constant or Balanced. Thus, a single query provides no distinguishing power to eliminate either category.

Scoring Rubric

- **(a) [5 pts]:** Award 5 points for providing valid constant and balanced functions matching $f(0)$. No partial credit is awarded.
- **(b) [5 pts]:** Award 5 points for providing valid constant and balanced functions matching $f(1)$. No partial credit is awarded.
- **(c) [5 pts]:** Award 5 points for synthesizing parts (a) and (b) to explicitly conclude that the output leaves the function type ambiguous.

PROBLEM 11: **20 Points**

Hint: Recall from Part II that quantum operators are linear, meaning you can distribute them across a sum: $H(|0\rangle + |1\rangle) = H|0\rangle + H|1\rangle$.

(a) **[5 pts]** Compute the 2×2 matrix representation of H.

(b) **[5 pts]** Compute the expanded state of $H(|0\rangle + |1\rangle)$.

(c) **[5 pts]** Compute the expanded state of $H(|0\rangle - |1\rangle)$.

(d) **[5 pts]** Show how your answers to parts (b) and (c) demonstrate constructive and destructive interference.

Solution:

(a) In the standard basis $(|0\rangle, |1\rangle)^T$, $H|0\rangle = (1, 1)^T$ and $H|1\rangle = (1, -1)^T$. The matrix is:

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

(b) By linearity: $H(|0\rangle + |1\rangle) = H|0\rangle + H|1\rangle = (|0\rangle + |1\rangle) + (|0\rangle - |1\rangle) = 2|0\rangle$.

(c) By linearity: $H(|0\rangle - |1\rangle) = H|0\rangle - H|1\rangle = (|0\rangle + |1\rangle) - (|0\rangle - |1\rangle) = 2|1\rangle$.

(d) In part (b), the $|0\rangle$ components add together $(1 + 1 = 2)$ causing **constructive** interference, while the $|1\rangle$ components cancel out $(1 - 1 = 0)$ causing **destructive** interference. The inverse happens in part (c), where $|0\rangle$ is destructively canceled and $|1\rangle$ is constructively amplified.

Scoring Rubric

- **(a) [5 pts]:** Award 5 points for the correct 2x2 matrix. No partial credit is awarded.
- **(b) [5 pts]:** Award 5 points for the final state $2|0\rangle$. No partial credit is awarded.
- **(c) [5 pts]:** Award 5 points for the final state $2|1\rangle$. No partial credit is awarded.
- **(d) [5 pts]:** Award 5 points for correctly identifying which specific coefficients are adding (constructive) and subtracting (destructive).

PROBLEM 12: **15 Points**

There are four possible one-bit hidden functions. Let Machine A be the Constant 0 function ($f(0) = 0, f(1) = 0$). Let Machine C be a balanced function ($f(0) = 0, f(1) = 1$).
Assume both machines start with the uniform superposition $|\psi\rangle = |0\rangle + |1\rangle$.

(a) **[5 pts]** For Machine A, compute $U_f|\psi\rangle$. Then, apply the filter to compute the final state $H(U_f|\psi\rangle)$.

(b) **[5 pts]** For Machine C, compute $U_f|\psi\rangle$. Then, apply the filter to compute the final state $H(U_f|\psi\rangle)$.

(c) **[5 pts]** Use your results from parts (a) and (b) to determine how the final state $H(U_f|\psi\rangle)$ distinguishes constant machines from balanced machines. Prove that the final state is supported only on one basis state in the constant case and only on the other basis state in the balanced case.

Solution:

(a) For Machine A, $U_f|\psi\rangle = |0\rangle + |1\rangle$.
Applying the filter: $H(|0\rangle + |1\rangle) = 2|0\rangle$.

(b) For Machine C, $U_f|\psi\rangle = |0\rangle - |1\rangle$.
Applying the filter: $H(|0\rangle - |1\rangle) = 2|1\rangle$.

(c) Machine A (Constant) concentrates 100% of the amplitude onto the $|0\rangle$ basis state. Machine C (Balanced) concentrates 100% of the amplitude onto the $|1\rangle$ basis state. Thus, measuring the final filtered state perfectly physically separates the two machines; one yields an un-overlapped $|0\rangle$ measurement, and the other yields $|1\rangle$.

