MATH 3QC3 Assignment 3

Matthew Yu — 400322243 — Yum77

April 15, 2025

In classical computing, an *oracle* for a function f is a "black box" subroutine that, when given input x, returns $f(x)$. In quantum computing, we need our operations to be *unitary* (and thus reversible). Therefore, a **quantum oracle** for f is built as a unitary operator U_f acting on two registers: one that holds the input x (in superposition) and one that holds the output. Concretely, if x is an n-bit string and $f(x)$ is an m-bit string, the oracle acts as:

$$U_f : |x\rangle|y\rangle \mapsto |x\rangle|y \boxplus f(x)\rangle$$

where $\boxplus$ denotes bitwise addition modulo 2. This transformation is reversible because from the pair $(x, y \oplus f(x))$, one can recover the original pair (x, y) when applying U_f again.

Whenever you see an expression like $|x\rangle|f(x)\rangle$, assume that this "encoding" was done by a *quantum oracle* of the form above.

1 The Deutsch-Jozsa Algorithm

Consider the following problem: you are given a function

$$f : \{0,1\}^n \to \{0,1\},$$

which is promised (i.e. you know) to be either:

- **Constant**: $f(x)$ is the same for all x (either always 0 or always 1).
- **Balanced**: Exactly half of the inputs yield 0, and the other half yield 1.

Classically, in the worst case, one needs multiple queries to f (can you think of how many on average?) to distinguish the two cases. Quantumly, the Deutsch-Jozsa algorithm can solve this with *just one* query to the quantum oracle U_f.

1.1 Warm up

Let's consider the single-bit example, where $f : \{0,1\} \to \{0,1\}$. Here, there are only two options: f is constant iff $f(0) = f(1)$ and otherwise it is balanced. The algorithm acts on two qubits, and

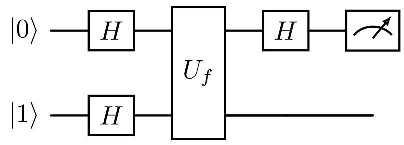
$$U_f|x, y\rangle = |x, y \boxplus f(y)\rangle = |x, y \oplus f(x)\rangle$$

QUESTION 1a

Matthew Yu - 400322243

- Initialize your state to $|01\rangle$.
- Apply Hadamard to both qubits i.e. $(H \otimes H)$.
- Apply U_f.
- Apply Hadamard to the first qubit.
- Measure the first qubit.

Solution 1a:



QUESTION 1b

Matthew Yu - 400322243 Calculate the state after each evolution through the system.

Solution 1b:

