Quantum Computers

Last updated: March 4^{th} 2019, at 9.42am

Contents

Why?

Complexity and Intractability

What:

- is 2×7?
- are the factors (divisors) of 14?

- is 5×11?
- are the factors of 55?
- is 13×19?
- are the factors of 247?
- is 229×557? (you may use pen and paper)
- are the factors of $127,553$? (you may use pen and paper)
- is $573,260,813 \times 879,193,169$? (you may use a calculator)
- are the factors of $504,006,965,615,712,893$? (you may use a calculator)

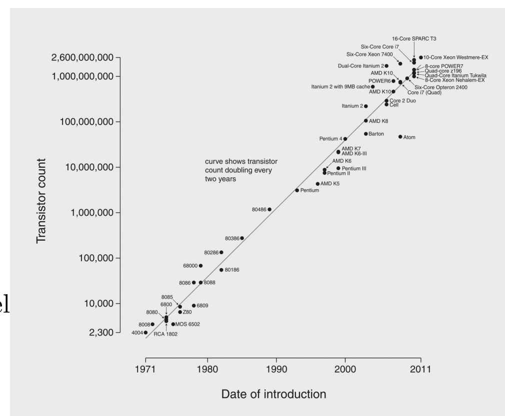
1 Limits of Moore's Law

1.1 Moore's Law

The processing power of chips doubles every…

- … year (1965)
- … two years (1975)

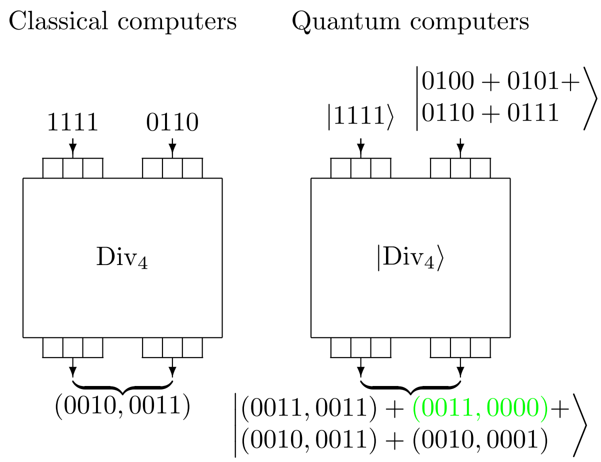
  Gordan Moore, Intel



But difficult to make a chip smaller than a hydrogen atom

1.2 Parallelism

1.2.1 Example



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

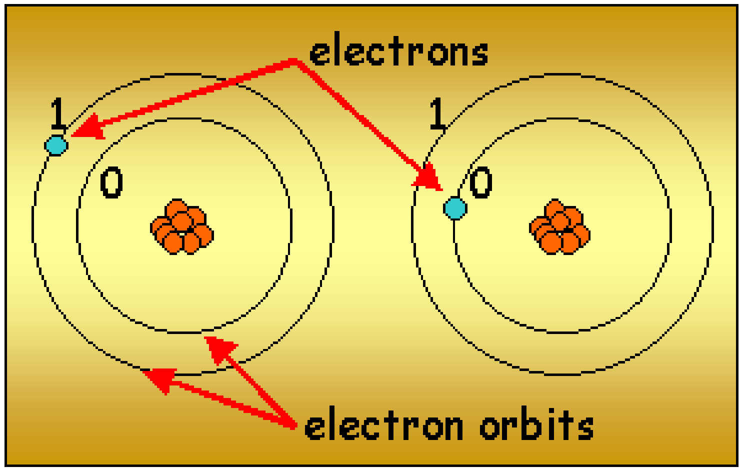
...

A 16 qubit word represents 65,536 values simultaneously, a 32 qubit word 4,294,967,296 values, and a 64 qubit word 18,446,744,073,709,551,616 values.

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.

2.2 Linear Optics

- Uses polarisation of photons
- Difficult to entangle

2.3 Others

NMR Qubit = spin state of many molecules in a fluid

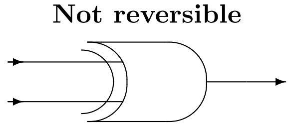
SQP[1] Qubit = frequency of oscillations in superfluids

3 Quantum Circuits

3.1 Reversible gates

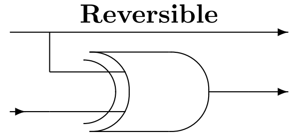
All quantum gates must be *reversible*. E.g.