Scoring Rubric

- **(a) [5 pts]:** Award 5 points for the correct sequence ending in $2|0\rangle$. No partial credit is awarded.
- **(b) [5 pts]:** Award 5 points for the correct sequence ending in $2|1\rangle$. No partial credit is awarded.
- **(c) [5 pts]:** Award 5 points for concluding that the states collapse into mutually exclusive basis vectors depending on the machine type.

PROBLEM 13: **20 Points**

Let's prove this rule holds for *any* 1-bit machine. Let $f : \{0, 1\} \to \{0, 1\}$ be promised to be either constant or balanced. Start with $|\psi\rangle = |0\rangle + |1\rangle$.

(a) **[5 pts]** Suppose f is constant. Prove that $U_f|\psi\rangle$ is either $(|0\rangle + |1\rangle)$ or $-(|0\rangle + |1\rangle)$.

(b) **[5 pts]** Use part (a) to show that if f is constant, measuring $H(U_f|\psi\rangle)$ will always result in a reading of $|0\rangle$.

(c) **[5 pts]** Suppose f is balanced. Prove that $U_f|\psi\rangle$ is either $(|0\rangle - |1\rangle)$ or $-(|0\rangle - |1\rangle)$.

(d) **[5 pts]** Use part (c) to prove that if f is balanced, measuring $H(U_f|\psi\rangle)$ will always result in a reading of $|1\rangle$, allowing you to classify the machine with 100% certainty in a single query.

Solution:

(a) If f is constant, either $f(x) = 0$ entirely, yielding $U_f|\psi\rangle = |0\rangle + |1\rangle$, or $f(x) = 1$ entirely, yielding $U_f|\psi\rangle = -|0\rangle - |1\rangle = -(|0\rangle + |1\rangle)$.

(b) By linearity, applying H to $\pm(|0\rangle + |1\rangle)$ yields $\pm H(|0\rangle + |1\rangle) = \pm 2|0\rangle$. A global minus sign does not change the physical observable, meaning 100% of measurements will return $|0\rangle$.

(c) If f is balanced, either $f(0) = 0, f(1) = 1$, yielding $|0\rangle - |1\rangle$, or $f(0) = 1, f(1) = 0$, yielding $-|0\rangle + |1\rangle = -(|0\rangle - |1\rangle)$.

(d) Applying H to $\pm(|0\rangle - |1\rangle)$ yields $\pm H(|0\rangle - |1\rangle) = \pm 2|1\rangle$. The state perfectly aligns onto the basis $|1\rangle$, meaning 100% of measurements will read $|1\rangle$, proving classification in one single query.

Scoring Rubric

- **(a) [5 pts]:** Award 3 points for enumerating both constant cases ($f \equiv 0$ and $f \equiv 1$) and correctly applying U_f. Award 2 points for correctly factoring to show $\pm(|0\rangle + |1\rangle)$.
- **(b) [5 pts]:** Award 3 points for correctly applying H to $\pm(|0\rangle + |1\rangle)$ via linearity. Award 2 points for invoking that a global sign does not affect measurement probability, concluding $|0\rangle$.
- **(c) [5 pts]:** Award 3 points for enumerating both balanced cases and applying U_f. Award 2 points for correctly factoring to show $\pm(|0\rangle - |1\rangle)$.
- **(d) [5 pts]:** Award 3 points for applying H to $\pm(|0\rangle - |1\rangle)$. Award 2 points for invoking global sign irrelevance to conclude $|1\rangle$ with 100% certainty.

PROBLEM 14:

15 Points

Definition: The dot product of two vectors $v = (a, b)$ and $w = (c, d)$ is defined as $ac + bd$. If the dot product is exactly 0, the two vectors are perfectly perpendicular, which is called being "orthogonal."

The transformation matrix $H = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ has rows $r_1 = (1, 1)$ and $r_2 = (1, -1)$.

(a) **[5 pts]** Compute the dot product $r_1 \cdot r_2$.

