Phys 396 2018

Lecture 21

Thurs: Class

Tues: Exam II

Covers Class 12–21

Project Topics due by Friday

* remaining HW assignments will include project updates.
* Final draft 7 December
* First " 30 November.
* Will produce rubric.

Deutsch-Jozsa algorithm

The DJ problem considers functions from n bits to 1 bit

$$(x_{n-1}, \ldots x_0) \longrightarrow f(x_{n-1}, \ldots, x_0)$$

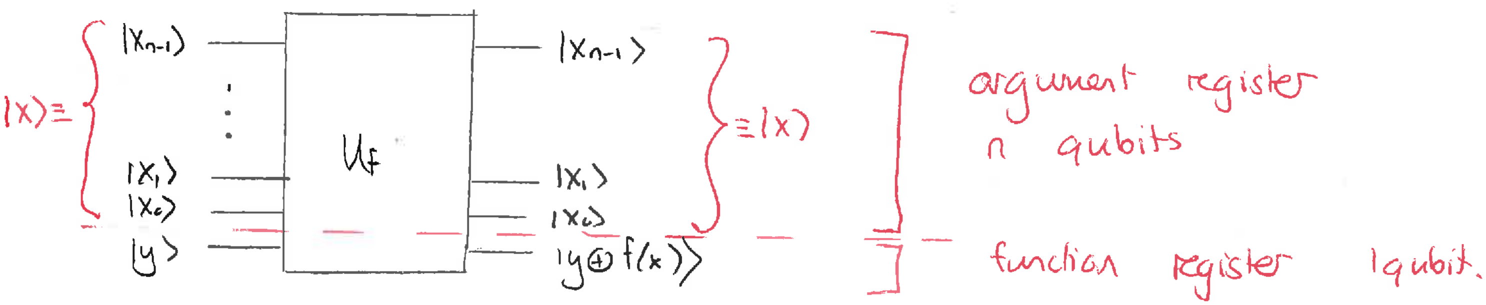
and these are restricted to two categories:

Category 1 (Constant)	Category 2 (Balanced)
function returns same value for all possible arguments, e.g. $f(x_{n-1}, \ldots, x_0) = 1$ regardless of input	function returns "0" for exactly half the arguments and "1" for exactly half the arguments. e.g. $f(x_{n-1}, \ldots, x_1, x_0) = x_1$

The D-J problem is:

> One party chooses a function and constructs an oracle that can evaluate the function. The other party has to determine the category to which the function belongs with a minimal number of oracle queries.

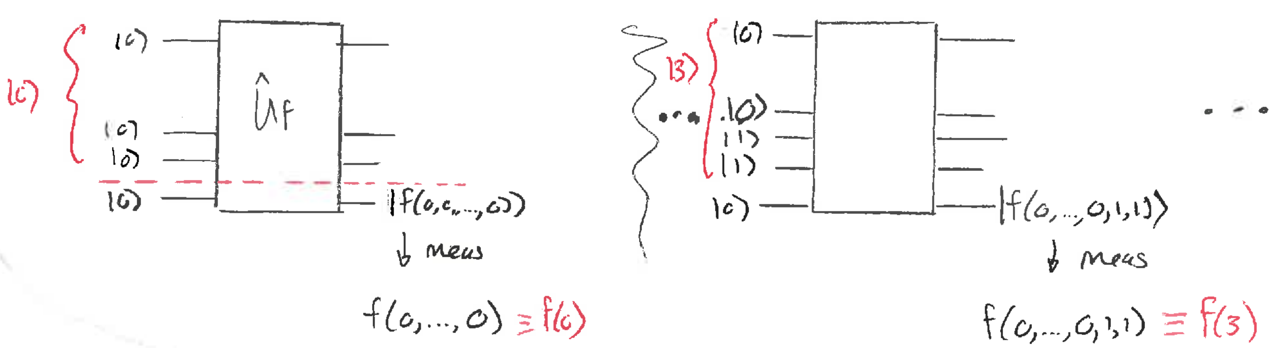
To be specific, the oracle operates as:



Then a classical algorithm would be:

Alice picks, f, and constructs oracle

Bob systematically evaluates function at various inputs - the oracle must be used repeatedly.



