Quantum Computers

March 4, 2019

- Limits of Moore's Law
- Implementing Qubits
- Quantum Circuits

Unexpected applications of AP&D

Unexpected applications of AP&D

From a Guardian report on US immigration controls, 28/2/17:

Unexpected applications of AP&D

Unexpected applications of AP&D

From a Guardian report on US immigration controls, 28/2/17:

> **Learn how to balance a binary search tree**
>
> *Harvard, Stanford, Yale, JFK's Terminal 3 ... some of the worlds most prestigious educational institutes are in the US. And, as some travellers are discovering, the country's pedagogical passion is evident the moment you land on US soil. David Thornton, a (white) Australian software engineer, was given a computer science test when he landed in Newark in February. And Celestine Omin, a Nigerian software engineer, claimed that he was asked to balance a binary search tree by immigration officials at New York's JFK airport. Yeah, I have no idea what that means but it's nice to see border agents taking the Stem subjects seriously.*
>
> `www.theguardian.com/commentisfree/2017/feb/28/trumps-america-holidays-tourism-down`

Why?

Why?
Complexity and Intractability
What:

- is $\mathbf{2} \times \mathbf{7}$?

Why?

Why?
Complexity and Intractability
What:

- is $\mathbf{2} \times \mathbf{7}$?
- are the factors (divisors) of $\mathbf{14}$?

Why?

Why?
Complexity and Intractability
What:

- is $\mathbf{2} \times \mathbf{7}$?
- are the factors (divisors) of $\mathbf{14}$?
- is $\mathbf{5} \times \mathbf{11}$?

Why?

Why?
Complexity and Intractability
What:

- is $\mathbf{2} \times \mathbf{7}$?
- are the factors (divisors) of $\mathbf{14}$?
- is $\mathbf{5} \times \mathbf{11}$?
- are the factors of $\mathbf{55}$?

Why?

Why?
Complexity and Intractability
What:

- is $\mathbf{2} \times \mathbf{7}$?
- are the factors (divisors) of $\mathbf{14}$?
- is $\mathbf{5} \times \mathbf{11}$?
- are the factors of $\mathbf{55}$?
- is $\mathbf{13} \times \mathbf{19}$?

Why?

Why?
Complexity and Intractability
What:

- is $\mathbf{2} \times \mathbf{7}$?
- are the factors (divisors) of $\mathbf{14}$?
- is $\mathbf{5} \times \mathbf{11}$?
- are the factors of $\mathbf{55}$?
- is $\mathbf{13} \times \mathbf{19}$?
- are the factors of $\mathbf{247}$?

Why?

Why?
Complexity and Intractability
What:

- is $\mathbf{2} \times \mathbf{7}$?
- are the factors (divisors) of $\mathbf{14}$?
- is $\mathbf{5} \times \mathbf{11}$?
- are the factors of $\mathbf{55}$?
- is $\mathbf{13} \times \mathbf{19}$?
- are the factors of $\mathbf{247}$?
- is $\mathbf{229} \times \mathbf{557}$?

Why?

Why?
Complexity and Intractability
What:

- is $\mathbf{2} \times \mathbf{7}$?
- are the factors (divisors) of $\mathbf{14}$?
- is $\mathbf{5} \times \mathbf{11}$?
- are the factors of $\mathbf{55}$?
- is $\mathbf{13} \times \mathbf{19}$?
- are the factors of $\mathbf{247}$?
- is $\mathbf{229} \times \mathbf{557}$?
- are the factors of $\mathbf{127,553}$?

Why?

Why?
Complexity and Intractability
What:

- is $\mathbf{2} \times \mathbf{7}$?
- are the factors (divisors) of $\mathbf{14}$?
- is $\mathbf{5} \times \mathbf{11}$?
- are the factors of $\mathbf{55}$?
- is $\mathbf{13} \times \mathbf{19}$?
- are the factors of $\mathbf{247}$?
- is $\mathbf{229} \times \mathbf{557}$?
- are the factors of $\mathbf{127,553}$?
- is $\mathbf{573,260,813} \times \mathbf{879,193,169}$?

Why?