(b) **[10 pts]** In quantum mechanics, states that can be reliably distinguished from one another must be orthogonal. Explain how the orthogonality of the H matrix allows the algorithm to physically separate the "constant" universe from the "balanced" universe without them overlapping.

Solution:

(a) $r_1 \cdot r_2 = (1)(1) + (1)(-1) = 1 - 1 = 0$.

(b) The orthogonality of the rows in H guarantees that the filter maps the two independent mathematical inputs (symmetric constant phases vs antisymmetric balanced phases) into two entirely disjoint physical states ($|0\rangle$ vs $|1\rangle$). Because the vectors have a 0 dot product, there is zero probability leakage between them, enabling perfect physical separation during measurement.

Scoring Rubric

- **(a) [5 pts]:** Award 5 points for the correct value 0. No partial credit is awarded.
- **(b) [10 pts]:** Award 5 points for explaining that the orthogonal rows of H map the symmetric phase pattern (constant) and antisymmetric phase pattern (balanced) into orthogonal output vectors. Award 5 points for connecting orthogonality to zero probability overlap between $|0\rangle$ and $|1\rangle$ outcomes during measurement.

PROBLEM 15: **20 Points**

Classical logic gates often destroy information. For example, if a classical AND gate outputs a 0, it is impossible to reverse the process to know for sure whether the original inputs were 00, 01, or 10. The information is permanently erased.

Quantum mechanics, however, requires perfect **reversibility**. Operators cannot erase information; they can only rearrange it. This means every quantum filter must act as its own "undo" button. Let's prove that the interference filter H is reversible.

(a) **[5 pts]** Apply the filter twice to the zero state. First, recall that $H|0\rangle = |0\rangle + |1\rangle$. Now, compute the expanded state of $H(H|0\rangle)$ by evaluating $H(|0\rangle + |1\rangle)$.

(b) **[5 pts]** Apply the filter twice to the one state. Compute the expanded state of $H(H|1\rangle)$ by evaluating $H(|0\rangle - |1\rangle)$.

(c) **[5 pts]** In standard quantum mechanics (which uses fractions to keep probabilities equal to 100%), applying the filter twice returns the exact original state: $H(H|\psi\rangle) = |\psi\rangle$. Because we are using an un-normalized model for this round to keep the math clean, applying H twice returns a scalar multiple of the original state. Based on your answers to (a) and (b), compute this scalar multiple.

(d) **[5 pts]** Show that the filter doesn't "destroy" any data and has perfect reversibility.

Solution:

(a) $H(H|0\rangle) = H(|0\rangle + |1\rangle) = H|0\rangle + H|1\rangle = (|0\rangle + |1\rangle) + (|0\rangle - |1\rangle) = 2|0\rangle$.

(b) $H(H|1\rangle) = H(|0\rangle - |1\rangle) = H|0\rangle - H|1\rangle = (|0\rangle + |1\rangle) - (|0\rangle - |1\rangle) = 2|1\rangle$.

(c) For both cases, applying H twice scales the initial vector by exactly a factor of 2. The scalar multiple is **2**.

(d) Since $H(H|\psi\rangle) = 2|\psi\rangle$, we can mathematically reverse any operation H by applying H a second time (and rescaling). Because we flawlessly recovered the initial state with no missing data, H acts as its own undo button, proving perfect reversibility.

Scoring Rubric

- **(a) [5 pts]:** Award 5 points for the answer $2|0\rangle$. No partial credit is awarded.
- **(b) [5 pts]:** Award 5 points for the answer $2|1\rangle$. No partial credit is awarded.
- **(c) [5 pts]:** Award 5 points for the scalar multiple 2. No partial credit is awarded.
- **(d) [5 pts]:** Award 5 points for linking the $2|\psi\rangle$ result back to mathematical reversibility.

