CS 506 – Class Notes

Scriber: Mohsen Dehghankar

October 1st 2025

1 Simon's Problem

Our goal is to solve the following problem:

Simon's problem Given a black-box function $f : \{0, 1\}^n \rightarrow \{0, 1\}^n$ with the guarantee that:

- There exists a vector $\vec{s} \in \{0, 1\}^n$, such that $\vec{s} \neq \vec{0}$ and we have:

$$f(\vec{x}) = f(\vec{x} \oplus \vec{s})$$

  for all $\vec{x} \in \{0, 1\}^n$

The goal is to find $\vec{s}$ using (a few) queries to f.

1.1 Classical Result on Hardness

In the classical setting, where no quantum queries are allowed, one can show the following claim:

Claim: Let $\mathcal{A}$ be a randomized algorithm that solves Simon's problem with probability of success at least $\frac{2}{3}$. Then, it should make $\Omega(2^{\frac{n}{3}})$ queries to function f. In other words, it's exponential to n.

However, here, in this context, we are allowed to have *Quantum Queries*. That's why this classical hardness result is not applied to what we are going to discuss.

2 Preliminaries

We start by giving some preliminaries on vector spaces from linear algebra. Then, we define *Generalized Simon's problem* and give an intuition on how to solve it with linear number of queries (linear to dimension n).

2.1 Standard Vector Space

Definition The set $\mathbb{Z}_2^n$ denotes the vector space consisting of all binary vectors $\vec{x} \in \{0, 1\}^n$.

- **Operations:** Vector addition is defined component-wise modulo 2, denoted by $\oplus$. For $\vec{x} = (x_1, \ldots, x_n)$ and $\vec{y} = (y_1, \ldots, y_n)$,

$$\vec{x} \oplus \vec{y} \equiv (x_1 \oplus y_1, \ldots, x_n \oplus y_n), \quad \text{where } \oplus \text{ is addition modulo 2.}$$

- **Dimension:** The dimension of $\mathbb{Z}_2^n$ is n, corresponding to the number of basis vectors.
- **Standard Basis:** A canonical basis for $\mathbb{Z}_2^n$ is given by

$$e_1 = (1, 0, 0, \ldots, 0), \quad e_2 = (0, 1, 0, \ldots, 0), \quad \ldots, \quad e_n = (0, 0, 0, \ldots, 1).$$

2.2 Example of a Vector Space

Consider the set $S = \{\vec{0}, \vec{s}\}$. The span of S is

$$\text{span}(S) = \{\vec{0}, \vec{s}\},$$

which is the same as S itself. Hence, S is a subspace of $\mathbb{Z}_2^n$.

- **Basis of S:** The only nonzero basis vector is $\vec{s}$, so the dimension of S is 1.

$$\vec{0} = \vec{s} + \vec{s}, \tag{1}$$
$$\vec{s} = \vec{s}. \tag{2}$$

Now consider the orthogonal subspace

$$S^\perp = \{\vec{z} \in \mathbb{Z}_2^n \mid \vec{z} \cdot \vec{s} = 0\},$$

where $\cdot$ denotes the inner product modulo 2.

- The dimension of $S^\perp$ is $n - 1$.
- In general, for a subspace $S \subseteq \mathbb{Z}_2^n$,

$$\dim(\mathbb{Z}_2^n) = \dim(S) + \dim(S^\perp).$$

- Thus, $S^\perp$ has $n - 1$ basis vectors, say $\{\vec{b}_1, \ldots, \vec{b}_{n-1}\}$, where

$$\vec{b}_i \cdot \vec{s} = 0 \quad \forall i \leq n - 1,$$

  and the basis vectors $\vec{b}_i, \vec{b}_j$ are mutually orthogonal (with respect to the modulo 2 inner product).

3 A Bridge Problem

We now consider the following problem: suppose you are given the subspace $S^\perp$, as defined above. Your goal is to recover the corresponding vector $\vec{s}$ such that

$$S^\perp = \{\vec{z} \in \mathbb{Z}_2^n \mid \vec{z} \cdot \vec{s} = 0\}.$$

Assuming you are allowed to sample from $S^\perp$, how can you determine $\vec{s}$?

Suppose that we sample uniformly at random vectors from $S^\perp$, $n-1$ times, and we get vectors $\vec{c_1}, \cdots \vec{c_{n-1}}$ and suppose that c_i are mutually *independent* (* what is the probability of this happening?).

3.1 Uniform Sampling

One approach is to sample $n - 1$ vectors $\vec{c}_1, \ldots, \vec{c}_{n-1}$ uniformly from $S^\perp$. If these vectors are linearly independent (discussed later), they form a basis for $S^\perp$. The corresponding vector $\vec{s}$ is then the unique vector orthogonal to all of them.