- We start with the two-qubit state:
$$|01\rangle$$
So the first qubit is $|0\rangle$ and the second qubit is $|1\rangle$
- We apple the Hadamard to both qubits $H \otimes H$:
$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$
So we get:
$$\begin{aligned} H(|0\rangle) \otimes H(|1\rangle) &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\ &= \frac{1}{2}(|0\rangle(|0\rangle - |1\rangle) + |1\rangle(|0\rangle - |1\rangle)) \\ &= \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle) \end{aligned}$$
- Apply oracle U_f where $U_f = |x, y \oplus f(x)\rangle$
$$\begin{aligned} U_f(H(|0\rangle) \otimes H(|1\rangle)) &= \frac{1}{2}(|0, 0 \oplus f(0)\rangle - |0, 1 \oplus f(0)\rangle + |1, 0 \oplus f(1)\rangle - |1, 1 \oplus f(1)\rangle) \\ &= \frac{1}{2}(|0, f(0)\rangle - |0, 1 \oplus f(0)\rangle + |1, f(1)\rangle - |1, 1 \oplus f(1)\rangle) \end{aligned}$$
- Now we apply Hadamard to the first qubit (right most) of each term:
$$\text{First Term} : |0, f(0)\rangle H|0\rangle|f(0)\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|f(0)\rangle.$$
$$\text{Second Term} : -|0, 1 \oplus f(0)\rangle - H|0\rangle|1 \oplus f(0)\rangle = -\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|1 \oplus f(0)\rangle.$$
$$\text{Third Term} : |1, f(1)\rangle H|1\rangle|f(1)\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)|f(1)\rangle.$$
$$\text{Fourth Term} : -|1, 1 \oplus f(1)\rangle - H|1\rangle|1 \oplus f(1)\rangle = -\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)|1 \oplus f(1)\rangle.$$
$$\text{Final State} = \frac{1}{2} \cdot \frac{1}{\sqrt{2}}\Big[(|0\rangle + |1\rangle)|f(0)\rangle - (|0\rangle + |1\rangle)|1 \oplus f(0)\rangle + (|0\rangle - |1\rangle)|f(1)\rangle - (|0\rangle - |1\rangle)|1 \oplus f(1)\rangle\Big].$$
- Group the terms based on the first qubit ($|0\rangle$ and $|1\rangle$)
$$\frac{1}{2\sqrt{2}}\Big[|0\rangle\big(|f(0)\rangle - |1 \oplus f(0)\rangle + |f(1)\rangle - |1 \oplus f(1)\rangle\big) + |1\rangle\big(|f(0)\rangle - |1 \oplus f(0)\rangle - |f(1)\rangle + |1 \oplus f(1)\rangle\big)\Big].$$
- When you measure the first qubit, the outcome depends on whether f is **constant** or **balanced**:
If f is constant, there are two possibilities:
All outputs are 0 ($f(0) = f(1) = 0$):
$$\begin{aligned} &= \frac{1}{2\sqrt{2}}\Big[|0\rangle\big(|0\rangle - |1 \oplus 0\rangle + |0\rangle - |1 \oplus 0\rangle\big) + |1\rangle\big(|0\rangle - |1 \oplus 0\rangle - |0\rangle + |1 \oplus 0\rangle\big)\Big] \\ &= \frac{1}{2\sqrt{2}}\Big[|0\rangle\big(|0\rangle - |1\rangle + |0\rangle - |1\rangle\big) + |1\rangle\big(|0\rangle - |1\rangle - |0\rangle + |1\rangle\big)\Big] \\ &= \frac{1}{2\sqrt{2}}\Big[|0\rangle\big(2|0\rangle - 2|1\rangle\big) + |1\rangle\,(0)\Big] \\ &= \frac{1}{\sqrt{2}}|0\rangle\big(|0\rangle - 2|1\rangle\big) \end{aligned}$$

We can see that the first qubit is not in a superposition but just as $|0\rangle$. Therefore it will measure 0 with probability 1.

If all outputs are 0 ($f(0) = f(1) = 1$):

$$
\begin{aligned}
&= \frac{1}{2\sqrt{2}}\Big[|0\rangle\big(|1\rangle - |0\rangle + |1\rangle - |0\rangle\big) + |1\rangle\big(|1\rangle - |0\rangle - |1\rangle + |0\rangle\big)\Big]. \\
&\frac{1}{2\sqrt{2}}\Big[|0\rangle\big(2|1\rangle - 2|0\rangle\big) + |1\rangle\big(0\big)\Big]. \\
&= \frac{1}{\sqrt{2}}|0\rangle\big(|1\rangle - |0\rangle\big).
\end{aligned}
$$

We can see that the first qubit is not in a superposition but just as $|0\rangle$. Therefore it will measure 0 with probability 1.
If f is balanced, we set f(0)=0, f(1)=1 then check f(0)=1, f(1)=0:

$$
\begin{aligned}
f(0) = 0, f(1) = 1 : &\frac{1}{2\sqrt{2}}\Big[|0\rangle\big(|0\rangle - |1\rangle + |1\rangle - |0\rangle\big) + |1\rangle\big(|0\rangle - |1\rangle - |1\rangle + |0\rangle\big)\Big]. \\
&= \frac{1}{\sqrt{2}}|1\rangle\big(|0\rangle - |1\rangle\big). \\
f(0) = 1, f(1) = 0 : &\frac{1}{2\sqrt{2}}\Big[|0\rangle\big(|1\rangle - |0\rangle + |0\rangle - |1\rangle\big) + |1\rangle\big(|1\rangle - |0\rangle - |0\rangle + |1\rangle\big)\Big]. \\
&= \frac{1}{\sqrt{2}}|1\rangle\big(|1\rangle - |0\rangle\big).
\end{aligned}
$$

As we can see the first qubit is measured to be $|1\rangle$ with probabiltiy 1.

