Lecture Notes: Simon's Problem

Introduction to Quantum Computing, CS 506

Scribe: Purvi Vadher

October 6, 2025

1 Simon's Problem

1.1 Problem Statement

Given a blackbox function $f : \{0,1\}^n \to X$ with the guarantee that:

$$\exists \vec{s} \in \{0,1\}^n, \vec{s} \neq 0^n \text{ such that}$$

$$f(\vec{x}^1) = f(\vec{x}^1 \oplus \vec{s}) \text{ for all } \vec{x} \in \{0,1\}^n$$

The function exhibits **bitwise exclusive or** behavior.
Goal: Find $\vec{s}$ using queries to f.
Query format: Input $\vec{x}$, get $f(\vec{x})$.

1.2 Generalized Simon's Problem

Key Insight: It is possible to design a quantum circuit without knowing all the elements of the subspace.

1.3 The U_f Gate

The quantum oracle implements:

$$U_f \left|\vec{x}\right\rangle \left|b\right\rangle = \left|\vec{x}\right\rangle \left|b \oplus f(\vec{x})\right\rangle$$

Where:

- $\vec{x}$ consists of n qubits: $x_1, x_2, \ldots, x_n$
- $\vec{b}$ contains ancilla qubits for the output: $b_1, b_2, \ldots$
- The operation maps: $\vec{x} \to \vec{x}$ and $\vec{b} \to \vec{b} \oplus f(\vec{x})$

Circuit diagram for U_f gate:

$$\begin{array}{ccccc}
 & & & & b_1 \oplus y_1 \\
\vec{b} & \{ & b_1 & \longrightarrow & \\
 & & b_n & \longrightarrow & b_n \oplus y_n \\
 & & & U_f & \\
 & & x_1 & \longrightarrow & x_1 \\
\vec{x} & \{ & \vdots & & \vdots \\
\in \{0,1\}^n & & x_n & \longrightarrow & x_n
\end{array}$$

Where $y_1 \cdots y_n = \vec{y} = f(\vec{x})$.

1.4 Complete Simon's Algorithm Circuit

The full quantum circuit for Simon's algorithm:

$$
\begin{array}{ccccccccc}
 & & H^{\otimes n} & & & & H^{\otimes n} & & \\
n & |0\rangle & -H- & \longrightarrow & & & -H- & \triangleright & \text{measure} \\
 & |0\rangle & -H- & \longrightarrow & & & -H- & \triangleright & \\
 & |0\rangle & & \longrightarrow & U_f & \longrightarrow & & \triangleright & \\
 & |0\rangle & & \longrightarrow & & & & & \\
\hline
 & & & & & & & & \\
 & & & t_1 & t_2 & t_3 & t_4 & t_5 & \\
 & & & |\psi_1\rangle & |\psi_2\rangle & |\psi_3\rangle & |\psi_4\rangle & |\psi_5\rangle &
\end{array}
$$

The circuit proceeds through five distinct states:

- $|\psi_1\rangle$ at t_1: Initial state (all qubits in $|0\rangle$)
- $|\psi_2\rangle$ at t_2: After first Hadamard transform $H^{\otimes n}$ (superposition)
- $|\psi_3\rangle$ at t_3: After U_f oracle query
- $|\psi_4\rangle$ at t_4: After second Hadamard transform $H^{\otimes n}$
- $|\psi_5\rangle$ at t_5: Final state before measurement

2 Circuit Evolution

2.1 State Evolution Through the Circuit

Initial State:

$$|\psi_1\rangle = |0\rangle^{\otimes n} \otimes |0\rangle$$

After Hadamard on first register ($H^{\otimes n}$):

$$|\psi_2\rangle = \left(H^{\otimes n} |0^n\rangle\right) |0^n\rangle = \left(\frac{1}{\sqrt{2^n}} \sum_{\vec{x} \in \{0,1\}^n} |\vec{x}\rangle\right) |0^n\rangle$$

After applying U_f:

$$|\psi_3\rangle = U_f(|\psi_2\rangle) = \frac{1}{\sqrt{2^n}} \sum_{\vec{x} \in \{0,1\}^n} U_f(|\vec{x}\rangle |0\rangle)$$

$$= \frac{1}{\sqrt{2^n}} \sum_{\vec{x} \in \{0,1\}^n} |\vec{x}\rangle |f(\vec{x})\rangle$$

After final Hadamard ($H^{\otimes n}$):

$$|\psi_4\rangle = \frac{1}{\sqrt{2^n}} \sum_{\vec{x} \in \{0,1\}^n} \left(H^{\otimes n} |\vec{x}\rangle\right) |f(\vec{x})\rangle$$

2.2 Example: $n = 3$, $\vec{s} = 010$

Let's trace through a specific example:

Function behavior:

- $f(000) = f(000 \oplus 010) = f(010)$
- $f(001) = f(001 \oplus 010) = f(011)$
- $f(100) = f(100 \oplus 010) = f(110)$

All pairs have the same output.

