Quantum Algorithms
part I

Ian Glendinning

November 6, 2001

Outline

- Introduction
- Quantum Bits and Registers
- Quantum Circuits
- Quantum Algorithms
- Summary and Outlook

Introduction

- What is Quantum Computing?
- Why all the Excitement?
- What is Quantum Mechanics?
- What Makes Quantum Computers Different?

What is Quantum Computing?

- A fundamentally new mode of information processing that can be performed only by harnessing physical phenomena unique to quantum mechanics
- A sub-discipline of quantum information processing, which also covers the related fields of:
  - Quantum information theory
  - Quantum communication
  - Quantum cryptography

Why all the Excitement?

- The security of public-key cryptosystems such as RSA relies on the difficulty of factorizing very large numbers
- This system is widely used by banks, for example, using numbers with around 250 digits
- In 1994 a 129 digit number known as RSA129 was factored in eight months using approx. 1600 workstations on the internet
- A quantum computer using Shor's algorithm with a clock speed of 100 MHz could factor RSA129 in a few seconds

The Power of Quantum Computing

- It would take roughly 800,000 years to factor a 250 digit number with the same computer power, and a 1000 digit number would take 10^{25} years (significantly longer than the age of the universe)
- Shor's algorithm can factor numbers in a number of steps that is is roughly quadratic in the input size, so factoring a 1000 digit number would require only a few million steps
- This explains the interest of various 'secret' government agencies around the world in the feasibility of building quantum computers!

What will Quantum Computers be good at?

The most important applications currently known are:

- Factorizing large numbers very rapidly (Shor's algorithm)
- Searching, especially algorithmic searching (Grover's algorithm)
- Cryptography: perfectly secure communication
- Simulating quantum-mechanical systems efficiently

But who knows what else will be discovered...

What is Quantum Mechanics?

- The mathematical description of the motion and interaction of sub-atomic particles
- The rules are very different to those in the classical world!
  - Wave-particle duality
  - Entanglement
- The most accurate and complete description of the world known
- Everything around us is governed by the rules of quantum mechanics, but we don't notice, as we are so much bigger than atoms: difference from classical physics tiny at everyday scale

The Early History of Quantum Mechanics

1900 Max Planck: discrete energy levels (Dec. 14th)

1925 Werner Heisenberg: matrix formulation of QM

1926 Erwin Schrödinger: wavefunction formulation

1941 Richard Feynman: sum over histories formulation

Recent History of Quantum Mechanics

1964 John Bell: Proposed test for hidden variables

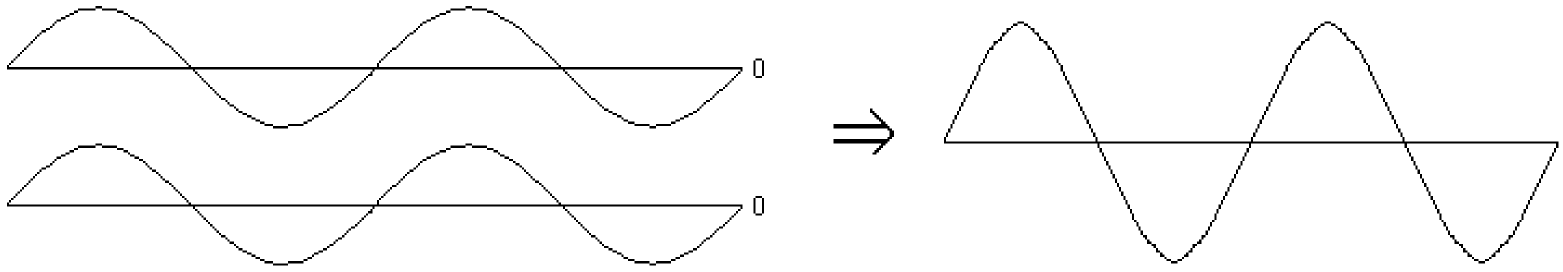
1982 Alain Aspect: Experimental test of Bell's inequality

