Simon's Algorithm

Samuel J. Lomonaco, Jr.
Dept. of Computer Science & Electrical Engineering
University of Maryland, Baltimore County
Baltimore, MD 21250
Email: Lomonaco@UMBC.EDU
WebPage: http://www.csee.umbc.edu/~lomonaco

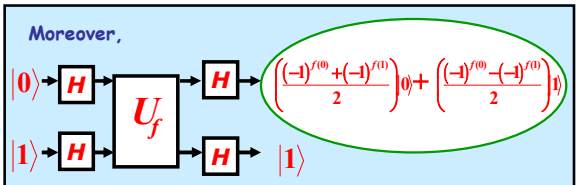
1

Evolution of an idea

- Deutsch: Quantum Turing Machine
  - Meyers found that QTM was flawed
- Deutsch-Jozsa algorithm
- Bernstein-Vazirani algorithm
- Simon's Algorithm
  - First Q algorithm exponentially faster classical algorithms
- Shor's algorithm
  - He recognized Simon's period find method could be applied to other problems
- Kitaev: Quantum Hidden subgroup algorithms

2

Moreover,



Case 1. f is fair, i.e., balanced

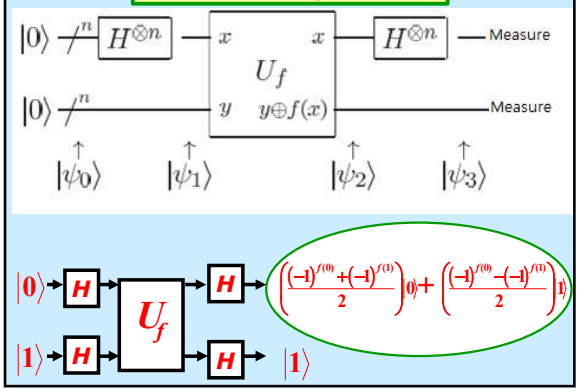
$$\text{Output} = 0 \bullet |0\rangle|1\rangle + \left(\frac{(-1)^{f(0)}-(-1)^{f(1)}}{2}\right)|1\rangle|1\rangle = \pm|1\rangle|1\rangle$$

Case 2. f is unfair, i.e., constant

$$\text{Output} = \left(\frac{(-1)^{f(0)}+(-1)^{f(1)}}{2}\right)|0\rangle|1\rangle + 0 \bullet |1\rangle|1\rangle = \pm|0\rangle|1\rangle$$

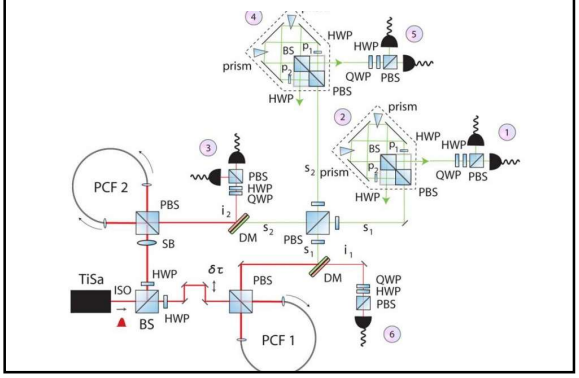
3

Simon's Algorithm



4

Simon's algorithm on optical workbench



5

Let $\mathbb{F}_2, +, \cdot$ be the field of two elements **0** and **1**, let $\mathbb{F}_2^{\,n}$ be the vector space of binary **n**-tuples, with inner product

$$(a_{n-1},\ldots,a_1,a_0)\bullet(b_{n-1},\ldots,b_1,b_0) = \sum_{j=0}^{n-1} a_j b_j \pmod 2$$

Simon's Problem: Given a 2-to-1 function (called an oracle) $f : \mathbb{F}_2^{\,n} \to \mathbb{F}_2^{\,n}$ with unknown period **a**, i.e., with element $a \in \mathbb{F}_2^{\,n}$ such that

$$f(x+a) = f(x), \forall x \in \mathbb{F}_2^{\,n},$$

find the period **a**.