Why?
Complexity and Intractability
What:

- is $\mathbf{2} \times \mathbf{7}$?
- are the factors (divisors) of $\mathbf{14}$?
- is $\mathbf{5} \times \mathbf{11}$?
- are the factors of $\mathbf{55}$?
- is $\mathbf{13} \times \mathbf{19}$?
- are the factors of $\mathbf{247}$?
- is $\mathbf{229} \times \mathbf{557}$?
- are the factors of $\mathbf{127,553}$?
- is $\mathbf{573,260,813} \times \mathbf{879,193,169}$?
- are the factors of $\mathbf{504,006,965,615,712,893}$?

Why?

Why?

Complexity and Intractability

What:

- is $\mathbf{2} \times \mathbf{7}$?
- are the factors (divisors) of $\mathbf{14}$?
- is $\mathbf{5} \times \mathbf{11}$?
- are the factors of $\mathbf{55}$?
- is $\mathbf{13} \times \mathbf{19}$?
- are the factors of $\mathbf{247}$?
- is $\mathbf{229} \times \mathbf{557}$?
- are the factors of $\mathbf{127,553}$?
- is $\mathbf{573,260,813} \times \mathbf{879,193,169}$?
- are the factors of $\mathbf{504,006,965,615,712,893}$?
- Ans: $\mathbf{573,260,783}$ and $\mathbf{879,193,171}$!

Limits of Moore's Law

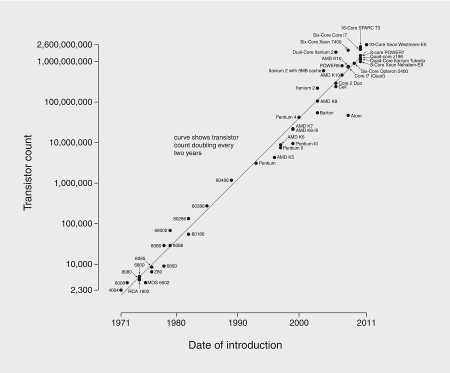
1: Limits of Moore's Law

1.1: Moore's Law

The processing power of chips doubles every...

- ... year (1965)
- ... two years (1975)

Gordan Moore, Intel

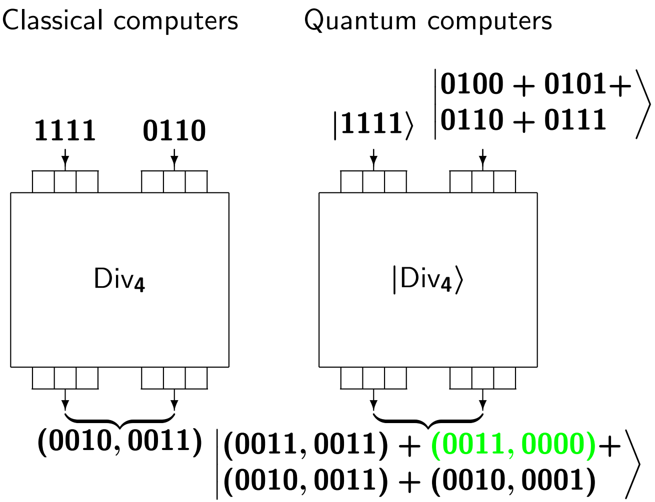


But difficult to make a chip smaller than a hydrogen atom

Limits of Moore's Law

1.2: Parallelism

1.2.1: Example



Limits of Moore's Law

1.2.2: Exponential Parallelism

One . . .

bit	Zero *or* one
qubit	Zero *and* one

Two . . .

bits	Zero *or* one *or* two *or* three
qubits	Zero *and* one *and* two *and* three

. . .

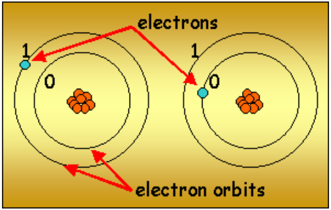
A 16 qubit word represents 65,536 values simultaneously.

Implementing Qubits

2: Implementing Qubits

2.1: Ion Traps

Use electron orbits to represent bits



- Ion trapped by electromagnetic field
- Use lasers to set and measure states

Long coherence time, reliable, but slow, and difficult to scale.

