Tuesday, October 23, 2018 12:30 PM

Simon's Algorithm.

We are given a function $f: \{0,1\}^n \to \{0,1\}^m$ $m \geq n-1$

f has the property that for some $a \in \{0,1\}^n$

$$f(x) = f(x \oplus a) \quad \forall x.$$

$\oplus \equiv$ addition mod 2.

$\hookrightarrow$ bit wise $\oplus$.

The string "a" defines a pairing between strings in $\{0,1\}^n$

Example: $n=3$

x	$f(x)$
000	01
001	00
010	10
011	11
100	00
101	01
110	11
111	10

Suppose

$$\begin{array}{r} 000 \\ a = 101 \\ \hline 101 \end{array}$$

If two strings x + y are paired then $f(x) = f(y)$.

If x + y are not paired then $f(x) \neq f(y)$.

Pairs have the same value. Different pairs have different values. (f is 2-to-1).

Simon - page 2

Tuesday, October 23, 2018 12:31 PM

Given function f with this property $(f(x) = f(x \oplus a))$ we would like to recover a.

Assume quantum oracle access to f:

$$|\underline{x}\rangle|\overbrace{y}^{m}\rangle \xrightarrow{U_f} |\underline{x}\rangle|y \oplus f(x)\rangle$$

Example $f(110) = (01)$ $\quad |110\rangle|11\rangle \xrightarrow{U_f} |110\rangle|10\rangle$

Quantum Algorithm: Start with $|\overbrace{0\cdots0}^{n}\rangle|\overbrace{0\cdots0}^{m}\rangle$

Perform $H^{\otimes n}$ on the first n qubits to get:

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

Apply U_f: $$\frac{1}{2^{n/2}} \sum_{x\in\{0,1\}^n} |x\rangle|f(x)\rangle$$

Simon - page 3

Tuesday, October 23, 2018 12:31 PM

Apply U_f: $\frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} |x\rangle |f(x)\rangle$

Now measure the last register:

$$\frac{1}{\sqrt{2}} \sum_{x : f(x) = d} |x\rangle |d\rangle.$$

d chosen at random from the range of f.

$f(z) = d$
$f(z \oplus a) = d$.

$$= \frac{1}{\sqrt{2}} \left(|z\rangle + |z \oplus a\rangle \right) |d\rangle$$

z chosen at random

Will now drop these last qubits.

$z \oplus (z \oplus a) = a$.

(If we knew z and $z \oplus a$, we could recover a).

Will perform $H^{\otimes n}$ again on first register.

