Quantum Computing

John A Clark
Dept. of Computer Science
University of York, UK
jac@cs.york.ac.uk

York CS Seminar 19 February 2003

Motivation

- To present some important quantum mechanical concepts and illustrate their application to communication and computing
- To summarise important differences with classical computing
- To suggest an avenue for symbiosis
  - Not physics
  - Not philosophy
    - "I've got some grad student. He's thinking about the meaning of quantum mechanics. He's doomed!"

— John McCarthy (quoted in Williams and Clearwater *Explorations in Quantum Computing*, chapter 3)

Feature

Qubits can exist in superpositions of states

Is it a bird? Is it is a bee? Neither, but it's got potential.

Qubits – Black and White

- In classical computing bits have value 0 or 1. Eigenstates of quantum systems are the states you can find yourself in if you look.
- Electrons: 0-1 ness encoded using the electron spin:

$|0\rangle$ **Spin down** $|\downarrow\rangle$

$|1\rangle$ **Spin up** $|\uparrow\rangle$

- Whenever you choose **to look** you will always find yourself in one of the **eigenstates** of the system

Superposition: Gray Qubits

- But quantum systems can simultaneously exist in a ***superposition*** of different states at the same time
- Technically, the is represented as mixture (with complex coefficients a and b)

$$|\Psi\rangle = a|0\rangle + b|1\rangle$$

$$|a|^2 + |b|^2 = 1$$

Will represent in matrix form

$$a|0\rangle + b|1\rangle \qquad \begin{pmatrix} a \\ b \end{pmatrix}$$

Superposition- Walsh Hadamard

- The Walsh Hadamard is a crucially important operation that forms a mixtures according to:

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

$$H|1\rangle = \tfrac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$$

- Can apply to n individual qubits to get superposition of all 2^n states

$$H^n(|000\ldots0\rangle) = \frac{1}{\sqrt{2^n}}(|0\rangle + |1\rangle) \otimes .. \otimes (|0\rangle + |1\rangle) = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1} x$$

Multiple Qubits

- The idea generalises to several qubits. We can now find ourselves in any of 2^n eigenstates.
- 2-qubit example (a,b,c,d complex as before)

$$|\Psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$$

$$|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$$

- As the number of qubits increases linearly, the number of states increases exponentially. Matrix representation much as before

$$\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}$$

Multiple Qubits

- 2-qubit example

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

$$a = b = c = d = \frac{1}{2}$$

$$|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$$

Multiple Qubits

- In 2-qubit example – could think of the combined states as the (direct) product of two qubits states

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

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

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

Feature

Quantum systems act differently when they are observed. They collapse.

Teaching quality assessment may be closer than you think.

Measurements

- A measurement of the system gives a random result. When the system is measured it is found to be in one of its eigenstates.
- The probability of being observed in one of the states depends on the coefficients in the superposition
- We find our system in

$|0\rangle$ **With probability $|a|^2$**

$|1\rangle$ **With probability $|b|^2$**

Multiple Measurement

- On previous system measure qubit 1. If you witness a |0> then the state space of qubit 1 collapses to |0> and the overall state space becomes

Only 0s now

$$\left|\Psi_{0X}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|00\right\rangle + \left|01\right\rangle\right)$$

- Note that there has been some readjustment of the probabilities – *renormalisation*.
- We can now observe qubit 2 and see a |0> with probability ½ and a |1> with probability ½.

Feature

Applying a quantum transformation to a superposition gives a superposition of applying the transformation to its constituent states.

Buy 1, get 2^n-1 free.

Unitary Transformations

- The stuff quantum computations are (mostly) made of (you will make observations too).
- Physically reversible operations.
- Essentially they take amplitude vectors (points in $\mathbf{C}^{2^n}$) and park them elsewhere.
- If we can compute a function f then we can find a reversible variant of f too, e.g. by keeping the inputs

$$|x\rangle|0\rangle \to |x\rangle|f(x)\rangle$$

Linearity of Transformations

- NOT N maps

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \qquad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$\mathrm{N}\left|0\right\rangle = \left|1\right\rangle \qquad \mathrm{N}\left|1\right\rangle = \left|0\right\rangle$$

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} b \\ a \end{pmatrix}$$

$$\mathrm{N}\left(\mathrm{a}\left|0\right\rangle + b\left|1\right\rangle\right) = a\mathrm{N}\left|0\right\rangle + b\mathrm{N}\left|1\right\rangle = a\left|1\right\rangle + b\left|0\right\rangle$$

Registers and Unitary Transformations

- So far we have worked on a single qubit
  - Multiple qubit registers are used for serious computations
  - An n-bit register can hold 2^n states in superposition
  - Unitary transformations can be applied to all superposition states in one go.

$$U\left(\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1} x\right) = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1} Ux$$

Feature

Qubits can get themselves into such a tangle.

You say tomato, I say tomato.

Entanglement

- Now consider the following superposition

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right)$$

- What qubit product would give rise to this?

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right) = \left(a|0\rangle + b|1\rangle\right) \otimes \left(c|0\rangle + d|1\rangle\right)?$$

Entanglement

- There isn't one! And this has consequences!
- Suppose we now choose to measure Qubit 1 and get a |0> say (which we obtain with probability ½). As before the state space collapses

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right) \xrightarrow{\text{ObserveQ1=0}} |01\rangle$$

- If we now measure Qubit 2 we see a |1> with probability 1.
- Similarly, if we had observed a |1> for Qubit 1 we would now be certain to see a |0> for Qubit 2.

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right) \xrightarrow{\text{ObserveQ1=1}} |10\rangle$$

Entanglement

- So the observational results on Qubit 1 effect the observational results on Qubit 2.
- Question....
  - What if Qubit 1 were on earth and Qubit 2 were on Pluto, or worse, in London?
  - Odd huh?
- We say that the qubits are ***<u>entangled</u>***
- Possibly the strangest phenomenon in physics.
- We cannot explain the overall system state in terms of the two individual systems states.