QUESTION 1c

Explain why the algorithm determines if f is balanced or not with probability 1.

Solution 1c: As shown in 1b where we measure the first qubit, when half the inputs are 0 and the other half are 1, the $|0\rangle$ part always cancels out leaving just $|1\rangle$. Therefore, we can conclude that when we measure the first qubit, we will always get $|1\rangle$ 100% of the time if f is balanced.

QUESTION 1d

Suppose now that $f : \{0,1\}^n \to \{0,1\}$. Assume that f is either balanced or constant. Explain why, classically, in the worst case we would need at least $2^{n-1} - 1$ queries to determine if f is either balanced or constant (hint: think of a particular example of an f).

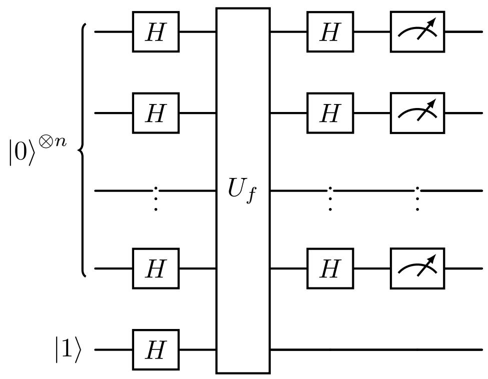
Solution 1d: In classical computing, determining whether a function $f : \{0,1\}^n \to \{0,1\}$ is constant or balanced requires querying enough inputs to ensure we observe conflicting outputs if f is balanced. In the worst-case scenario, f could return the same value (e.g., 0) for as many inputs as possible before revealing its true nature. For a balanced function, exactly half (2^{n-1}) of the inputs yield 0 and the other half yield 1. If we query $2^{n-1} - 1$ inputs and all return 0, there are still $2^{n-1} + 1$ inputs left unchecked. If the next query (the 2^{n-1}-th) also returns 0, we have 2^{n-1} 0s, confirming f is balanced. If all $2^{n-1} + 1$ queried inputs return 0, f must be constant. Therefore, in the worst case, we need to query at least $2^{n-1} + 1$ inputs to definitively determine whether f is constant or balanced.

QUESTION 1e

Consider the following algorithm that acts on $\sqcap^{\otimes n} \otimes \sqcap^{\otimes n}$:

- Input the vector $|0\rangle^n \otimes |1\rangle = |0 \ldots 0\rangle \otimes |1\rangle$,
- Apply Hadamard to all qubits,
- Apply U_f to all qubits,
- Apply Hadamard to the first n qubits,
- Measure the first n qubits.

Solution 1e:



This circuit is similar to the one done in part a but uses the input vector $|0\rangle^n$ and $|1\rangle$ instead

QUESTION 1f

Show that the output determines with probability 1 whether f is balanced or not.

Solution 1f: This problem is set up similar to 1a but instead of just 2 qubits, we have n $|0\rangle$ and $|1\rangle$:

- Apply the Hadamard gate H to each of the first n qubits and the last qubit:

$$H^{\otimes n}|0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle,$$

  and

$$H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

  The combined state becomes:

$$\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

- Apply U_f

$$\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle \otimes \frac{|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle}{\sqrt{2}}.$$

  Simplifying:

$$\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

- Apply Hadamard to first n qubits:

$$H^{\otimes n}\left(\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle\right) = \frac{1}{2^n} \sum_{z\in\{0,1\}^n} \left(\sum_{x\in\{0,1\}^n} (-1)^{x\cdot z}\right) |z\rangle.$$

  The state becomes:

$$\frac{1}{2^n} \sum_{z\in\{0,1\}^n} \left(\sum_{x\in\{0,1\}^n} (-1)^{x\cdot z}\right) |z\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

- Measure the first n qubits:
  The probability of measuring $z = 0^n$ is:

$$\left|\frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{x\cdot 0^n}\right|^2 = \left|\frac{1}{2^n} \sum_{x\in\{0,1\}^n} 1\right|^2 = 1.$$

  If f is constant:
  The state remains unchanged, and the measurement result is $z = 0^n$ with probability 1.
  If f is balanced:
  The interference caused by the Hadamard transform cancels out the amplitude for $z = 0^n$, and the measurement result is some other z with probability 1.