Formulation. We need to solve the system of equations

$$\vec{c}_i \cdot \vec{s} = 0 \pmod 2, \quad \forall i = 1, \ldots, n - 1.$$

This can be expressed in matrix form as:

$$M = \begin{bmatrix} \vec{c}_1^\top \\ \vec{c}_2^\top \\ \vdots \\ \vec{c}_{n-1}^\top \end{bmatrix}, \qquad s = \begin{bmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{bmatrix}, \qquad Ms \equiv \vec{0} \pmod 2.$$

Solution. Solving this linear system over $\mathbb{Z}_2$ can be done using Gaussian elimination in $O(n^3)$ time. The nontrivial solution obtained gives the desired vector $\vec{s}$.

3.1.1 Probability of Independence of Sampled Vectors

Problem. What is the probability that the sampled vectors $\vec{c}_1, \ldots, \vec{c}_{n-1}$ from $S^\perp$ are linearly independent?

Step 1: Conditional probability. The probability can be decomposed as

$$P[\text{all independent}] = P[\vec{c}_2 \text{ independent} \mid \vec{c}_1] \cdot P[\vec{c}_3 \text{ independent} \mid \vec{c}_1, \vec{c}_2] \cdots P[\vec{c}_{n-1} \text{ independent} \mid \vec{c}_1, \ldots, \vec{c}_{n-2}].$$

Step 2: Single step. Suppose $T_{k-1} = \{\vec{c}_1, \ldots, \vec{c}_{k-1}\}$ is linearly independent. Then the span of T_{k-1} contains 2^{k-1} vectors. Since there are in total 2^{n-1} possible vectors in $S^\perp$, the probability that a newly chosen vector $\vec{c}_k$ lies outside this span (and is therefore independent) is

$$P[\vec{c}_k \text{ independent} \mid T_{k-1}] = \frac{2^{n-1} - 2^{k-1}}{2^{n-1}}.$$

Step 3: Full product. Thus, the overall probability that $n-1$ sampled vectors are linearly independent is

$$P[\text{success}] = \prod_{k=2}^{n-1} \left(1 - \frac{2^{k-1}}{2^{n-1}}\right) = \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{4}\right) \cdots \left(1 - \frac{1}{2^{n-2}}\right)$$

Here, we skipped $k = 1$, because for the first vector $\vec{c_1}$, the probability is always 1.

Step 4: Limit. As $n \to \infty$, this product converges to a constant known as the *binary q-series* (or 2-series). As a result, we get:

$$\lim_{n\to\infty} P[\text{success}] > 0.288.$$

3.1.2 How to Avoid Complicated Calculations

In general, for any $0 < a_i \leq 1$, we have the inequality

$$(1 - a_1)(1 - a_2) \cdots (1 - a_t) \;\geq\; 1 - (a_1 + a_2 + \cdots + a_t).$$

Application. Applying this bound to $P[\text{success}]$, we obtain:

$$P[\text{success}] = \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{2^2}\right) \cdots \left(1 - \frac{1}{2^{n-2}}\right) \geq \left(1 - \frac{1}{2}\right) \cdot \left(1 - \sum_{i=2}^{n-2} \frac{1}{2^i}\right)$$

Simplification. We can obtain an upper bound for the right term based on the geometric series:

$$\sum_{i=2}^{n-2} \frac{1}{2^i} \leq \sum_{i=2}^{\infty} \frac{1}{2^i} = \frac{\frac{1}{4}}{1 - \frac{1}{2}} = \frac{1}{2}$$

So we have:

$$P[\text{success}] \geq (1 - \frac{1}{2}) \cdot (1 - \frac{1}{2}) = \frac{1}{4} = 0.25$$

3.2 How to Sample

We randomly sample $n-1$ vectors from $S^\perp$. **But how can we sample from $S^\perp$ without knowing $\vec{s}$ in the first place?** This step cannot be carried out classically in a straightforward way, it requires a quantum algorithm!

4 Generalized Simon's Problem

Consider a black-box function

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

which implicitly defines a hidden subspace $S \subseteq \mathbb{Z}_2^n$. The promise is that for all $\vec{x}, \vec{y} \in \mathbb{Z}_2^n$,

$$f(\vec{x}) = f(\vec{y}) \iff \big(\vec{x} = \vec{y} \text{ or } \vec{x} - \vec{y} \in S\big).$$

Goal. The task is to determine a basis for the subspace S using as few (quantum) queries to f as possible.

Result.

- The number of quantum queries required is

$$O\big(n - \dim(S)\big).$$

- This follows the same intuition we get from the previous Bridge Problem.