PROBLEM 16: **20 Points**

Now let the hidden machine take n inputs: $f : \{0,1\}^n \to \{0,1\}$. After querying the machine simultaneously using the uniform superposition, the state becomes:

$$U_f|\psi\rangle = \sum_{x\in\{0,1\}^n} (-1)^{f(x)}|x\rangle.$$

Recall from Part II (Problem 7) that you proved the amplitude sum $S = \sum_{x\in\{0,1\}^n}(-1)^{f(x)}$ must be exactly $\pm 2^n$ if f is constant, and exactly 0 if f is balanced.

(a) **[10 pts]** Let

$$S = \sum_{x\in\{0,1\}^n} (-1)^{f(x)}.$$

Prove that S is equal to the number of inputs x for which $f(x) = 0$ minus the number of inputs x for which $f(x) = 1$.

(b) **[10 pts]** Suppose the final interference filter sends the coefficient of $|00\cdots0\rangle$ to

$$S = \sum_{x\in\{0,1\}^n} (-1)^{f(x)}.$$

Prove whether the final measurement can output $|00\cdots0\rangle$ when f is balanced. Then prove whether the final measurement must output $|00\cdots0\rangle$ when f is constant.

Solution:

(a) Let N_0 be the number of inputs with $f(x) = 0$ and N_1 be the number of inputs with $f(x) = 1$. In the sum S, each of the N_0 inputs contributes $(-1)^0 = 1$. Each of the N_1 inputs contributes $(-1)^1 = -1$. Grouping these terms together gives exactly $S = N_0(1) + N_1(-1) = N_0 - N_1$.

(b) **Balanced:** If f is balanced, exactly half the inputs are 0 and half are 1. Thus $N_0 = N_1$, meaning $S = 0$. Since the coefficient of $|00\cdots0\rangle$ is zero, the probability of measuring it is 0. It *cannot* output $|00\cdots0\rangle$. **Constant:** If f is constant, all inputs are either 0 ($S = 2^n$) or 1 ($S = -2^n$). Because quantum operations are unitary and conserve total probability (or by referencing the complete interference expansion), a single coefficient of $\pm 2^n$ mathematically accounts for 100% of the un-normalized system's total possible squared amplitude. Therefore, all other coefficients must vanish to 0. Since no probability remains for any other state, the measurement *must* output $|00\cdots0\rangle$.

Scoring Rubric

- **(a) [10 pts]:** Award 5 points for identifying the mapping of $(-1)^0$ to 1 and $(-1)^1$ to -1. Award 5 points for accurately concluding $N_0 - N_1$.
- **(b) [10 pts]:** Award 5 points for showing Balanced implies $S = 0$, so it cannot be measured. Award 5 points for showing Constant yields $S = \pm 2^n$, and explicitly justifying why this forces all other amplitudes to vanish (e.g., by invoking unitarity, normalization, or conservation of probability) ensuring it must be measured.

Part IV: The Secret String

PROBLEM 17: **15 Points**

Suppose the machine takes 3-bit inputs ($n = 3$). A junior researcher queried the machine classically three times, but the computer crashed before they could finish testing all 8 inputs. They hand you the following data log:

Input (x)	Output $f(x)$
100	1
010	0
001	1

(a) **[5 pts]** Compute the secret string s.

(b) **[5 pts]** Let e_i denote the n-bit string with a 1 in the ith position and 0s elsewhere. Show that entering the following queries determines s

$$e_1, e_2, \ldots, e_n$$

(c) **[5 pts]** For a general n-bit machine, find the absolute minimum number of classical queries required to find the secret string s with 100% certainty.

Solution:

(a) We can decode s bit by bit using the modulo-2 dot product.
$100 \cdot s = s_1 \pmod 2 = 1 \implies s_1 = 1.$
$010 \cdot s = s_2 \pmod 2 = 0 \implies s_2 = 0.$
$001 \cdot s = s_3 \pmod 2 = 1 \implies s_3 = 1.$
Thus, $s = 101$.

(b) A query of e_i is a string full of 0s except for a 1 in the i-th spot. When we calculate $e_i \cdot s$, the zeros cancel out every single bit of s except for the i-th bit: $0(s_1) + \cdots + 1(s_i) + \cdots = s_i$. Querying all n basis vectors e_i sequentially will explicitly reveal every individual bit of s.