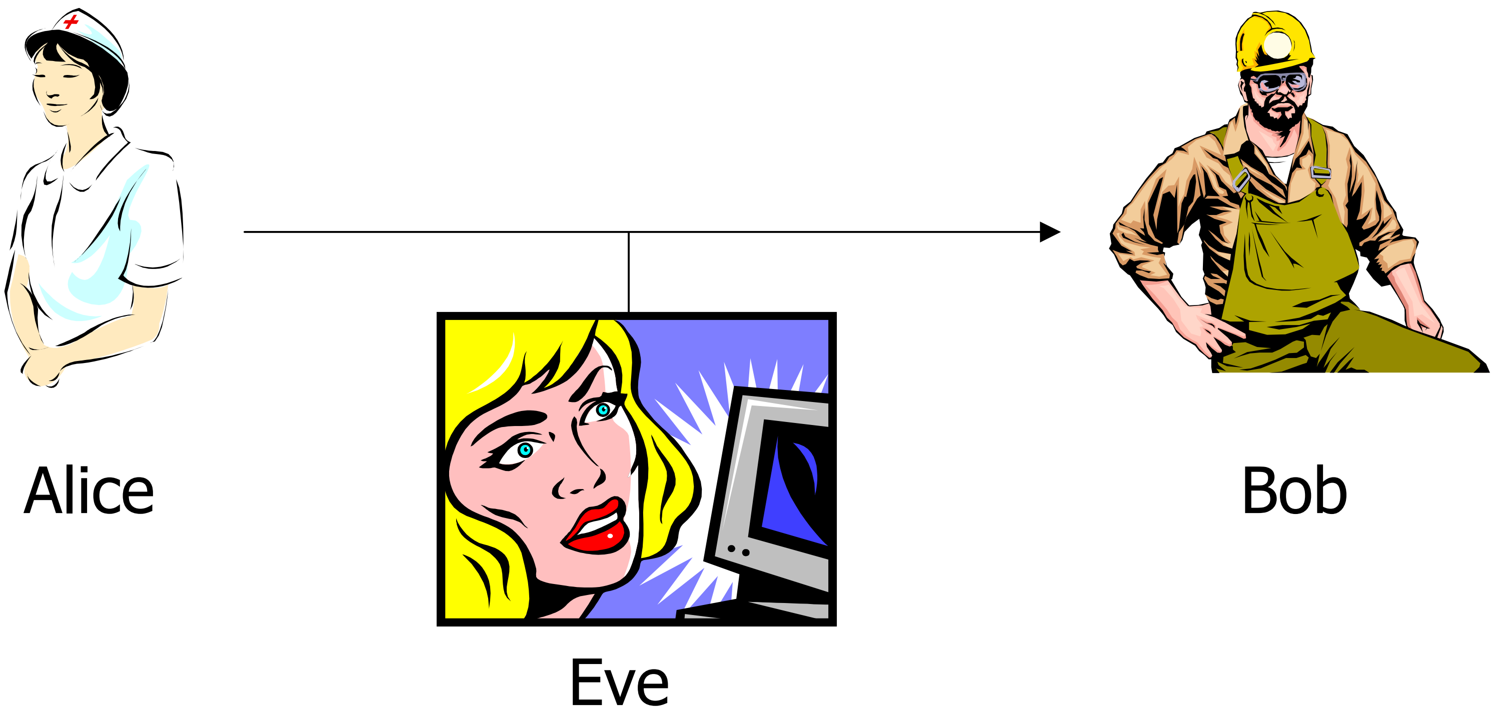
Feature

Qubits cannot be cloned.

When Alice met Bob…..

When Alice met Bob

- Communicants will (following tradition) be Alice and Bob, trying to communicate their love…

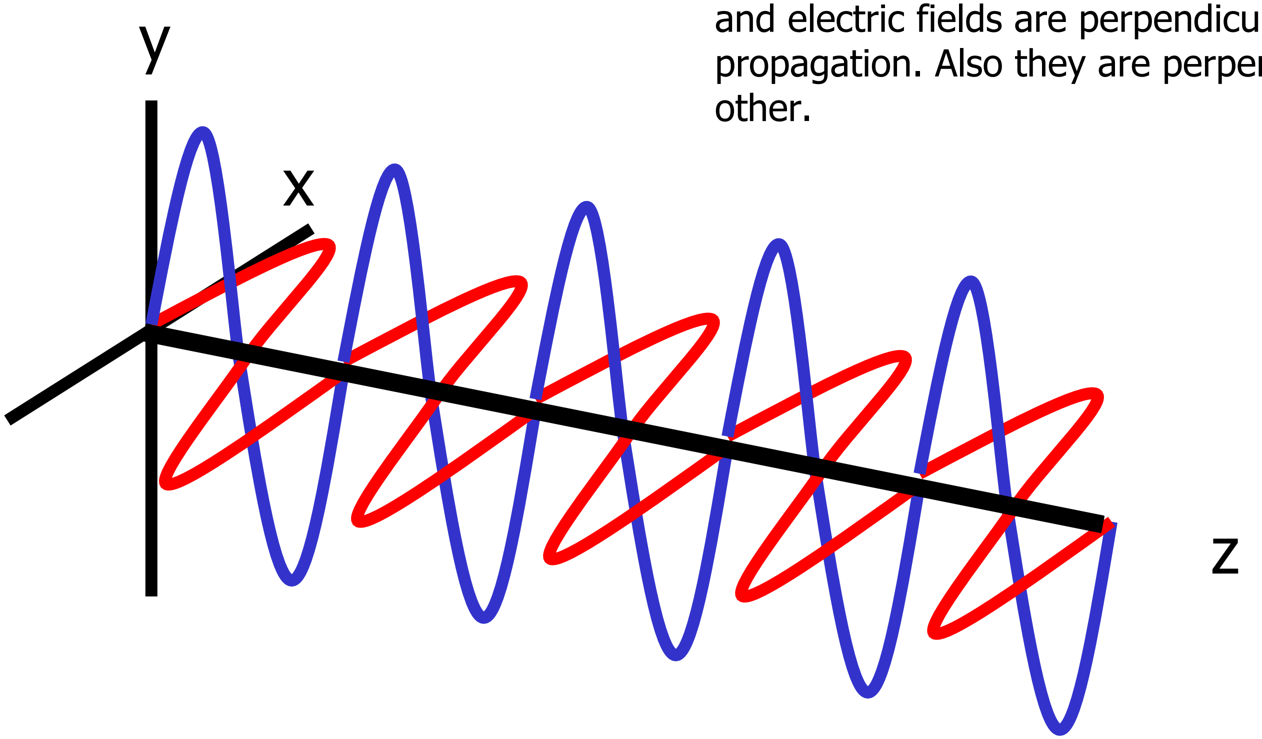


- Eve isn’t happy about this. She wants to listen in and interfere

Basic Scheme

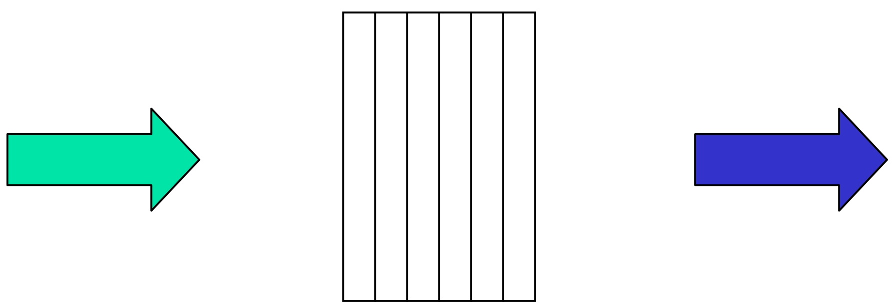
- Basic scheme based on polarisation of photons

Photons are transverse magnetic waves – magnetic and electric fields are perpendicular to the direction of propagation. Also they are perpendicular to each other.



Photons

- We will assume that we are dealing with linearly polarised light but other schemes are possible.
- We need to create photons that with an electric field oscillating in the desired magnetic plane.
- One way to do this is by passing light through an appropriate polariser