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

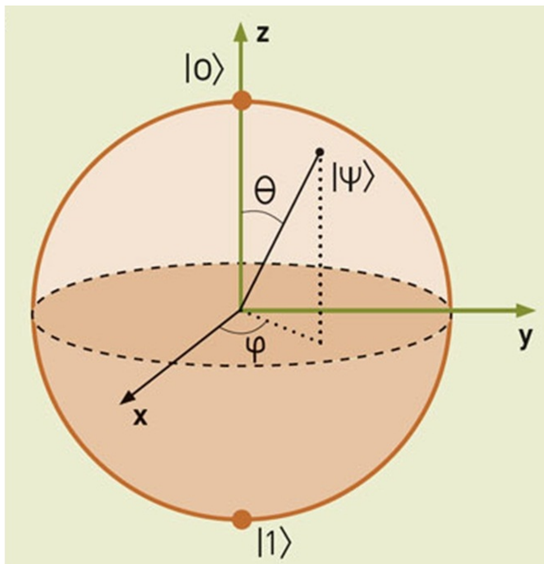
3.2 Qubits

A qubit is a matrix with complex numbers:

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

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

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



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

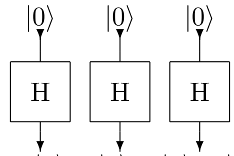
3.3 Quantum gates

3.3.1 Single qubit gates

Hadamard gate

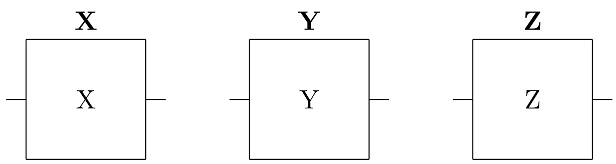
$$-\boxed{\mathrm{H}}- \quad \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

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



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

Pauli gates



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

Rotate the Bloch sphere through 180° around the x, y, z axes

Square root of NOT

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

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

$$R_{\overrightarrow{v}}(\theta) = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}\left(xX + yY + zZ\right)$$

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

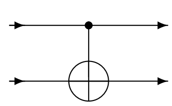
Special cases:

$$\begin{aligned}
R_{\overrightarrow{x}}(\theta) &= \cos\tfrac{\theta}{2}I - i\sin\tfrac{\theta}{2}X &= \begin{bmatrix}\cos\frac{\theta}{2} & -i\sin\frac{\theta}{2}\\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2}\end{bmatrix}\\
R_{\overrightarrow{y}}(\theta) &= \cos\tfrac{\theta}{2}I - i\sin\tfrac{\theta}{2}Y &= \begin{bmatrix}\cos\frac{\theta}{2} & -\sin\frac{\theta}{2}\\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2}\end{bmatrix}\\
R_{\overrightarrow{z}}(\theta) &= \cos\tfrac{\theta}{2}I - i\sin\tfrac{\theta}{2}Z &= \begin{bmatrix}e^{-i\theta/2} & 0\\ o & e^{i\theta/2}\end{bmatrix}
\end{aligned}$$

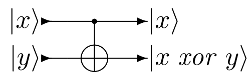
$e^{i\theta/2}R_{\overrightarrow{z}}(\theta) = \begin{bmatrix}1 & 0\\0 & e^{\theta}\end{bmatrix}$ is known as a *phase shift* gate

3.3.2 Multiple qubit gates

Controlled not

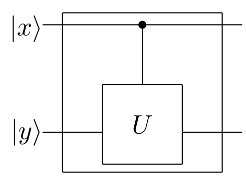


$$\begin{bmatrix}1 & 0 & 0 & 0\\0 & 1 & 0 & 0\\0 & 0 & 0 & 1\\0 & 0 & 1 & 0\end{bmatrix}$$



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

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

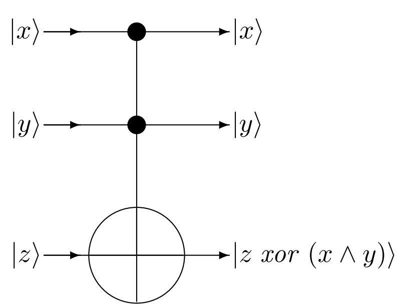
This generalises to n-qubit gates. E.g. if U_2 is

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

then a $^{C}U_2$ gate is

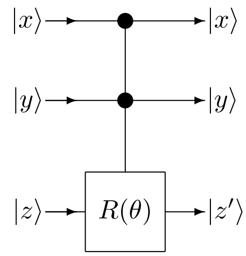
$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & u_{0,0} & u_{0,1} & u_{0,2} & u_{0,3} \\ 0 & 0 & 0 & 0 & u_{1,0} & u_{1,1} & u_{1,2} & u_{1,3} \\ 0 & 0 & 0 & 0 & u_{2,0} & u_{2,1} & u_{2,2}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

Toffoli gate



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

Deutsch gates




```
if (|x⟩==|1⟩ && |y⟩==|1⟩) {
    |z′⟩ = R(θ)|z⟩
} else {
    |z′⟩ = |z⟩
}
```

3.4 Universal quantum gate sets

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

are both universal quantum gate sets

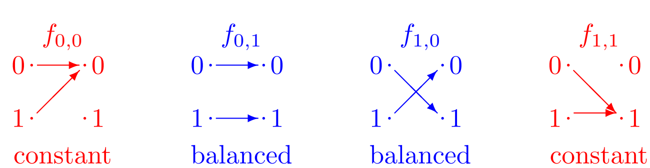
3.5 Example — Deutsch's Algorithm

Implementing algorithms

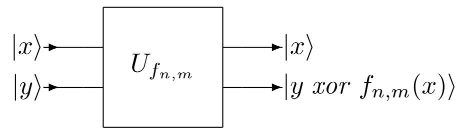
- Start in a classical state
- Move to a superposition of states
- Act on the superposition
- Measure qubits