1982 Dieks *and* Wooters & Zurek: No cloning theorem

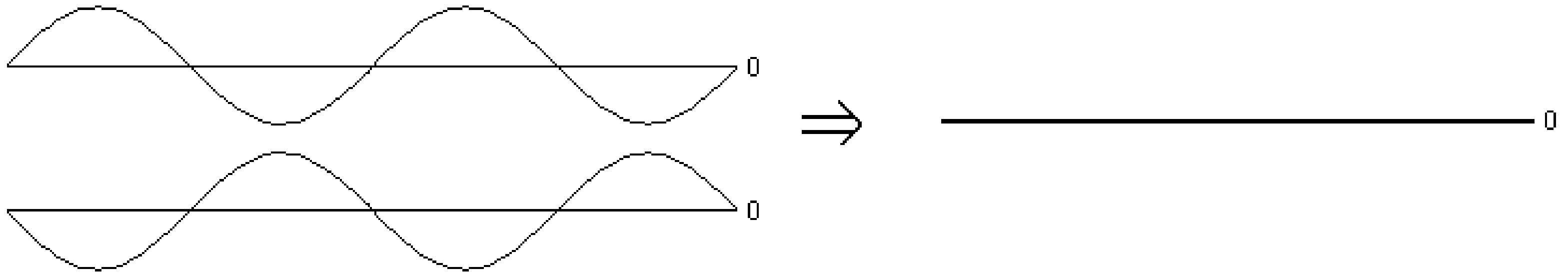
1998 Dürr, Nonn & Rempe: Origin of complementarity

Wave Interference

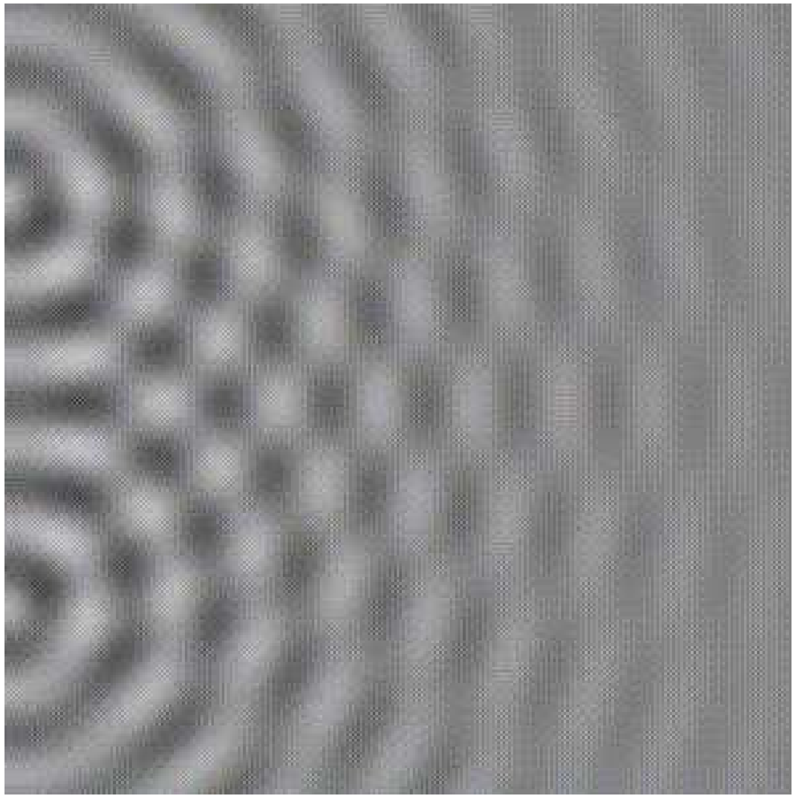
Constructive Interference:



Destructive Interference:



