For $|\psi_3\rangle$ (my notes page 93)

We apply $H^{\otimes n}$ to the first n bits of $|\psi_2\rangle$

$$H^{\otimes n}\left(\frac{1}{\sqrt{2^n}} \sum_{z\in\{0,1\}^n} (-1)^{f(z)} |z\rangle\right)$$

$$= \frac{\sum_{z\in\{0,1\}^n} (-1)^{f(z)} H^{\otimes n}(|z\rangle)}{\sqrt{2^n}}$$

by linearity

$$= \sum_z \frac{(-1)^{f(z)}}{\sqrt{2^n}} \left(\frac{\sum_{y\in\{0,1\}^n} (-1)^{z\cdot y} |y\rangle}{\sqrt{2^n}} \right)$$

$$= \frac{1}{2^n} \sum_y \sum_z (-1)^{f(z)} (-1)^{z\cdot y} |y\rangle$$

So $|\psi_3\rangle =$

$$1/2^n \sum_y \sum_z (-1)^{f(z)} (-1)^{z\cdot y} |y\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

Look at the amplitude of $|y\rangle = |0^n\rangle$

It is

$$a = \frac{1}{2^n} \sum_z (-1)^{f(z)} (-1)^0 \quad \leftarrow z \cdot y = 0$$

$$f(z) = 0 \rightarrow a = 2^n / 2^n = \underline{1}$$

$$f(z) = 1 \rightarrow a = \frac{-2^n}{2^n} = \underline{-1}$$

$f(z)$ is half 0, half $\underline{1}$ $\quad a = 0$

Thus if f is balanced, measurement of the first n qubits returns $a^2 = 0$

If f is constant, $a^2 = \underline{1}$

END!

Simon's Problem

Consider $f: \{0,1\}^n \to \{0,1\}^{n-1}$

Pairs of n-bit strings map to same output. The pairs are related by a secret s:

$$f(x) = f(x+s) \qquad s \neq 0^n$$

Example $s = 101$

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

00	01	10	11
001	000	011	010
100	101	110	111

Problem: discover s given black box f

Preliminary notes

1) Deutsch Josza can decide balanced or not 2/3 of the time using ~~$\theta(1)$~~ (2) evalutations

How?

Pick a, b from $\{0,1\}^n$
randomly and uniquely

if $f(a) \neq f(b)$ say balanced
if $f(a) = f(b)$
w/ prob $1/3$ say balanced
w/ prob $2/3$ say constant

Suppose f is balanced

$1/2$ time $f(a) \neq f(b)$
$1/2$ time $f(a) = f(b) \cdot 1/3$

$1/2 + 1/6$ we get the right answer
$= 2/3$

Suppose f is constant

Always $f(x) = f(y) \cdot 2/3$
we get the right answer
$= 2/3$

$\square$

2') Deutsch-Josza error rate drops
exponentially with each query

Query n times - if any disagree
say balanced else say constant

If f is constant
always get correct answer

If f is balanced
Do 1 query - say it's 0
What's the probability $n-1$
subsequent queries are the same?

If we query at random, see 0 1/2 the time

$$P(\text{see } n \text{ 0s}) = \underbrace{1/2 \cdot 1/2 \cdot \ldots \cdot 1/2}_{n-1} = 1/2^{n-1}$$

We can only do better if we keep track of previous queries

AND if we are methodical
0 error after $2^{n-1}+1$ queries

3) Can we probabilistically & efficiently solve Simon's problem?