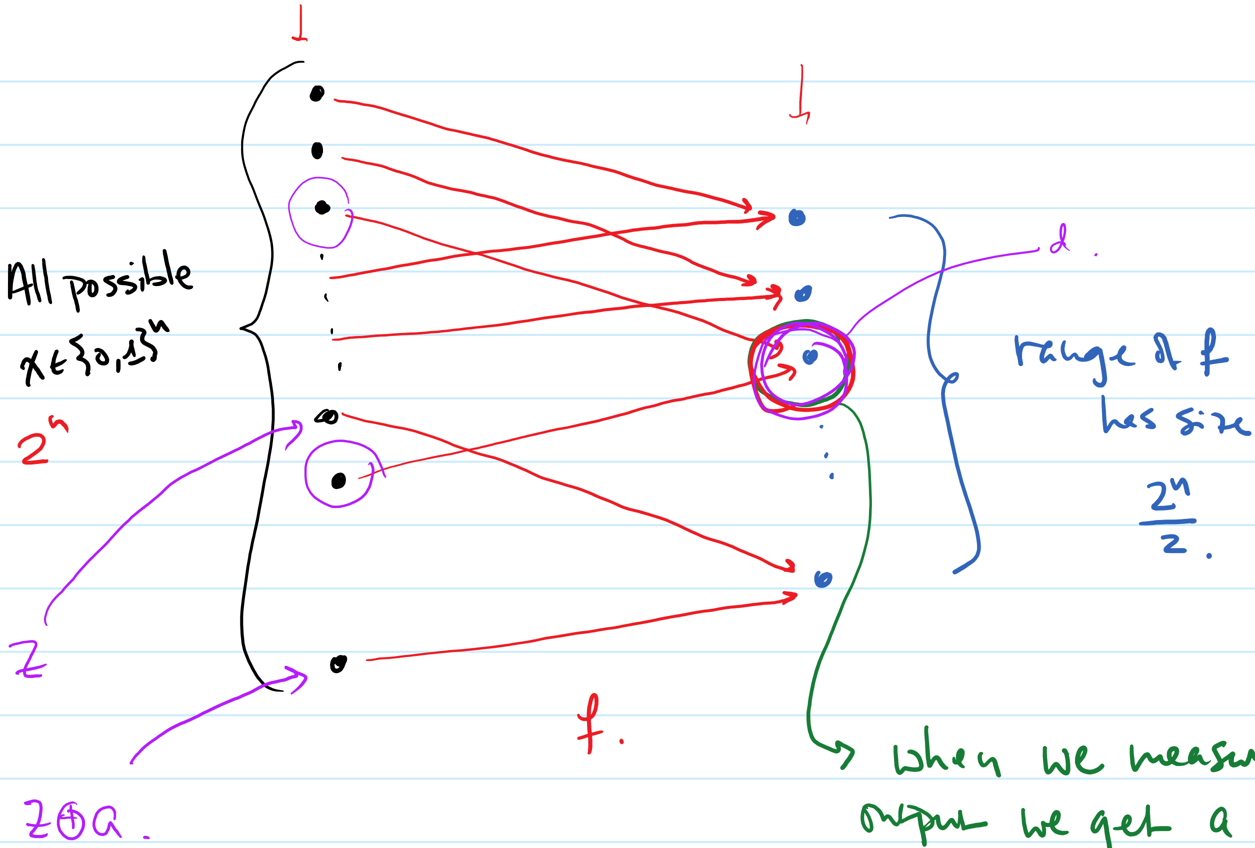
What is $H^{\otimes n} |z\rangle$?

$$H^{\otimes 3} |101\rangle = |-+-\rangle = \left(\frac{1}{\sqrt{2}}\right)^3 (|0\rangle - |1\rangle)(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)$$

$$= \left(\frac{1}{\sqrt{2}}\right)^3 \Big(|000\rangle - |001\rangle + |010\rangle - |011\rangle - |100\rangle + |101\rangle - |110\rangle + |111\rangle \Big)$$

Simon - page 3.5

Friday, October 26, 2018 8:24 AM



When we measure output we get a random element of the range.

1st register has random z $z \oplus a$ pair.

Simon - page 4

Tuesday, October 23, 2018 1:23 PM

$$H^{\otimes 3}\,|\overset{z_1 z_2 z_3}{101}\rangle = |-+-\rangle = \left(\frac{1}{\sqrt{2}}\right)^3 (|0\rangle - |1\rangle)(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)$$

$$= \left(\frac{1}{\sqrt{2}}\right)^3 \Big(|000\rangle - |001\rangle + |010\rangle - |011\rangle - |100\rangle$$

$$+ |101\rangle - \overset{101}{|110\rangle} + |111\rangle \Big)$$

pick up a factor of (-1) every time $z_j = x_j = 1$.