Bob compares the measured outputs as he acquires them:

run 1 $\rightsquigarrow$ $f(0)$
run 2 $\rightsquigarrow$ $f(1)$
compare
if different (balanced)
if same

run 3 $\rightsquigarrow$ $f(2)$ — compare to $f(1)$ — if different $\Rightarrow$ balanced
if same

run 4 $\rightsquigarrow$ $f(3)$

In the worst case of a balanced function (first $2^n/2$ all give same outcome) Bob has to evaluate on $2^n/2 + 1 = 2^{n-1} + 1$ arguments.

Thus

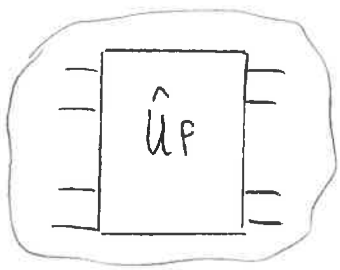
$$\boxed{\text{To determine the function type classically, Bob must use } 2^{n-1}+1 \text{ oracle queries}}$$

This grows exponentially in the number of bits on which the function can be evaluated. This is a "difficult" problem to assess.

Note that Bob uses the oracle in a very conventional function evaluation way.

input function argument $\Rightarrow$

e.g. $00..01110$
$\equiv 14$



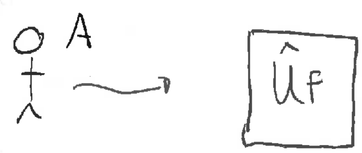
$\Rightarrow$ get function evaluated

e.g. $f(0...01110) \equiv f(14)$

But it is only coincidental to the classical strategy that Bob evaluates the function on various arguments. In terms of solving the problem he does not care if e.g. $f(14)=0$ or $f(14)=1$. He only needs to know whether f differs on some pair of inputs, and not what those values are. So the issue is not a typical one of evaluating $f(14)$ or $f(21)$, etc, ...

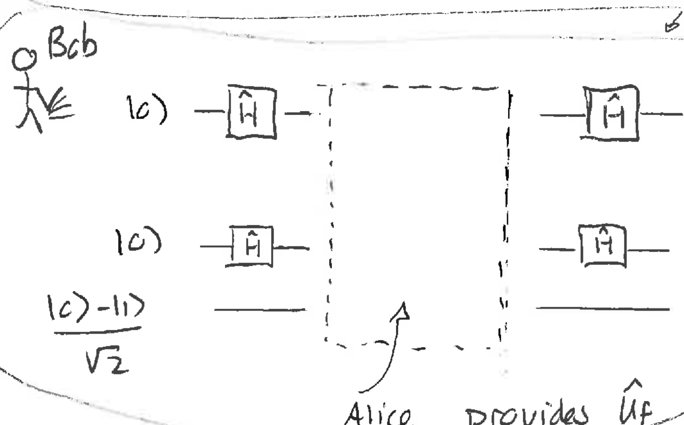
The quantum algorithm avoids this. Here

Alice chooses f and constructs the oracle as before

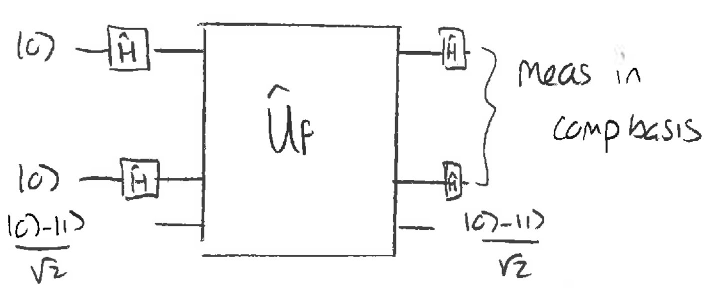


Different f's give different $\hat{U}_f$

Bob sets up quantum circuit in anticipation of receiving the oracle:

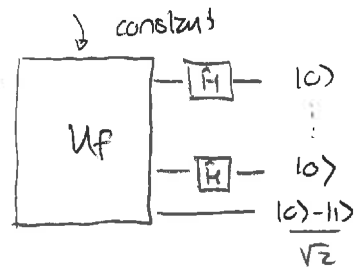


After Alice provides $\hat{U}_f$, Bob measures the argument register in the computational basis



Use quantum physics one can track the state of all qubits as they pass through the process. We find.