  If the measurement result is $z = 0^n$, f is **constant**. If the measurement result is any other z, f is **balanced**.

$$\boxed{\text{The output } z = 0^n \text{ guarantees } f \text{ is constant; any other } z \text{ guarantees } f \text{ is balanced.}}$$

2 Simon's Problem

Let's consider $\{0,1\}^n$ as the n-dimensional $\mathbb{Z}/2\mathbb{Z}$-vector-space $V = (\mathbb{Z}/2\mathbb{Z})^n$ (recall that $\mathbb{Z}/2\mathbb{Z}$ is a field, so we can just do linear algebra as usual). Assume that there is some secret (string) vector $\vec{s} \in V$ (it's a secret from you!). Imagine now that we have a function $f : V \to V$, where you are guaranteed that for any $\vec{x}, \vec{y} \in V$,

$$f(\vec{x}) = f(\vec{y}) \Leftrightarrow \vec{x} = \vec{y} \text{ or } \vec{x} = \vec{y} +_V \vec{s}$$

(note that addition in V is just the same as bit-wise addition $\mod 2$, $+_V \equiv \boxplus$). Assume we have a quantum oracle that can perform f, i.e.,

$$U_f|x, y\rangle = |x, y \boxplus f(x)\rangle.$$

Question: Can we discover the secret string $\vec{s}$?
The following is a non-trivial fact:
Theorem 0.1. *Any classical algorithm that solves this problem with probability at least 2/3 for any such f must evaluate f on the order of $O(2^{n/3})$ times.*
So solving this problem efficiently on a classical computer requires exponentially more computations as n grows.

In this exercise, we will see that an algorithm with a quantum sub-algorithm can do much better.

QUESTION 2a

2.1 Quantum Algorithm

(a) Show that for any $\vec{x} \in V$,

$$H^{\otimes n}|\vec{x}\rangle = \frac{1}{\sqrt{2^n}} \sum_{\vec{z} \in V} (-1)^{\vec{x}\cdot\vec{z}} |z\rangle,$$

where, $\vec{x} \cdot \vec{z}$ is just the usual dot product over $\mathbb{Z}/2\mathbb{Z}$, and $|\vec{v}\rangle$ is just the standard basis vector of $\mathbb{C}^{\otimes n}$ corresponding to the sequence of 0's and 1's in $\vec{v}$.

Solution 2a: We know the output for Hadamard on $|0\rangle$ and $|1\rangle$:

$$H\,|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad H\,|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

To generalize for $|x_i\rangle$ we observe that the difference between $|0\rangle$ and $|1\rangle$ is a sign change on $|1\rangle$. We can implement a phase factor:

$$(-1)^{x_i z_i}, \text{ where } z \text{ is the index of the basis state } |z_i\rangle\,, (z_i \in \{0,1\})$$

For $z_i = 0$: $(-1)^{x_i 0} = 1$ This means the coefficient of $|0\rangle$ is always $+1$, regardless of x_i.
For $z_i = 1$: $(-1)^{x_i 1} = (-1)^{x_i}$ This means the coefficient of $|1\rangle$ is $+1$ if $x_i = 0$ and -1 if $x_i = 1$.
We can now write Hadamard on $|x_i\rangle$ as:

$$H\,|x_i\rangle = \frac{1}{\sqrt{2}} \sum_{z_i=1}^{1} (-1)^{x_i z_i}\,|z_i\rangle$$

Applying $H^{\otimes n}$ to $|\vec{x}\rangle = |x_1 x_2 ... x_n\rangle$ gives:

$$H^{\otimes n}|\vec{x}\rangle = \bigotimes_{i=1}^{n} H|x_i\rangle = \frac{1}{\sqrt{2^n}} \sum_{z_1,\ldots,z_n \in \{0,1\}} (-1)^{\sum_{i=1}^n x_i z_i} |z_1 z_2 \ldots z_n\rangle.$$