A year with 2^{n-1} days

2^n people, each has a birthday 'buddy'

We need to find 2 people with the same birthday

Worst case 2^n queries

$\frac{1}{2^n - 1}$ to get one birthday
to find the buddy

If we keep track of findings

$\underbrace{\ \ ,\ \ ,\ \ ,\ \ }$ are there 2 bdays the same

Need $2^n/2 + 1 = 2^{n-1} + 1$ queries
like Deutsch Jozsa

Probabilistically? See the birthday problem

$f(p, d)$ = # queries to find 2 identical values among d values with probability p

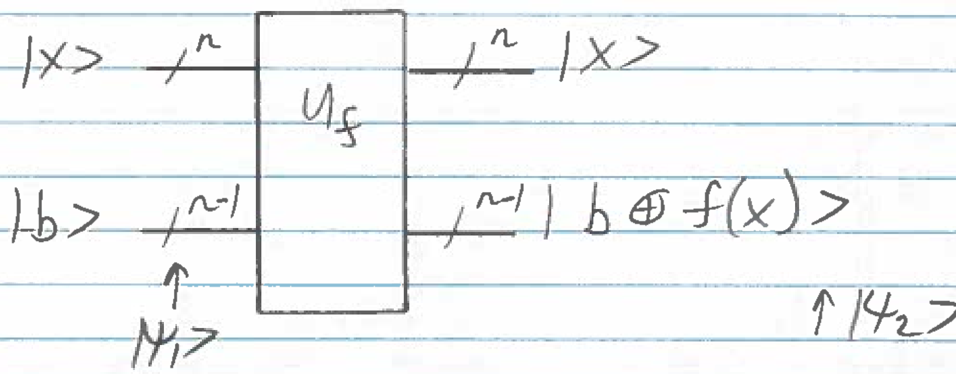
$$f(p, 2^n) = \sqrt{2 \cdot 2^n \cdot \ln\left(\frac{1}{1-p}\right)}$$

Pick p as constant,

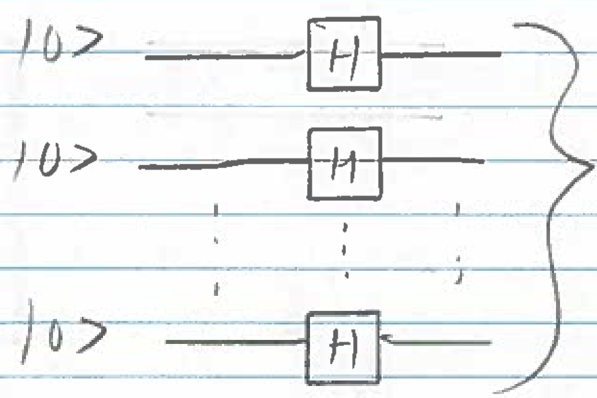
\# queries is $\Omega\left(\sqrt{2^n}\right)$

No efficient solution probabilistically

Quantum circuit to solve Simon's problem



Here we prepare $|x\rangle$ as



$$|x\rangle = H^{\otimes n}(|0^n\rangle)$$

and $|b\rangle = |0^{n-1}\rangle$

$$|\psi_0\rangle = |0^n\rangle|0^{n-1}\rangle$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \otimes |0^{n-1}\rangle$$

$|\psi_2\rangle$ after U_f ?

$$|\psi_2\rangle = U_f\left(H^{\otimes n}(|0^n\rangle) \otimes |0^{n-1}\rangle\right)$$

$$= \frac{1}{\sqrt{2^n}} U_f\left(\sum_{x \in \{0,1\}^n} |x\rangle \otimes |0^{n-1}\rangle\right)$$