$z = z_1 z_2 \cdots z_n$

$$H^{\otimes n}|z\rangle = \left(\frac{1}{\sqrt{2}}\right)^n \bigotimes_{j=1}^{n} \left(|0\rangle + (-1)^{z_j}|1\rangle\right)$$

$z_j = 1 \quad |-\rangle$

$z_j = 0 \quad |+\rangle$

$0+1+0+1 = 2 \equiv 0$

$z = 1101$

$x = 0111$

$z \cdot x = 0$

$$= \left(\frac{1}{\sqrt{2}}\right)^n \sum_{x \in \{0,1\}^n} \prod_{j=1}^{n} (-1)^{x_j \cdot z_j} |x\rangle$$

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

$x \cdot z \to \sum_{j=1}^{n} x_j \cdot z_j \mod 2$

Apply $H^{\otimes n}$ to $\frac{1}{\sqrt{2}}\left(|z\rangle + |z \oplus a\rangle\right)$

$$\frac{1}{2^{n/2}} \cdot \frac{1}{\sqrt{2}} \left[\sum_x (-1)^{x \cdot z} |x\rangle + \sum_x (-1)^{x \cdot (z \oplus a)} |x\rangle \right]$$

$$= \frac{1}{2^{(n+1)/2}} \left[\sum_x \left((-1)^{x \cdot z} + (-1)^{x \cdot (z \oplus a)} \right) |x\rangle \right]$$

Simon - page 4.5

Friday, October 26, 2018 1:46 PM

$$x \cdot a = \left(\sum_{i=1}^{n} x_i \cdot a_i \right) \bmod 2 .$$

$$(110101) \cdot (011011) = 1+1 \bmod 2 = 0$$

$$011011$$

$$\prod_{i=1}^{n} (-1)^{x_i \cdot a_i} = (-1)^0 (-1)^1 (-1)^0 (-1)^0 (-1)^0 (-1)^1$$

$$= 1 .$$

$$(-1)^{x \cdot a} = 1^0$$

Simon - page 5

Tuesday, October 23, 2018 1:34 PM

$$H^{\otimes n} \frac{1}{\sqrt{2}}\left(|z\rangle + |z\oplus a\rangle\right) = \frac{1}{2^{\frac{n+1}{2}}} \sum_x \left[(-1)^{x\cdot z} + (-1)^{x\cdot(z\oplus a)}\right]|x\rangle$$

$$x\cdot(z\oplus a) = \sum_{j=1}^{n} x_j\cdot(z_j\oplus a_j) \mod 2.$$

$$\begin{array}{r} z_1 z_2 \cdots z_n \\ \oplus\; a_1 a_2 \cdots a_n \\ \hline \end{array}$$

$$= \sum_{j=1}^{n} x_j\cdot(z_j + a_j)$$

$$= \sum_{j=1}^{n} x_j z_j + x_j\cdot a_j = \sum_j x_j z_j + \sum_j x_j a_j$$

$$x\cdot z + x\cdot a.$$

$$= \frac{1}{2^{n+1/2}} \sum_x \left((-1)^{x\cdot z} + (-1)^{x\cdot z}\cdot(-1)^{x\cdot a}\right)|x\rangle$$

$$= \frac{1}{2^{n+1/2}} \sum_x (-1)^{x\cdot z}\left[1 + (-1)^{x\cdot a}\right]|x\rangle$$

If $x\cdot a = 1$ then amplitude of $|x\rangle$ is 0

If $x\cdot a = 0$ then amplitude of $|x\rangle = \pm\frac{2}{2^{n+1/2}}$

$$\pm\frac{1}{2^{\frac{n+1}{2}}}\cdot 2 = \pm\frac{1}{2^{n-1/2}}.$$

If we measure x then we get an x such that $x\cdot a = 0$, chosen among all x that have this property.

Simon - page 6

Tuesday, October 23, 2018 5:33 PM

$$X \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_\ell \end{bmatrix} \begin{bmatrix} a \end{bmatrix} = \begin{bmatrix} \vec{0} \end{bmatrix}$$

If we repeat this process, we get
$x_1, x_2, \ldots, x_\ell$ $x_i \cdot a = 0$.

We can use Gaussian elimination (mod 2)
to solve for a.

How many x's do we need?

There are 2^n n-bit vectors total.
strings.