$\sum_{i=1}^n x_i z_i \mod 2 = \vec{x} \cdot \vec{z}$. Thus:

$$\boxed{H^{\otimes n}|\vec{x}\rangle = \frac{1}{\sqrt{2^n}} \sum_{\vec{z} \in V} (-1)^{\vec{x}\cdot\vec{z}} |\vec{z}\rangle.}$$

QUESTION 2b

Matthew Yu - 400322243 (b) Let $S = \text{span}\{\vec{s}\}$ and $S^\perp$ its orthogonal complement. Use the previous part to show that for $\vec{x} \in V$, if $\vec{y} = \vec{x} + \vec{s}$, then

$$H^{\otimes n}\left(\frac{1}{\sqrt{2}}|\vec{x}\rangle + \frac{1}{\sqrt{2}}|\vec{y}\rangle\right) = \frac{1}{\sqrt{2^{n-1}}}\sum_{\vec{z}\in S^\perp}(-1)^{\vec{x}\vec{z}}|\vec{z}\rangle.$$

Important! What is the dimension of $S^\perp$? Relatedly, what is the cardinality (size) of $S^\perp$?

Solution 2b: Dimension and Cardinality of $S^\perp$:

- $S = \text{span}\{\vec{s}\}$ is 1-dimensional (assuming $\vec{s} \neq \vec{0}$).
- $S^\perp$ has dimension $n-1$ (orthogonal complement in n-dimensional space).
- Cardinality: $|S^\perp| = 2^{n-1}$.

From part 2(a) we have:

$$H^{\otimes n}|\vec{x}\rangle = \frac{1}{\sqrt{2^n}}\sum_{\vec{z}\in V}(-1)^{\vec{x}\cdot\vec{z}}|\vec{z}\rangle,$$

Add s:

$$H^{\otimes n}|\vec{x}+\vec{s}\rangle = \frac{1}{\sqrt{2^n}}\sum_{\vec{z}\in V}(-1)^{(\vec{x}+\vec{s})\cdot\vec{z}}|\vec{z}\rangle.$$

Adding both:

$$\begin{aligned}H^{\otimes n}\left(\frac{1}{\sqrt{2}}|\vec{x}\rangle + \frac{1}{\sqrt{2}}|\vec{x}+\vec{s}\rangle\right) &= \frac{1}{\sqrt{2^{n+1}}}\sum_{\vec{z}\in V}\left[(-1)^{\vec{x}\cdot\vec{z}} + (-1)^{(\vec{x}+\vec{s})\cdot\vec{z}}\right]|\vec{z}\rangle.\\ &= \frac{1}{\sqrt{2^{n+1}}}\sum_{\vec{z}\in V}\left[(-1)^{\vec{x}\cdot\vec{z}}\left[1+(-1)^{\vec{s}\cdot\vec{z}}\right]\right]|\vec{z}\rangle.\end{aligned}$$

If $\vec{s}\cdot\vec{z} = 0$, the coefficient is $2(-1)^{\vec{x}\cdot\vec{z}}$; otherwise, it cancels to 0. Thus, the sum reduces to vectors $\vec{z} \in S^\perp$:

$$\boxed{\frac{1}{\sqrt{2^{n-1}}}\sum_{\vec{z}\in S^\perp}(-1)^{\vec{x}\cdot\vec{z}}|\vec{z}\rangle.}$$

QUESTION 2c

(c) **IMPORTANT!** Conclude that the result from the previous part is a uniform superposition of kets, each of which encode a vector in $S^\perp$. In other words, by measuring the state, we can determine an element of $S^\perp$ with probability 2^{1-n}.

Solution 2c: From part (b), we have the state:

$$H^{\otimes n}\left(\frac{1}{\sqrt{2}}|\vec{x}\rangle + \frac{1}{\sqrt{2}}|\vec{y}\rangle\right) = \frac{1}{\sqrt{2^{n-1}}}\sum_{\vec{z}\in S^\perp}(-1)^{\vec{x}\cdot\vec{z}}|\vec{z}\rangle,$$