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

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

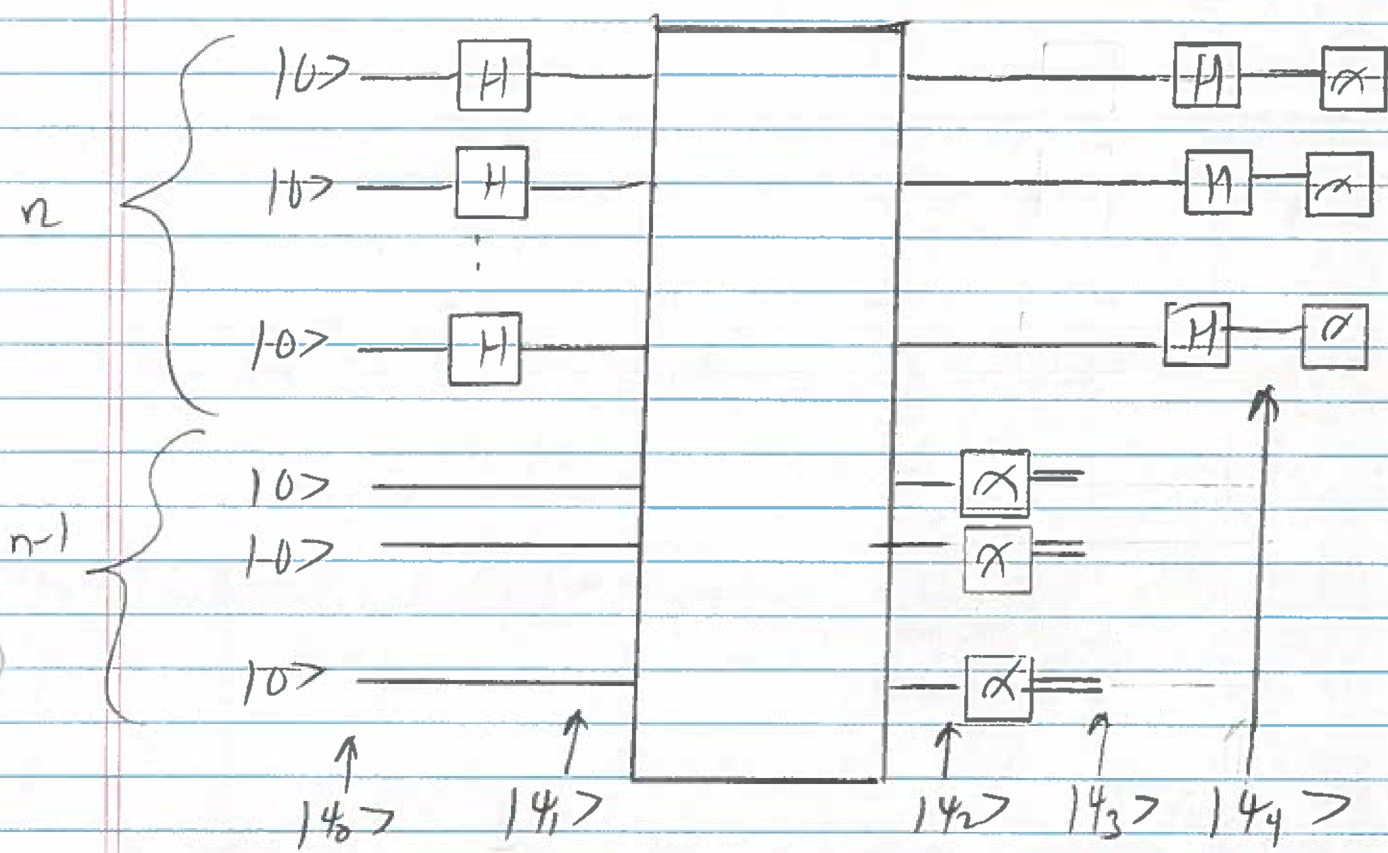
$$= \frac{1}{\sqrt{2^n}} \sum_x |x\rangle|f(x)\rangle$$

in factored-tensor form so top n wires are $|x\rangle$ bottom n-1 wires are f(x)

Output $|\psi_2\rangle$ is the uniform superposition of each

x tensored with f(x)

The circuit so far is (& finally is)



Measuring $|\psi_2\rangle$ provides a single $|x\rangle \otimes |f(x)\rangle$

What if we only measure the bottom n qubits? Partial measurement as shown above

The state collapses into

$$|\psi_2\rangle = \tfrac{1}{\sqrt{2}}\left(|x_1\rangle + |x_2\rangle\right) * f(|x_1\rangle)$$

such that $f(|x_1\rangle) = f(|x_2\rangle)$

for some random $|x_1\rangle \rightarrow x_2 = x_1 \oplus s$

From our example perhaps measuring $|f(x)\rangle$ yields

$|10\rangle$

so input $|x\rangle$ now

$$1/\sqrt{2} \, (|011\rangle + |110\rangle)$$

because $f(011) = f(110) = 10$ in our example

If we then measure $|x\rangle$ we see one "buddy" but not the ~~other~~

Eg we may see $|011\rangle$ <u>or</u> $|110\rangle$

Once we measure game over, can't re-measure ~~to~~ see the other buddy

Can't redo the circuit because it's unlikely we'd see the same $f(\,)$ output of $|10\rangle$