(c) The absolute minimum is n queries. Each classical boolean query yields at most 1 bit of information, and the password itself contains n unknown bits.

Scoring Rubric

- **(a) [5 pts]:** Award 5 points for the correct string 101. No partial credit is awarded.
- **(b) [5 pts]:** Award 5 points for showing mathematically that the dot product isolates s_i.
- **(c) [5 pts]:** Award 5 points for the correct bound n. No partial credit is awarded.

PROBLEM 18: **15 Points**

Your team connects the new machine to the prototype quantum chip. You start with the uniform superposition $|\psi\rangle$ of all possible inputs. Just like in Part II, the machine encodes its output into the phase of the states:

$$U_f|\psi\rangle = \sum_{x \in \{0,1\}^n} (-1)^{x \cdot s} |x\rangle$$

Let $n = 2$ and assume the secret string is $s = 11$.

(a) **[5 pts]** Compute the dot product $(x \cdot s) \pmod 2$ for all four possible inputs: $x \in \{00, 01, 10, 11\}$.

(b) **[5 pts]** Determine the fully expanded quantum state $U_f|\psi\rangle$ for this specific machine, using $+/-$ signs.

(c) **[5 pts]** Looking at your resulting state, show why immediately measuring it right now is useless

for finding s.

Solution:

(a) $00 \cdot 11 = 0 \implies 0$
$01 \cdot 11 = 1 \implies 1$
$10 \cdot 11 = 1 \implies 1$
$11 \cdot 11 = 2 \equiv 0 \pmod 2 \implies 0$

(b) $U_f|\psi\rangle = (-1)^0|00\rangle + (-1)^1|01\rangle + (-1)^1|10\rangle + (-1)^0|11\rangle = |00\rangle - |01\rangle - |10\rangle + |11\rangle$.

(c) Because the amplitudes for each component are all exactly ± 1, their probabilities (which are proportional to the magnitude squared, $(\pm 1)^2$) are identical. Measuring this state immediately will collapse into a completely uniform random classical bitstring, yielding 0 information about s.

Scoring Rubric

- **(a) [5 pts]:** Award 5 points for the outputs 0, 1, 1, 0. No partial credit is awarded.
- **(b) [5 pts]:** Award 5 points for the correct state with proper negative signs. No partial credit is awarded.
- **(c) [5 pts]:** Award 5 points for a valid explanation relating the identical squared amplitudes to uniformly random measurement outcomes.

PROBLEM 19: **25 Points**

To extract s, we must apply the interference filter from Part III to every single bit simultaneously. We denote this massive filter as $H^{\otimes n}$.
When applied to our n-bit state, the filter mathematically transforms it into the following double-sum (you do not need to derive this):

$$H^{\otimes n}(U_f|\psi\rangle) = \sum_{y\in\{0,1\}^n} \left[\sum_{x\in\{0,1\}^n} (-1)^{(x\cdot s)+(x\cdot y)} \right] |y\rangle$$

This looks intimidating, but it behaves exactly like the constructive and destructive collisions you explored in Part III. Let's evaluate the expression inside the brackets for a specific resulting state $|y\rangle$.

(a) **[5 pts]** **Constructive Interference:** Suppose we are looking at the specific state where $y = s$. The expression inside the brackets becomes $(-1)^{(x\cdot s)+(x\cdot s)}$. Prove that for any binary strings x and s, the value of $(x \cdot s) + (x \cdot s)$ is always even.

(b) **[5 pts]** Determine what the term $(-1)^{(x\cdot s)+(x\cdot s)}$ simplifies to.

(c) **[5 pts]** Using your answer to (b), compute the sum inside the brackets for $y = s$:

$$\sum_{x\in\{0,1\}^n} (-1)^{(x\cdot s)+(x\cdot s)}.$$

(d) **[5 pts]** **Destructive Interference:** It is a mathematical fact that if $y \neq s$, the positive and negative signs perfectly balance out, meaning the sum inside the brackets is exactly 0. Using this fact and your answer to (c), determine the final, un-normalized quantum state of the system.