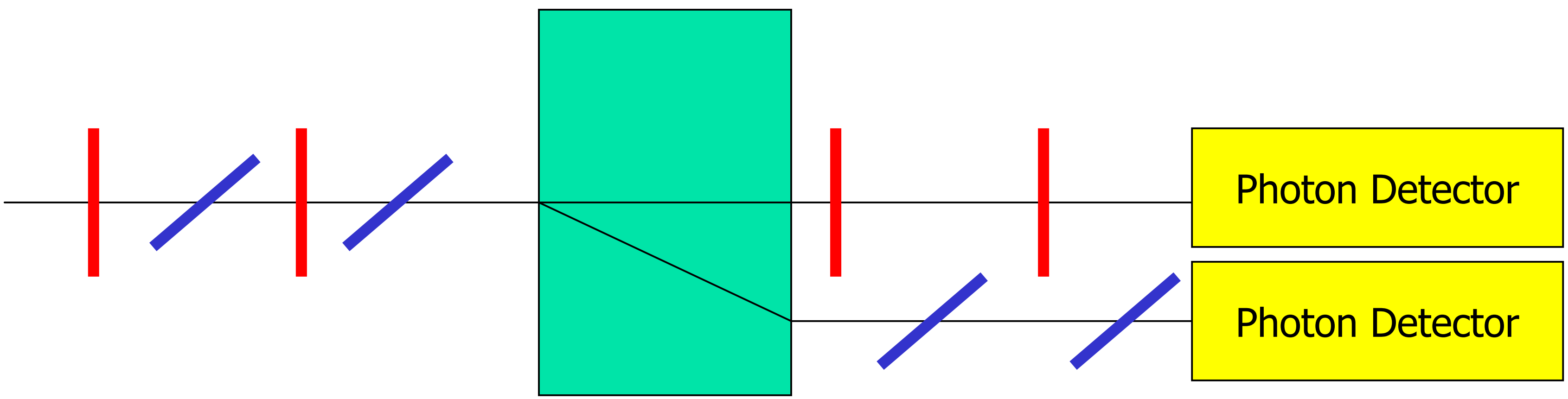


Only vertically polarised photons emerge

- More sophisticated way is to use a Pockels Cell.

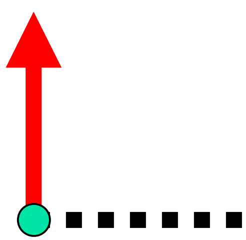
Detecting Photons

- Possible to detect absorption by using a Calcite crystal

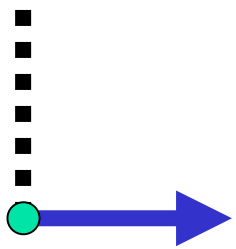


Basic Scheme

- Basic scheme assumes that the polarisation of photons can be arranged. For example



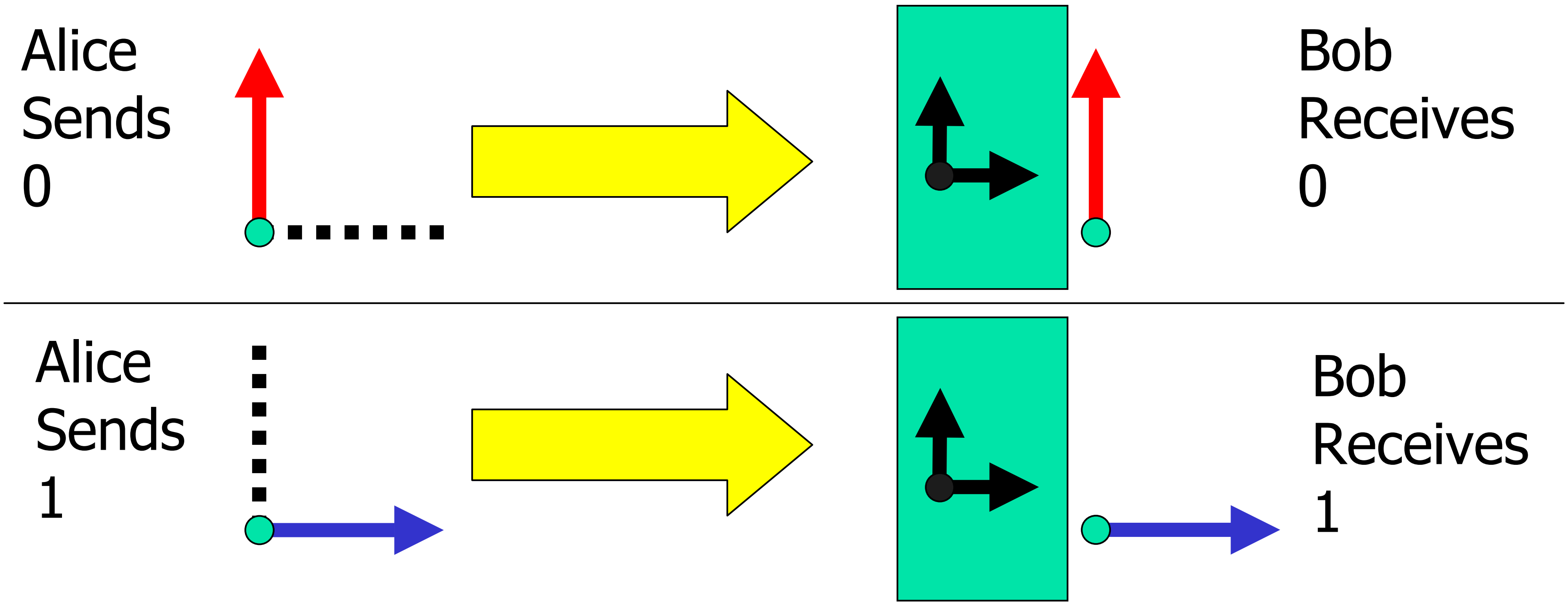
Vertical Polarisation denotes 0



Horizontal Polarisation denotes 1

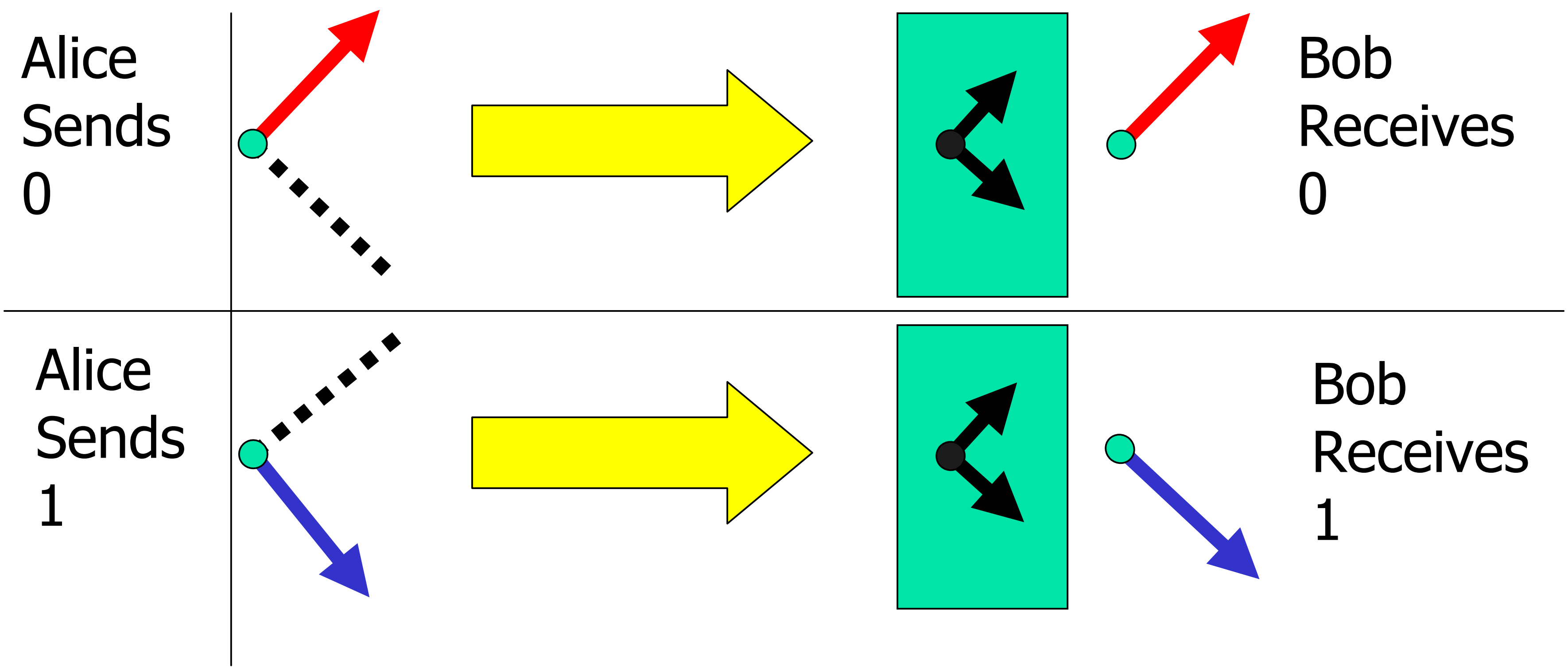
Rectilinear Basis

- Suppose now that Alice sends a 0 in this scheme and that Bob uses a photon detector with the same basis.