Implementing Qubits

2.2: Linear Optics

- Uses polarisation of photons
- Difficult to entangle

Implementing Qubits

2.3: Others

NMR	Qubit = spin state of many molecules in a fluid
SQP[1]	Qubit = frequency of oscillations in superfluids

[1] Superconductor Quantum Computers

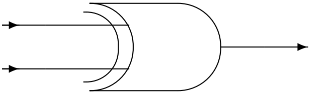
Reversible gates

3: Quantum Circuits

3.1: Reversible gates

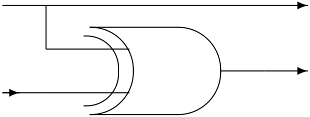
All quantum gates must be *reversible*. E.g.

Not reversible



x	y	x xor y
0	0	0
0	1	1
1	0	1
1	1	0

Reversible



x	y	x	x xor y
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

3.2: Qubits

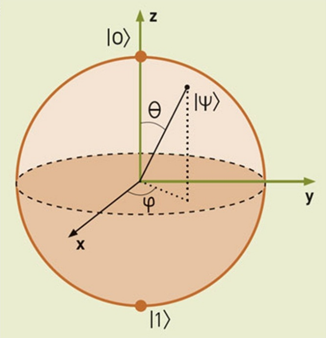
A qubit is a matrix with complex numbers:

$$\begin{bmatrix} \mathbf{c_0} \\ \mathbf{c_1} \end{bmatrix}$$

with $|\mathbf{c_0}|^2 + |\mathbf{c_1}|^2 = \mathbf{1}$ and $|\mathbf{c_n}|^2$ (with $\mathbf{n} \in \{\mathbf{0}, \mathbf{1}\}$) the probability the qubit is in state $|\mathbf{n}\rangle$.

Quantum circuits

A single qubit can be represented as a point on a *Bloch sphere*.



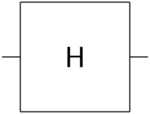
- Latitude — probability of $|\mathbf{0}\rangle$, $|\mathbf{1}\rangle$
- Longitude — evolution

Quantum circuits

3.3: Quantum gates

3.3.1: Single qubit gates

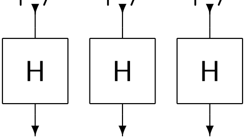
3.3.1 A: Hadamard gate



$$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$\mathbf{H}\,|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \mathbf{H}\,|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

$|0\rangle$ $|0\rangle$ $|0\rangle$

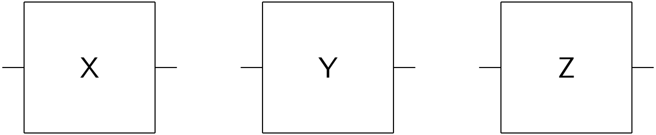


$$\frac{1}{2^{3/2}}\left(|0\rangle + |1\rangle + |2\rangle + |3\rangle + |4\rangle + |5\rangle + |6\rangle + |7\rangle\right)$$

Quantum circuits

3.3.1 B: Pauli gates

X **Y** **Z**



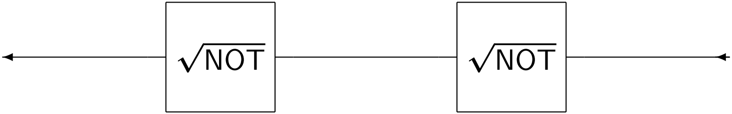
$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \qquad \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Rotate the Bloch sphere through $\mathbf{180^\circ}$ around the $\mathbf{x}$, $\mathbf{y}$, $\mathbf{z}$ axes

3.3.1 C: Square root of NOT

$$\sqrt{\mathsf{NOT}} = \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}\begin{bmatrix} \mathbf{1} & -\mathbf{1} \\ \mathbf{1} & \mathbf{1} \end{bmatrix}$$

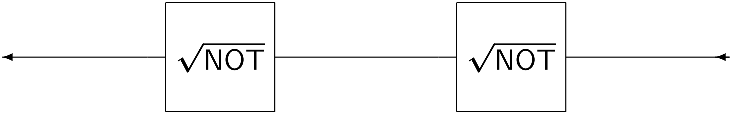
Quantum circuits



$$\begin{bmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix} * \qquad \begin{bmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix} * |\mathbf{0}\rangle$$

$$\begin{bmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix} * \qquad \begin{bmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix} * |\mathbf{1}\rangle$$