1) If Alice choses constant function then the final state for

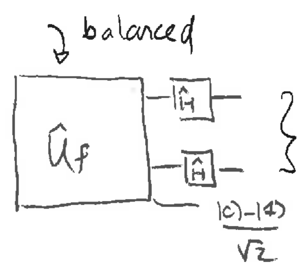


the argument register is

$|0\rangle|0\rangle \ldots |0\rangle|0\rangle \equiv |00\ldots 00\rangle \equiv |0\rangle$ decimal

with certainty

2) If Alice choses a constant function then the final state for



the argument register is a superposition of computational basis states but $|0\ldots 00\rangle$ never appears in the superposition

State is:

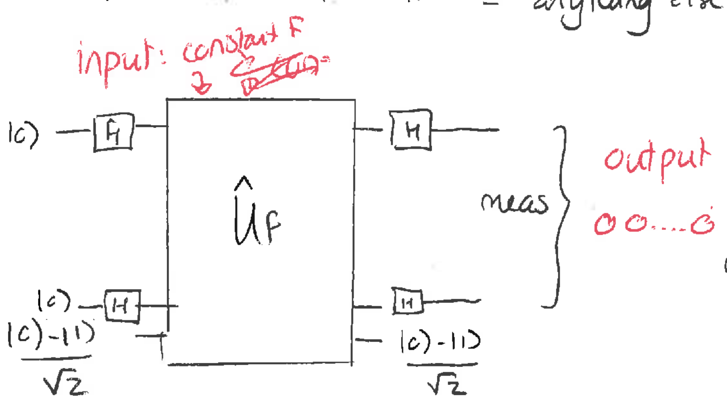
$$\alpha_1|0\ldots 01\rangle + \alpha_2|0\ldots 010\rangle + \alpha_3|0\ldots 11\rangle + \ldots + \alpha_{2^n-1}|1\ldots 11\rangle$$

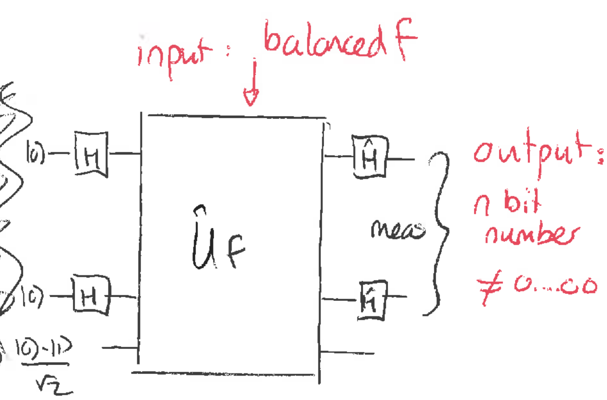
The coefficients depend on the function.

Thus the final step is:

If comp basis meas $= 0\ldots 0 \Rightarrow f$ is constant

" " " $=$ anything else $\Rightarrow f$ is balanced





Simon's algorithm

Simons algorithm considers a function that maps in an exactly two to one function - thus for each output there are exactly two inputs

$$\begin{array}{lll} 000\ldots00 & \searrow & f(0,0\ldots0) = f(0,0,\ldots0,1) \\ 000\ldots01 & \nearrow & \\ 000\ldots10 & \searrow & f(0,0,\ldots1,0) = f(0,0,\ldots1,1) \\ 000\ldots11 & \nearrow & \end{array}$$

not equal

Additionally it requires that the function be periodic. So there exist some $a = a_{n-1}, \ldots a_1 a_0$ so that for all $x_{n-1}, \ldots x_0$

$$f(x_{n-1} \oplus a_{n-1}, x_{n-2} \oplus a_{n-2}, \ldots, x_1 \oplus a_1, x_0 \oplus a_0)$$
$$= f(x_{n-1}, \ldots, x_0)$$

Then the task is to find a. We will use as a shorthand

$$\underbrace{x \oplus a}_{\text{decimal}} \equiv \underbrace{x_{n-1} \oplus a_{n-1}, x_{n-2} \oplus a_{n-2}, \ldots, x_0 \oplus a_0}_{\text{binary}}$$

So we need to find a s.t.

$$f(x \oplus a) = f(x)$$

Classically we need to evaluate f on various inputs until we find two that return the same output. Note that if $f(x') = f(x)$ we know $x' = x \oplus a$ and $a = x' \oplus x$

1 Simon's problem

Consider functions that map two bits onto a single bit:

$$(x_1, x_0) \mapsto f(x_2, x_1, x_0).$$

Which of these are $2 \to 1$ and satisfy $f(x \oplus a) = f(x)$ for all possible x? Determine the value of a in those cases.

a) $f(x_1, x_0) = x_1$.

b) $f(x_1, x_0) = x_1 \oplus x_0$.

c) $f(x_1, x_0) = x_1 x_0$.