6

It has been proven that all classical algorithms for solving Simon's algorithm have time complexity $\Omega\left(2^{n/2}\right)$.

Most amazingly, the quantum algorithm by Daniel Simon solves this problem in polytime!

7

Before we begin to describe Simon's algorithm, we should mention that there are two different types of vector spaces involved in this algorithm, namely:

1) The 2^n – D Hilbert space $\mathcal{H}_{2^n}$ over the complex numbers $\mathbb{C}$, which is the state space for **n** qubits, and

2) The **n**-D vector space $\mathbb{F}_2^{\,n}$, where the **n** bit binary vectors in $\mathbb{F}_2^{\,n}$ are used to label the standard basis kets of $\mathcal{H}_{2^n}$.

8

To simply our description of Simon's algorithm, we identify $\mathbb{F}_2^{\,n}$ with the set $\{0,1\}^n$ of binary strings of length **n**. And in turn, identify $\{0,1\}^n$ with the integers $\{0,1,2,\ldots,2^n-1\}$.

Under the above identifications, the standard linear ordering **<** on the integers induces a linear ordering on $\mathbb{F}_2^{\,n}$ and $\{0,1\}^n$, also denoted by **<**.

9

All unitary transformations are reversible actions. So, before continuing, we need to know how to implement a non-reversible Boolean function

$$\begin{array}{ccc} g:\{0,1\}^n & \to & \{0,1\}^m \\ x & \mapsto & g(x) \end{array}$$

This can be done by enlarging **g** to the reversible function

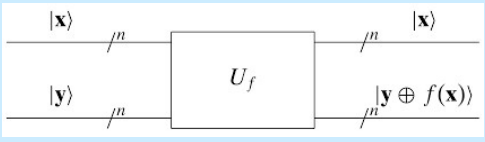
$$\begin{array}{ccc} \tilde{g}:\{0,1\}^n\times\{0,1\}^m & \to & \{0,1\}^n\times\{0,1\}^m \\ (x,y) & \mapsto & (x,y+g(x)\ ) \end{array}$$

where "**+**" denotes bitwise addition **mod 2**.

10

Thus, the Boolean function **f** can be implemented as the unitary transformation

$$\begin{array}{ccc} U_g:\mathcal{H}_{2^n}\otimes\mathcal{H}_{2^m} & \to & \mathcal{H}_{2^n}\otimes\mathcal{H}_{2^m} \\ |x\rangle|y\rangle & \mapsto & |x\rangle|y+g(x)\rangle \end{array}$$



Exercise: Find the inverse of the above unitary transformation. Hint: Compute $U_g^{\,2}$.

11

In preparation for our description of Simon's algorithm, we proceed to implement the oracle f as a unitary transformation U_f.

Let $\mathcal{H}_{2^n}$ be the **2ⁿ**- D Hilbert space with orthonormal basis $\{|b\rangle : b\in\mathbb{F}_2^{\,n}\}$, and let $\mathbf{U_f}$ denote the unitary transformation

$$\begin{array}{ccc} U_f:\mathcal{H}_{2^n}\otimes\mathcal{H}_{2^n} & \to & \mathcal{H}_{2^n}\otimes\mathcal{H}_{2^n} \\ |x\rangle|y\rangle & \mapsto & |x\rangle|y+g(x)\rangle \end{array}$$

Where "**+**" denotes vector addition in $\mathbb{F}_2^{\,n}$.

12

Simon's Algorithm

Step 0. Initialize by preparing the state

$$|\psi_0\rangle = |0\rangle|0\rangle \in \mathcal{H}_{2^n} \otimes \mathcal{H}_{2^n}$$

Step 1. Apply the Hadamard transform $H^{\otimes n} \otimes I^{\otimes n}$ to obtain

$$|\psi_1\rangle = \left(H^{\otimes n} \otimes I^{\otimes n}\right)|\psi_0\rangle = 2^{-n/2}\sum_{j=0}^{2^n-1}|j\rangle|0\rangle,$$

Step 2. Apply U_f to obtain

$$|\psi_2\rangle = U_f|\psi_1\rangle = 2^{-n/2}\sum_{j=0}^{2^n-1}|j\rangle|f(j)\rangle$$

13

Simon's Algorithm (Cont.)