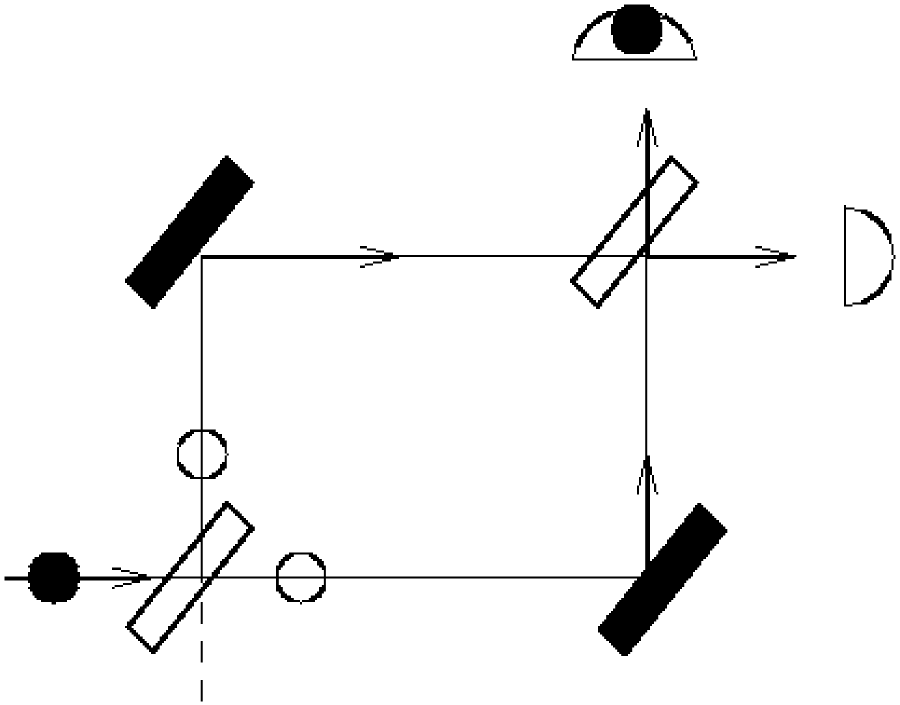
Interference Patterns



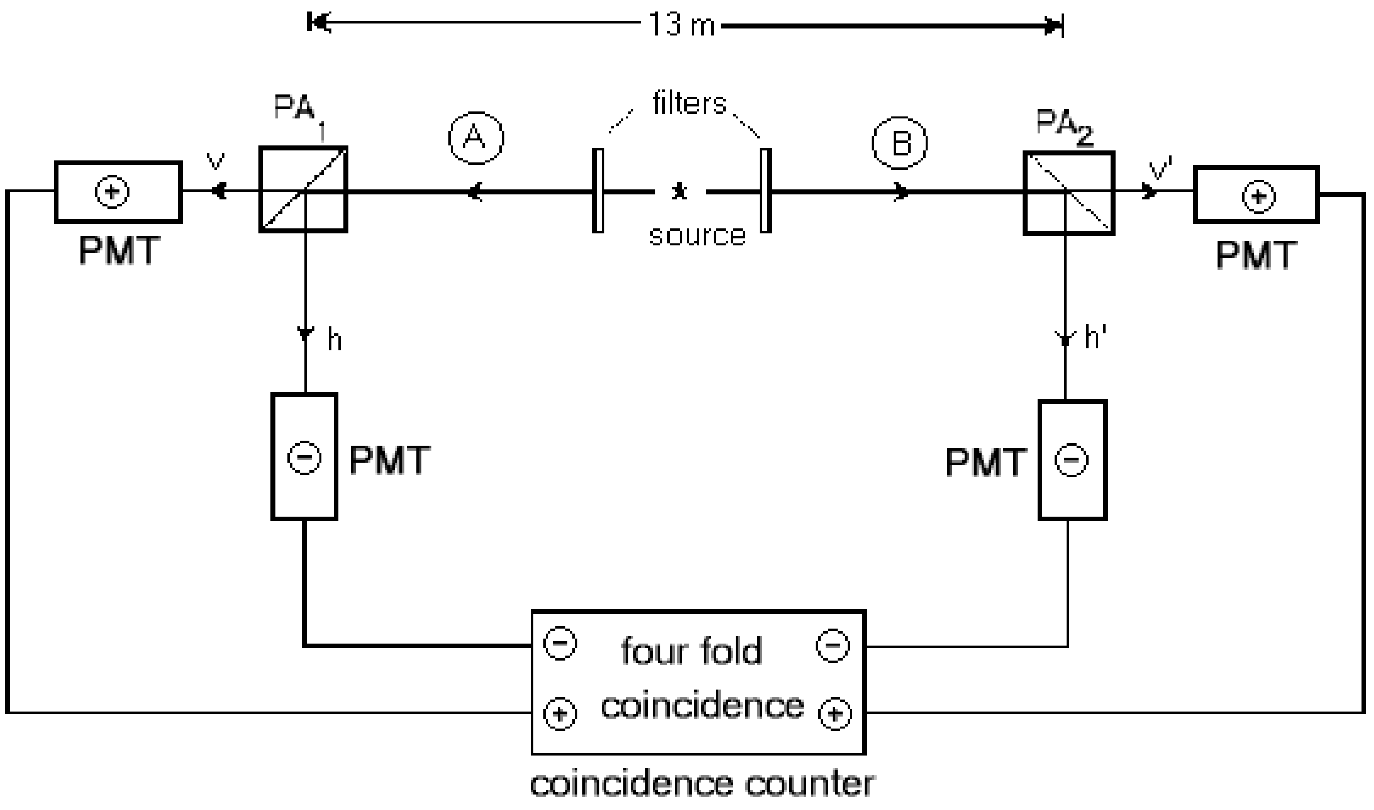
Wave-Particle Duality

- Light is an electromagnetic wave, but it turns out that it is always detected as individual particles (photons)
- Electrons are classically regarded as particles, but it turns out that they can interfere like waves
- How can particles (localized) have wave-like properties (spread out) and vice versa? - Classically they can't!
- Quantum objects travel like waves but interact like particles: *wave-particle duality*

The Mach-Zehnder Interferometer



Entanglement - The Aspect Experiment



Entanglement

- How can this be interpreted? Either:
  - Accept Quantum Mechanics and its non-local correlations - Einstein: spooky action at a distance *(spukhafte Fernwirkung)*
  - Quantum Mechanics is incomplete and there are 'hidden variables'
- Violation of Bell's inequality rules out any *local* hidden variable theory
- Aspect's experiment, and others, do indeed violate Bell's inquality, as predicted by quantum mechanics!

What Makes Quantum Computers Different?

- What Makes Quantum Computers Different from classical computers?
  - The basic unit of information in a classical computer is the bit, a 2-state device that can represent the values 0 or 1
  - The quantum analogue of a bit is a 2-state quantum system, e.g. electron spin or photon polarization w.r.t. to some axis
  - Such a 2-state quantum system is called a *qubit*
  - Not only can a qubit exist in the classical 0 and 1 states, it can also be in a *superposition* of both

