Deutsch-Jozsa Algorithm

School on Quantum Computing @Yagami

Day 1, Lesson 3

13:00-14:00, March 22, 2005

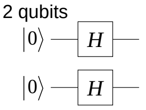
Eisuke Abe

Department of Applied Physics and Physico-Informatics, and CREST-JST, Keio University

The inventors

Hadamard on n qubits

2 qubits

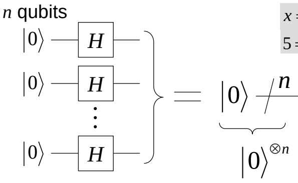


$$
\begin{aligned}
&H|0\rangle \otimes H|0\rangle \\
&= \frac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right)\otimes\frac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right) \\
&= \frac{1}{2}\left(|00\rangle+|01\rangle+|10\rangle+|11\rangle\right) \\
&= \frac{1}{2}\left(|0\rangle+|1\rangle+|2\rangle+|3\rangle\right)=\frac{1}{2}\sum_{x=0}^{3}|x\rangle
\end{aligned}
$$

n qubits

$x = x_1x_2\cdots x_n$ with $x_i = 0,1$

$5 = 101 = 2^2\times 1+2^1\times 0+2^0\times 1$



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

Hadamard on n qubits

$$
|x\rangle \xrightarrow{\;/^{n}\; H^{\otimes n}} \frac{1}{2^{n/2}}\sum_{z}(-1)^{x\cdot z}|z\rangle
$$

$$
\begin{aligned}
&H^{\otimes n}|x_1\rangle|x_2\rangle\cdots|x_n\rangle \\
&= \frac{1}{2^{n/2}}\left(\sum_{z_1}(-1)^{x_1\cdot z_1}|z_1\rangle\right)\cdots\left(\sum_{z_n}(-1)^{x_n\cdot z_n}|z_n\rangle\right) \\
&= \frac{1}{2^{n/2}}\sum_{z_1,z_2\cdots z_n}(-1)^{x_1\cdot z_1}(-1)^{x_2\cdot z_2}\cdots(-1)^{x_n\cdot z_n}|z_1z_2\cdots z_n\rangle \\
&= \frac{1}{2^{n/2}}\sum_{z}(-1)^{x\cdot z}|z\rangle
\end{aligned}
$$

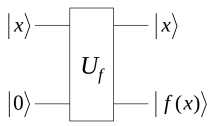
$x\cdot z \equiv x_1\cdot z_1 + x_2\cdot z_2 + \cdots + x_n\cdot z_n$

Bitwise inner product of x and z modulo 2

Quantum parallelism

Suppose we are given a quantum gate U_f

$$
U_f|x\rangle|y\rangle = |x\rangle|y\oplus f(x)\rangle
$$



where $f(x)$ is a binary function

Remarkably, for proper inputs, we can encode all the information on $f(x)$ by applying U_f only once

$$
\frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}|x\rangle|0\rangle \xrightarrow{U_f} \frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}\underline{|x\rangle|f(x)\rangle}
$$

Entangled

Quantum parallelism

$$
\frac{1}{2}\left(|0\rangle+|1\rangle+|2\rangle+|3\rangle\right)|0\rangle
$$

$$
\xrightarrow{U_f} \frac{\cancel{|0\rangle|f(0)\rangle}+|1\rangle|f(1)\rangle+\cancel{|2\rangle|f(2)\rangle}+\cancel{|3\rangle|f(3)\rangle}}{2}
$$

Is this useful?

The answer is ***NO***, because we must observe the state to extract information out of it, which prevents us from enjoying the full power of quantum entanglement and quantum parallelism

Quantum interference is the key

Deutsch's problem

Definition

A binary function $f(x)$ is called ***constant*** if it outputs only 0, or only 1, for all values of x

A binary function $f(x)$ is called ***balanced*** if it outputs 0 for half of all the possible x, and 1 for the other half

Constant

x	$f(x)$
0	0
1	0
2	0
3	0

Balanced

x	$f(x)$
0	0
1	0
2	1
3	1

Neither *C* or *B*

x	$f(x)$
0	0
1	0
2	0
3	1

Deutsch's problem

Constant or balanced, that is the problem

Alice x_0 — Query → Bob $f(x_0)$

← Answer

How many times does Alice have to query Bob to determine the type of his function?

