Санкт-Петербургский
политехнический университет
Петра Великого
Институт
электроники
и телекоммуникаций

Simon's Algorithm (Part 1)

Предмет:
Оптоинформатика и
квантовая криптография

Учитель:
Ушаков Николай
Александрович

Студент:
Парра Орельяна
Фредди Андрес

Дата:
10 марта 2023 г.

Content

Concepts used

1. Predecent

1.1. What is Simon problem?

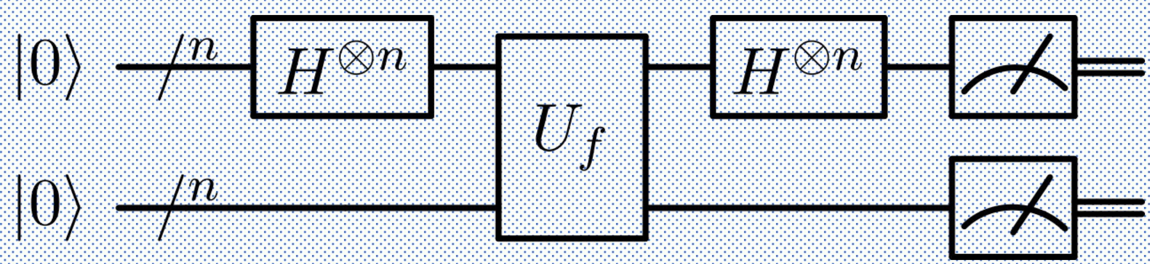
Simon's problem is a computational problem that is proven to be solved exponentially faster on a quantum computer than on a classical computer. In 1994 Daniel Simon exhibited a quantum algorithm_that solves Simon's problem.

The quantum algorithm solving Simon’s problem = Simon's Algorithm

2. Simon´s Algorithm

Given a function f: $\{0,1\}^n \rightarrow \{0,1\}^n$, such that $f(x) = f(x \oplus s)$ for $s \in \{0,1\}^n$. Our goal is to find s.

<u>Quantum circuit</u>



3. Explanation of Simon´s Algorithm by stages

3.1. First stage $|\varphi_1\rangle$

$$|\varphi_1\rangle = |x\rangle_A^{\otimes n} \, |y\rangle_B^{\otimes n}$$

3.2. Second stage $|\varphi_2\rangle$

Hadamard gate is applied to register A.

$$|\varphi_2\rangle = \boldsymbol{H}^{\otimes n}|x\rangle_A^{\otimes n} \, |y\rangle_B^{\otimes n} = \frac{1}{\sqrt{2^2}} \sum_{x=0}^{2^n-1} |x\rangle_A^{\otimes n} \, |y\rangle_B^{\otimes n}$$

3.2. Third stage $|\varphi_3\rangle$

Registers A and B are inputs 1 and 2 for Module Oracle model

$$|\varphi_3\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle_1 \cdot |y \otimes f(x)\rangle_2 = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \cdot |f(x)\rangle$$

3. Explanation of Simon´s Algorithm by stages

3.3. Fourth stage $|\varphi_4\rangle$

$$|\varphi_3\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle|f(x)\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (|x\rangle + |x \oplus s\rangle)\, |f(x)\rangle$$

$$|\varphi_4\rangle = \frac{1}{\sqrt{2}} (|x\rangle + |x \oplus s\rangle)$$

3.4. Fifth stage $|\varphi_5\rangle$

$$|\varphi_5\rangle = \frac{1}{\sqrt{2}} (\boldsymbol{H}^{\otimes n}|x\rangle + \boldsymbol{H}^{\otimes n}|x \oplus s\rangle)|f(x)\rangle$$

$$|\varphi_5\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} \sum_{z=0}^{2^n-1} (-1)^{z \cdot x}|z\rangle\, |f(x)\rangle$$

3. Explanation of Simon´s Algorithm by stages

3.4. Fifth stage

When we measure this state, we will obtain a uniformly random element of the set Y_s

$$Y_s = \{z: z \cdot s = 0 \, mod \, 2\}$$

Now we repeat this whole process k times to obtain $y_1, \dots, y_k \in Y_s$.

Put the $y_1, \dots, y_k$ as the rows of a matrix A.

$$A\,X = 0$$

$$\begin{bmatrix} \cdots & y_1 & \cdots \\ \cdots & y_2 & \cdots \\ & \vdots & \\ \cdots & y_k & \cdots \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_{n-1} \end{bmatrix} = 0$$

If the rank of A is $n-1$ then 0_n and s are the only solutions to this equation. The excepted number of trials to find $n-1$ lineal independent string is at most $2n$

4. Examples

4.1. Example 1

Quantum algorithm that solves Simon's problem exponentially faster and with exponentially fewer queries than the best probabilistic (or deterministic) classical algorithm

$$Birthday\ problem \rightarrow \begin{cases} P(x=0)=0{,}92566 \\ P(at\ least\ 2)=0{,}074335 \\ P(x=2)=0{,}07239 \\ P(x=3)=4{,}03x10^{-4} \\ P(x=2\ \cup x=3) \\ P(x\leq 3)=P(x=0,x=2,x=3) \end{cases}$$

4.2. Example 2

$n=3, f(0)=f(5)=4, f(1)=f(4)=1, f(2)=f(7)=2, f(3)=f(6)=7$. Find s.

Classical solution (desktop test - Python function)

$s=101; O(2^n)$

Quantum solution (desktop test - доска школьная)

$s=101; O(n)$

4. Bibliography

Simon, Daniel R. (1997-10-01). "On the Power of Quantum Computation". SIAM Journal on Computing. 26 (5): 1474–1483. doi:10.1137/S0097539796298637. ISSN 0097-5397

Concepts used

1. Hadamard Gate

Is nothing more than a 2×2 Discrete Fourier Transform matrix (two-point DFT).

$$\boldsymbol{H} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

The qubit $|x\rangle$ ($x \in \{0,1\}$) can be represented using the standard euclidean basis.

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

<u>The equation for Hadamard gate transformation on multiple qubits is:</u>

$$\boldsymbol{H}^{\otimes n}|x_1, \dots, x_n\rangle = \frac{1}{\sqrt{2^n}} \sum_{z=0}^{2^n - 1} (-1)^{x_n \cdot z} |z\rangle$$

<u>Hadamard Gate gives a superposition of all possible stages of qubit.</u>

Examples:

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

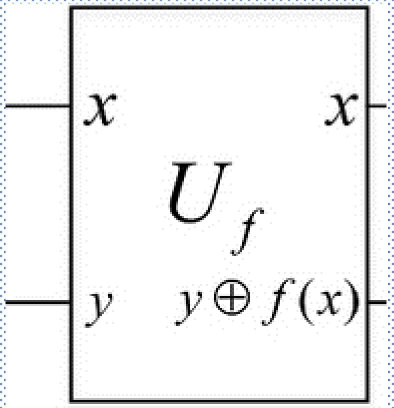
$$\boldsymbol{H}|00\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

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

2. Module Oracle model

Is a **black box** where encodes a function $f\colon \{0,1\}^n \to \{0,1\}$

The behavior of black box is determined by the unitary map O_f



$$O_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$$

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

3. Combinations without repetition

$$C_n^r = \binom{n}{r} = \frac{n!}{r! \cdot (n-r)!}$$