Deutsch-Jozsa algorithm DJA

x is now $\underline{n}$ bits wide

$$X \longrightarrow \boxed{\quad B \quad} \longrightarrow f(x)$$

B is opaque, an ORACLE

B implements some function

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

Boolean valued function on bit strings of length n

f is either one of the two constant functions

$$\forall x \quad f(x) = 1$$
$$\text{or} \quad \forall x \quad f(x) = 0$$

OR it is balanced, returning 1 for ½ the inputs, 0 for the other half

Which is f? How hard is it to figure that out?

We are <u>promised</u> that f is one or the other

DJA shows off a problem that is
classically expensive
quantum cheap

DJA $\in$ EQP exact quantum poly time

DJA distinguishes EQP from P

Exact solution is important here
as compared to the Elitzur Vaidman bomb!

Classically we need a majority
to decide this problem

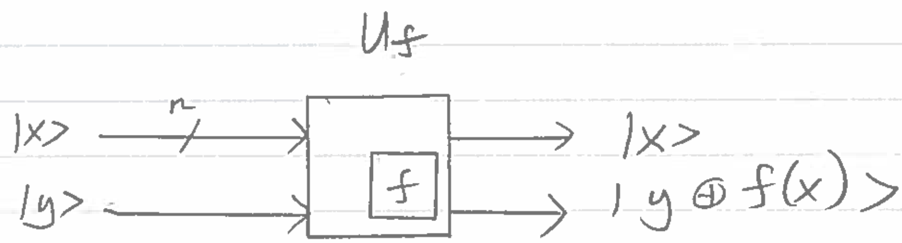
$2^{n-1} + 1$ probes $\theta(2^n)$

Proof Worst case f hides its
balanced behavior until
1/2 the possible inputs have
been tried

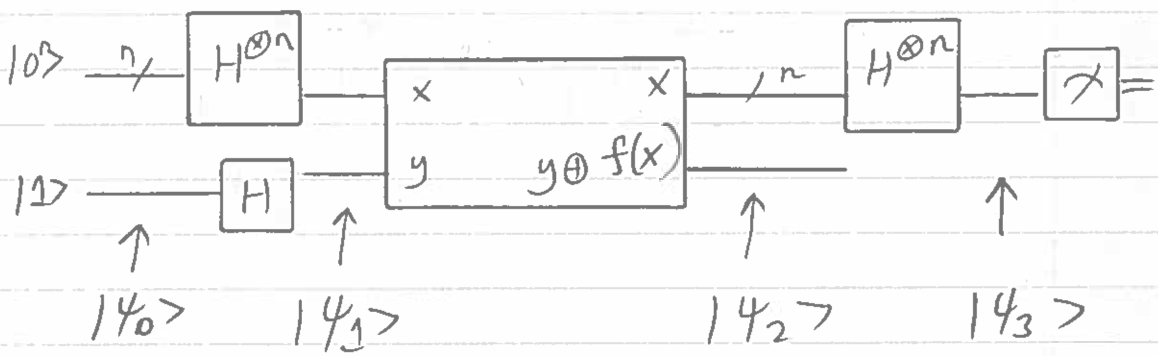
DJA on quantum computer
requires 1 probe of f
$\theta(1)$ time, exponentially
better

Algorithm uses constructive +
destructive interference
to advantage

1) Embed f in a quantum gate



$|x\rangle$ is n qubits
$|y\rangle$ is 1 qubit



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

$|\psi_1\rangle = H^{\otimes n}|0^n\rangle(|0\rangle - |1\rangle)/\sqrt{2}$

Example

$n = 2$

$$|\psi_0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}1\\0\\0\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix}$$

$$H^{\otimes 2}\begin{pmatrix}1\\0\\0\\0\end{pmatrix} = \frac{1}{\sqrt{4}}\begin{pmatrix}1\\1\\1\\1\end{pmatrix} \qquad H\begin{pmatrix}0\\1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$$

$$|\psi_1\rangle = H^{\otimes 3}|\psi_0\rangle = \frac{1}{\sqrt{8}}\begin{pmatrix}1\\-1\\1\\-1\\1\\-1\\1\\-1\end{pmatrix}$$

$$\begin{aligned} = &|000\rangle - |001\rangle \\ &+ |010\rangle - |011\rangle \\ &+ |100\rangle - |101\rangle \\ &+ |110\rangle - |111\rangle \end{aligned}$$

$$= (|00\rangle + |01\rangle + |10\rangle + |11\rangle)|0\rangle - (|00\rangle + |01\rangle + |10\rangle + |11\rangle)|1\rangle$$

$$= \sum_{x=0}^{3 \swarrow 2^n - 1} \frac{|x\rangle}{\sqrt{2^2}} \frac{(|0\rangle - |1\rangle)}{\sqrt{2}}$$

