Introduction to Quantum Information Processing

QIC 710 / CS 768 / PH 767 / CO 681 / AM 871

Lecture 5 (2016)

Jon Yard
QNC 3126
jyard@uwaterloo.ca
http://math.uwaterloo.ca/~jyard/qic710


H⊗H⊗···⊗H

Viewing $\{0,1\}^n$ as a vector space

$\mathbb{F}_2 = \{0,1\}$ with addition and multiplication mod 2 is a ***field.***

$xy = x \wedge y, \qquad x \oplus y = x + y, \qquad x = -x, \qquad \neg x = x + 1$

$\mathbb{F}_2^n = \{0,1\}^n$ is a n-dimensional vector space over $\mathbb{F}_2$

The usual vector space notions like subspace and dimension make sense here.

$x \cdot y = x_1 y_1 + \cdots + x_n y_n$ is like a "dot product" of the vectors

$x \cdot y = 0$ can be interpreted as the vectors being ***"orthogonal"***

but this notion of orthogonality has some weird properties,

such as the possibility that $x \cdot x = 0$, even for non-zero vectors.

Caution: For n-qubit systems, do not confuse the n-dimensional vector space $\mathbb{F}_2^n$ with the 2^n-dimensional Hilbert space.

About $H \otimes H \otimes \cdots \otimes H = H^{\otimes n}$

Theorem: for $x \in \mathbb{F}_2^n$, $\quad H^{\otimes n}|x\rangle = \frac{1}{2^{n/2}} \sum_{y \in \mathbb{F}_2^n} (-1)^{x \cdot y} |y\rangle$

where $x \cdot y = x_1 y_1 + \cdots + x_n y_n$

Example: $H \otimes H = \frac{1}{2} \begin{pmatrix} +1 & +1 & +1 & +1 \\ +1 & -1 & +1 & -1 \\ +1 & +1 & -1 & -1 \\ +1 & -1 & -1 & +1 \end{pmatrix}$

Proof: For all $x_i \in \mathbb{F}_2$, $H|x_i\rangle = |0\rangle + (-1)^{x_i}|1\rangle = \sum_{y_i \in \mathbb{F}_2} (-1)^{x_i} |y_i\rangle$

Thus, $H^{\otimes n}|x_1, \ldots, x_n\rangle = \left(\sum_{y_1 \in \mathbb{F}_2} (-1)^{x_1} |y_1\rangle \right) \cdots \left(\sum_{y_n \in \mathbb{F}_2} (-1)^{x_n} |y_n\rangle \right)$

$$= \sum_{y \in \mathbb{F}_2^n} (-1)^{x_1 y_1 + \cdots + x_n y_n} |y_1, y_2, \ldots, y_n\rangle$$

Simon’s problem

Quantum vs. classical separations

black-box problem	quantum	classical	
constant vs. balanced	**1** (query)	**2** (queries)	
1-out-of-4 search	**1**	**3**	
constant vs. balanced	**1**	**½ 2^n + 1**	**(only for exact)**
Simon's problem			**(probabilistic)**

Simon's problem

Let $f: \mathbb{F}_2^n \to \mathbb{F}_2^n$ have the property that there exists an $r \in \mathbb{F}_2^n$ such that $f(x + r) = f(x)$ for every $x \in \mathbb{F}_2^n$.

In other words, such that $f(x) = f(y)$ iff $x + y = r$ or $x = y$.

Simons problem: Find r.

Example:

x	$f(x)$
000	011
001	101
010	000
011	010
100	101
101	011
110	010
111	000

What is r is this case? _____

Answer: r = **101**

A classical algorithm for Simon

Search for a ***collision***, an $x \neq y$ such that $f(x) = f(y)$

1. Choose $x_1, x_2, \ldots, x_k \in \mathbb{F}_2^n$ randomly (independently)

2. For all $i \neq j$, if $f(x_i) = f(x_j)$, then output $x_i + x_j$ and halt

A hard case is where r is chosen randomly from nonzero vectors in $\mathbb{F}_2^n$, and then the "table" for f is filled out randomly subject to the structure implied by r.

How big does k have to be for the probability of a collision to be a constant, such as $3/4$?

