Each w_i eliminates 1/2 the possibilities for s

We learn something new by w_i only if its 1/2 elim are not already eliminated

That is w_i is NOT a linear combination of the w's we've seen so far

1st probe - anything but 0^n

2^{n-1} possible measures

FAIL $1/2^{n-1}$ probability

How do we know if next w_i makes progress?

4 bit example
$s = 1010$
poss w = 0000, 0001, 0100, 0101
1010, 1011, 1110, 1111

Verify each $w \cdot s = 0$

113.5

SKIP - but here is the work

$s = 1010$ our secret

w	$w \wedge s$	$w \cdot s$	Poss w?
0000	0000	0	✓
0001	0000	0	✓
0010	0010	1	
0011	0010	1	
0100	0000	0	✓
0101	0000	0	✓
0110	0010	1	
0111	0010	1	
1000	1000	1	
1001	1000	1	
1010	1010	0	✓
1011	1010	0	✓
1100	1000	1	
1101	1000	1	
1110	1010	0	✓
1111	1010	0	✓

Consider

$w_1 = 0101$
$w_2 = 1010$
$w_3 = 1111$

w_1 & w_2 leave for possible s (work next page)

0101
1010
1111

each $\cdot w_1$ or $\cdot w_2$ is 0

\+ 0000 of course

w_3 does not make progress
All 3 are still possible for s
Note

$w_3 = w_1 + w_2$

w_3 is not linearly indep of w_1 & w_2
is in span of w_1 + w_2

Likewise w_1 IN span of w_3 + w_2

$w_1 = w_3 - w_2$

If we have so far chosen

$w_1\ w_2, \ldots, w_k$ that are linearly independent

$(w_1 \cdots w_k)$ and now w_{k+1}

doubles the span of $w_1 \ldots w_k$ if
w_{k+1} is also linearly independent

114.5

Work from p. 114

s	$0101 \cdot s$	$1010 \cdot s$	$1111 \cdot s$
0000	0	0	0
0001	1	0	1
0010	0	1	1
0011	1	1	0
0100	1	0	1
0101	0	0	0
0110	1	1	0
0111	0	1	1
1000	0	1	1
1001	1	1	0
1010	0	0	0
1011	1	0	1
1100	1	1	0
1101	0	1	1
1110	1	0	1
1111	0	0	0

No new info!

because w_{k+1} can be added (or not) to each $w_1 .. w_k$ to reach a new element of $\{0,1\}^n$

So
1) Each new w_i doubles the number of values we cannot pick

2) There are 2^{n-1} possible w's seen by measurement

3) We need $n-1$ w's

FAIL

$$1/2^{n-1} \quad \text{then} \quad 2/2^{n-1} \quad \text{then} \quad 4/2^{n-1}$$

Succeed

$$(1 - 1/2^{n-1})(1 - 2/2^{n-1})(1 - 4/2^{n-1}) \ldots (1 - 2^{n-2}/2^{n-1})$$

$$\prod_{k=n-2}^{0} \left(1 - 2^k/2^{n-1}\right)$$

$$= (1-1/2)(1-1/4)\cdot(1-1/8)\cdots(1-1/2^{n-1})$$

$$= 1/2 \cdot 3/4 \cdot 7/8 \cdots (1-1/2^{n-1})$$

Note $(1-a)(1-b) \geq (1-a-b)$
if $a+b \geq 0$

$$= 1/2 \cdot [3/4 \cdot 7/8 \cdot 1-1/2^{n-1}]$$

$$\geq 1/2 \ [1 - 1/4 - 1/8 - 1/16 - \cdots]$$

$$\geq 1/2 \cdot 1/2$$

$$\geq 1/4$$

Each fresh computation up to $|4 \rangle$
succeeds at least 3/4 of the time

So Simon's alg:

Run the circuit until you have
n-1 indep w's, expected in $O(n)$ runs

Solve $W s = 0$ Gaussian Elim
$\theta(n^3)$

Exercise Bernstein Vazirani problem

Recall $H(|x\rangle) = 1/\sqrt{2}\left(|0\rangle + (-1)^x |1\rangle\right)$

if $|x\rangle$ is $|0\rangle$ or $|1\rangle$

And recall for a basis state $|x\rangle$

$H^{\otimes n}(|x\rangle)$

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

We (CS) can think of $|x\rangle$ as a bit string

$x_1 x_2 \cdots x_n$

the info about $|x\rangle$ is encoded into ± 1 phases of $|y\rangle$ using

$x \cdot y$

Recall $H(H(|x\rangle)) = |x\rangle$

$$H(H) = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$$

$$= I$$

H is its own inverse, & by induction so is $H^{\otimes n}$ its own inverse

So $H^{\otimes n}\left(\frac{1}{\sqrt{2^n}} \sum_y (-1)^{x \cdot y} |y\rangle\right)$

$= H^{*n}(H^{*n}(|x\rangle)) = |x\rangle$

Example

$|x\rangle = |110\rangle \quad (n=3)$

$H^{\otimes 3}(|110\rangle) = ?$

y	$x \wedge y$	$x \cdot y$	$(-1)^{x \cdot y}$
000	000	0	1
001	000	0	1
010	010	1	-1
011	010	1	-1
100	100	1	-1
101	100	1	-1
110	110	0	1
111	110	0	1

Can we see that

some $x \wedge y$ would change
if any bit of
x were different?

Also $x \cdot y$ is a parity bit on $x \wedge y$
So some $x \cdot y$ also changes if
any bit of $|x\rangle$ is different

→ the signs on $|y\rangle$ are a
unique signature of basis state $|x\rangle$
Why are there not 2^8 possible sigs?