It is convenient to use
$x = 00$
01
10
11
as an iterator in
$|x\rangle|0\rangle$

$|w\rangle|v\rangle = |wv\rangle$

tensor product of $|w\rangle$ and $|v\rangle$

So Σ becomes a sum of tensors

More generally we get for $|\psi_1\rangle$

$$|\psi_1\rangle = H^{\otimes n}|0^n\rangle(|0\rangle - |1\rangle)/\sqrt{2}$$

$$= \sum_{x \in \{0,1\}^n} \frac{|x\rangle}{\sqrt{2^n}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

We need a concise notation for

$H^{\otimes n}|x\rangle$ for n-qubit x

Theorem For $|x\rangle$ a basis vector $|x\rangle = \underset{x_1}{\_}\underset{x_2}{\_}\underset{\cdots}{\_}\ldots\underset{x_n}{\_}$

$$P(n): H^{\otimes n}|x\rangle = \frac{\sum_{z \in \{0,1\}^n} (-1)^{x_1 z_1 + \ldots + x_n z_n} |z\rangle}{\sqrt{2^n}}$$

$$P(0): H^{\otimes 0}|x\rangle = \frac{(-1)^0}{1} = 1 \checkmark$$

Now show $P(k) \rightarrow P(k+1)$

Consider $x \in \{0,1\}^k$

$$H^{\otimes k}|x\rangle = \frac{1}{\sqrt{2^k}} \sum_{z \in \{0,1\}^k} (-1)^{x_1 z_1 + \ldots x_k z_k} |z\rangle$$

$$H^{\otimes k+1}|x\rangle|\psi\rangle = H^{\otimes k}|x\rangle \boxed{H|\psi\rangle}$$

Two cases $|\psi\rangle = |0\rangle$, $|\psi\rangle = |1\rangle$

Let $s = x_1 z_1 + x_2 z_2 + \ldots + x_k z_k$

Case $|\psi\rangle = |0\rangle$

$$H^{\otimes k+1}|x\rangle|0\rangle = \frac{1}{\sqrt{2^k}} \sum_{z \in \{0,1\}^k} (-1)^s |z\rangle [|0\rangle + |1\rangle] / \sqrt{2}$$

$$= \frac{1}{\sqrt{2^{k+1}}} \left(\sum_z (-1)^s \,|\,|z\rangle \left((-1)^{0 \cdot 0} |0\rangle + (-1)^{0 \cdot 1} \right) |1\rangle \right)$$

$$= \frac{1}{\sqrt{2^{k+1}}} \left(\sum_{z} (-1)^{s} \cdot (-1)^{0 \cdot 0} |z0\rangle \right.$$

$$\left. + \sum_{z} (-1)^{s} \cdot (-1)^{0 \cdot 1} |z1\rangle \right)$$

$$= \frac{1}{\sqrt{2^{k+1}}} \sum_{z \in \{0,1\}^{k+1}} (-1)^{x_1 z_1 + \ldots + x_{k+1} z_{k+1}} |z\rangle$$

Case $|4\rangle = |1\rangle$

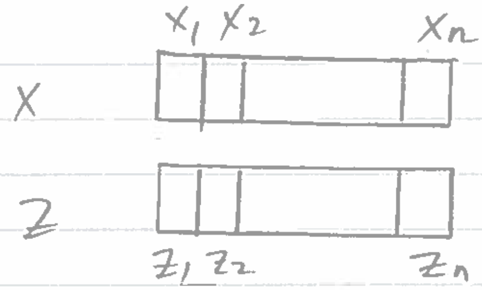
$$H^{\otimes k+1} |x\rangle|1\rangle = \frac{1}{\sqrt{2^k}} \sum_{z} (-1)^{s} |z\rangle \frac{[|0\rangle - |1\rangle]}{\sqrt{2}}$$

$$= \frac{1}{\sqrt{2^{k+1}}} \sum_{z} (-1)^{s} |z\rangle \left[(-1)^{1 \cdot 0} |0\rangle + (-1)^{1 \cdot 1} |1\rangle \right]$$

$$= \frac{1}{\sqrt{2^{k+1}}} \sum_{z \in \{0,1\}^{k+1}} (-1)^{x_1 z_1 + \ldots + x_{k+1} z_{k+1}} |z\rangle$$