What Makes Quantum Computers Different

- Quantum Parallelism
  - A register with L qubits can be in a superposition of 2^L states, storing all numbers from 0 to $2^L - 1$ simultaneously!
  - Operations act on values 0 and 1 at the same time, and can act on all 2^L values simultaneously: Quantum Parallelism
  - That's what I call *really* high performance computing!
- Where's the catch?
  - Measurement yields only one of the 2^L states
  - Decoherence: disturbance from their environment

Quantum Bits and Registers

- Qubits
- The Bloch Sphere
- Multiple Qubits

Qubits

The states of a qubit corresponding to the classical values 0 and 1 are written $|0\rangle$ and $|1\rangle$, but in general a qubit can take on any value:

$$\alpha|0\rangle + \beta|1\rangle$$

where α and β are complex numbers.

A *measurement* of the state of a qubit always gives either the result 0, with probability $|\alpha|^2$, or the result 1, with probability $|\beta|^2$, so

$$|\alpha|^2 + |\beta|^2 = 1$$

since the probabilities must sum to one.

Qubits

For example, a qubit can be in the state

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

which, when measured, gives the result 0 fifty percent ($|1/\sqrt{2}|^2$) of the time, and the result 1 fifty percent of the time.

Geometrically, we can interpret the constraint $|\alpha|^2 + |\beta|^2 = 1$ as the qubit being normalized to length 1, and thus the general state of a qubit is a unit vector in a two-dimensional complex vector space.