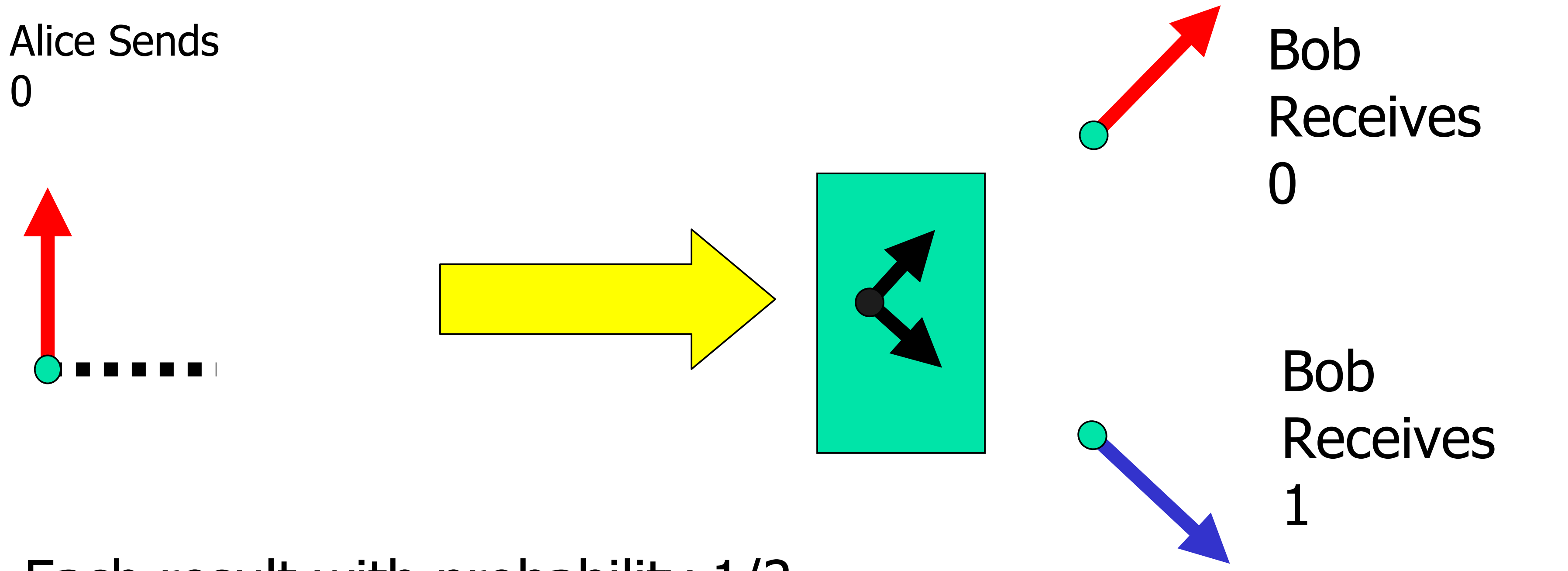
Diagonal Basis

- Can also arrange this with a diagonal basis



Basis Mismatch

- What if Alice and Bob choose different bases?



Each result with probability 1/2

Use of Basis Summary

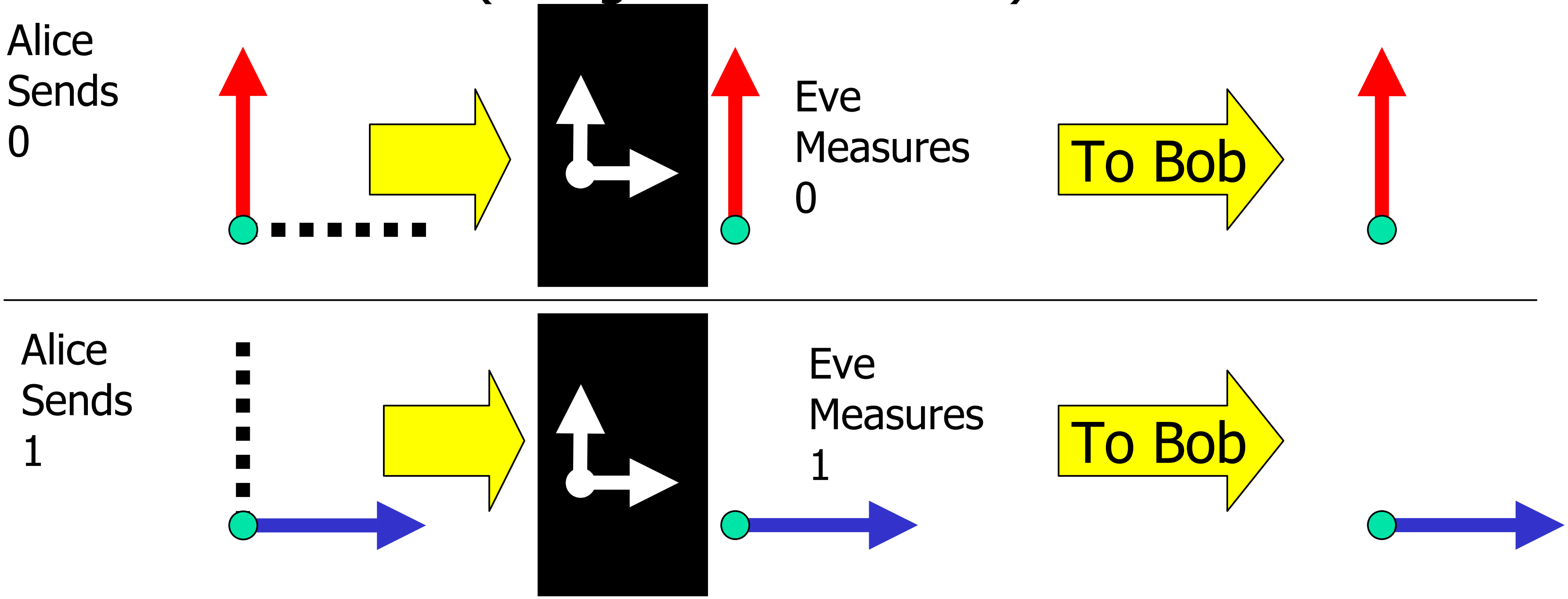
- A sender can encode a 0 or a 1 by choosing the polarisation of the photon with respect to a basis
  - Vertical => 0 Horizontal => 1; or
  - 45 degrees => 0, 135^{o} =>1
- The receiver Bob can observe (measure) the polarisation with respect to either basis.
  - If same basis then bits are correctly received
  - If different basis then only 50% of bits are correctly received.
- This notion underpins one of the basic quantum cryptography key distribution schemes.

What’s Eve up To?