Where $\vec{y} = \vec{x} + \vec{s}$, and $S^\perp$ is the orthogonal complement of $S = span\{\vec{s}\}$.
The state is a superposition of all vectors $\vec{z} \in S^\perp$, with each term $|\vec{z}\rangle$ having an amplitude of $\frac{1}{\sqrt{2^{n-1}}}$. The phase factor $(-1)^{\vec{x}\cdot\vec{z}}$ does not affect the magnitude of the amplitude, so all terms in the superposition have equal magnitude. This means the state is a **uniform superposition** over $S^\perp$.
The dimension of $S^\perp$ is $n-1$, so the size of $S^\perp$ is $|S^\perp| = 2^{n-1}$. Each term $|\vec{z}\rangle$ in the superposition has probability:

$$\left|\frac{1}{\sqrt{2^{n-1}}}\right|^2 = \frac{1}{2^{n-1}} = 2^{1-n}.$$

Since all $\vec{z} \in S^\perp$ are equally likely, measuring the state yields a uniformly random element of $S^\perp$, with each outcome occurring with probability 2^{1-n}.

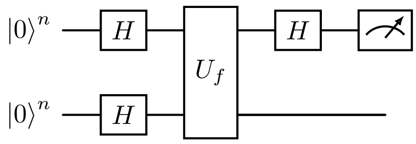
QUESTION 2d

(d) Consider the following algorithm:

- Initialize with the state $|0\rangle^n \otimes |0\rangle^n \in \mathbb{C}^{\otimes n} \otimes \mathbb{C}^{\otimes n}$.
- Apply $H^{\otimes n} \otimes \mathbf{1}$.
- Apply U_f.
- Apply $H^{\otimes n} \otimes \mathbf{1}$ again.
- Measure the first n qubits.

Show that the output encodes a vector $\vec{z} \in S^{\perp}$.

Solution 2d:



- Initialize: Start with the state $|0\rangle^{\otimes n} \otimes |0\rangle^{\otimes n}$.
- Apply Hadamard Transform ($H^{\otimes n}$): Apply $H^{\otimes n}$ to the first n qubits, creating a superposition:

$$\frac{1}{\sqrt{2^n}} \sum_{x \in V} |x\rangle.$$

- Apply Oracle U_f: Apply U_f to compute $f(x)$, resulting in:

$$\frac{1}{\sqrt{2^n}} \sum_{x \in V} |x\rangle \otimes |f(x)\rangle.$$

- Apply Hadamard Transform ($H^{\otimes n}$) Again: Apply $H^{\otimes n}$ to the first n qubits again, transforming the state to:

$$\frac{1}{2^n} \sum_{x \in V} \sum_{z \in V} (-1)^{x \cdot z} |z\rangle \otimes |f(x)\rangle.$$

- Measure the Input Register: Measure the first n qubits, collapsing the state to $|z\rangle$ for some $z \in V$.

QUESTION 2e

Matthew Yu - 400322243 (e) Conclude that each run of the algorithm yields an element of $S^\perp$ uniformly at random. Suppose now that you have generated $\{\vec{v}_1, \ldots, \vec{v}_k\} \subseteq S^\perp$ linearly independent vectors. Show that the probability that the next generated vector is not in span$\{\vec{v}_1, \ldots, \vec{v}_k\}$ is $1 - \frac{2^k}{2^{n-1}}$, and so the expected number of runs to find the $k+1$-st independent vector $\vec{v}_{k+1}$ is $\frac{2^{n-1}}{2^{n-1}-2^k}$ (hint: it's a Bernoulli trial).

Solution 2e: After generating k linearly independent vectors $\{\vec{v}_1, \ldots, \vec{v}_k\} \subseteq S^\perp$, the span span$\{\vec{v}_1, \ldots, \vec{v}_k\}$ contains 2^k vectors. Since $S^\perp$ has 2^{n-1} vectors in total, the number of vectors not in the span is:

$$2^{n-1} - 2^k.$$

The probability that a new vector is not in the span is:

$$\frac{2^{n-1} - 2^k}{2^{n-1}} = 1 - \frac{2^k}{2^{n-1}}.$$

Each trial is a Bernoulli experiment with success probability $p = 1 - \frac{2^k}{2^{n-1}}$. The expected number of trials to achieve the first success in a geometric distribution is $\frac{1}{p}$. Substituting p, the expected number of trials is:

$$\text{Expected trials} = \frac{1}{1 - \frac{2^k}{2^{n-1}}} = \frac{2^{n-1}}{2^{n-1} - 2^k}.$$

QUESTION 2f

Matthew Yu - 400322243 (f) **Optional:** Prove that the expected number of trials to generate $n-1$ linearly independent vectors is then

$$\sum_{k=0}^{n-2} \frac{2^{n-1}}{2^{n-1}-2^k} = (n-1) + \sum_{i=1}^{n-1} \frac{1}{2^i - 1} \sim O(n)$$

and so we can generate $n-1$ linearly independent vectors from $S^{\perp}$ with on the order of n trials.