Answer.

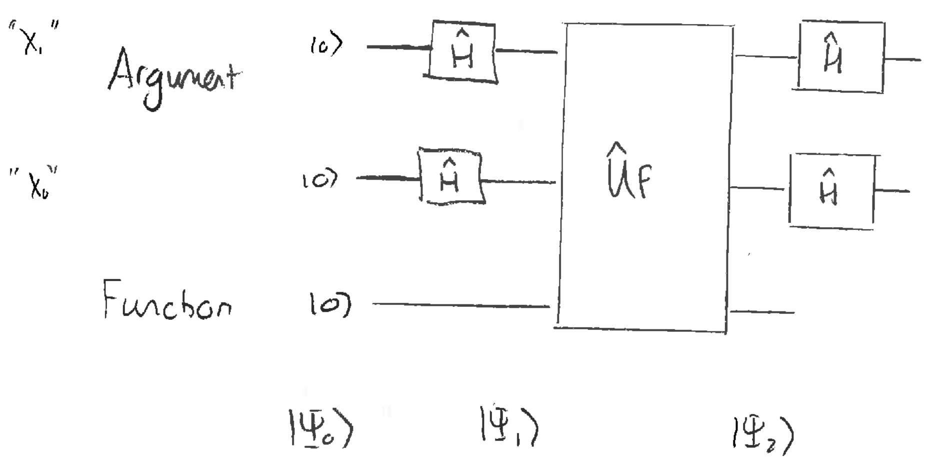
x_1	x_0	$f = x_1$	$f = x_1 \oplus x_0$	$f = x_1 x_0$
0	0	0	0	0
0	1	0	1	0
1	0	1	1	0
1	1	1	0	1
		is $2 \to 1$	is $2 \to 1$	not $2 \to 1$
		$a = 01$ works	$a = 11$ works	

In order to determine the period we need to evaluate the function at least twice (for $n=2$)

A detailed analysis shows that the admissible functions are:

$$f(x_1,x_0) = x_1 \qquad a = 01$$
$$f(x_1,x_0) = x_1 \oplus 1 \qquad a = 01$$
$$f(x_1,x_0) = x_0 \qquad a = 10$$
$$f(x_1,x_0) = x_0 \oplus 1 \qquad a = 10$$
$$f(x_1,x_0) = x_1 \oplus x_0 \qquad a = 11$$
$$f(x_1,x_0) = x_1 \oplus x_0 \oplus 1 \qquad a = 11$$

Now consider the scheme



So
$$|\Psi_1\rangle = \frac{1}{2}\sum_{x_1,x_0} |x_1 x_0\rangle\,|0\rangle$$

$$\xrightarrow{\hat{U}_F} \;=\; \frac{1}{2}\sum_{x_1,x_0} |x_1 x_0\rangle\,|f(x_1,x_0)\rangle$$

The exact structure here depends on the function and we consider the first case $f(x_1,x_0) = x_1$

Then

$$|\Psi_2\rangle = \frac{1}{2} \sum |x_1 x_0\rangle |x_1\rangle$$

$$= \frac{1}{2}\left\{ |00\rangle \overset{f(0)}{|0\rangle} + |01\rangle \overset{f(1)}{|0\rangle} + |10\rangle \overset{f(2)}{|1\rangle} + |11\rangle \overset{f(3)}{|1\rangle} \right\}$$

$$= \frac{1}{2} \left(|00\rangle + |01\rangle\right)|0\rangle + \frac{1}{2}\left(|10\rangle + |11\rangle\right)|1\rangle$$

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

We see that the doubling up has produced a periodicity in the argument register. Finally

$$|\Psi_3\rangle = \frac{1}{2} \quad H|0\rangle\, H\left(|0\rangle + |1\rangle\right)|0\rangle + \frac{1}{2} H|1\rangle\, \hat{H}\left(|0\rangle + |1\rangle\right)|1\rangle$$

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

$$= \frac{1}{2} \quad |00\rangle\left(|0\rangle + |1\rangle\right) + \frac{1}{2}|10\rangle\left(|0\rangle - |1\rangle\right)$$

Note that measurement in the computational basis gives either $x = 00$ or $x = 10$ and these both satisfy $x \cdot a = 0$

Each are equally likely.