- Now Eve gets in on the act and chooses to measure the photon against some basis and then retransmit to Bob.

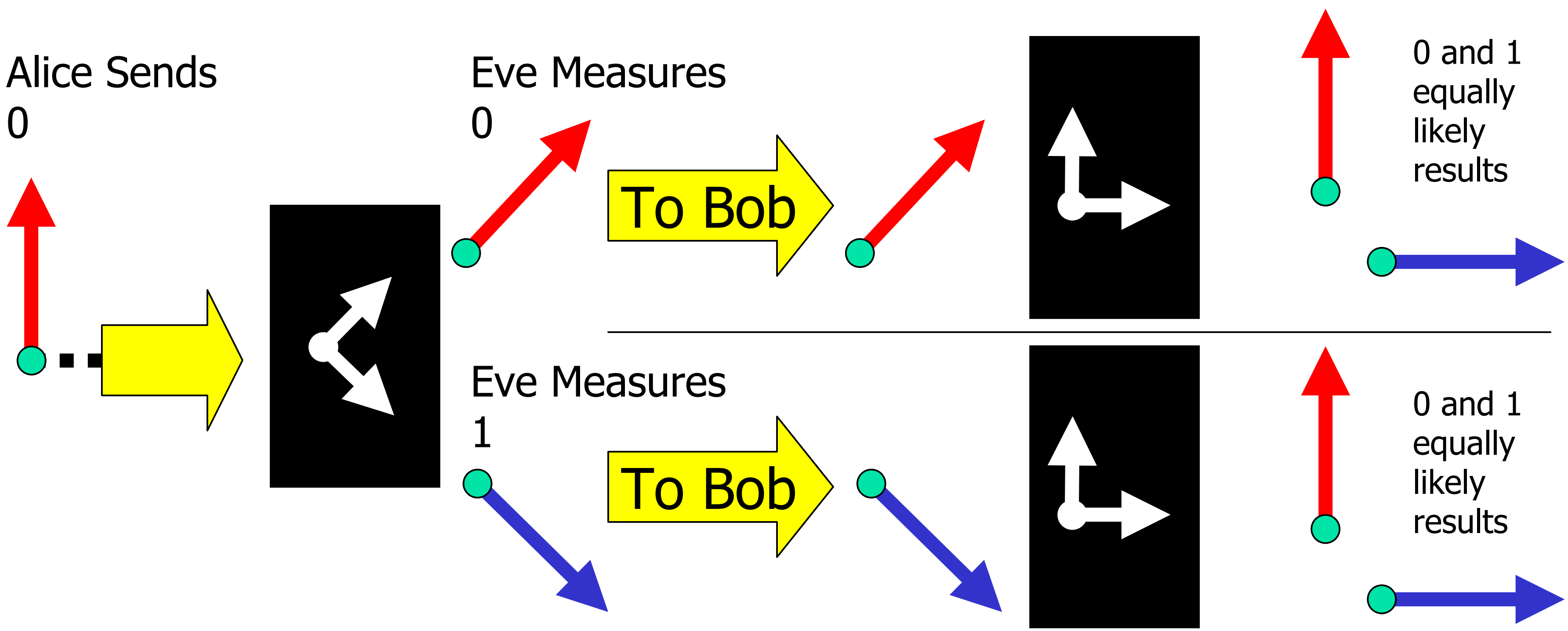
Eve's Dropping In

- Suppose Eve listens in using the <u>same basis</u> as Alice, measures the photon and retransmits a photon as measured (she goes undetected)



Eve's Dropping In

- Suppose Eve listens in using a different basis to Alice



- Similarly if Alice sends a 1 (or if Alice uses diagonal basis and Eve uses rectilinear one)

Summary of Eve's Droppings

- If Eve gets the basis wrong, then even if Bob gets the same basis as Alice his measurements will only be 50 percent correct.
- If Alice and Bob become aware of such a mismatch they will deduce that Eve is at work.
- A scheme can be created to exploit this.

Deutsch's Algorithm

Deutch's Algorithm

- The first real quantum algorithm that showed that things can be done more efficiently on a Quantum Computer than on a classical one.

You have a function $f: \{0,1\} \rightarrow \{0,1\}$ and you want to know whether it is balanced or not (it is balanced if $f(0)=f(1)$)

Not Balanced:

$$f_1 : f(0) = f(1) = 0$$

$$f_2 : f(0) = f(1) = 1$$

Balanced:

$$f_3 : f(0) = 0, f(1) = 1$$

$$f_4 : f(0) = 1, f(1) = 0$$

How many function evaluations do this require?

Deutch's Algorithm

- Start with two qubit register in the state $|01\rangle$ and apply the Walsh Hadamard Transformation to each qubit

$$H^{(2)}|01\rangle = \tfrac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \otimes \tfrac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$$

$$H^{(2)}|01\rangle = \tfrac{1}{2}\left(|00\rangle + |10\rangle - |01\rangle - |11\rangle\right)$$

- Now apply the unitary (reversible) transformation defined by

$$U|i\,,j\rangle = |i\,,j \oplus f(i)\rangle$$

$$U|00\rangle = |0\,,0 \oplus f(0)\rangle$$

$$U|01\rangle = |0\,,1 \oplus f(0)\rangle$$

$$U|10\rangle = |1\,,0 \oplus f(1)\rangle$$

$$U|11\rangle = |1\,,1 \oplus f(1)\rangle$$

Deutch's Algorithm

- Applying the transformation to the superposition

$$U\left(\tfrac{1}{2}\left(|00\rangle+|10\rangle-|01\rangle-|11\rangle\right)\right)=\tfrac{1}{2}\left(U|00\rangle+U|10\rangle-U|01\rangle-U|11\rangle\right)$$
$$=\tfrac{1}{2}\left(|0,0\oplus f(0)\rangle+|1,0\oplus f(1)\rangle-|0,1\oplus f(0)\rangle-|1,1\oplus f(1)\rangle\right)$$

- Depending on which particular *f* we have this gives

$$For\quad f_1: \quad \tfrac{1}{2}\left(|0,0\rangle+|1,0\rangle-|0,1\rangle-|1,1\rangle\right)$$
$$For\quad f_2: \quad \tfrac{1}{2}\left(|0,1\rangle+|1,1\rangle-|0,0\rangle-|1,0\rangle\right)$$
$$For\quad f_3: \quad \tfrac{1}{2}\left(|0,0\rangle+|1,1\rangle-|0,1\rangle-|1,0\rangle\right)$$
$$For\quad f_4: \quad \tfrac{1}{2}\left(|0,1\rangle+|1,0\rangle-|0,0\rangle-|1,1\rangle\right)$$

Deutch's Algorithm

- But if we now apply the Walsh Hadamard Transformation to both qubits we get (depending on which particular *f* we have)

$$For \quad f_1: \quad W\left(\tfrac{1}{2}\left(|0,0\rangle + |1,0\rangle - |0,1\rangle - |1,1\rangle\right)\right) = |0,1\rangle$$

$$For \quad f_2: \quad W\left(\tfrac{1}{2}\left(|0,1\rangle + |1,1\rangle - |0,0\rangle - |1,0\rangle\right)\right) = -|0,1\rangle$$

Not Balanced

$$For \quad f_3: \quad W\left(\tfrac{1}{2}\left(|0,0\rangle + |1,1\rangle - |0,1\rangle - |1,0\rangle\right)\right) = |1,1\rangle$$

$$For \quad f_4: \quad W\left(\tfrac{1}{2}\left(|0,1\rangle + |1,0\rangle - |0,0\rangle - |1,1\rangle\right)\right) = -|1,1\rangle$$

Balanced

- But we can now simply measure the first qubit and we are guaranteed to see a 0 if the function *f* is balanced and a 1 if it isn't.
- Note we have learned a global property about the system: we don't actually know the value of any of *f*(0) or *f*(1); just that they are (or are not) the same.