Output equivalence classes:

$$\{000, 010\}, \{001, 011\}, \{100, 110\}, \{101, 111\}$$

State $|\psi_3\rangle$ becomes:

We can group the terms based on which pairs map to the same function value:

$$\begin{aligned} |\psi_3\rangle = \frac{1}{\sqrt{2^3}} & (|000\rangle |f(000)\rangle + |001\rangle |f(001)\rangle + |010\rangle |f(010)\rangle + |011\rangle |f(011)\rangle \\ & + |100\rangle |f(100)\rangle + |101\rangle |f(101)\rangle + |110\rangle |f(110)\rangle + |111\rangle |f(111)\rangle) \end{aligned}$$

Since $f(\vec{x}) = f(\vec{x} \oplus \vec{s})$, we have $f(000) = f(010)$, $f(001) = f(011)$, $f(100) = f(110)$, and $f(101) = f(111)$. Grouping:

$$\begin{aligned} |\psi_3\rangle = & \frac{1}{\sqrt{2^3}} (|000\rangle + |010\rangle) |f(000)\rangle + \frac{1}{\sqrt{2^3}} (|001\rangle + |011\rangle) |f(001)\rangle \\ & + \frac{1}{\sqrt{2^3}} (|100\rangle + |110\rangle) |f(100)\rangle + \frac{1}{\sqrt{2^3}} (|101\rangle + |111\rangle) |f(101)\rangle \end{aligned}$$

Factoring out $\frac{1}{\sqrt{2}}$:

$$|\psi_3\rangle = \frac{1}{\sqrt{2}} \sum_{\vec{x} \in \{0,1\}^n} \frac{1}{\sqrt{2^{n-1}}} (|\vec{x}\rangle + |\vec{x} \oplus \vec{s}\rangle) |f(\vec{x})\rangle$$

For some representative $\vec{x}$ from each equivalence class.

3 Hadamard Analysis

3.1 Computing $H^{\otimes n}$ on basis states

For a general basis state $|\vec{x}\rangle$:

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

Where $\vec{x} \cdot \vec{z} = \sum_{i=1}^n x_i z_i$ is the bitwise inner product.

3.2 State $|\psi_5\rangle$ after final Hadamard

$$|\psi_5\rangle = H^{\otimes n} \left(\frac{1}{\sqrt{2}} (|\vec{x}\rangle + |\vec{x} \oplus \vec{s}\rangle) \right) |f(\vec{x})\rangle$$

Let's expand this step by step:

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

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

Since $(\vec{x} \oplus \vec{s}) \cdot \vec{z} = \vec{x} \cdot \vec{z} + \vec{s} \cdot \vec{z} \pmod 2$:

$$= \frac{1}{\sqrt{2^n}} \sum_{\vec{z} \in \{0,1\}^n} (-1)^{\vec{x} \cdot \vec{z}} (-1)^{\vec{s} \cdot \vec{z}} |\vec{z}\rangle$$

Combining both terms:

$$|\psi_5\rangle = \frac{1}{\sqrt{2}} \cdot \frac{1}{\sqrt{2^n}} \sum_{\vec{z} \in \{0,1\}^n} (-1)^{\vec{x} \cdot \vec{z}} \left(1 + (-1)^{\vec{s} \cdot \vec{z}} \right) |\vec{z}\rangle |f(\vec{x})\rangle$$

4 Key Observation

$$1 + (-1)^{\vec{s} \cdot \vec{z}} = \begin{cases} 2 & \text{if } \vec{s} \cdot \vec{z} = 0 \\ 0 & \text{if } \vec{s} \cdot \vec{z} = 1 \end{cases}$$

Simplification:

$$|\psi_5\rangle = \frac{1}{\sqrt{2^{n-1}}} \sum_{\vec{z} : \vec{s} \cdot \vec{z} = 0} (-1)^{\vec{x} \cdot \vec{z}} |\vec{z}\rangle |f(\vec{x})\rangle$$

$$= \frac{1}{\sqrt{2^{n-1}}} \sum_{\vec{z} \in \vec{s}^{\perp}} |\vec{z}\rangle |f(\vec{x})\rangle$$

Where $\vec{s}^{\perp} = \{\vec{z} : \vec{s} \cdot \vec{z} = 0\}$ is the orthogonal subspace.