$\square$

97.1



$$(-1)^{x_1 z_1 + \dots + x_n z_n}$$

$$= (-1)^{\overbrace{[x_1 z_1 + \dots + x_n z_n]}^{s} \bmod 2}$$

Proof

$$-1^0 = 1 \qquad -1^1 = -1$$

$$(-1)^K \quad K > 2 \quad = (-1)^{K-1}(-1)^1 \qquad m = 0 \text{ or } 1$$

$K \bmod 2 = 0 \rightarrow K-1$ odd $= (-1)(-1) = 1$

$K \bmod 2 = 1 \rightarrow K-1$ even $= (1)(-1) = -1$

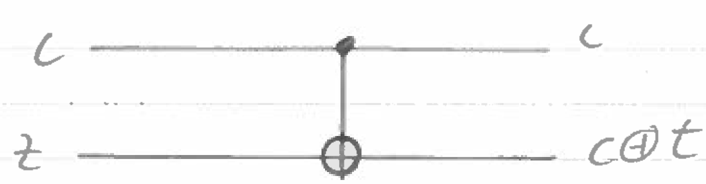
Then $x_1 z_1 + \dots + x_n z_n = X \cdot Z$

inner product of X & Z, with sum taken mod 2, same as XOR

Corollary

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

Remember CNOT

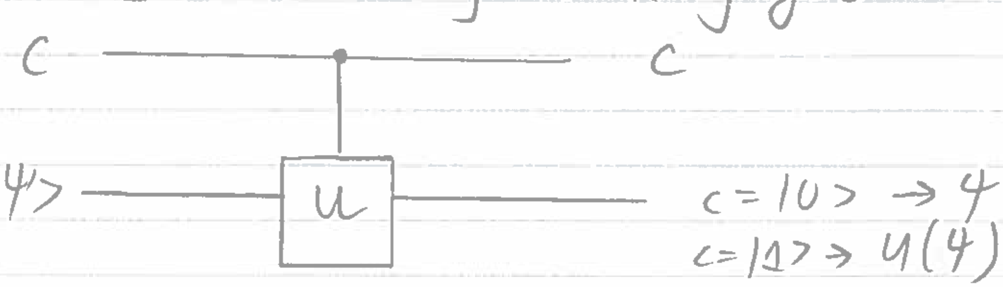


2^{nd} qubit is
- the exclusive or of c + t
- flipped t, as controlled by c

  c = 0 you get t

  c = 1 you get $\bar{t}$

Generalization - controlled U
where U is any Unitary gate



c-U gate is

$$|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U$$

So revisiting $|\psi_1\rangle$

$$= H^{\otimes n}|0\rangle \otimes H|1\rangle$$

$$= \frac{1}{\sqrt{2^n}} \sum_{z \in \{0,1\}^n} (-1)^{0z_1 + 0z_2 + \dots + 0z_n} |z\rangle \otimes H|1\rangle$$

$$= \sum_{z \in \{0,1\}^n} \frac{|z\rangle}{\sqrt{2^n}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

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

recall $U_f : |xy\rangle \to |x, y \oplus f(x)\rangle$

Consider some $z \in \{0,1\}^n$

$$U_f(|z-\rangle) = \frac{U_f(|z0\rangle) - U_f(|z1\rangle)}{\sqrt{2}}$$

$$= \frac{|z\rangle|0 \oplus f(x)\rangle - |z\rangle|1 \oplus f(x)\rangle}{\sqrt{2}}$$

this is a single qubit a state, NOT a scalar!

$f(x)=0$ or $f(x)=1$ Two cases

$$f(x)=0 \rightarrow U_f(|z-\rangle) = \frac{|z0\rangle - |z1\rangle}{\sqrt{2}}$$

$$= |z\rangle(-1^0)\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

$$f(x)=1 \rightarrow U_f(|z-\rangle) = \frac{|z1\rangle - |z0\rangle}{\sqrt{2}}$$

$$= |z\rangle(-1)^1\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

$$\rightarrow U_f(|z-\rangle) = |z\rangle(-1)^{f(x)}\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

So

$|\psi_2\rangle =$

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