Another View

- The following is a perfectly well defined unitary transformation

$$|x\rangle \otimes \tfrac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) \rightarrow |x\rangle \otimes (-1)^{f(x)}\tfrac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$$

$$|0\rangle \otimes \tfrac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) \rightarrow |0\rangle \otimes (-1)^{f(0)}\tfrac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$$

$$|1\rangle \otimes \tfrac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) \rightarrow |1\rangle \otimes (-1)^{f(1)}\tfrac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$$

Superposition gives (followed by WH)

$$\tfrac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \otimes \tfrac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) \rightarrow \tfrac{1}{\sqrt{2}}\left((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\right) \otimes \tfrac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$$

$$\rightarrow \tfrac{1}{\sqrt{2}}\left[\left((-1)^{f(0)} + (-1)^{f(1)}\right)|0\rangle + \left((-1)^{f(0)} - (-1)^{f(1)}\right)|1\rangle\right] \otimes \tfrac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$$

Constructive or destructive interference to give result

Grover’s Algorithm

Grover's Algorithm

- Grover's algorithm is probably the most important general search algorithm to date.
- It searches a database of 2^N values of x to find the element v satisfying a particular predicate, represented below by $C(x)$

$$x : [0, 2^N - 1]$$
$$(x = v) \Rightarrow C(v) = 1$$
$$(x \neq v) \Rightarrow C(v) = 0$$

- A classical search would require on average $2^{(N-1)}$ tests of values of x.

Grover's Algorithm

- Start with the register of N qubits as all zeroes and place that register into a superposition of all possible states using the Hadamard transformation on the register

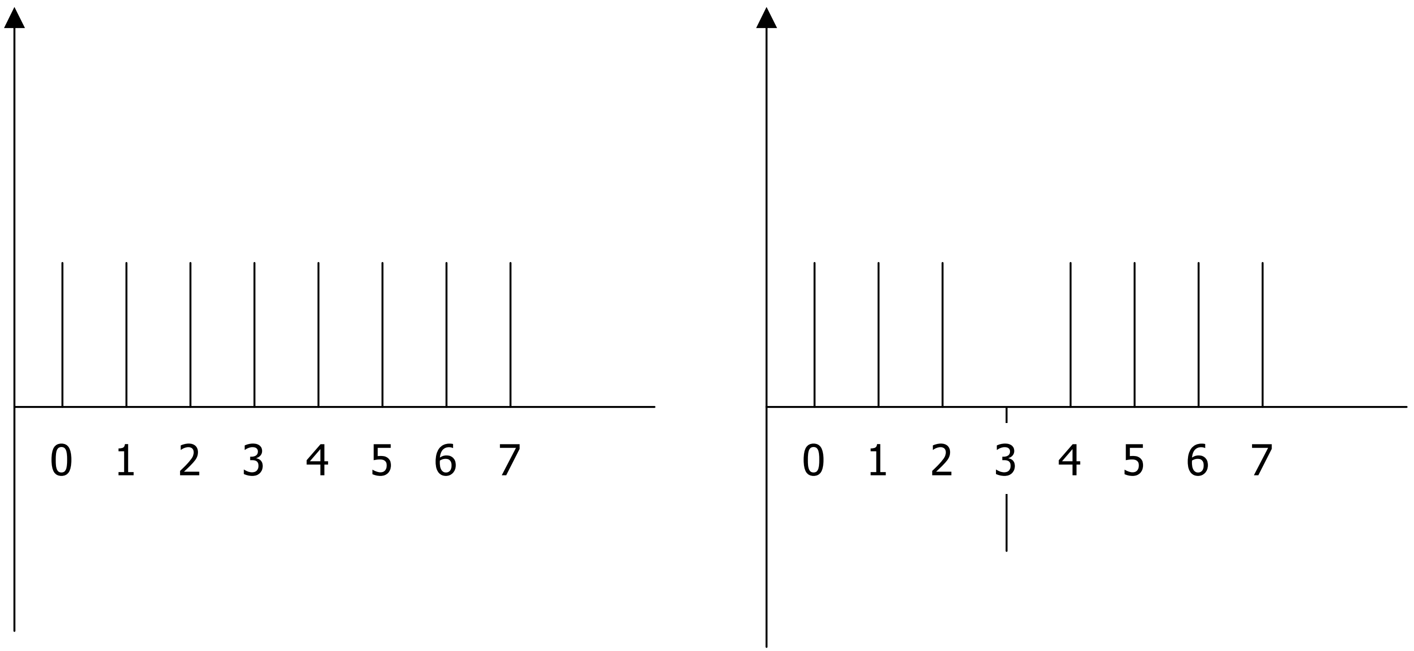
$$H^{(N)}|0\rangle = \frac{1}{\sqrt{2^N}} \sum_x |x\rangle$$

- Apply the following loop $O(\sqrt{N})$ times
  - Negate the phase of the state component of v (leaving everything else the same)
  - Invert about the average
- Measure register. There is a 50% chance of obtaining a result $z = v$.

