Quantum Computers and Quantum Cyrptography

Mary Beth Ruskai
mbruskai@gmail.com

March, 2021

Public Key Cryptography

Encoding method is public; Decoding is secret

Factor: $15 = 3 \times 5$ $77 = 7 \times 11$ $221 = 13 \times 17$

$$25902545284885204252 7 = 2971215073 \times 87178291199$$

Encoding uses large number; Decoding needs prime factors

Security: Factoring hard even on a supercomputer

"Hard" means grows exponentially with number of digits

BUT Quantum Computer can factor large numbers easily

Would Make Current Public Key Cryptography Insecure

BUT can also use Quantum Particles for New Better Cryptography

Aside: RSA Encryption

$N = p \cdot q$ large number product of two prime numbers

Find x, y with $x \cdot y = m(q-1)(p-1)+1 = 1 \mod (q-1)(p-1)$

and no common factors with $p-1$ or $q-1$

Message M satisfies $0 \leq M < N$ (If not break into smaller blocks)

Encode M as $C = M^x - kN = M^x \mod N$ so $0 \leq C < N$

Decode $C^y \mod N = M$ y is kept secret.

Public Info: N, x If you know p, q can find y

Shor's algorithm finds period r of function $f(s+r) = f(s)$

where $f(s) = s^x \mod N$ Quantum Part

can get y to decode can find p, q (not needed)

What Can Quantum Computers Really Do?

Quantum Computers NOT Faster - uses a different method

Example: How long to go Charlotte, VT to Essex, NY ??

Entirely by Car takes $\approx$ 90 minutes (63 miles) 21 MPH

Use Ferry takes $\approx$ 30 minutes (3 miles) 6 MPH

Ferry Boat is faster even though it goes more slowly

Only Certain Problems Solved faster on Quantum Computer

"Promise Problems" Answers Hard to Find, but Easy to Check

Check factors by multiplying

Quant Computer only gets correct answer with high probability

Polynomial growth

Suppose # of steps to process N items on computer is cN^2

Computer can process 5,000 items in 1 hour. # steps is $c(5,000)^2$

New computer is 1 million$= 1,000,000 = 10^6$ times faster

Question: How many items can new computer process in 1 hour?

New computer can do $c(5,000)^2 \times 10^6 = c(5,000)^2(10^3)^2$ steps

New computer can process $5,000 \times 10^3 = 5,000,000$ items

10^6 times faster only gives increase by factor of $10^3 = 1,000$ items

Same question when # of steps is cN^3 ?

10^6 times faster only gives increase by factor of $10^2 = 100$

If # of steps is $c\sqrt{N}$, but new computer only 100 times faster?

items new computer can process increases by factor of $10,000$

Exponential Growth

$2^{10} = 1024$ Use estimate $2^{10} \approx 1000 = 10^3$

Exponential Growth: Computer requires $c2^N$ steps

Even $N = 50$ means $c2^{50} = c(2^{10})^5 = c(10^3)^5 = c10^{15}$ steps

Question: New computer is 1,000 times faster. How many now?

$\#$ of steps is $c\,2^{50} \cdot 10^3 \approx c\,2^{50} \cdot 2^{10} = c\,2^{60}$

$N = 60 = 50 + 10$ Can only process 10 more !!

Same Question: New computer is 1 million $= 10^6$ times faster ?

$\#$ of steps is $c\,2^{50} \cdot 10^6 \approx c\,2^{50} \cdot 2^{20} = c\,2^{70}$

$N = 70$ Can only process 20 more – not even double !!

Exp growth – hit a wall – bigger, faster computer has small effect

Digitizing Information

Convert info to long strings of 0 & 1 , e.g., 1101000110

Classical Bit: Use "On" or "Off" switch to rep 0, 1.

Instead of "On/Off" use electron spin – little magnet

$0 \sim \uparrow$ spin up (North) $\qquad$ $1 \sim \downarrow$ spin up (South)

BUT also $\qquad \rightarrow$ spin right (East) $\qquad \leftarrow$ spin left (West)

What does this mean ??