Deutsch's problem: Classical case

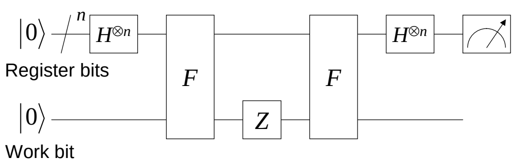
	Alice		Bob
Before the game starts	knows $n = 2$		has a ***balanced*** function $f(x)$
	$x = 0$	Query → / ← Answer	$f(0) = 0$
Still cannot distinguish from $f(x) = (0,0,0,0)$	$x = 1$	Query → / ← Answer	$f(1) = 0$
The game ends	$x = 2$	Query → / ← Answer	$f(2) = 1$

x	$f(x)$
0	0
1	0
2	1
3	1

$0 \le x \le 2^n - 1$

The worst case requires $2^{n/2}+1$ queries

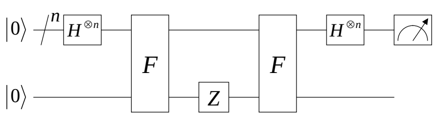
Quantum circuit for DJ



$$H^{\otimes n}|x\rangle = \frac{1}{2^{n/2}}\sum_z (-1)^{x\cdot z}|z\rangle \qquad F|x\rangle|w\rangle = |x\rangle|w \oplus f(x)\rangle$$

$$x\cdot z \equiv x_1\cdot z_1 + x_2\cdot z_2 + \cdots + x_n\cdot z_n \qquad Z|w\rangle = (-1)^w|w\rangle$$

Implementing DJ



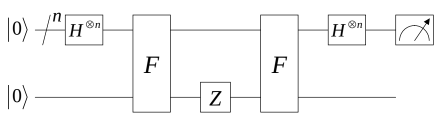
$$|0\rangle^{\otimes n}|0\rangle \xrightarrow{H^{\otimes n}} \frac{1}{2^{n/2}}\sum_x |x\rangle|0\rangle$$

Create a linear superposition state

$$\xrightarrow{F} \frac{1}{2^{n/2}}\sum_x |x\rangle|f(x)\rangle$$

Encode information on $f(x)$ into the work bit

Implementing DJ



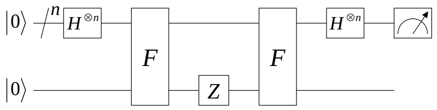
$$\frac{1}{2^{n/2}}\sum_x |x\rangle|f(x)\rangle \xrightarrow{Z} \frac{1}{2^{n/2}}\sum_x (-1)^{f(x)}|x\rangle|f(x)\rangle$$

Add nonlocal phase shifts which carry information on $f(x)$

$$\xrightarrow{F} \frac{1}{2^{n/2}}\sum_x (-1)^{f(x)}|x\rangle|0\rangle$$

Erase information on $f(x)$ from the work bit

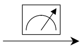
Implementing DJ



$$\frac{1}{2^{n/2}}\sum_x (-1)^{f(x)}|x\rangle|0\rangle \xrightarrow{H^{\otimes n}} \sum_z \boxed{\sum_x \frac{(-1)^{f(x)+x\cdot z}}{2^n}}|z\rangle|0\rangle$$

$$H^{\otimes n}|x\rangle = \frac{1}{2^{n/2}}\sum_z (-1)^{x\cdot z}|z\rangle$$

Probability amplitude for the state $|z\rangle$



Get $z = 0$ if and only if f is a constant function

Implementing DJ

Probability amplitude for the state $|0\rangle^{\otimes n}$

$$\sum_x \frac{(-1)^{f(x)}}{2^n} = \begin{cases} \pm 1 & \text{(constant)} \\ 0 & \text{(balanced)} \end{cases}$$

Only the constant functions bring the register back to the initial state

$n = 2$, constant case

Constructive interference

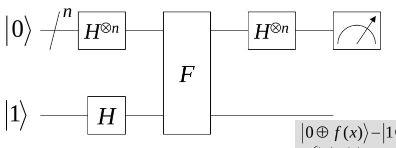
$$\sum_{x=0}^{3}\frac{(-1)^{f(x)}}{2^2} = \frac{(-1)^0+(-1)^0+(-1)^0+(-1)^0}{4} = 1$$

$n = 2$, balanced case

Destructive interference

$$\sum_{x=0}^{3}\frac{(-1)^{f(x)}}{2^2} = \frac{(-1)^0+(-1)^1+(-1)^0+(-1)^1}{4} = 0$$