This is true in general of Simons algorithm. The algorithm always returns x s.t $x \cdot a = 0$. We run the algorithm multiple times and obtain a set

x, $\tilde{x}$, $\tilde{\tilde{x}}$, etc....

such that each satisfies $x \cdot a = 0$.

This gives a set of linear equations:

$$x_{n-1} a_{n-1} + x_{n-2} a_{n-2} + \cdots + x_0 a_0 = 0$$

$$\tilde{x}_{n-1} a_{n-1} + \tilde{x}_{n-2} a_{n-2} + \cdots + \tilde{x}_0 a_0 = 0$$

$$\vdots$$

If we have n independent equations, then we can invert these to find $a_{n-1}, \ldots, a_0$.

So typically we need n oracle invocations and $O(n^2)$ classical operations to invert the equations. A classical algorithm requires $O(2^{n/2})$ oracle queries

2 Simon's algorithm for a two bit function

Consider the standard scheme for implementing Simon's algorithm. Suppose that the function is $f(x_1, x_0) = x_0$.

a) Determine the state of the system immediately before the oracle query.

b) Determine the state of the system immediately after the oracle query.

c) Determine the state of the system immediately before the measurement on the argument register.

d) Describe the possible outcomes of the measurement on the argument register.

e) The period is a number that satisfies $x \cdot a = 0$ where x is a measurement outcome. What would the posible outcomes here reveal about the period?

Ans: a) $\frac{1}{2^{n/2}} \sum_{x_1, x_0} |x_1 x_0\rangle |0\rangle = \frac{1}{2}\left[|00\rangle|0\rangle + |01\rangle|0\rangle + |10\rangle|0\rangle + |11\rangle|0\rangle\right] \equiv |\Psi_1\rangle$

b) $|\Psi_2\rangle = \hat{U}_f |\Psi_1\rangle = \frac{1}{2}\left[\hat{U}_f |00\rangle|0\rangle + \hat{U} |01\rangle|0\rangle + \cdots\right]$

$$= \frac{1}{2}\left[|00\rangle|f(0)\rangle + |01\rangle|f(1)\rangle + |10\rangle|f(2)\rangle + |11\rangle|f(3)\rangle\right]$$

But
$$f(0) = 0$$
$$f(1) = 1$$
$$f(2) = 0$$
$$f(3) = 1$$

$$\Rightarrow \quad |\Psi_2\rangle = \frac{1}{2}\left[|00\rangle|0\rangle + |01\rangle|1\rangle + |10\rangle|0\rangle + |11\rangle|1\rangle\right]$$

$$= \frac{1}{2}\left[\left(|00\rangle + |10\rangle\right)|0\rangle + \left(|01\rangle + |11\rangle\right)|1\rangle\right]$$

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

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

c) A Hadamard acts on each argument register.

$$|\Psi_3\rangle = \frac{1}{2}\hat{H}(|0\rangle+|1\rangle)\,\hat{H}|0\rangle\,|0\rangle + \frac{1}{2}\hat{H}(|0\rangle+|1\rangle)(\hat{H}|1\rangle)\,|1\rangle$$

$$= \frac{1}{2}\sqrt{2}\,|0\rangle\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\,|0\rangle + \frac{1}{2}\sqrt{2}\,|0\rangle\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\,|1\rangle$$

$$= \frac{1}{2}(|00\rangle+|01\rangle)\,|0\rangle + \frac{1}{2}(|00\rangle-|01\rangle)\,|1\rangle$$

d) either 00 or 01

If one gets 00 then

$$0a_0 + 0a_1 = 0$$

does not say anything. If one gets 01 then

$$0a_0 + 1a_1 = 0 \Rightarrow a_1 = 0$$

The only non-trivial possibility is $a_0 = 1$, $a_1 = 0$

This is the period