Vector Representation

We can thus represent qubit states as vectors, and it is conventional to define:

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

so the general qubit state is

$$\alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

Vector Representation

If we call our general state $|\psi\rangle$

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

then $\langle\psi|$ is defined to be the row vector

$$\langle\psi| = \begin{pmatrix} \alpha^* & \beta^* \end{pmatrix}$$

The Inner Product

If $|\phi\rangle = \gamma|0\rangle + \delta|1\rangle$ then the *inner product* of $|\phi\rangle$ and $|\psi\rangle$ is defined as

$$\langle\phi|\psi\rangle = \begin{pmatrix} \gamma^* & \delta^* \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \gamma^*\alpha + \delta^*\beta$$

and so

$$\langle\psi|\psi\rangle = \alpha^*\alpha + \beta^*\beta = |\alpha|^2 + |\beta|^2$$

and we can write our normalisation condition $|\alpha|^2 + |\beta|^2 = 1$ succinctly as $\langle\psi|\psi\rangle = 1$.

Orthogonality

If $\langle\phi|\psi\rangle = 0$ then $|\phi\rangle$ and $|\psi\rangle$ are said to be *orthogonal* states.

The special states $|0\rangle$ and $|1\rangle$ are known as *computational basis states*, and form an *orthonormal basis* for this vector space:

$$\langle 0|1\rangle = \langle 1|0\rangle = 0$$
$$\langle 0|0\rangle = \langle 1|1\rangle = 1$$

The Bloch Sphere

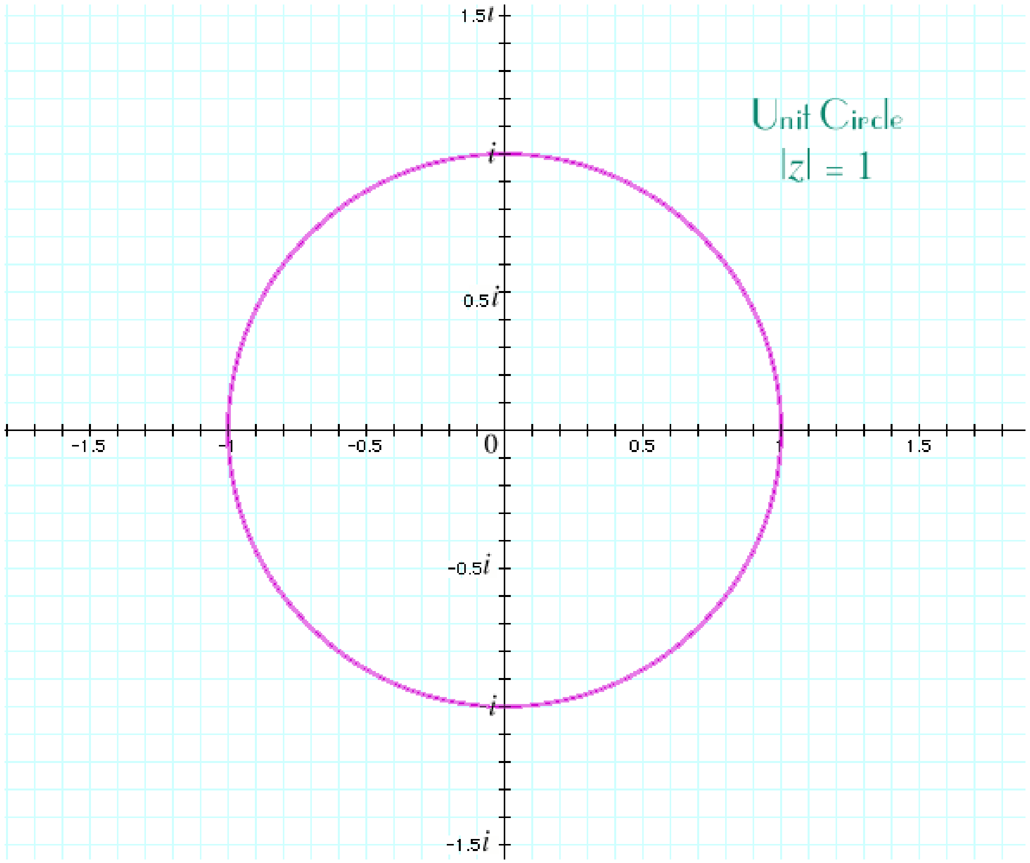
A useful geometric representation of qubit states is as points on the surface of a unit sphere.