Revised version



$$|0\oplus f(x)\rangle - |1\oplus f(x)\rangle = \begin{cases} |0\rangle-|1\rangle & \text{if } f(x)=0 \\ |1\rangle-|0\rangle & \text{if } f(x)=1 \end{cases} = (-1)^{f(x)}(|0\rangle-|1\rangle)$$

A clever choice of the work bit simplifies the circuit

$$|0\rangle^{\otimes n}|1\rangle \xrightarrow{H^{\otimes n+1}} \frac{1}{2^{n/2}}\sum_x |x\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] \xrightarrow{F} \frac{1}{2^{n/2}}\sum_x (-1)^{f(x)}|x\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$$

State after the 2nd F gate

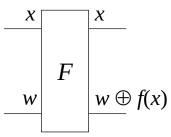
$$\xrightarrow{H^{\otimes n}} \frac{1}{2^n}\sum_{x,z}(-1)^{f(x)+x\cdot z}|z\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$$

1-bit $f(x)$

x	Constant		Balanced	
	f_{c0}	f_{c1}	f_{b0}	f_{b1}
0	0	1	0	1
1	0	1	1	0

$f_{c0}(x) = 0$ $\quad f_{b0}(x) = x$

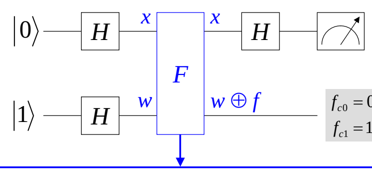
$f_{c1}(x) = 1$ $\quad f_{b1}(x) = \bar{x}$



$$F|x\rangle|w\rangle = |x\rangle|w\oplus f(x)\rangle$$

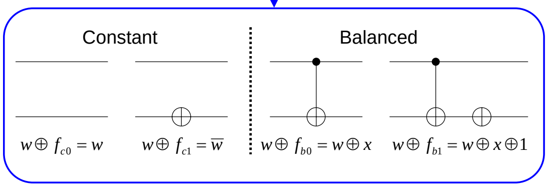
What is the explicit quantum circuit for the F gate?

1-bit F gate

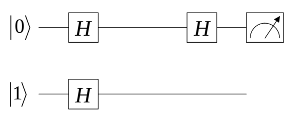


$f_{c0} = 0$ $\quad f_{b0} = x$

$f_{c1} = 1$ $\quad f_{b1} = \bar{x}$



1-bit DJ: Constant f_{c0}

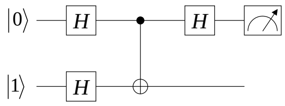


$$HH|0\rangle = \frac{1}{2}\left(|0\rangle+|1\rangle+|0\rangle-|1\rangle\right) = |0\rangle$$

Constructive interference

The initial state $|0\rangle$ "survives" due to the constructive interference, while the other state $|1\rangle$ is erased due to the destructive interference

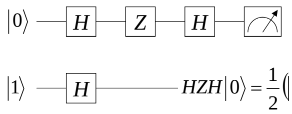
1-bit DJ: Balanced f_{b0}



$$|0\oplus x\rangle-|1\oplus x\rangle = \begin{cases}|0\rangle-|1\rangle & \text{if } x=0\\ |1\rangle-|0\rangle & \text{if } x=1\end{cases} = (-1)^x(|0\rangle-|1\rangle)$$

$$|0\rangle|1\rangle \xrightarrow{H^{\otimes 2}} \frac{1}{\sqrt{2}}\sum_{x=0}^{1}|x\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] \xrightarrow{C_{rw}} \frac{1}{\sqrt{2}}\sum_{x=0}^{1}\underline{(-1)^x|x\rangle}\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$$

Z gate on the register



Destructive interference

$$HZH|0\rangle = \frac{1}{2}\left(|1\rangle+|0\rangle+|1\rangle-|0\rangle\right) = |1\rangle$$

2-bit $f(x)$

x	ab	Constant		Balanced ($_4C_2 = 6$)					
		f_{c0}	f_{c1}	f_{b0}	f_{b1}	f_{b2}	f_{b3}	f_{b4}	f_{b5}
0	00	0	1	0	0	0	1	1	1
1	01	0	1	0	1	1	1	0	0
2	10	0	1	1	0	1	0	1	0
3	11	0	1	1	1	0	0	0	1