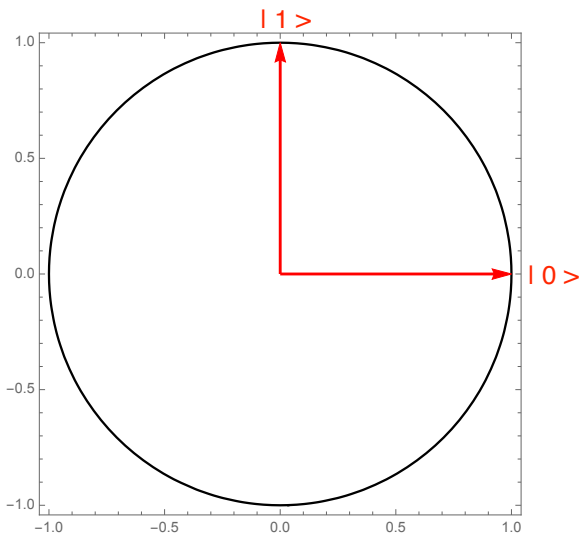
Can you represent any direction in 2-dim ?? $\qquad$ NNW

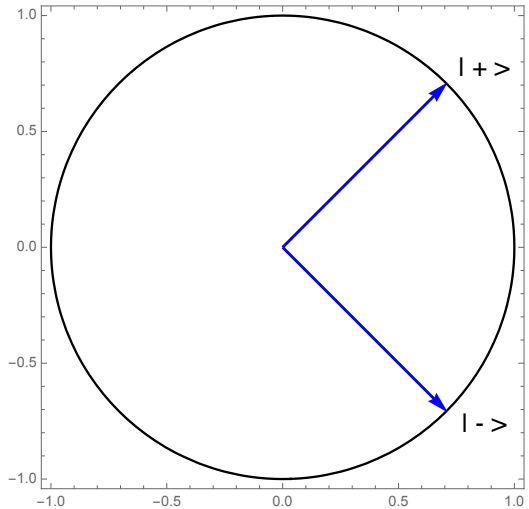
Qubit: Basic Unit of Quantum Info

Qubit state is unit vector in 2-dim $\begin{pmatrix} x \\ y \end{pmatrix}$ $\quad x^2 + y^2 = 1$

Notation: $\quad \uparrow \simeq |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad \downarrow \simeq |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

$$\rightarrow \simeq |+\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \qquad \leftarrow \simeq |-\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$





Vectors in 2-dim don't match spin arrows. Problem? Not Really.

Mathematical vectors vs. arrows

Physics: use vecs in 2 and 3-dim to rep. force, momentum, etc.

these applications – arrows correspond to physics

Many applications of vectors go beyond 2- and 3- dims

Multiple qubits , e.g, 010011 vector in $2^6 = 64$ dims

Unit vectors in 2-dim give a math description of qubit state

Quantum systems vectors of complex numbers – won't need

Many different physical systems used to construct qubits

Another method better for visualizing with 2-dim real vectors

Aside: There is way to associate vectors with points on unit ball in 3-dim that corresponds to up-down, right-left spin arrows

Aside on Bloch sphere

$$|v\rangle = \begin{pmatrix} a \\ b \end{pmatrix} \quad \langle v| = \begin{pmatrix} \bar{a} & \bar{b} \end{pmatrix} \qquad a = c + id \quad \bar{a} = c - id$$

unit vector $\langle v|v\rangle = \begin{pmatrix} \bar{a} & \bar{b} \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = |a|^2 + |b|^2 = 1$

$$|v\rangle\langle v| = \begin{pmatrix} a \\ b \end{pmatrix} \begin{pmatrix} \bar{a} & \bar{b} \end{pmatrix} = \begin{pmatrix} |a|^2 & a\bar{b} \\ \bar{a}b & |b|^2 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1+z & x-iy \\ x+iy & 1-z \end{pmatrix}$$

$$= (2 \times 1)(1 \times 2) = 2 \times 2 \qquad x^2 + y^2 + z^2 = 1$$

$$x = a\bar{b} + \bar{a}b \quad y = -i(a\bar{b} - \bar{a}b) \quad z = 2|a|^2 - 1 = 1 - 2|b|^2$$