Answer: order $2^{n/2}$ (each (x_i, x_j) collides with prob. $O(2^{-n})$)

Classical lower bound

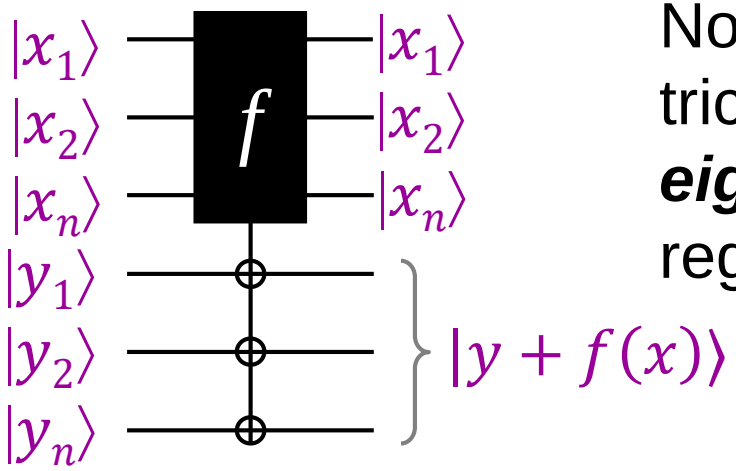
Theorem: ***any*** classical algorithm solving Simon's problem must make at least $\sqrt{\frac{6}{11}2^n} - 1 = \boldsymbol{\Omega}\left(\boldsymbol{2^{n/2}}\right)$ queries

Proof is omitted here (see note on course website) —note that the performance analysis of the previous algorithm does ***not*** imply the theorem.

… how can we know that there isn't a ***different*** algorithm that performs better?

A *quantum* algorithm for Simon I

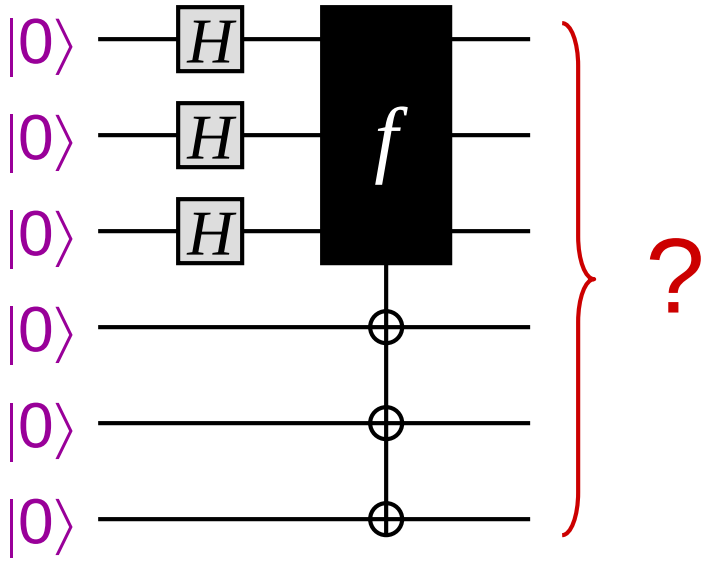
Queries:



Not clear how to apply old trick from Deutch. Which ***eigenvector*** of target registers to use?

Proposed start of quantum algorithm: query all values of f in superposition

What is the output state of this circuit?



A quantum algorithm for Simon II

Answer: the output state is $\sum_{x \in \mathbb{F}_2^n} |x\rangle|f(x)\rangle$

Let $T \subset \mathbb{F}_2^n$ be such that ***one*** element from each matched pair is in T (assume $r \neq$ **00...0**)

Example: could take $T = \{\mathbf{000}, \mathbf{001}, \mathbf{011}, \mathbf{111}\}$

Then the output state can be written as

$$\sum_{x \in T} (|x\rangle|f(x)\rangle + |x+r\rangle|f(x+r)) = \sum_{x \in T} (|x\rangle + |x+r\rangle)|f(x)\rangle$$

x	$f(x)$
000	011
001	101
010	000
011	010
100	101
101	011
110	010
111	000

A quantum algorithm for Simon III

Measuring the second register yields $|x\rangle + |x + r\rangle$ in the first register, for a random $x \in T$.

How can we use this to obtain ***some*** information about r?

Try applying $H^{\otimes n}$ to the state, yielding

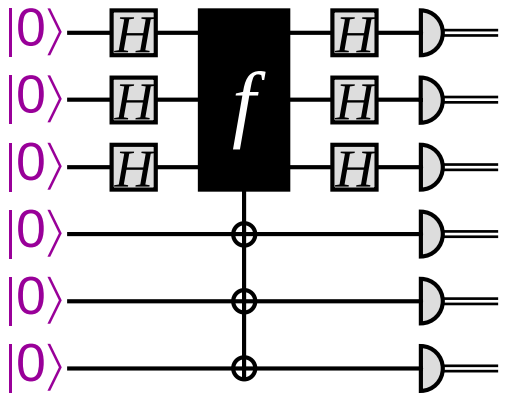
$$\sum_{y \in \mathbb{F}_2^n} (-1)^{x \cdot y} |y\rangle + \sum_{y \in \mathbb{F}_2^n} (-1)^{(x+r) \cdot y} |y\rangle$$

$$= \sum_{y \in \mathbb{F}_2^n} (-1)^{x \cdot y} (1 + (-1)^{r \cdot y}) |y\rangle$$

Measuring this state yields y with prob. $\begin{cases} (1/2)^{n-1} & \text{if } r \cdot y = 0 \\ 0 & \text{if } r \cdot y \neq 0 \end{cases}$

A quantum algorithm for Simon IV

Executing this algorithm $k = O(n)$ times yields random $y_1, y_2, \ldots, y_k \in \mathbb{F}_2^n$ such that $r \cdot y_1 = r \cdot y_2 = \cdots = r \cdot y_k = 0$.