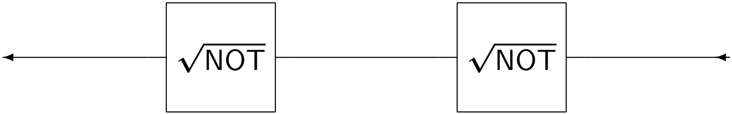
Quantum circuits



$$\begin{bmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix} * \qquad \begin{bmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix} * \begin{bmatrix} \mathbf{1} \\ \mathbf{0} \end{bmatrix}$$

$$\begin{bmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix} * \qquad \begin{bmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix} * \begin{bmatrix} \mathbf{0} \\ \mathbf{1} \end{bmatrix}$$

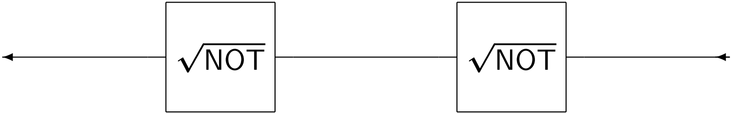
Quantum circuits



$$\begin{bmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix} * \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} \qquad |0\rangle$$

$$\begin{bmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix} * \begin{bmatrix} -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} \qquad |1\rangle$$

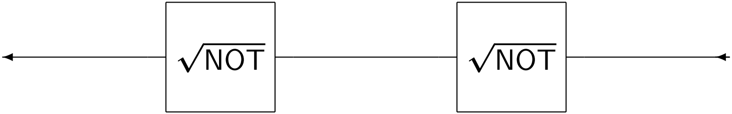
Quantum circuits



$$\begin{bmatrix} \mathbf{0} \\ \mathbf{1} \end{bmatrix} \qquad |0\rangle$$

$$\begin{bmatrix} \mathbf{-1} \\ \mathbf{0} \end{bmatrix} \qquad |1\rangle$$

Quantum circuits



$|\mathbf{1}\rangle$ $\qquad$ $|\mathbf{0}\rangle$

$-|\mathbf{0}\rangle$ $\qquad$ $|\mathbf{1}\rangle$

3.3.1 D: Rotational gates
Let $\overrightarrow{\mathbf{v}} = (\mathbf{x}, \mathbf{y}, \mathbf{z})$ be a unit vector in the Bloch sphere, then

$$\mathbf{R}_{\overrightarrow{\mathbf{v}}}(\theta) = \cos\frac{\theta}{2}\mathbf{I} - \mathbf{i}\sin\frac{\theta}{2}(\mathbf{xX} + \mathbf{yY} + \mathbf{zZ})$$

rotates the Bloch sphere round $\overrightarrow{\mathbf{v}}$ by θ.

Quantum circuits

Special cases:

$$R_{\vec{x}}(\theta) = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}X = \begin{bmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}$$

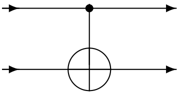
$$R_{\vec{y}}(\theta) = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Y = \begin{bmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}$$

$$R_{\vec{z}}(\theta) = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Z = \begin{bmatrix} e^{-i\theta/2} & 0 \\ o & e^{i\theta/2} \end{bmatrix}$$

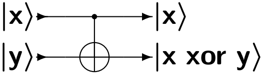
$e^{i\theta/2}R_{\vec{z}}(\theta) = \begin{bmatrix} 1 & 0 \\ 0 & e^{\theta} \end{bmatrix}$ is known as a *phase shift* gate

Quantum circuits

3.3.2: Multiple qubit gates
3.3.2 A: Controlled not



$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

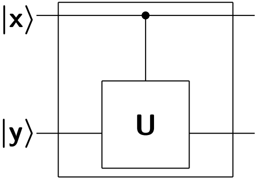


Quantum circuits

3.3.2 B: Controlled U

If **U** is a single qubit gate then a controlled **U** gate is

```
if (x == 0) {
    0,y;
} else {
    1,U(y);
}
```



If $\mathbf{U} = \begin{bmatrix} \mathbf{a} & \mathbf{b} \\ \mathbf{c} & \mathbf{d} \end{bmatrix}$ then

$$^{c}\mathbf{U} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \mathbf{a} & \mathbf{b} \\ 0 & 0 & \mathbf{c} & \mathbf{d} \end{bmatrix}$$