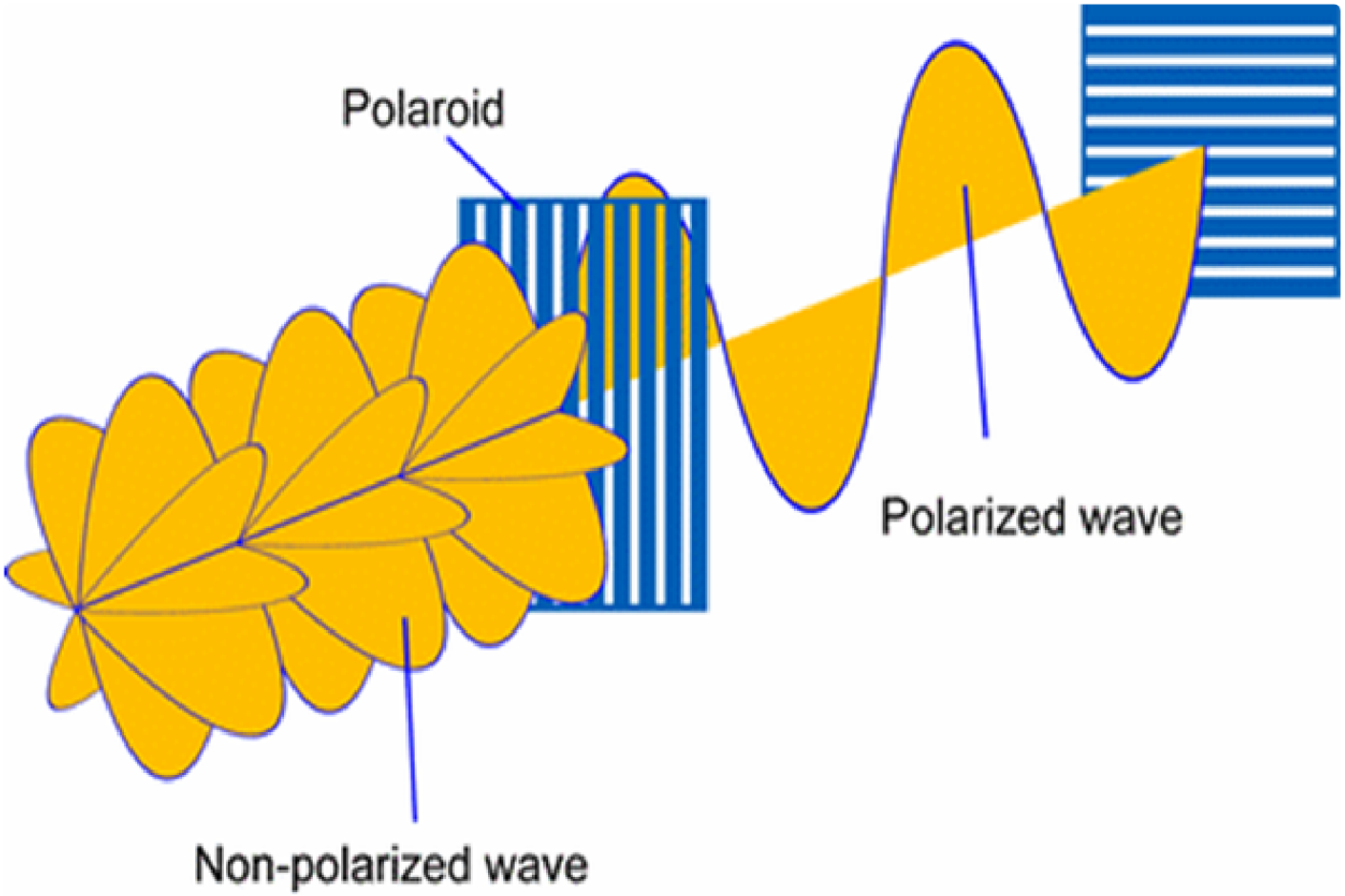
$$|0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \qquad |+\rangle\langle +| = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

$$(x, y, z) = (0, 0, 1) \qquad (x, y, z) = (1, 0, 0)$$

Plot 3-dim in x-z plane, get spin up $\uparrow$, down $\downarrow$, right $\rightarrow$ left $\leftarrow$

Polarized Light

polarization of light.