3.5.1 Problem statement

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



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



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

3.5.2 Classical circuits

Table for, e.g., $U_{f_{1,0}}$

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

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

Constructing matrices Construct matrix for, e.g. $U_{f_{1,0}}$

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

Matrices:

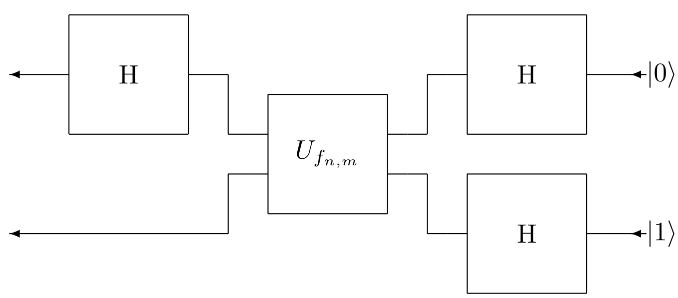
$$\begin{array}{c|c|c} & m=0 & m=1 \\ \hline n=0 & \begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix} & \begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix} \\ \hline n=1 & \begin{bmatrix}0&1&0&0\\1&0&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix} & \begin{bmatrix}0&1&0&0\\1&0&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}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

In general

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

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

3.5.4 Deutsch's circuit



The matrix representation for this is

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

where H is the matrix for the Hadamard gate, I is a two-by-two identity matrix, $U_{f_{n,m}}$ is the matrix for our mystery controlled function gate (Note: n and m will have concrete values — we just don't know which ones), and $|01\rangle$ is our input. The reasoning behind these values is (from right to left):

- $|01\rangle$ — the input. This is given.
- $H \otimes H$ — the parallel composition of two Hadamard gates

- $U_{f_{n,m}}$ — the mystery gate
- $H \times I$ — the parallel composition of a Hadamard gate with an "identity gate" (i.e. the wire that just passes the lower qubit straight through).

The circuit is a sequential composition of these components, hence the use of ordinary matrix multiplication ($*$) to put them together.

We now need the matrix representations of these values:

- $|01\rangle$

  This is the tenor product of $|0\rangle$ and $|1\rangle$.

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

- $H \times H$

  The matrix for a Hadamard gate is

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

  so this parallel composition is

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

- $U_{f_{n,m}}$

  This is given.

$$U_{f_{n,m}} = \begin{bmatrix}\overline{n} & n & 0 & 0\\n & \overline{n} & 0 & 0\\0 & 0 & \overline{m} & m\\0 & 0 & m & \overline{m}\end{bmatrix}$$

- $H \otimes I$

  The two-by-two identity matrix is

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

  so our parallel composition is

$$H \otimes I = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix} \otimes \begin{bmatrix}1 & 0\\0 & 1\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 0 & 1 & 0\\0 & 1 & 0 & 1\\1 & 0 & -1 & 0\\0 & 1 & 0 & -1\end{bmatrix}$$

So the whole circuit is

$$
\begin{aligned}
(H \otimes I) * U_{f_{n,m}} * (H \otimes H) * |01\rangle &= (H \otimes I) * U_{f_{n,m}} * \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} * \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \\
&= (H \otimes I) * U_{f_{n,m}} * \begin{bmatrix} +\frac{1}{2} \\ -\frac{1}{2} \\ +\frac{1}{2} \\ -\frac{1}{2} \end{bmatrix} \\
&= (H \otimes I) * \begin{bmatrix} \overline{n} & n & 0 & 0 \\ n & \overline{n} & 0 & 0 \\ 0 & 0 & \overline{m} & m \\ 0 & 0 & m & \overline{m} \end{bmatrix} * \begin{bmatrix} +\frac{1}{2} \\ -\frac{1}{2} \\ +\frac{1}{2} \\ -\frac{1}{2} \end{bmatrix} \\
&= (H \otimes I) * \begin{bmatrix} \frac{\overline{n}-n}{2} \\ \frac{n-\overline{n}}{2} \\ \frac{\overline{m}-m}{2} \\ \frac{m-\overline{m}}{2} \end{bmatrix} \\
&= \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} * \begin{bmatrix} \frac{\overline{n}-n}{2} \\ \frac{n-\overline{n}}{2} \\ \frac{\overline{m}-m}{2} \\ \frac{m-\overline{m}}{2} \end{bmatrix} \\
&= \frac{1}{\sqrt{2}}\begin{bmatrix} \frac{(\overline{n}+\overline{m})-(n+m)}{2} \\ \frac{(n+m)-(\overline{n}+\overline{m})}{2} \\ \frac{(\overline{n}+m))-(n+\overline{m})}{2} \\ \frac{(n+\overline{m})-(\overline{n}+m)}{2} \end{bmatrix}
\end{aligned}
$$

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

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

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

This is the superposition of two qubits, q_0 and q_1, say, which can be written as

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

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

For the other possible values of n and m:

	n	m			q_0	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 q_0.

- If $q_0 = |0\rangle$ function is constant.
- If $q_0 = |1\rangle$ function is balanced.

The sign also disappears on measurement.