Quantum circuits

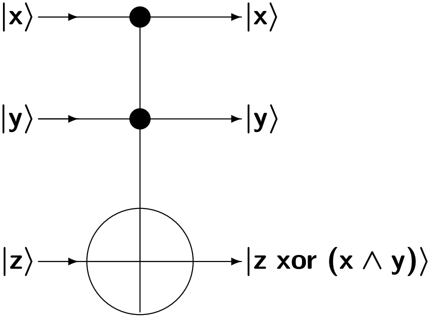
This generalises to $\mathbf{n}$-qubit gates. E.g. if $\mathbf{U_2}$ is

$$\begin{bmatrix} u_{0,0} & u_{0,1} & u_{0,2} & u_{0,3} \\ u_{1,0} & u_{1,1} & u_{1,2} & u_{1,3} \\ u_{2,0} & u_{2,1} & u_{2,2} & u_{2,3} \\ u_{3,0} & u_{3,1} & u_{3,2} & u_{3,3} \end{bmatrix}$$

then a ${}^{\mathbf{C}}\mathbf{U_2}$ gate is

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & u_{0,0} & u_{0,1} & u_{0,2} & u_{0,3} \\ 0 & 0 & 0 & 0 & u_{1,0} & u_{1,1} & u_{1,2} & u_{1,3} \\ 0 & 0 & 0 & 0 & u_{2,0} & u_{2,1} & u_{2,2} & u_{2,3} \\ 0 & 0 & 0 & 0 & u_{3,0} & u_{3,1} & u_{3,2} & u_{3,3} \end{bmatrix}$$

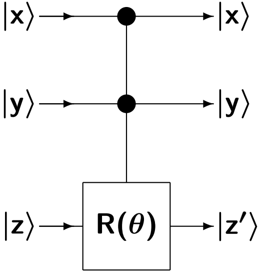
3.3.2 C: Toffoli gate



The Toffoli gate is $^{\mathbf{C}}\left(^{\mathbf{C}}\mathrm{NOT}\right)$

Quantum circuits

3.3.2 D: Deutsch gates



if $(|x\rangle == |1\rangle$ **&&** $|y\rangle == |1\rangle)$ {

$\quad |z'\rangle = R(\theta)\,|z\rangle$

} **else** {

$\quad |z'\rangle = |z\rangle$

}

Quantum circuits

3.4: Universal quantum gate sets

- $\left\{\mathbf{H}, {}^{\mathsf{C}}\mathsf{NOT}, \mathbf{R}\left(\mathbf{cos}^{-1}\frac{\mathbf{3}}{\mathbf{5}}\right)\right\}$
- $\{\mathbf{D}(\boldsymbol{\theta})\}$, for some $\boldsymbol{\theta}$ for which $\frac{\boldsymbol{\pi}}{\boldsymbol{\theta}}$ is irrational

are both universal quantum gate sets

3.5: Example — Deutsch's Algorithm

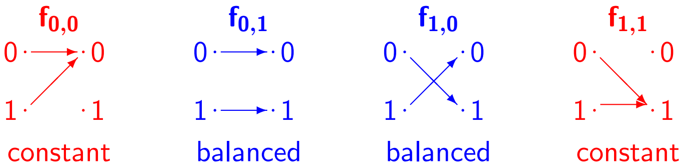
Implementing algorithms

- Start in a classical state
- Move to a superposition of states
- Act on the superposition
- Measure qubits

Quantum circuits

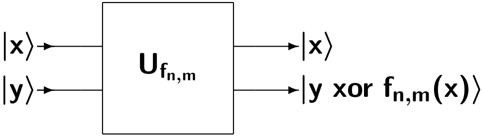
3.5.1: Problem statement

Considers functions from $\{0, 1\}$ to $\{0, 1\}$.



Quantum circuits

Given a $\mathbf{U_{f_{n,m}}}$ "black box"



decide if $\mathbf{f_{n,m}}$ is constant or balanced

Quantum circuits

3.5.2: Classical circuits

Table for, e.g., $\mathbf{U}_{\mathbf{f}_{1,0}}$

x	y	$f_{1,0}(x)$	y xor $f_{1,0}(x)$	$U_{f_{1,0}}(x, y)$
0	0	1	1	01
0	1	1	0	00
1	0	0	0	10
1	1	0	1	11

Quantum circuits

All functions

x	y	$U_{f_{0.0}}$	$U_{f_{0,1}}$	$U_{f_{1,0}}$	$U_{f_{1,1}}$
0	0	$\boxed{00}$	$\boxed{00}$	01	01
0	1	$\boxed{01}$	$\boxed{01}$	00	00
1	0	$\boxed{10}$	11	$\boxed{10}$	11
1	1	$\boxed{11}$	10	$\boxed{11}$	10