Let A = set of x's such that $x \cdot a = 0$.
Claim: $|A| = 2^n/2$.

a : 1 1 0 1 0 1
0/1 $x_2\ x_3\ x_4\ x_5\ x_6$

For every way to fix $x_2 \cdots x_6$
one choice of $x_1 = 0/1$
will cause $x \cdot a = 0$.

For $x, y \in \{0,1\}^n$ $x + y$ = bit-wise addition mod 2.
(same as $x \oplus y$)

Will denote $\underbrace{0 \cdots 0}_{n}$ by $\vec{0}$

Note $x + x = 0$
$\forall x$.

Simon - page 6.5

Wednesday, October 24, 2018 7:56 AM

Repeat $n-1$ times:

1 U_f. ⟹ Quantum algorithm to generate a random x such that $x \cdot a = 0$

$(x_1, \dots, x_{n-1})$

Classical algorithm for Gaussian Elimination

Probability 3/4

If $x_1 \cdots x_{n-1}$ are linearly dependent start again.

Probability 1/4

a

If $x_1, \dots, x_{n-1}$ are linearly indep. then Gaussian elimination finds a deterministically.

Simon - page 6.75

Friday, October 26, 2018 1:42 PM

1. Start with $|\overbrace{0 \cdots 0}^{n}\rangle |\overbrace{0 \cdots 0}^{m}\rangle$

2. $H^{\otimes n} \otimes I^{\otimes m} \longrightarrow \sum_{x \in \{0,1\}^n} |x\rangle |0 - 0\rangle$.

3. Apply $U_f \longrightarrow \sum_x |x\rangle |f(x)\rangle$

4. Measure last register

$$\frac{1}{\sqrt{2}} \left(|z\rangle + |z \oplus a\rangle \right) |d\rangle$$

z chosen at random

5. Apply $H^{\otimes n}$ (drop last register)

$$\frac{1}{2^{n-1/2}} \sum_{x:\, x \cdot a = 0} (-1)^{?} |x\rangle$$

6. Measure 1st register.

U_f overall is $O(n)$.

$\begin{pmatrix}1\\1\\0\\1\end{pmatrix} + \begin{pmatrix}1\\1\\0\\1\end{pmatrix} = \begin{pmatrix}0\\0\\0\\0\end{pmatrix}$ $b_i = 0/1$.

$\vec{x}_1 + \vec{x}_1 =$

Tuesday, October 23, 2018 6:56 PM

$\vec{x}_1, \dots, \vec{x}_k$ are linearly independent if
$$b_1 x_1 + b_2 x_2 \cdots + b_k x_k = \vec{0}$$
implies $b_1 = b_2 \cdots \cdots = b_k = 0$.

Since $b_i = 0/1$ this is the same as saying that no subset of the x_i's sums to $\vec{0}$.
(except the empty set).

This implies that two different subsets of the x_i's result in different vectors:

$$x_1 + x_2 + x_4 \neq x_2 + x_4 + x_5$$

$\Rightarrow$ if $x_1 + \cancel{x_2} + \cancel{x_4} = \cancel{x_2} + \cancel{x_4} + x_5$ then $x_1 + x_5 = 0$.

$+x_2 + x_4$ $\quad x_2 + x_4$

$x_1 = x_5$

$x_1 + x_5 = \vec{0}$.

Span $(x_1, \dots, x_k)$ has 2^k vectors.
Sum of any subset of the vectors is unique.

If $x_{k+1} \notin$ Span $(x_1, \dots, x_k)$ then

$x_1 x_2 \dots x_{k+1}$ is linearly independent.

Suppose $x_2 + x_5 + x_{k+1} = 0$

then $x_2 + x_5 = x_{k+1}$

$x_{k+1} \in$ Span $(x_1, \dots, x_k)$

Simon - page 8

Tuesday, October 23, 2018 7:07 PM

$A = \{x \mid x \cdot a = 0\}$ $|A| = 2^{n-1}$

A is closed under addition:

$x \cdot a = 0$ & $y \cdot a = 0 \Rightarrow x \cdot a + y \cdot a = 0$

$\Rightarrow (x+y) \cdot a = 0$.