In practice a bit more complex to form the amplification step

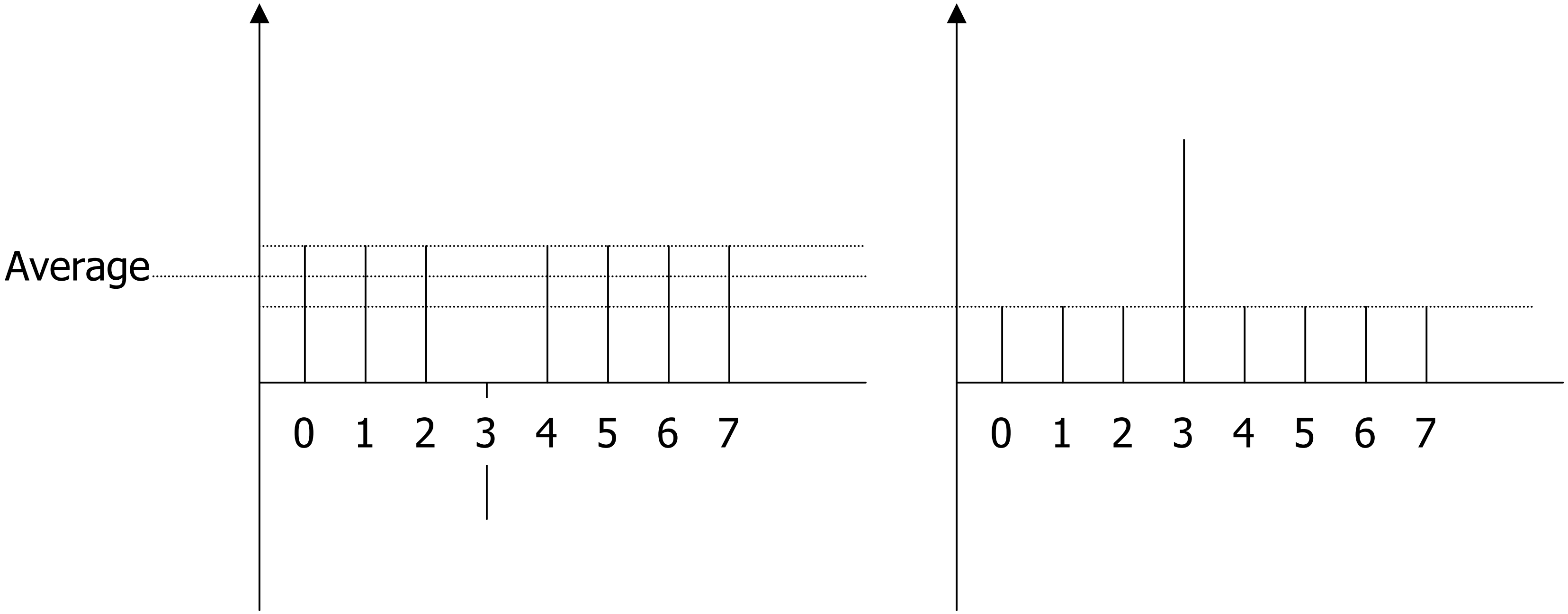
Amplitude Negation

- Negation of the amplitude of v. Suppose we have 8 values of x and $C(3)=1$



Inversion About Average

- Invert about the new average amplitude



- We can see that the magnitude of the amplitude for 3 is getting bigger (more likely to be observed)

Inversion About Average

- The inversion operator is given formally by (with E the average of the a_i)

$$D_N : \sum_{i=0}^{2^N-1} a_i |i\rangle \rightarrow \sum_{i=0}^{2^N-1} (2E - a_i)|i\rangle$$

- This has matrix

$$\begin{pmatrix} -1+\frac{2}{2^N} & \frac{2}{2^N} & \cdots & \frac{2}{2^N} \\ \frac{2}{2^N} & -1+\frac{2}{2^N} & \cdots & \frac{2}{2^N} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{2}{2^N} & \frac{2}{2^N} & \cdots & -1+\frac{2}{2^N} \end{pmatrix}$$

Going Too Far

- After some point applying another loop body iteration actually lowers the amplitude of the desired state to be measured.
- It is possible to ‘overcook’ it.

Generalising

- Grover's search is very important. The original result has been generalised to the case where there are R marked states (i.e. states satisfying the search predicate).
- Not surprisingly, if there are more possible states to find the algorithm one of them can be found quicker. Order of search is now

$$O(\sqrt{\frac{N}{R}})$$

- Also similar results concerning non-uniform starting states.
- But what if you do not know how many states satisfy the predicate?

Question

- What meaningful problems can be addressed using this technique?

Shor’s Algorithm

Shor's Algorithm

- Probably the most high profile of all quantum algorithms.
- Shor made news all over the world when he announced an algorithm that can factor effectively products into primes.

$$n = p \times q$$

- **Problem: given n find p and q**
- Basis of a great deal of cryptographic security, e.g. RSA

Preliminaries

- Shor's factoring algorithm based on finding periodicity of a function *f*.
- Suppose we want to factor 15. We pick a value a relatively prime to 15, e.g. 7 and look at values of

$$7^x \bmod 15$$

Preliminaries

- These are given by

$$7^0 \bmod 15 = 1 \qquad 7^4 \bmod 15 = 1$$
$$7^1 \bmod 15 = 7 \qquad 7^5 \bmod 15 = 7 \qquad \cdots$$
$$7^2 \bmod 15 = 4 \qquad 7^6 \bmod 15 = 4$$
$$7^3 \bmod 15 = 13 \qquad 7^7 \bmod 15 = 13$$

- The period *R*=4 here.
- But we can use this to factor 15

$$7^{\frac{4}{2}} = 49 \quad \gcd(7^{\frac{4}{2}} + 1, 15) = 5 \quad \gcd(7^{\frac{4}{2}} - 1, 15) = 3$$

- More generally

$$\gcd(a^{\frac{R}{2}} + 1, N) \quad \gcd(a^{\frac{R}{2}} - 1, N)$$

Shor's Algorithm

- Using the usual superposition and quantum computation we can calculate all values of $f(x)$ in parallel.

$$\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}\left|x\right\rangle\left|a^x \bmod N\right\rangle$$

- Now we can observe the second register and then the first to obtain particular values of (x, a^x mod N)

Shor's Algorithm

- If we observe the second register then the state collapses to give a superposition in the first register of those values of *x* consistent with the result obtained.
- Thus if we observed a 4 then the first register is now in a superposition of 3, 7, 11,…
- If we could reliably observe a result of 4 then simply sampling the first register to obtain a value (and repeating the process) would be enough to allow us to obtain the period.
  - E.g. 0,8,12 would allow us to deduce that R=4
- But we cannot reliably observe the same value for the second register when we repeat.

$$\left(|0\rangle + |4\rangle + |8\rangle + \ldots\right)|1\rangle$$

$$\left(|3\rangle + |7\rangle + |11\rangle + \ldots\right)|4\rangle$$

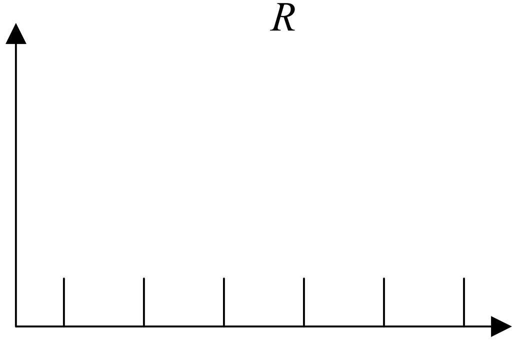
$$\left(|1\rangle + |5\rangle + |9\rangle + \ldots\right)|7\rangle$$

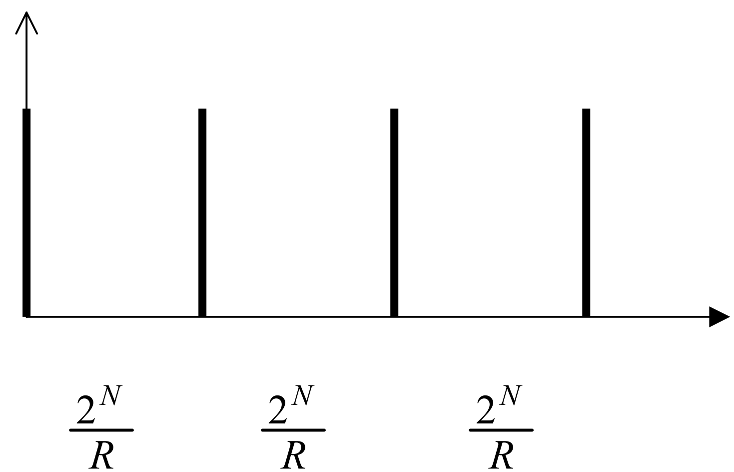
$$\left(|2\rangle + |6\rangle + |10\rangle + \ldots\right)|13\rangle$$

Shor's Algorithm

- Shor's algorithm gets round this problem by applying a Quantum Fourier Transform
- Essentially this encodes the offsets as a phase and you can derive a final state for the *x* where the *x* are in superposition but with very high amplitudes at periods of

$$\frac{2^N}{R}$$





Phenomena Exploited

- Used superposition as usual but have severely exploited problem structure (periodicity) to break a hugely difficult problem.
- Interference via QDFT.
- And of course, entanglement for collapsing.

Other Algorithms

- Minimum finding algorithm
- Maximum finding algorithm
- Quantum counting algorithm
- Collision detection
- SAT problems

Summary

- Various algorithms have been found.
  - But they are not that great in number.
- Basic notion of finding appropriate transformations in order to increase the amplitudes of what we actually want to see.
- Deutch's promise algorithm showed the why we should care.
- Grover's and Shor's algorithms the most influential
  - Many new algorithms to be found?????