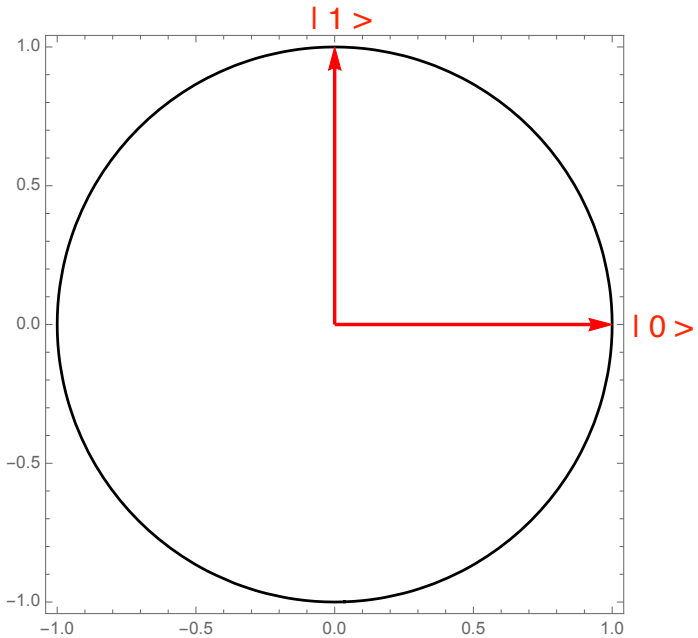
Polarized photons as qubits

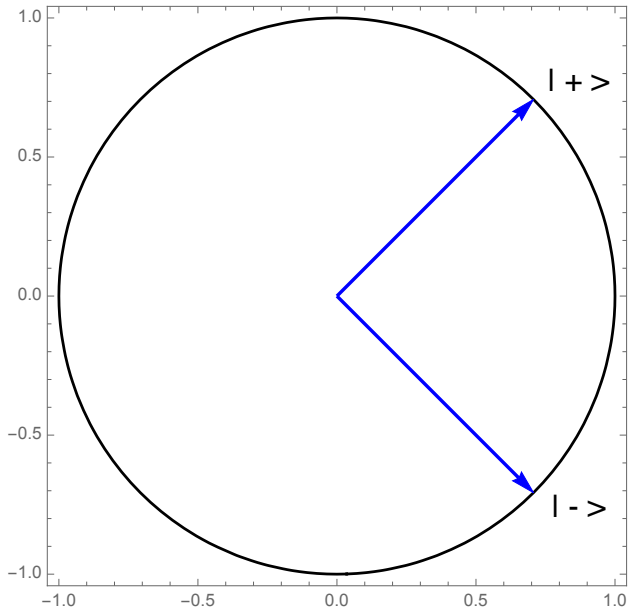
Usually think of beam of light as waves – true, But also

Light composed of particles called photons which have polarization

horizontal $\rightarrow \simeq |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ vertical $\uparrow \simeq |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

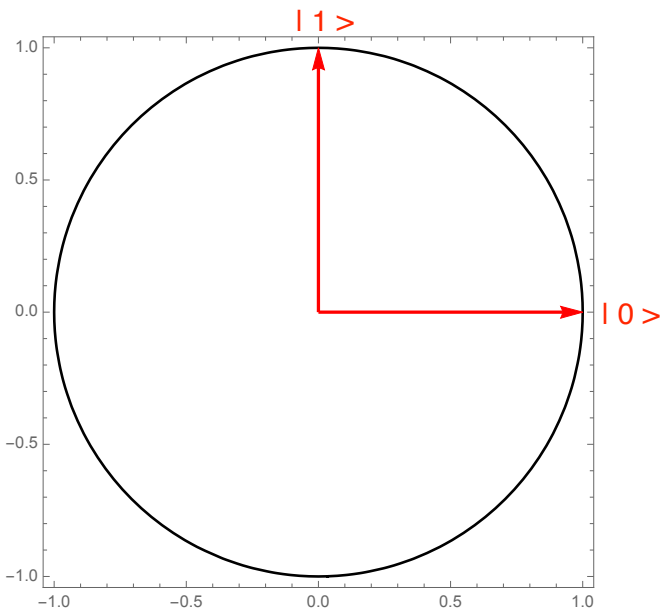
Can rotate 45^o $\nearrow \simeq |+\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ $\searrow \simeq |-\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$