Step 2. Apply U_f to obtain

$$|\psi_2\rangle = U_f|\psi_1\rangle = 2^{-n/2}\sum_{j=0}^{2^n-1}|j\rangle|f(j)\rangle$$

Step 2'. Measure the right register to obtain

$$|\psi_{2'}\rangle = \frac{1}{\sqrt{2}}\left[\left(|j_0\rangle + |j_0+a\rangle\right)|f(j_0)\rangle\right]$$

where $j_0 < j_0+a$,

14

Simon's Algorithm (Cont.)

Step 2'. Measure the right register to obtain

$$|\psi_{2'}\rangle = \frac{1}{\sqrt{2}}\left[\left(|j_0\rangle + |j_0+a\rangle\right)|f(j_0)\rangle\right]$$

Step 3. Apply the Hadamard transform to the left register qubits to obtain

$$\begin{aligned}|\psi_3\rangle &= \left(H^{\otimes n} \otimes I^{\otimes n}\right)|\psi_{2'}\rangle \\ &= 2^{-(n+1)/2}\sum_{k=0}^{2^n-1}\left[(-1)^{j_0\cdot k}|k\rangle + (-1)^{(j_0+a)\cdot k}|k\rangle\right]|f(j_0)\rangle \\ &= 2^{-(n+1)/2}\sum_{k=0}^{2^n-1}\left[(-1)^{j_0\cdot k}\left(1+(-1)^{a\cdot k}\right)|k\rangle\right]|f(j_0)\rangle,\end{aligned}$$

15

Simon's Algorithm (Cont.)

Step 3. Apply the Hadamard transform to the left register qubits to obtain

$$\begin{aligned}|\psi_3\rangle &= \left(H^{\otimes n} \otimes I^{\otimes n}\right)|\psi_{2'}\rangle \\ &= 2^{-(n+1)/2}\sum_{k=0}^{2^n-1}\left[(-1)^{j_0\cdot k}|k\rangle + (-1)^{(j_0+a)\cdot k}|k\rangle\right]|f(j_0)\rangle \\ &= 2^{-(n+1)/2}\sum_{k=0}^{2^n-1}\left[(-1)^{j_0\cdot k}\left(1+(-1)^{a\cdot k}\right)|k\rangle\right]|f(j_0)\rangle,\end{aligned}$$

But

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

16

Simon's Algorithm (Cont.)

Step 3. Apply the Hadamard transform to the left register qubits to obtain

$$|\psi_3\rangle = 2^{-(n+1)/2}\sum_{\substack{k=0 \\ a\cdot k=0}}^{2^n-1}\left[(-1)^{j_0\cdot k}|k\rangle\right]|f(j_0)\rangle)$$

Step 4. Measure the left register to obtain

$$|\psi_4\rangle = |k_0\rangle|f(j_0)\rangle$$

where k_0 is a binary n-tuple such that $k_0 \cdot a = 0$ is a linear equation over $\mathbb{F}_2$ satified by unknown a .

17

Simon's Algorithm (Cont.)

Step 4. Measure the left register to obtain

$$|\psi_4\rangle = |k_0\rangle|f(j_0)\rangle$$

where k_0 is a binary n-tuple such that $k_0 \cdot a = 0$ is a linear equation over $\mathbb{F}_2$ satified by unknown a .

Step 5. Repeat Steps 0 through 4 until enough linear equations have been obtained to solve the system of equations for the unknown period a .

18

Simon's Algorithm

Exercise: Given the oracle

$$f: \begin{cases} 00 \mapsto 01 \\ 01 \mapsto 11 \\ 10 \mapsto 11 \\ 11 \mapsto 01 \end{cases}$$

Find in (the standard basis) the **16X16** matrix for the unitary transformation U_f .

19