Start with $x_1 \in A$.

For $j = 2 \ldots n-1$

$x_j =$ any vector in $A - \text{span}(x_1, \ldots, x_{j-1})$

$|\text{Span}(x_1, \ldots, x_j)| = 2^j$

$\text{Span}(x_1, \ldots, x_j) \subseteq A$. when $j = n-1$ then

$\text{Span}(x_1, \ldots, x_{n-1}) = A$.

Tuesday, October 23, 2018 7:29 PM

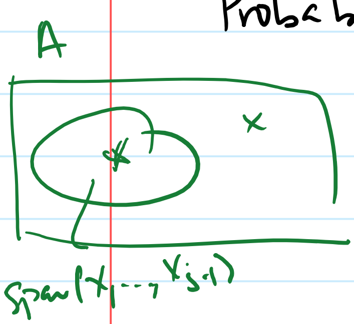
Goal: Collect $n-1$ linearly independent $x_1, \ldots, x_{n-1}$ in A.

The quantum algorithm can only generate a random $x \in A$.

What is the probability that a random $x_1, \ldots, x_{n-1}$ chosen from A are linearly indep?

Start with $x_1 \in A$ (chosen at random).
For $j = 2, \ldots, n-1$
Select a random x_j in A ← Quantum.
Stop if $x_j \in \text{Span}(x_1, \ldots, x_{j-1})$

Probability of stopping in round j:



$$\frac{|\text{Span}(x_1, \ldots, x_{j-1})|}{|A|} = \frac{2^{j-1}}{2^{n-1}} = \frac{1}{2^{n-j}}$$

Probability of continuing in round j:

$$\left(1 - \frac{1}{2^{n-j}}\right).$$

Probability of making it through $n-2$ rounds:

$$\left(1 - \frac{1}{2^{n-2}}\right)\left(1 - \frac{1}{2^{n-3}}\right) \cdots \left(1 - \frac{1}{2}\right) \geq 1/4.$$

Tuesday, October 23, 2018 7:36 PM

$x_i \in \{0,1\}^n$.

Suppose have $x_1, \dots, x_{n-1}$ linearly independent.
and $x_j \cdot a = 0$ for unknown a.

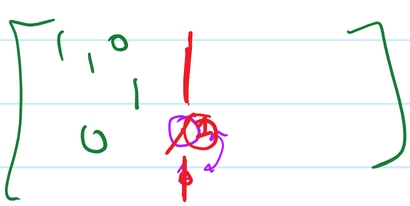
Algorithm to find a (Gaussian elimination).

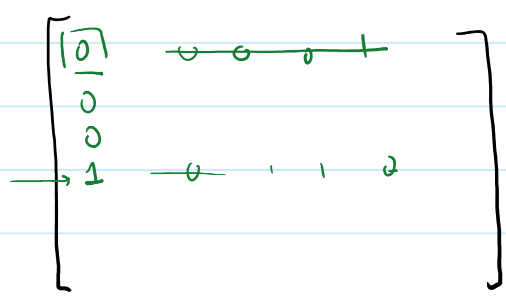
Matrix X each x_j is a row. $n-1 \times n$.

$$
n-1 \left\{ \begin{array}{cccc} \overbrace{x_{11} \; x_{12} \; \cdots \; x_{1n}}^{n} \\ x_{21} \; \cdots \; x_{2n} \\ \vdots \\ x_{n-1,1} \; \cdots \; x_{n-1,n} \end{array} \right. \quad \begin{array}{c} (x_1) \\ (x_2) \\ \vdots \\ (x_{n-1}) \end{array}
$$

$$
\begin{matrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{matrix} \rightarrow \begin{matrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{matrix} \qquad \begin{matrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{matrix}
$$

Initialize $r = 1$, $c = 1$.
While $r \le n-1$ and $c \le n$.
If $x_{rc} = 0$ and all the entries below x_{rc} are 0
$c \leftarrow c+1$
Else find smallest $s \ge r$ s.t. $x_{sc} = 1$.
Swap rows r + s.
For every r' s.t. $x_{r'c} = 1$, add row r to row r'
$r \leftarrow r+1$, $c \leftarrow c+1$
End.
End.