(e) **[5 pts]** Based on your final state, find the number of quantum queries required to find the secret password s, regardless of how large n is.

Solution:

(a) Let the integer dot product be k. The expression is $k + k = 2k$. Because any integer multiplied by 2 is

an even integer, it is always even.

(b) Since the exponent is an even number, $(-1)^{\text{even}} = 1$. It simplifies to $+1$.

(c) The inner sum evaluates to adding $+1$ for every possible input $x \in \{0,1\}^n$. Since there are 2^n combinations for x, the sum is 2^n.

(d) If all brackets evaluate to 0 except when $y = s$, then all states cancel out except for $|s\rangle$. Its coefficient is 2^n. The final, un-normalized state is exactly $2^n|s\rangle$.

(e) Because the final state collapses mathematically into solely the state $|s\rangle$, a single measurement will reveal the entire secret string with 100% accuracy. It requires exactly **1 query**.

Scoring Rubric

- **(a) [5 pts]:** Award 5 points for a rigorous mathematical logic proving $k + k$ is even.
- **(b) [5 pts]:** Award 5 points for the correct simplification to $+1$. No partial credit is awarded.
- **(c) [5 pts]:** Award 5 points for the correct sum 2^n. No partial credit is awarded.
- **(d) [5 pts]:** Award 5 points for the state $2^n|s\rangle$ (or just $|s\rangle$ if normalization is assumed). No partial credit is awarded.
- **(e) [5 pts]:** Award 5 points for exactly 1 query. No partial credit is awarded.

PROBLEM 20:

25 Points

Your research team must draft a budget proposal to justify using the prototype quantum chip over standard classical server farms.

According to the hardware department:

- A **Classical Query** costs \$5 in electricity and takes 2 milliseconds.
- A single **Quantum Query** requires supercooling the hardware. It costs \$15,000 in liquid helium and takes exactly 300 milliseconds.

Assume you are trying to crack a secret string of length n.

(a) **[5 pts]** Find the function $T_c(n)$ for the time (in milliseconds) it takes the classical computer to find the string. Find the function $T_q(n)$ for the time it takes the quantum computer.

(b) **[5 pts]** Compute the minimum string length n does the quantum computer become *faster* than the classical computer?

(c) **[5 pts]** Find the function $C_c(n)$ for the cost (in dollars) of the classical computer. Find the function $C_q(n)$ for the cost of the quantum computer. Compute the minimum string length n that the quantum computer become *cheaper* than the classical computer?

(d) **[10 pts]** Modern bank encryption uses 2048-bit strings ($n = 2048$). If your team is tasked with cracking a bank's security, determine exactly how much time (in milliseconds) and how much money (in dollars) the quantum chip will save compared to the classical server farm.

Solution:

(a) The classical computer needs n queries. The quantum computer always needs exactly 1 query.
$T_c(n) = 2n$ ms.
$T_q(n) = 300$ ms.

(b) $2n > 300 \implies n > 150$. The minimum string length is 151.

(c) $C_c(n) = 5n$ dollars.
$C_q(n) = 15000$ dollars.
$5n > 15000 \implies n > 3000$. The minimum string length is 3001.

(d) For $n = 2048$:
Time: Classical takes $2(2048) = 4096$ ms. Quantum takes 300 ms.
Time saved $= 4096 - 300 =$ **3796 milliseconds.**
Cost: Classical costs $5(2048) = 10,240$ dollars. Quantum costs 15,000 dollars.

Money saved $= 10,240 - 15,000 =$ **-4,760 dollars** (Meaning it costs $\$4,760$ more, it doesn't save money).

Scoring Rubric

- **(a) [5 pts]:** Award 5 points for the correct time functions. No partial credit is awarded.
- **(b) [5 pts]:** Award 5 points for the correct minimum length 151. No partial credit is awarded.
- **(c) [5 pts]:** Award 5 points for the correct cost functions and minimum length 3001. No partial credit is awarded.
- **(d) [10 pts]:** Award 5 points for computing 3796 ms. Award 5 points for explicitly stating a negative savings of -4,760 dollars (or stating it costs $\$4,760$ more). No partial credit is awarded.