This is a generalisation of the representation of a single complex number z with $|z|^2 = 1$ as a point on the unit circle in the complex plane. If $z = x + iy$, where x and y are real, then:

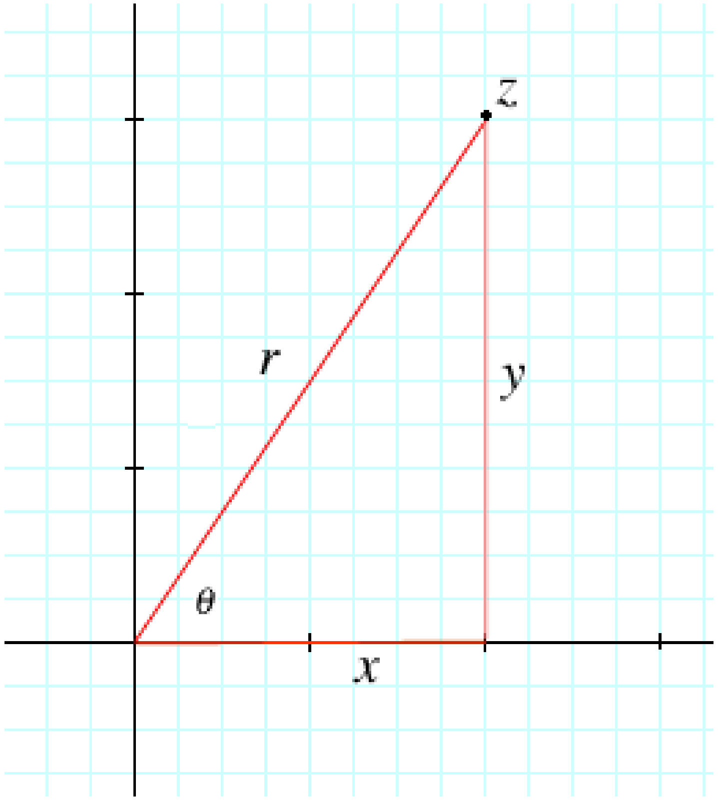
$$|z|^2 = z^* z = (x - iy)(x + iy) = x^2 + y^2 = 1$$

is the equation of a circle of radius one, centered on the origin.

The Unit Circle



Polar Coordinates



Polar Coordinates

For arbitrary $z = x + iy$ we can write $x = r\cos\theta$, $y = r\sin\theta$, so

$$z = r(\cos\theta + i\sin\theta)$$

and using Euler's beautiful identity:

$$e^{i\theta} = \cos\theta + i\sin\theta$$

we have

$$z = re^{i\theta}$$

and the unit circle $(r = 1)$ can be written in the compact form:

$$z = e^{i\theta}$$

Notice that the constraint $|z|^2 = 1$ has left just one degree of freedom.

The Bloch Sphere

Our general qubit state $\alpha|0\rangle + \beta|1\rangle$ can thus be written:

$$r_\alpha e^{i\phi_\alpha}|0\rangle + r_\beta e^{i\phi_\beta}|1\rangle$$

which has four parameters. However, the only measurable quantities are the probabilities $|\alpha|^2$ and $|\beta|^2$, so multiplying the state by an arbitrary factor $e^{i\delta}$ (a global phase) has no observable consequences:

$$|\alpha|^2 \rightarrow |e^{i\delta}\alpha|^2 = (e^{i\delta}\alpha)^*(e^{i\delta}\alpha) = (e^{-i\delta}\alpha^*)(e^{i\delta}\alpha) = \alpha^*\alpha = |\alpha|^2$$

and similarly for $|\beta|^2$. So, we can multiply our state by $e^{-i\phi_\alpha}$, giving:

$$r_\alpha|0\rangle + r_\beta e^{i(\phi_\beta - \phi_\alpha)}|1\rangle = r_\alpha|0\rangle + r_\beta e^{i\phi}|1\rangle$$

which now has only three parameters.