Initialize $r = 1$, $c = 1$.

While $r \le n-1$ and $c \le n$.

If $x_{rc} = 0$ and all the entries below x_{rc} are 0

$c \leftarrow c+1$

Else find smallest $s \ge r$ s.t. $x_{sc} = 1$.

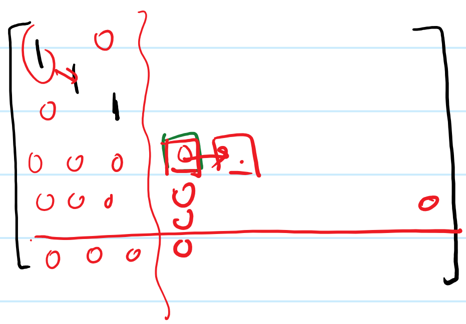
Swap rows r & s.

For every r' s.t. $x_{r'c} = 1$, add row r to row r'

$r \leftarrow r+1$, $c \leftarrow c+1$

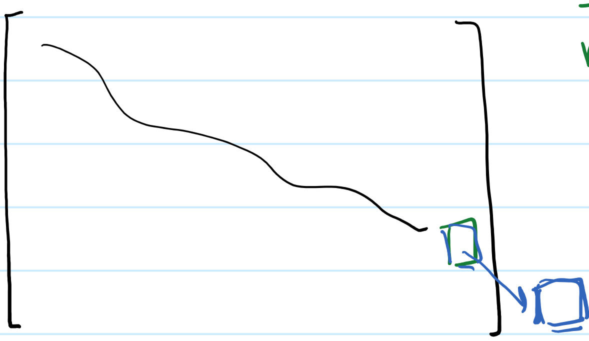
End.

End.



n

n-1



If

$r \le n-2$ $c = n$.

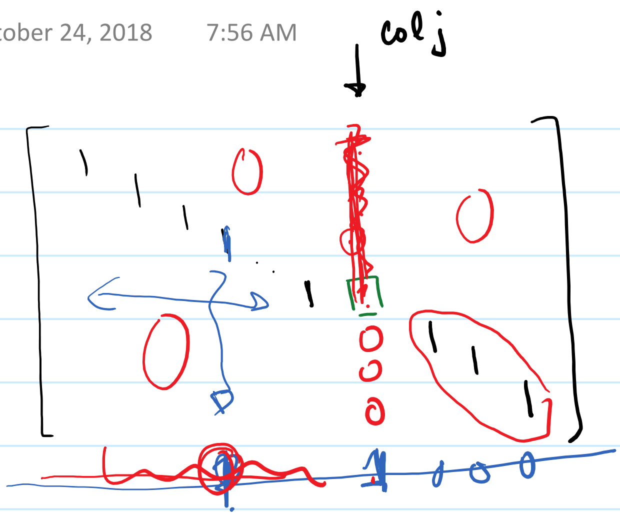
then x's are lin. dep.

$r \le n-1$

$c > n$.