On each line:

- boxed outputs are identical
- unboxed outputs are identical
- one boxed output is from a constant function, one from a balanced
- one unboxed output is from a constant function, one from a balanced

so cannot find input that will discriminate

3.5.3: Quantum circuit

3.5.3 A: Constructing matrices

Construct matrix for, e.g. $\mathbf{U_{f_{1,0}}}$

x	0	0	1	1
y	0	1	0	1
$f_{1,0}(x)$	1	1	0	0
y xor $f_{1,0)(x)}$	1	0	0	1
$\|x, y \text{ xor } f_{1,0}(x)\rangle$	$\|01\rangle$	$\|00\rangle$	$\|10\rangle$	$\|11\rangle$
	0	1	0	0
	1	0	0	0
	0	0	1	0
	0	0	0	1

Quantum circuits

Matrices:

$$
\begin{array}{c|c|c}
 & \mathbf{m=0} & \mathbf{m=1} \\
\mathbf{n=0} & \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} & \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \\
\hline
\mathbf{n=1} & \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} & \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}
\end{array}
$$

Quantum circuits

Matrices:

$$
\begin{array}{c|c|c}
 & \mathbf{m = 0} & \mathbf{m = 1} \\
\mathbf{n = 0} & \begin{bmatrix} \overline{\mathbf{n}} & \mathbf{n} & 0 & 0 \\ \mathbf{n} & \overline{\mathbf{n}} & 0 & 0 \\ 0 & 0 & \overline{\mathbf{m}} & \mathbf{m} \\ 0 & 0 & \mathbf{m} & \overline{\mathbf{m}} \end{bmatrix} & \begin{bmatrix} \overline{\mathbf{n}} & \mathbf{n} & 0 & 0 \\ \mathbf{n} & \overline{\mathbf{n}} & 0 & 0 \\ 0 & 0 & \overline{\mathbf{m}} & \mathbf{m} \\ 0 & 0 & \mathbf{m} & \overline{\mathbf{m}} \end{bmatrix} \\
\hline
\mathbf{n = 1} & \begin{bmatrix} \overline{\mathbf{n}} & \mathbf{n} & 0 & 0 \\ \mathbf{n} & \overline{\mathbf{n}} & 0 & 0 \\ 0 & 0 & \overline{\mathbf{m}} & \mathbf{m} \\ 0 & 0 & \mathbf{m} & \overline{\mathbf{m}} \end{bmatrix} & \begin{bmatrix} \overline{\mathbf{n}} & \mathbf{n} & 0 & 0 \\ \mathbf{n} & \overline{\mathbf{n}} & 0 & 0 \\ 0 & 0 & \overline{\mathbf{m}} & \mathbf{m} \\ 0 & 0 & \mathbf{m} & \overline{\mathbf{m}} \end{bmatrix}
\end{array}
$$

Quantum circuits

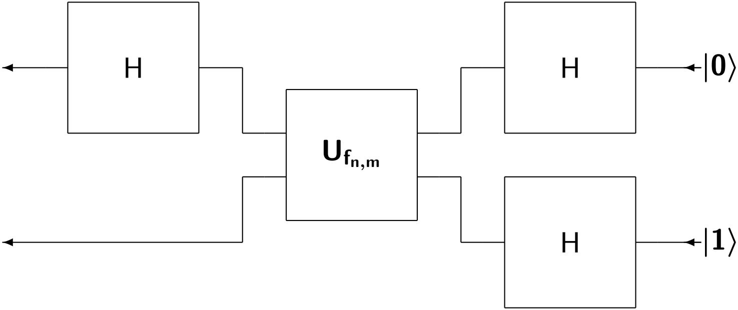
In general

$$\mathbf{U_{f_{n,m}}} = \begin{array}{c} \begin{array}{cccc} \mathbf{00} & \mathbf{01} & \mathbf{10} & \mathbf{11} \end{array} \\ \begin{bmatrix} \overline{\mathbf{n}} & \mathbf{n} & \mathbf{0} & \mathbf{0} \\ \mathbf{n} & \overline{\mathbf{n}} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \overline{\mathbf{m}} & \mathbf{m} \\ \mathbf{0} & \mathbf{0} & \mathbf{m} & \overline{\mathbf{m}} \end{bmatrix} \end{array}$$