How does this help?

This is a system of k linear equations:

$$\begin{bmatrix} y_{11} & y_{12} & \cdots & y_{1n} \\ y_{21} & y_{22} & \cdots & y_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ y_{k1} & y_{k2} & \cdots & y_{kn} \end{bmatrix} \begin{bmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

With high probability, there is a unique non-zero solution that is r (which can be efficiently found by linear algebra)

Conclusion of Simon's algorithm

- Any classical algorithm has to query the black box $\boldsymbol{\Omega(2^{n/2})}$ times, even to succeed with probability ¾ for a random f.
- There is a quantum algorithm that queries the black box only $\boldsymbol{O(n)}$ times, performs only $\boldsymbol{O(n^3)}$ auxiliary operations (for the Hadamards, measurements, and linear algebra), and succeeds with probability ¾

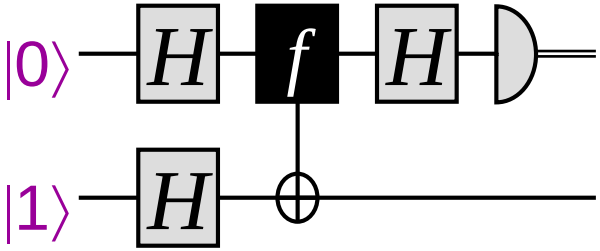
black-box problem	quantum	classical
constant vs. balanced	**1** (query)	**2** (queries)
1-out-of-4 search	**1**	**3**
constant vs. balanced	**1**	**4**
Simon's problem	$\boldsymbol{O(n^3)}$	$\boldsymbol{\Omega(2^{n/2})}$

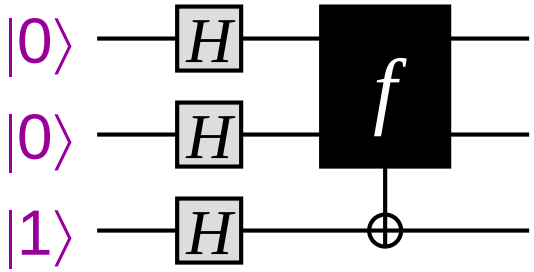
} for success probability ≧¾

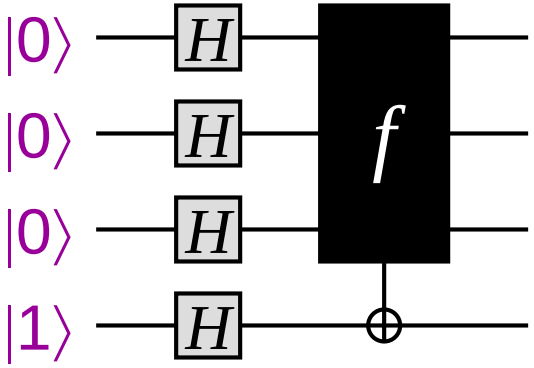
Quantum vs classical

black-box problem	quantum	classical
constant vs. balanced	**1** (query)	**2** (queries)
1-out-of-4 search	**1**	**3**
constant vs. balanced	**1**	**4**
Simon's problem	$O(n^3)$	$\Omega(2^{n/2})$

} for success probability ≧¾







Thursday class in **QNC 0101**

Sept. 19	QNC 1501	Sept. 21	MC 4058
Sept. 26	QNC 1501	Sept. 28	**QNC 0101**
Oct. 3	**OPT 309**	Oct. 5	QNC 1501
Oct. 10	QNC 0101	Oct. 12	QNC 0101
Oct. 17	QNC 0101	Oct. 19	QNC 0101
Oct. 24	QNC 0101	Oct. 26	QNC 1501
Oct. 31	QNC 0101	Nov. 2	QNC 0101
Nov. 7	QNC 0101	Nov. 9	QNC 0101
Nov. 14	QNC 0101	Nov. 16	QNC 0101
Nov. 21	QNC 0101	Nov. 23	QNC 0101
Nov. 28	QNC 0101	Nov. 30	QNC 0101