Where Now?

Where Now?

- Grover's search may give us square root speed in the state space but is still very limited (it is known to be optimal).
- But it is a search over an *unstructured* database
- So we really need to exploit ***problem structure*** effectively.
- Need to ask smarter questions.

Pointcheval's Perceptron Schemes

- Interactive identification protocols based on NP-complete problem.
- Perceptron Problem.

Given | **Find** | **So That**

$$A_{m\times n} \qquad S_{n\times 1} \qquad A_{m\times n} S_{n\times 1}$$

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ : \\ : \\ s_n \end{pmatrix} = \begin{pmatrix} w_1 \\ w_2 \\ : \\ w_m \end{pmatrix} \geq \begin{pmatrix} 0 \\ 0 \\ : \\ 0 \end{pmatrix}$$

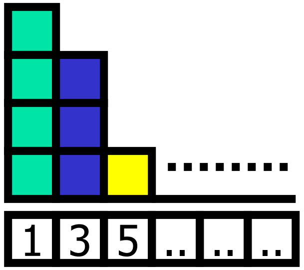
$$a_{ij} = \pm 1 \qquad s_j = \pm 1$$

Pointcheval's Perceptron Schemes

- <u>Permuted</u> Perceptron Problem (PPP). Make Problem harder by imposing extra constraint.

Given $A_{m\times n}$ **Find** $S_{n\times 1}$ **So That** $A_{m\times n} S_{n\times 1}$ **Has <u>particular</u> histogram H of positive values**

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ \vdots \\ s_n \end{pmatrix} \geq \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_m \end{pmatrix}$$



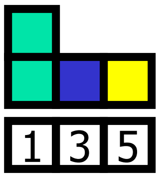
$$a_{ij} = \pm 1 \qquad s_j = \pm 1$$

Example: Pointcheval’s Scheme

- PP and PPP-example
- Every PPP solution is a PP solution.

$$\begin{pmatrix} 1 & -1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 & -1 \\ -1 & 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ -1 \\ 1 \\ -1 \end{pmatrix} = \begin{pmatrix} 3 \\ 1 \\ 1 \\ 5 \end{pmatrix}$$

Has particular histogram H of positive values



$$\begin{aligned} H &= (h(1), h(3), h(5)) \\ &= (2,1,1) \end{aligned}$$

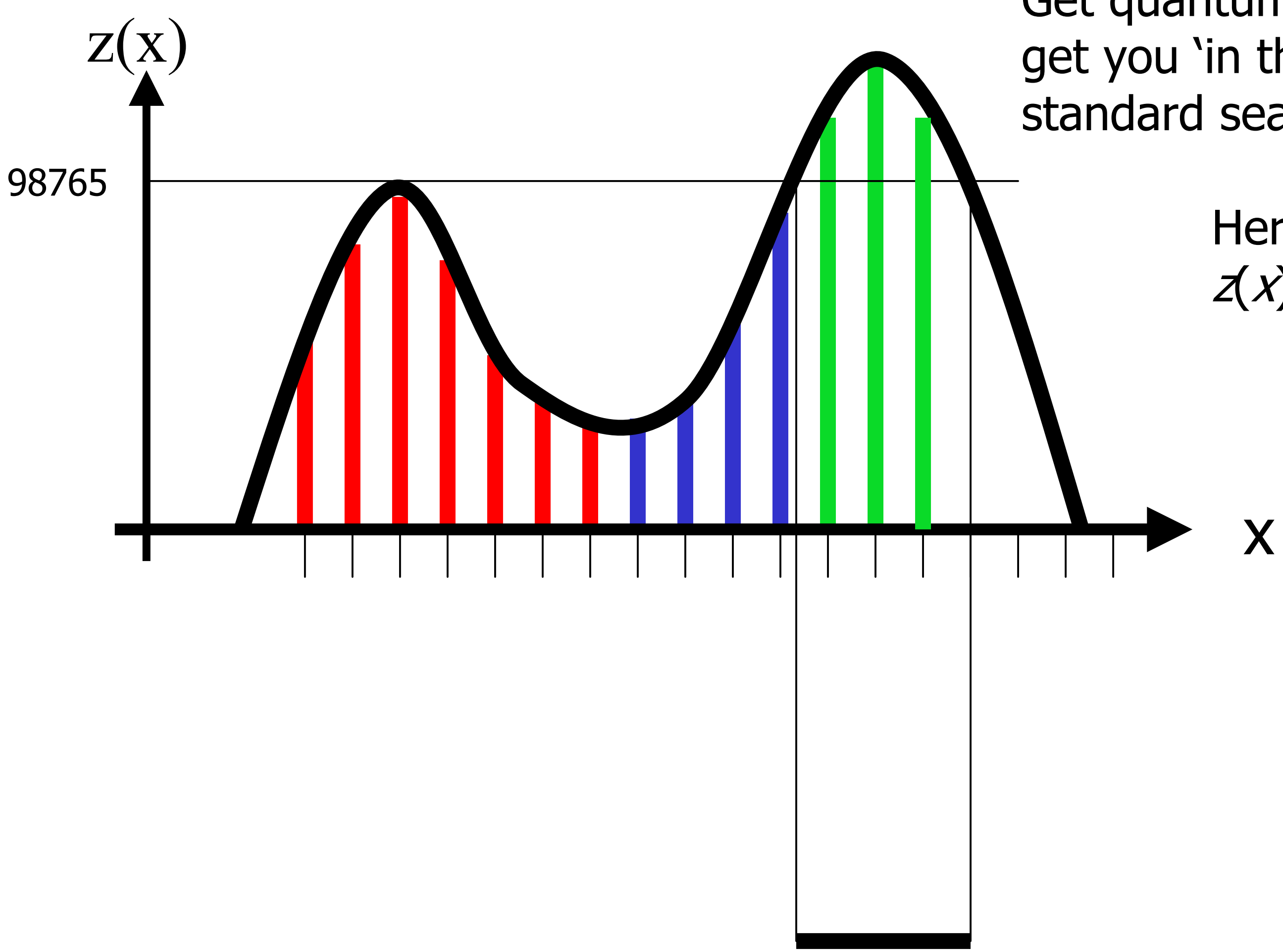
Evolutionary Techniques

- You can throw your usual evolutionary techniques at this problem.
- In some cases you can get very good results:
  - E.g. for (101,117) matrices, simulated annealing attacks have so far produce instances with 108 bits correct.
  - In practice we wouldn't know which 9 bits were incorrect.

Evolutionary Techniques

- However, what if we now ask the question:
  - “Which 9 indices have wrong values?”
- Can form a superposition of all possible wrong indices
  - |index1,index2,…,index8,index9>
- Of the order 7*9=63 bits.
- And now use Grover-like search to find the correct one with order 2^{32} iterations (will require a good number of scratch qubits).
- In general, use standard crunching techniques to get in the right area and use quantum to give the correcting delta.
  - Note: the real first stage problem is to obtain a quantum solvable problem.
  - Perhaps directing the initial search with this aim would be useful (i.e. quantum gets quality leftovers, not just leftovers).

Seeding Standard Techniques



Get quantum (or other technique) to get you 'in the right area' for a more standard search.

Here find an *x* such that *z*(*x*)>98765

Summary

- Features
- Quantum ideas:
  - superposition,
  - unitary transforms,
  - interference,
  - state collapse,
  - entanglement,
- Exploiting structure.
- What further algorithms are there and what are the smarter questions?