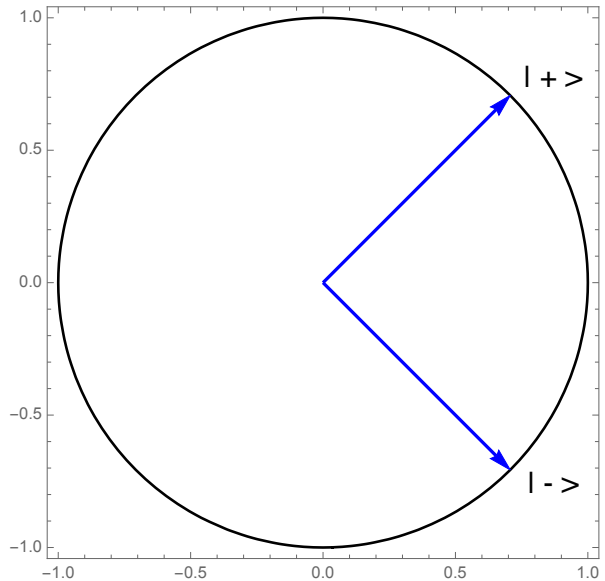




Notation summary

	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$
$\begin{pmatrix} x \\ y \end{pmatrix}$	$\begin{pmatrix} 1 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 1 \end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix}$
spin	$\uparrow$	$\downarrow$	$\rightarrow$	$\leftarrow$
polarization	$\rightarrow$	$\uparrow$	$\nearrow$	$\searrow$





Principles of Quantum Mechanics

- States are represented by vectors $|v\rangle$
- Time development given by Schrödinger equation (don't need)
- Physical observables are represented by operators (matrices) associated with special numbers a_k (called eigenvalues) and vectors (called eigenvectors) which satisfy $A|u_k\rangle = a_k|u_k\rangle$
- The result of measuring observable A is one of the numbers a_k. System orig in state $|v\rangle$ ends in $|u_k\rangle$ with probability $|\langle v, u_k\rangle|^2$

$\Rightarrow$ Measuring destroys original state !!

$\Rightarrow$ No Cloning !! Can NOT clone quantum states

Polarization as Example of Measurement

Example: polarized sunglasses – light comes out polarized

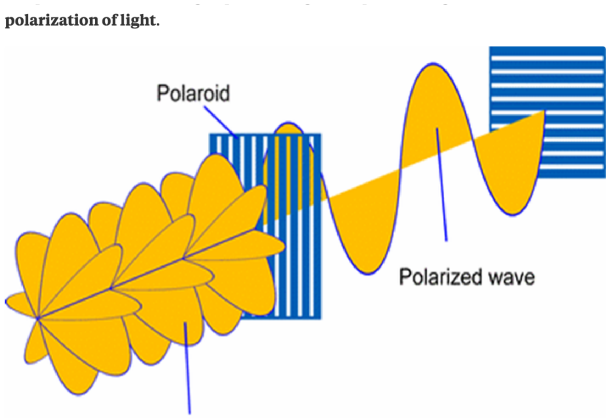
single photon (light particle) has a polarization

beam of light can split – single photon must choose

photon in state $|v\rangle = \begin{pmatrix} x \\ y \end{pmatrix} = x|0\rangle + y|1\rangle = x|\uparrow\rangle + y|\rightarrow\rangle$

Send thru vertical $\uparrow$ polar filter. Go through with prob y^2

But must come out vertically polarized in state $|1\rangle = |\uparrow\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.



Consequence of Measurement

Start with unknown $|\nearrow\rangle$ direction

Can choose measurement that decides between North and South

$+1$ North $|\uparrow\rangle$ -1 South $|\downarrow\rangle$

but now left in N $|\uparrow\rangle$ or S $|\downarrow\rangle$

Can't get any useful info about East or West

OR Can choose measurement that decides between East and West

but now left in E $|\rightarrow\rangle$ or W $|\leftarrow\rangle$

Can't get any useful info about North or South

Measurement process destroys orig. state – can't go back & forth

Qubits can store more info, but you can NOT extract more info

Vectors

Operations $\begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} w \\ z \end{pmatrix} = \begin{pmatrix} x+w \\ y+z \end{pmatrix} \qquad a\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax \\ ay \end{pmatrix}$

Key Prop of vector space $\mathcal{V}$ is $|u\rangle, |v\rangle$ in $\mathcal{V} \Longrightarrow a|u\rangle + b|v\rangle$ in $\mathcal{V}$