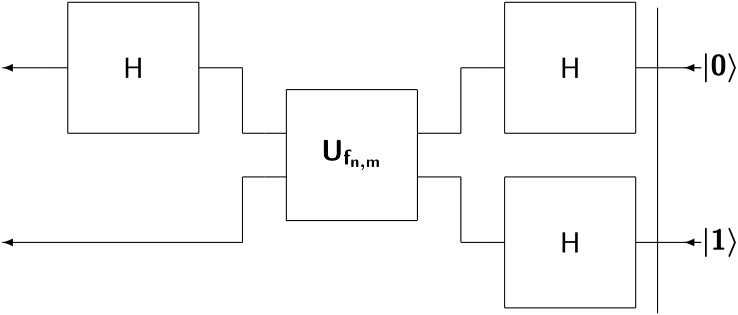
The top row gives the $|\mathbf{xy}\rangle$ input, the column is the matrix for the output. E.g., the output for input $\mathbf{11}$ is $\begin{bmatrix}\mathbf{0} & \mathbf{0} & \mathbf{m} & \overline{\mathbf{m}}\end{bmatrix}^{\mathbf{T}}$ (which, e.g., for $\mathbf{f_{1,1}}$ is $\begin{bmatrix}\mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0}\end{bmatrix}^{\mathbf{T}} = |\mathbf{10}\rangle$)

Quantum circuits

3.5.4: Deutsch's circuit

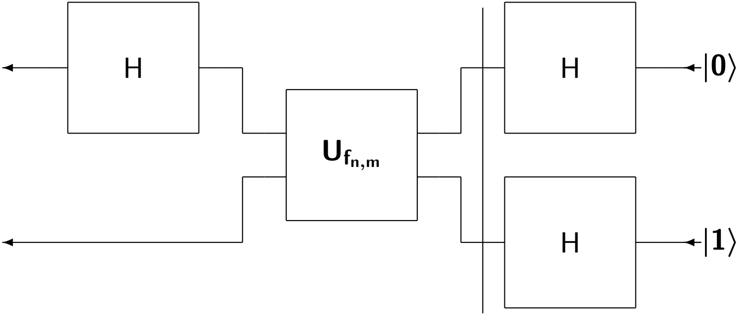


Quantum circuits



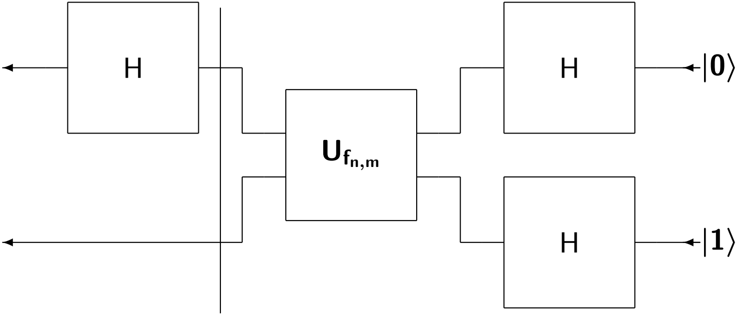
$$\mathbf{H} \otimes \mathbf{I} \quad * \quad \mathbf{U_{f_{n,m}}} \quad * \quad \mathbf{H} \otimes \mathbf{H} \quad * \, |\mathbf{01}\rangle$$

Quantum circuits



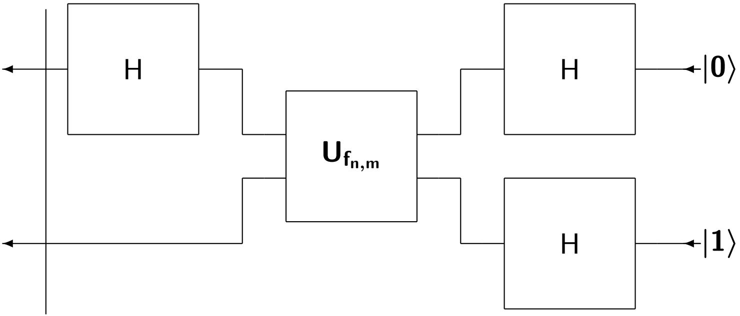
$$\mathbf{H} \otimes \mathbf{I} \quad * \quad \mathbf{U_{f_{n,m}}} \quad * \begin{bmatrix} +\frac{1}{2} \\ -\frac{1}{2} \\ +\frac{1}{2} \\ -\frac{1}{2} \end{bmatrix}$$