$f_{c0}(x)=0$ $\quad f_{b0}(x)=a$ $\quad f_{b3}(x)=\bar{a}$

$f_{c1}(x)=1$ $\quad f_{b1}(x)=b$ $\quad f_{b4}(x)=\bar{b}$

$f_{b2}(x)=a\oplus b$ $\quad f_{b5}(x)=\overline{a\oplus b}$

2-bit *F* gates can be constructed from only CNOT and NOT

3-bit balanced $f(x)$

$f_{b0}=a$

$f_{b1}=a\oplus b$

$f_{b2}=a\oplus b\oplus c$

$f_{b3}=ab\oplus c$

$f_{b4}=ab\oplus a\oplus c$

$f_{b5}=ab\oplus a\oplus b\oplus c$

$f_{b6}=ab\oplus bc\oplus a$

$f_{b7}=ab\oplus bc\oplus a\oplus b$

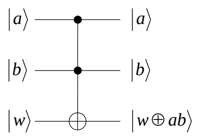
$f_{b8}=ab\oplus bc\oplus ca$

$f_{b9}=ab\oplus bc\oplus ca\oplus a\oplus b$

Number of balanced functions

$$_8C_4 = 70$$

3-bit *F* gates require not only CNOT but Toffoli



3-bit balanced $f(x)$

x	abc	f_{b0}	f_{b1}	f_{b2}	f_{b3}	f_{b4}	f_{b5}	f_{b6}	f_{b7}	f_{b8}	f_{b9}
0	000	0	0	0	0	0	0	0	0	0	0
1	001	0	0	1	1	1	1	0	0	0	0
2	010	0	1	1	0	0	1	0	1	0	1
3	011	0	1	0	1	1	0	1	0	1	0
4	100	1	1	1	0	1	1	1	1	0	1
5	101	1	1	0	1	0	0	1	1	1	0
6	110	1	0	0	1	0	1	0	1	1	1
7	111	1	0	1	0	1	0	1	0	1	1
# of blcd fns		6	6	2	6	12	6	12	12	2	6

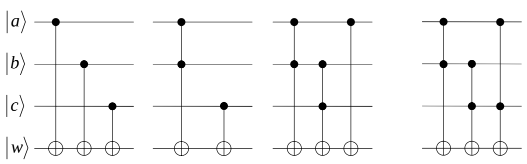
$f_{b0}=a$ $\quad f_{b4}=ab\oplus a\oplus c$ $\quad f_{b8}=ab\oplus bc\oplus ca$

$f_{b1}=a\oplus b$ $\quad f_{b5}=ab\oplus a\oplus b\oplus c$ $\quad f_{b9}=ab\oplus bc\oplus ca\oplus a\oplus b$

$f_{b2}=a\oplus b\oplus c$ $\quad f_{b6}=ab\oplus bc\oplus a$

$f_{b3}=ab\oplus c$ $\quad f_{b7}=ab\oplus bc\oplus a\oplus b$

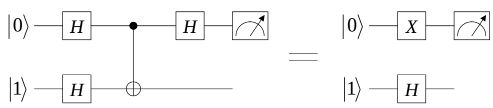
3-bit DJ: Balanced



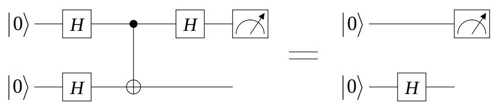
$w\oplus f_{b2} = w\oplus a\oplus b\oplus c$ $\quad w\oplus f_{b3} = w\oplus ab\oplus c$ $\quad w\oplus f_{b6} = w\oplus ab\oplus bc\oplus a$ $\quad w\oplus f_{b8} = w\oplus ab\oplus bc\oplus ca$

Quiz 1

Prove the following circuit identity by converting the circuit sequentially



Also show that *X* in the upper line vanish if the initial state of the second qubit is $|0\rangle$



Quiz 2

Construct all the 2-bit F gates based on the list below

x	ab	Constant		Balanced					
		f_{c0}	f_{c1}	f_{b0}	f_{b1}	f_{b2}	f_{b3}	f_{b4}	f_{b5}
0	00	0	1	0	0	0	1	1	1
1	01	0	1	0	1	1	1	0	0
2	10	0	1	1	0	1	0	1	0
3	11	0	1	1	1	0	0	0	1

$f_{c0}(x) = 0$ $\quad f_{b0}(x) = a$ $\quad f_{b3}(x) = \overline{a}$

$f_{c1}(x) = 1$ $\quad f_{b1}(x) = b$ $\quad f_{b4}(x) = \overline{b}$

$f_{b2}(x) = a \oplus b$ $\quad f_{b5}(x) = \overline{a \oplus b}$