Solution 2f:

1. Simplify the Summation
   Substitute $i = n-1-k$. When k ranges from 0 to $n-2$, i ranges from 1 to $n-1$. The summation becomes:
   $$\sum_{i=1}^{n-1} \frac{2^i}{2^i - 1}.$$
2. Split the Term
   Notice that:
   $$\frac{2^i}{2^i - 1} = 1 + \frac{1}{2^i - 1}.$$
   Thus, the summation splits into:
   $$\sum_{i=1}^{n-1} 1 + \sum_{i=1}^{n-1} \frac{1}{2^i - 1} = (n-1) + \sum_{i=1}^{n-1} \frac{1}{2^i - 1}.$$
3. Analyze the Second Sum
   The series $\sum_{i=1}^{\infty} \frac{1}{2^i - 1}$ converges to a constant (approximately 1.606). Therefore:
   $$\sum_{i=1}^{n-1} \frac{1}{2^i - 1} \le \sum_{i=1}^{\infty} \frac{1}{2^i - 1} = O(1).$$

QUESTION 2g -

(g) Suppose we have performed the algorithm n times, and so (with high probability!) we have a set of linearly independent $\{\vec{z}_1, \ldots, \vec{z}_{n-1}\} \subseteq S^{\perp}$. Show that $\vec{s} \in V$ is the unique solution to the system of equations

$$\vec{z}_1 \cdot \vec{s} = 0$$
$$\vdots$$
$$\vec{z}_{n-1} \cdot \vec{s} = 0.$$

(Hint: $\text{span}(\vec{s}) = \{\vec{0}, \vec{s}\}$).

Solution 2g:

We are given $n-1$ linearly independent vectors $\{\vec{z}_1, \ldots, \vec{z}_{n-1}\} \subseteq S^{\perp}$, where $S = \text{span}\{\vec{s}\}$. We need to show that $\vec{s}$ is the unique solution to the system of equations:

$$\begin{cases} \vec{z}_1 \cdot \vec{s} = 0, \\ \quad \vdots \\ \vec{z}_{n-1} \cdot \vec{s} = 0. \end{cases}$$

The vectors $\{\vec{z}_1, \ldots, \vec{z}_{n-1}\}$ span $S^{\perp}$, which is an $(n-1)$-dimensional subspace of $V = (\mathbb{Z}/2\mathbb{Z})^n$. The system $\vec{z}_i \cdot \vec{s} = 0$ for $i = 1, \ldots, n-1$ defines a homogeneous linear system over $\mathbb{Z}/2\mathbb{Z}$. Since the $\vec{z}_i$ are linearly independent, the system has rank $n-1$, and the solution space has dimension $n - (n-1) = 1$.

The solution space consists of all vectors orthogonal to $S^{\perp}$. By definition, $\vec{s} \in S$, and S is orthogonal to $S^{\perp}$, so $\vec{s}$ satisfies $\vec{z}_i \cdot \vec{s} = 0$ for all i. Over $\mathbb{Z}/2\mathbb{Z}$, the solution space is $S = \text{span}\{\vec{s}\}$, which contains exactly two vectors: $\vec{0}$ and $\vec{s}$. Since $\vec{0}$ is trivial, the only non-trivial solution is $\vec{s}$.

Therefore, the system $\vec{z}_i \cdot \vec{s} = 0$ for $i = 1, \ldots, n-1$ has a unique non-trivial solution $\vec{s}$. $\vec{s}$ is uniquely determined by these equations.

$$\boxed{\vec{s} \text{ is the unique solution to the system } \vec{z}_i \cdot \vec{s} = 0 \text{ for } i = 1, \ldots, n-1.}$$