IDEA: Rotate again by applying Hadamard ~~to~~ top n qubits

Measurement of bottom n-1 qubits leaves the top n qubits in the state at $|\psi_3\rangle$

$$\frac{1}{\sqrt{2}}\left(|x\rangle + |x\oplus s\rangle\right)$$

$$|\psi_4\rangle = H^{\otimes n}\left(\frac{1}{\sqrt{2}}\left(|x\rangle + |x\oplus s\rangle\right)\right)$$

for some $|x\rangle$

$$= \frac{1}{\sqrt{2}}\left(H^{\otimes n}(|x\rangle) + H^{\otimes n}(|x\oplus s\rangle)\right)$$

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

So

$$|\psi_4\rangle = \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2^n}}\sum_w (-1)^{x\cdot w}|w\rangle + \frac{1}{\sqrt{2^n}}\sum_{w'}(-1)^{(x\oplus s)\cdot w'}|w'\rangle\right)$$

We can regroup the Σ so w & w' are the same

$$|\psi_4\rangle = \frac{1}{\sqrt{2\cdot 2^n}}\left[\sum_w (-1)^{x\cdot w} + (-1)^{(x\oplus s)\cdot w}|w\rangle\right]$$

$$= 1/\sqrt{2^{n+1}}\left[\sum_w (-1)^{x\cdot w} + (-1)^{\underbrace{x\cdot w \oplus s\cdot w}} |w\rangle\right]$$

only rightmost bit matters

4 cases

	$x\cdot w$ even	$x\cdot w$ odd
$s\cdot w$ even	$1+1$	$-1+-1$
$s\cdot w$ odd	$1-1$	$-1+1$

When $s\cdot w$ even $s\cdot w = 0 \mod 2$
occurs 1/2 the time
$x\cdot w$ determines whether the value added is -2 or $+2$

When $s\cdot w$ odd, no amplitude!

1/2 have amplitude 1/2 do not

renormalizing

$$|\psi\rangle = \sqrt{\frac{1}{2^n/2}} \sum_{w \mid w\cdot s \text{ is even}} (-1)^{x\cdot w} |w\rangle$$

$$= \sqrt{2/2^n} \sum_{w \mid w\cdot s = 0 \bmod 2} (-1)^{x\cdot w} |w\rangle$$

If we measure the top n qubits we obtain some $w \mid w \cdot s = 0$

This reveals bits of the secret s!

Let's say $s = 101$ as earlier

Here are all the w values we might see:

w	w∧s	w·s
000	000	0
001	001	1
010	000	0
011	001	1
100	100	1
101	101	0
110	100	1
111	101	0

We could see

000, 010, 101, 111

Say $w_1 = 010$ $w_2 = 111$

s	010·s	111·s	101·s
000	0	0	0
001	0	1	1
010	1	1	0
011	1	0	1
100	0	1	1
101	$\boxed{0}$	$\boxed{0}$	0 ✗
110	1	0	1
111	1	1	0

More generally $s = s_2 s_1 s_0$ 3 bits

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} s_2 \\ s_1 \\ s_0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

$$s_1 = 0 \quad = 0$$
$$s_2 + s_0 \quad = 0$$

s_2 + s_0 both 0 — No 000

s_2 + s_0 both 1 — Yes

$s_2\ s_1\ s_0$

1 0 1

$$\begin{pmatrix} \sim\ w_1\ \sim \\ \sim\ w_2\ \sim \\ \vdots \\ \sim\ w_{n-1}\ \sim \end{pmatrix} \begin{pmatrix} s_{n-1} \\ s_{n-2} \\ \vdots \\ s_0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

$n-1$ equations n unknowns
we end up with 2 solutions
0 + the actual s

We must learn something new from each probe → w_i must be linearly independent