Use 2-dim real vector spaces $\quad \vec{v} = \mathbf{v} = \begin{pmatrix} x & y \end{pmatrix} = \langle v|$

row vecs $\quad \langle u| = \begin{pmatrix} w & z \end{pmatrix} \qquad$ col vecs $\quad |v\rangle = \begin{pmatrix} x \\ y \end{pmatrix}$

inner product (dot prod) $\quad \mathbf{u} \cdot \mathbf{v} = \langle u, v\rangle \equiv wx + zy = \begin{pmatrix} w & z \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$

Def: orthogonal (perpendicular) $\quad \langle u, v\rangle = 0$

Meas $\quad A|u_k\rangle = a_k|u_k\rangle \qquad$ Fact: $a_j \neq a_k \;\Rightarrow\; \langle u_j, u_k\rangle = 0$

Assume orthog vecs can be distinguished by measurement

But, e.g. $\langle +, 0\rangle = \frac{1}{\sqrt{2}} \neq 0$ not orthog, can't distinguish

Simple Examples

Flip operator: $X \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} y \\ x \end{pmatrix}$

$X|\pm\rangle = \pm 1|\pm\rangle \qquad X|0\rangle = |1\rangle \quad X|1\rangle = |0\rangle$

$$X|-\rangle = X \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \begin{pmatrix} -1 \\ 1 \end{pmatrix} = -1 \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

Sign operator: $Z \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} x \\ -y \end{pmatrix} = \begin{pmatrix} x \\ -y \end{pmatrix}$

$Z|0\rangle = +1|0\rangle \quad Z|1\rangle = -1|1\rangle \qquad Z|\pm\rangle = |\mp\rangle$

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

X distinguish $|+\rangle$ and $|-\rangle$ $\qquad$ Z distinguish $|0\rangle$ and $|1\rangle$

$a_j = \pm 1$ for Z assoc $a_j = 1$ with $|0\rangle$, $a_j = -1$ with $|1\rangle$

What do $|+\rangle$ and $|-\rangle$ mean?

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\end{pmatrix} + \frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\end{pmatrix} \qquad \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\end{pmatrix} - \frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\end{pmatrix}$$

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

Superposition of $|0\rangle$ and $|1\rangle$ each with prob $\frac{1}{2}$

Interpret: If we measure $\{0,1\}$, get each with prob $\frac{1}{2} = |\langle \pm, 0\rangle|^2$

Note: Could interchange roles of $0,1$ and $+,-$

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

Qubit states correspond to unit vectors on half-circle in 2-dim

prob given by $|\langle u_k, v\rangle|^2 \;\Rightarrow\; |v\rangle$ and $-|v\rangle$ rep same physical state

Multiple Qubits

$|1001\rangle = |1\rangle \otimes |0\rangle \otimes |0\rangle \otimes |1\rangle$ where $\otimes$ is tensor prod – won't define

$$\begin{aligned} |+\rangle \otimes |+\rangle \otimes |+\rangle &= 2^{-3/2}\big(|0\rangle + |1\rangle\big) \otimes \big(|0\rangle + |1\rangle\big) \otimes \big(|0\rangle + |1\rangle\big) \\ &= 2^{-3/2}\big(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle \\ &\qquad + |101\rangle + |110\rangle + |111\rangle\big) \end{aligned}$$

N qubits $|+\rangle \otimes |+\rangle \otimes \ldots \otimes |+\rangle$ superposition of all possible 2^N combinations of N 0's and 1's, each with prob 2^{-N}

This is where quantum computer gets its power

BUT at end, measure in prods of 0,1 basis only gives one answer

Challenge: Not enough to compute correctly. Also need to change 2^{-N} prob to one peaked around correct answer

Quantum Cryptography

One Time Key Pad: Long string 0110101110010 . . .

Encoding Process: 1 in Key Pad flips bit in message

Key Pad or Code	011 010 111 001 . . .
Orig. Message	110 100 100 111 . . .
Coded message	101 110 011 110 . . .

