Quantum Computing 106: Simon's Algorithm

Kshipra Wadikar

March 26, 2025

Simon's algorithm demonstrates exponential speedup using quantum mechanics and highlights the power of quantum parallelism and entanglement. It laid the foundation for real-world quantum advantages, including Shor's algorithm, which breaks classical cryptography.

1 Problem Statement: Simon's Algorithm

Throughout this article, unless explicitly stated otherwise, the **oracle function** $f(x)$ is as defined below.
We are given a function $f : \{0,1\}^n \to \{0,1\}^n$ that is either:

1. **One-to-one (injective)**: Each input maps to a unique output.
2. **Two-to-one (periodic)**: There exists a hidden string $s \in \{0,1\}^n$ such that for all $x,\ y \in \{0,1\}^n$:

$$f(x) = f(y) \text{ if and only if } y = x \oplus s$$

where $\oplus$ is bitwise XOR.

The goal is to determine whether $f(x)$ is one-to-one or two-to-one, and in the later case find the hidden string s.

1.1 Example Scenario:

Let us consider a function $f : \{0,1\}^2 \to \{0,1\}^2$ defined as below.

Input x	Output $f(x)$
00	11
01	01
10	11
11	01

Table 1: Example Scenario for $f(x)$

We can See that:

- Since $f(00) = f(10) = 11$, we use the equation $y = x \oplus s$. Substituting $x = 00$ and $y = 10$, we get:

$$10 = 00 \oplus s = s. \text{ Thus } s = 10_2.$$

- Since $f(01) = f(11) = 01$, we use the equation $y = x \oplus s$. Substituting $x = 01$ and $y = 11$, we get:

$$11 = 01 \oplus s = s. \text{ Thus } s = 10_2.$$

1.2 Quantum Circuit for Simon's Algorithm (2 Qubits)

1. For $n = 2$ we start with:
   - 2 input qubits to store x
   - 2 output qubits to store $f(x)$
2. Initialize the qubits in $|0\rangle^{\otimes 4}$ state.

$$|00\rangle |00\rangle$$

.

3. Apply Hadamard transformation $H^{\otimes 2}$ on the first two qbits to create an equal superpoistion of all x values.

$$\frac{1}{\sqrt{2}} \sum_{x \in \{0,1\}^2} |x\rangle |00\rangle$$

.

4. Apply the quantum oracle U_f which maps $|x\rangle |00\rangle \rightarrow |x\rangle |f(x)\rangle$.

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

.

5. **Measure the second register (output qubits)**: This collapses it into a particular $f(x)$ value, leaving a superposition of the two corresponding inputs x and $x \oplus s$.
6. Apply Hadamard Transform on the first qubit register, obtaining an equation for s.
7. Measure the first qubits, that gives a linear equation in s.
8. Repeat as needed until s is determined.

2 Generalization for Any n-Bit Key

For any n-bit key, Simon's algorithm follows these steps:

1. Initialize an n-qubit register in the $|0\rangle^{\otimes n}$ state.
2. Apply Hadamard transform $H^{\otimes n}$ to create uniform superposition:

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

3. Apply the function $f(x)$ as a quantum oracle, entangling the states:

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

4. Measure the second register (output). This collapses it into one of the possible function outputs and entangles the input register into a superposition of two states x and $|x \oplus s$.

5. Apply Hadamard Transform to the first n-qubit register.

6. Measure the first register to get an equation of the form:

$$s \cdot z = 0 \pmod 2$$

where z is a random measurement outcome.

7. Repeat steps until $n - 1$ linearly independent equations are obtained.

8. Solve for s using Gaussian elimination.

3 Conclusion and Next Steps

Simon's algorithm provides one of the first examples of an exponential quantum speedup over classical algorithms, demonstrating the power of quantum parallelism and entanglement. Moreover, it laid the foundation for real-world quantum advantages, particularly influencing Shor's algorithm.

In the next article, we will explore **Shor's Algorithm**, which extends these principles to efficiently factor large integers, posing a significant challenge to classical cryptographic systems.

References

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2010. See Section 5.2.3 for a discussion of Simon's algorithm, including its role in demonstrating quantum advantage and its connection to Shor's algorithm.