Quantum circuits



$$\mathbf{H} \otimes \mathbf{I} \quad * \quad \begin{bmatrix} \frac{\bar{n}-n}{2} \\ \frac{n-\bar{n}}{2} \\ \frac{\bar{m}-m}{2} \\ \frac{m-\bar{m}}{2} \end{bmatrix}$$

Quantum circuits



$$\frac{1}{\sqrt{2}}\begin{bmatrix} \frac{(\bar{n}+\bar{m})-(n+m)}{2} \\ \frac{(n+m)-(\bar{n}+\bar{m})}{2} \\ \frac{(\bar{n}+m))-(n+\bar{m})}{2} \\ \frac{(n+\bar{m})-(\bar{n}+m)}{2} \end{bmatrix}$$

Quantum circuits

The values of the entries in the:

$$\frac{1}{\sqrt{2}}\begin{bmatrix} \frac{(\overline{n}+\overline{m})-(n+m)}{2} \\ \frac{(n+m)-(\overline{n}+\overline{m})}{2} \\ \frac{(\overline{n}+m))-(n+\overline{m})}{2} \\ \frac{(n+\overline{m})-(\overline{n}+m)}{2} \end{bmatrix}$$

matrix, for the possible values of **n** and **m** are:

n	**0**	**0**	**1**	**1**
m	**0**	**1**	**0**	**1**
$\frac{(\overline{n}+\overline{m})-(n+m)}{2\sqrt{2}}$	$+\frac{1}{\sqrt{2}}$	0	0	$-\frac{1}{\sqrt{2}}$
$\frac{(n+m)-(\overline{n}+\overline{m})}{2\sqrt{2}}$	$-\frac{1}{\sqrt{2}}$	0	0	$+\frac{1}{\sqrt{2}}$
$\frac{(\overline{n}+m)-(n+\overline{m})}{2\sqrt{2}}$	0	$+\frac{1}{\sqrt{2}}$	$-\frac{1}{\sqrt{2}}$	0
$\frac{(n+\overline{m})-(\overline{n}+m)}{2\sqrt{2}}$	0	$-\frac{1}{\sqrt{2}}$	$+\frac{1}{\sqrt{2}}$	0

Quantum circuits

E.g., if $\mathbf{n} = \mathbf{0}$ and $\mathbf{m} = \mathbf{0}$ the output of this circuit is

$$\begin{bmatrix} +\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 & 0 \end{bmatrix}^{\mathsf{T}}.$$

This is the superposition of two qubits, $\mathbf{q_0}$ and $\mathbf{q_1}$, say, which can be written as

$$+\frac{|00\rangle - |01\rangle}{\sqrt{2}}.$$

Here $\mathbf{q_0}$ is $|0\rangle$, and $\mathbf{q_1}$ is $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$.

Quantum circuits

For the other possible values of **n** and **m**:

	n	**m**			$\mathbf{q_0}$	$\mathbf{q_1}$
constant	**0**	**0**	$+\frac{\lvert 00\rangle - \lvert 01\rangle}{\sqrt{2}}$	$=$	$+\lvert 0\rangle$	$\frac{\lvert 0-1\rangle}{\sqrt{2}}$
balanced	**0**	**1**	$+\frac{\lvert 10\rangle - \lvert 11\rangle}{\sqrt{2}}$	$=$	$+\lvert 1\rangle$	$\frac{\lvert 0-1\rangle}{\sqrt{2}}$
balanced	**1**	**0**	$-\frac{\lvert 10\rangle - \lvert 11\rangle}{\sqrt{2}}$	$=$	$-\lvert 1\rangle$	$\frac{\lvert 0-1\rangle}{\sqrt{2}}$
constant	**1**	**1**	$-\frac{\lvert 00\rangle - \lvert 01\rangle}{\sqrt{2}}$	$=$	$-\lvert 0\rangle$	$\frac{\lvert 0-1\rangle}{\sqrt{2}}$

So measure $\mathbf{q_0}$.

- If $\mathbf{q_0} = \lvert 0\rangle$ function is constant.
- If $\mathbf{q_0} = \lvert 1\rangle$ function is balanced.