$|y\rangle = \begin{pmatrix} \ \end{pmatrix}$ col shown on previous page

In our example

$$|y\rangle = \frac{1}{\sqrt{8}} \left[\begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} - \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} \right]$$

$$= \frac{1}{\sqrt{8}}\Big[\,|000\rangle + |001\rangle + |110\rangle + |111\rangle\,\Big]$$

$$- \frac{1}{\sqrt{8}}\Big[\,|010\rangle + |011\rangle + |100\rangle + |101\rangle\,\Big]$$

$H(|000\rangle)$

$|y\rangle$ \ $|x\rangle$	000	001	110	111	Σ	010	011	100	101	Σ
000	1	1	1	1	4	1	1	1	1	4
001	1	-1	1	-1	0	1	-1	1	-1	0
010	1	1	-1	-1	0	-1	-1	1	1	0
011	1	-1	-1	1	0	-1	1	1	-1	0
100	1	1	-1	-1	0	1	1	-1	-1	0
101	1	-1	-1	1	0	1	-1	-1	1	0
110	1	1	1	1	4	-1	-1	-1	-1	-4
111	1	-1	1	-1	0	-1	1	-1	1	0

Grand sum

$$\frac{1}{\sqrt{8}}\,\frac{1}{\sqrt{8}}\left(8\,|110\rangle\right)$$

$$= |110\rangle \quad !$$ we got it back

$H^{\otimes n}(|x\rangle)$ encodes $|x\rangle$ in phases of $|y\rangle$ uniquely for basis state $|x\rangle$

B-V problem

$$f(x) = x \cdot s = \left(\sum x_i s_i \right) \bmod 2$$

for some secret s

Recalling how to encode a state

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

If I can produce

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

I can $H^{\otimes n}$ that state to retrieve s
Because H is its own inverse

I can create

$$\frac{1}{\sqrt{2^n}} \sum_x |x\rangle$$ easily from
$$H^{\otimes n}(|0^n\rangle)$$

Need

$$\underbrace{\frac{1}{\sqrt{2^n}} \sum_x |x\rangle}_{\text{n qubits input}} \underbrace{(-1)^{s \cdot x} \boxed{}}_{\text{some qubit}}$$

To get phase kick back:

$$\frac{1}{\sqrt{2^n}} \sum_x |x\rangle \, (-1)^{s\cdot x} \, \square$$

same over all $|x\rangle$

World become

$$\boxed{\frac{1}{\sqrt{2^n}} \sum_x (-1)^{s\cdot x} |x\rangle} \otimes \square$$

$H^{\otimes n}$ the above & you get $|s\rangle$ on the first n qubits!

$\square$ $\quad s\cdot x = 0$ want $\square$

$\quad\quad s\cdot x = 1$ want $-\square$

$|0\rangle, |1\rangle$ don't work – "–" would be global

$|+\rangle$ same deal

$|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$ AHA

Try

$$|\psi_0\rangle = |0^n 1\rangle$$

$$|\psi_1\rangle = H(|0^n\rangle)\, H(|1\rangle)$$

$$= \left(\frac{1}{\sqrt{2^n}} \sum_x |x\rangle\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

Now drive toward inputs $f(\ )$ can handle - basis states

$$= \frac{1}{\sqrt{2^{n+1}}}\left(\sum_x |x0\rangle - \sum_x |x1\rangle\right)$$

$$|\psi_2\rangle = U_f(|\psi_1\rangle)$$

$$= \frac{1}{\sqrt{2^{n+1}}} \sum_x \left[\,|x\, f(x)\rangle - |x\,(1-f(x))\rangle\right]$$

$$= \frac{1}{\sqrt{2^n}} \sum_x |x\rangle \left[\frac{|f(x)\rangle - |1-f(x)\rangle}{\sqrt{2}}\right]$$

$$= \frac{1}{\sqrt{2}} \sum_x |x\rangle \left[\frac{|x\cdot s\rangle - |1-x\cdot s\rangle}{\sqrt{2}}\right]$$

$x \cdot s = 0$ or 1

$x \cdot s = 0 \quad [\sim \quad] \rightarrow \frac{[|0\rangle - |1\rangle]}{\sqrt{2}}$

$x \cdot s = 1 \quad [- -] \rightarrow \frac{[|1\rangle - |0\rangle]}{\sqrt{2}}$

$= (-1)^{x \cdot s} \frac{[|0\rangle - |1\rangle]}{\sqrt{2}}$

so $|\psi_2\rangle = 1/\sqrt{2^n} \sum_x |x\rangle \; (-1)^{x \cdot s} \frac{[|0\rangle - |1\rangle]}{\sqrt{2}}$

phase
kickback

$= \left(1/\sqrt{2^n} \sum_x (-1)^{x \cdot s} |x\rangle \right) \frac{[|0\rangle - |1\rangle]}{\sqrt{2}}$

$H^{\otimes n}(|\psi_2\rangle) = |s\rangle$! $\square$

Consider (as some sources do for B-Z problem)

$U = \boxed{?}$

promise box is either

$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

or $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

How can we tell which we have?

$U(|0\rangle)$?

$I(|0\rangle) = |0\rangle$
$Z(|0\rangle) = |0\rangle$

$U(|1\rangle)$?

$\left.\begin{array}{l} I(|1\rangle) = |1\rangle \\ Z(|1\rangle) = -|1\rangle \end{array}\right\}$ can't measure the difference

$I(|+\rangle) = |+\rangle$ AHA
$Z(|+\rangle) = |-\rangle$

$H(U(H(|0\rangle)))$ $|0\rangle$ - I
$|1\rangle$ - Z