The Bloch Sphere

But in addition we have the normalization constraint $\langle\psi|\psi\rangle = 1$

Switching back to cartesian representation for the coefficient of $|1\rangle$

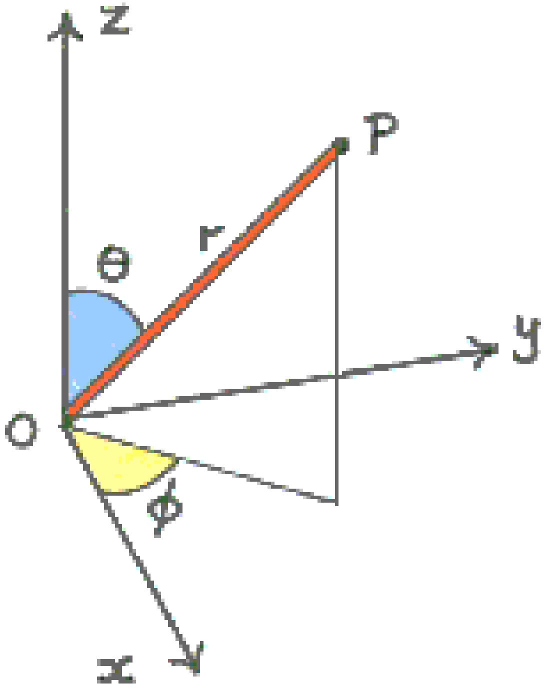
$$r_\alpha|0\rangle + r_\beta e^{i\phi}|1\rangle = r_\alpha|0\rangle + (x_\beta + iy_\beta)|1\rangle$$

The constraint is:

$$\begin{aligned} |r_\alpha|^2 + |x_\beta + iy_\beta|^2 &= r_\alpha^* r_\alpha + (x_\beta + iy_\beta)^*(x_\beta + iy_\beta) \\ &= {r_\alpha}^2 + ({x_\beta}^* - i{y_\beta}^*)(x_\beta + iy_\beta) \\ &= {r_\alpha}^2 + {x_\beta}^2 + {y_\beta}^2 = 1 \end{aligned}$$

which is the equation of a unit sphere in a 3D space with cartesian coordinates $(x_\beta, y_\beta, r_\alpha)$!

Spherical Polar Coordinates



The Bloch Sphere

Cartesian coordinates (x, y, z) can be expressed in terms of equivalent polar cooridnates (r, θ, ϕ) as:

$$\begin{aligned} x &= r \sin\theta \cos\phi \\ y &= r \sin\theta \sin\phi \\ z &= r \cos\theta \end{aligned}$$

so identifying $(x_\beta, y_\beta, r_\alpha)$ with (x, y, z), and remembering $r = 1$, we can write our qubit state:

$$\cos\theta|0\rangle + \sin\theta(\cos\phi + i\sin\phi)|1\rangle = \cos\theta|0\rangle + \sin\theta e^{i\phi}|1\rangle$$

Now we have just two parameters defining points on a unit sphere.

The Bloch Sphere

This is still not *quite* the Bloch sphere however. Let

$$|\psi\rangle = \cos\theta'|0\rangle + \sin\theta' e^{i\phi}|1\rangle$$

and notice that $\theta' = 0 \Rightarrow |\psi\rangle = |0\rangle$ and $\theta' = \frac{\pi}{2} \Rightarrow |\psi\rangle = |1\rangle$

Also, it it not necessary to consider negative values of $\cos\theta'$ because a sign change is just a global phase change of $e^{i\pi}$ $(= -1)$, which has no observable consequences.

Therefore $0 \leq \theta' \leq \frac{\pi}{2}$ generates all possible qubit states (together with $0 \leq \phi \leq 2\pi$) up to an arbitrary global phase.