Simon - page 12

Wednesday, October 24, 2018 7:56 AM



$a_k = 0$ for $k > j$

$a_j = 1.$

$a_k = x_{kj}$ for $k < j.$

$$\begin{bmatrix} 1&0&1&1&1\\0&1&0&0&0\\1&1&1&1&0\\0&0&0&1&1 \end{bmatrix} \longrightarrow \begin{bmatrix} 1&0&1&1&1\\0&1&0&0&0\\0&1&0&0&1\\0&0&0&1&1 \end{bmatrix} \quad \begin{bmatrix} 1&0&1&1&1\\0&1&0&0&0\\0&0&0&0&1\\0&0&0&1&1 \end{bmatrix}$$

$$\begin{bmatrix} 1&0&1&1&1\\0&1&0&0&0\\0&0&0&1&1\\0&0&0&0&1 \end{bmatrix} \quad \begin{bmatrix} 1&0&1&0&0\\0&1&0&0&0\\0&0&0&1&0\\0&0&0&0&1\\ \boxed{1}&\boxed{0}&1&0&0 \end{bmatrix} \leftarrow a$$

Simon - page 13

Wednesday, October 24, 2018 7:56 AM

Repeat $n-1$ times:

$$\boxed{\text{Quantum algorithm to generate a random } x \text{ such that } x \cdot a = 0}$$

$(x_1, \ldots, x_{n-1})$

$$\boxed{\text{Classical algorithm for Gaussian Elimination}}$$

Probability 3/4

If $x_1 \cdots x_{n-1}$ are linearly dependent start again.

Probability 1/4

a

If $x_1, \ldots, x_{n-1}$ are linearly indep. then Gaussian elimination finds a deterministically.

Simon - page 14

Wednesday, October 24, 2018 8:17 AM

How well can a probabilistic classical algorithm do?

Construct f randomly:

Pick random $a \in \{0,1\}^n - \vec{0}$

Suppose that k queries have been made.

$f(x_1) \ldots f(x_k)$.

What do we know about a?

If $x_i \neq x_j$ and $f(x_i) = f(x_j)$ then

$\cancel{x_i \oplus} \; \cancel{x_j \oplus} \; a = x_j \oplus x_i$ $\Rightarrow$ $a = x_i \oplus x_j$

Otherwise $a \neq x_i \oplus x_j$ for all $i \neq j$.

We have eliminated $\binom{k}{2}$ possibilities

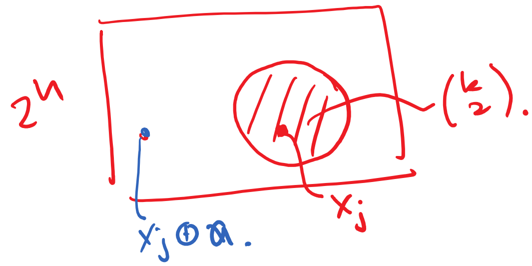
but otherwise learned nothing about a.

The other $2^n - 1 - \binom{k}{2}$ are equally likely since they are all fully consistent with the observed $f(x_1), f(x_2), \ldots, f(x_k)$

The next choice x_{k+1} will reveal a if it happens that $a = x_{k+1} \oplus x_j$ for some $j \in \{1, .., k\}$

Simon - page 15

Wednesday, October 24, 2018 8:26 AM



The next choice x_{k+1} will reveal a if it happens that $a = x_{k+1} \oplus x_j$ for some $j \in \{1, .., k\}$

$\equiv x_{k+1} = a \oplus x_j$.

Prob $x_{k+1} = a \oplus x_j$ for a particular x_j $\quad \dfrac{1}{2^n - 1 - \binom{k}{2}}$

Prob $x_{k+1} = a \oplus x_j$ for any x_j $\quad \leq \dfrac{k}{2^n - 1 - \binom{k}{2}}$

The probability that m choices $x_1, \ldots, x_m$ reveal a is:

$$\sum_{k=1}^{m} \frac{k}{2^n - 1 - \binom{k}{2}} \leq \sum_{k=1}^{m} \frac{k}{2^n - k^2} \leq \frac{m^2}{2^n - m^2}$$

m must be $\Omega(2^{n/2})$ for this probability to be a constant.

$\exists\, c > 0 \qquad \geq c \cdot 2^{n/2}$ queries.

$c = \frac{1}{10}$