CLASS HANDOUT ON SIMON'S ALGORITHM

SAMUEL J. LOMONACO

Abstract. This is a class handout describing Simon's algorithm.

Contents

1. Preliminaries

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

Problem 1 (Simon's Problem)**.** ***Given a 2-to-1 map*** $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n$ *(not necessarily a morphism) with unknown period* a*, i.e., an 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*.*

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 set of integers $\{j \in \mathbb{Z} : 0 \leq j < 2^n\}$. Under these identifications, the standard linear orderling $<$ of the integers induces a linear ordering on $\mathbb{F}_2^n$ and $\{0,1\}^n$, also denoted by $<$.

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

$$\begin{array}{rccc} U_f : \mathcal{H}_{2^n} \otimes \mathcal{H}_{2^n} & \longrightarrow & \mathcal{H}_{2^n} \otimes \mathcal{H}_{2^n} \\ |x\rangle\,|y\rangle & \longmapsto & |x\rangle\,|y + f(x)\rangle \end{array}\ ,$$

where "+" denotes addition in $\mathbb{F}_2^n$.

Date: May 3, 2015.

2. Simon's Algorithm

Simon's algorithm for finding the unknown period a is as follows:

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 $H^{\otimes n} \otimes 1^{\otimes n}$ to obtain

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

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

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

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

where $j_0 < j_0 + a$.

Step 3. Apply the Hadamard transform $H^{\otimes n} \otimes 1^{\otimes n}$ to obtain

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

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

where "$\cdot$" denotes the inner product for $\mathbb{F}_2^n$. But

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

Hence,

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

Step 4. Measure the left register to obtain

$$|\psi_3\rangle = |k_0\rangle\,|f(j_0)\rangle \ ,$$

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

Step 5. Repeat Steps 0 to 4 until enough k's have been obtained to be able to use Gaussian elimination to solve the system of equations to find a.

References

[1] Barenco, Andriano, **Quantum Computation: An Introduction**, in **"Introduction to Quantum Computation and Infornmation,"** by Lo, Hoi-Kwong, Sandu Popescu, and Tim Spiller, (editors), World Scientific, (1998). (Read pages 156-159.)

[2] Nielsen, Michael A., and Isaac L. Chuang, **"Quantum Computation and Information,"** Cambridge University Press, (2000).

[3] Reiffel, Eleanor, and Wolfgang Polak, **"Quantum Computing: A Gentle Introduction,"** MIT Press, (2011). (Read pages 144-145.)

University of Maryland Baltimore County, 1000 Hilltop Circle, Baltimore, MD 21250

E-mail address: lomonaco@umbc.edu

URL: http://www.csee.umbc.edu/~lomonaco