The Bloch Sphere

Thus we only have a hemisphere! However, we can map points on this hemisphere onto points on a sphere by defining

$$\theta = 2\theta' \quad \Rightarrow \quad \theta' = \frac{\theta}{2}$$

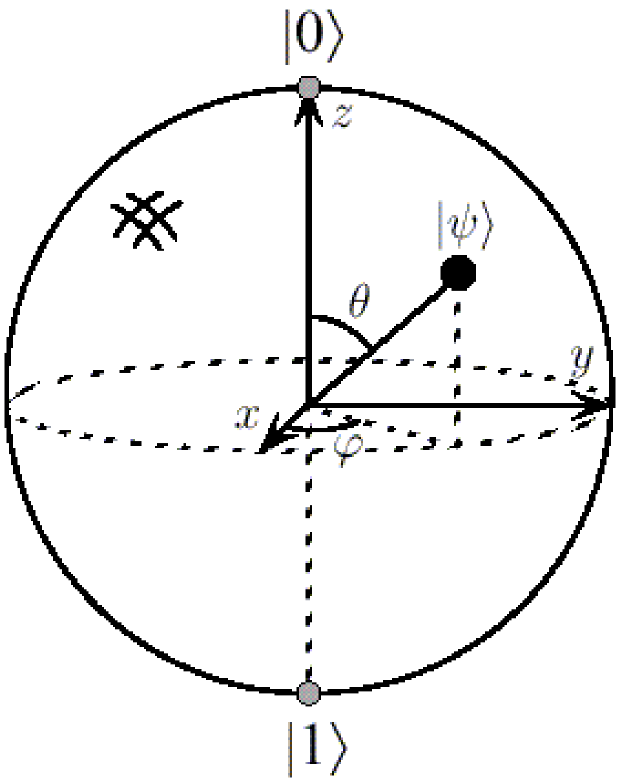
and we now have

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}e^{i\phi}|1\rangle$$

where $0 \leq \theta \leq \pi$, $0 \leq \phi \leq 2\pi$ are the coordinates of points covering a sphere - the *Bloch sphere*.

Note that opposite points correspond to orthogonal qubit states.

The Bloch Sphere



The Bloch Sphere

- Notice that $\theta = 2\theta'$ is a one-to-one mapping except at $\theta' = \frac{\pi}{2}$, where all the points on the 'equator' are mapped to the single point $\theta = \pi$, the 'south pole' on the Bloch sphere
- This is okay, since at the south pole $|\psi\rangle = e^{i\phi}|1\rangle$ and ϕ is a global phase with no significance. (Longitude is meaningless at a pole!)
- What about the other hemisphere, $\frac{\pi}{2} \leq \theta' \leq \pi$?
- Since $\cos(\pi - \theta) = -\cos\theta$ and $e^{i(\phi+\pi)} = -e^{i(\phi)}$
- If $\theta' \rightarrow \pi - \theta'$, $\phi \rightarrow \phi + \pi$ then $|\psi\rangle \rightarrow -|\psi\rangle$

The Bloch Sphere

- i.e. opposite points on the sphere differ only by a factor of -1 and so are physically equivalent
- Representations of rotations in a 2D complex vector space contain a double representation of rotations in 3D real space
- Formally, there is a 2 to 1 homomorphism of SU(2) on SO(3)
- Notice also that the Bloch sphere interpretation holds as we cross the θ'-equator, e.g. as we cross the equator going south, we effectively start going north again on the other side of the Bloch sphere, because opposite points are equivalent

Global Phase

This double-valued representation has the interesting consequence that rotations of 360° do not restore the absolute global phase to its initial value, and a rotation through 720° is needed. For example:

$$\begin{aligned} \theta = 0 &\quad\Rightarrow\quad |\psi\rangle = |0\rangle \\ \theta = 2\pi &\quad\Rightarrow\quad |\psi\rangle = -|0\rangle \\ \theta = 4\pi &\quad\Rightarrow\quad |\psi\rangle = |0\rangle \end{aligned} \tag{1}$$

For an isolated qubit this has no physical significance, but in relation to other qubits there is a difference

Orientation-Entanglement Relation

- e.g. a rotation of 360° of an electron about its 'spin' axis changes its state - a 720° rotation is needed to restore it
- What's more, this kind of phenomenon is not restricted to the world of quantum mechanics
- It affects the 'orientation-entanglement relation' of objects in everyday 3D real space
- And I have a demo!