If Key Pad is random, Then Encoded Message appears random

To Decode repeat process

Key Pad or Code	011 010 111 001 . . .
Orig. Message	110 100 010 111 . . .
Coded message	101 110 101 110 . . .
Key Pad or Code	011 010 111 001 . . .
decoded message	110 100 010 111

Quantum Key Distribution

QKD: Alice wants to send message to Bob

- Alice uses polar photons to send random string of 0 and 1

  randomly switches between $|0, 1\rangle$ basis and $|\pm\rangle$ basis

- Bob measures randomly switching between $|0, 1\rangle$ and $|\pm\rangle$ basis

- Alice & Bob talk on insecure cell phone – which basis they used

  Discard all info on which they used different bases

  Keep the rest (about half) to use as a 1-time Key Pad

  With same basis both have 0 or both have 1 — only they know

- Use Secure Key Pad to Encode and Decode Message

What About Eavesdropper?

Eve only gets reliable info IF she uses same basis as Alice and Bob

single photon – No Cloning of quantum states

What if Alice sends using $|0,1\rangle$ and Eve measures using $|\pm\rangle$?

- Her result only matches Alice $\frac{1}{2}$ time
- More Important If she forwards to Bob using $|\pm\rangle$ and he measures using $|\pm\rangle$ doesn't matter (Bob doesn't match Alice)
- If she forwards to Bob using $|\pm\rangle$ and he measures using $|0,1\rangle$ (like Alice) Bob's result only agrees with Alice $\frac{1}{2}$ time

Q.M. $\Rightarrow$ Eavesdropper can NOT get info without introducing error

Alice & Bob don't use entire Key Pad – use part for error detection

With QKD can always tell if Homeland Security is Listening

Remarks on QKD

- Remote procedure – Alice and Bob don't meet

  But they do need to have short ID code exchange at start

- Several protocols using similar idea – this one called BB84

  Bennett and Brassard 1984

- History – proposal for Quantum Money could not counterfeit

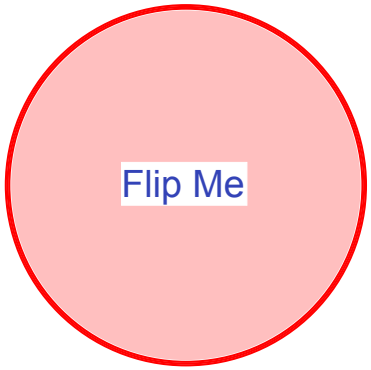
  But grad student S. Weisner (1970) could not get it published

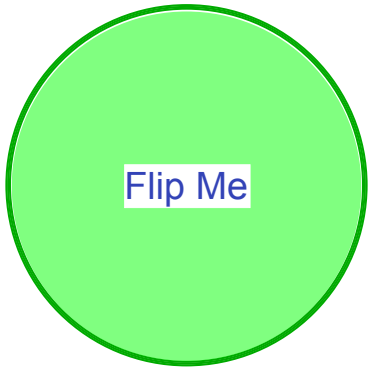
- There are commercial devices fibre optic good for $\approx$ 100 km

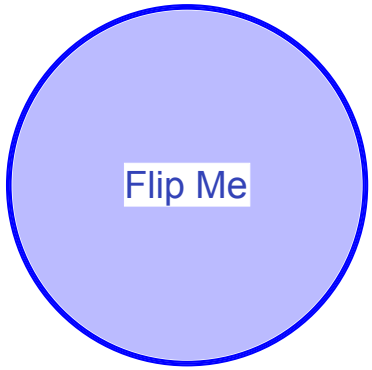
  free space, e.g, ground to satellite better

- Gisin (Geneva) sells to casinos as random number generators

(John) Bell's Cell Phone Puzzle







- Coins seem fair, win half the time Compare with friend
- If Alice and Bob pick same color, one wins (H) – other loses (T)

  BUT can't exploit – phone locked – no messages until after choice is made. Many possible explanations
- If Alice and Bob pick different colors, expect no correlations

	A	Red	H	H	T	T
But Actual	B	**Green**	H	T	H	T
	prob		$\frac{3}{8}$	$\frac{1}{8}$	$\frac{1}{8}$	$\frac{3}{8}$

First Bell Inequality Violation

- A and B pick same color, one H – other T Prob $= 1$
- A and B pick different colors, one H – other H Prob $= \frac{3}{8}$

When Bob gets H, Alice assumes Bob's coin is T on her side

Pick		Alice's side			Prob
A	B	R	G	B	
R	G	H	T		3/8
G	B		H	T	3/8
B	R	T		H	3/8

Bell: 3 mutually exclusive events $\Rightarrow$ sum of probabilities is ≤ 1.

Violation: But observed Probability $\frac{3}{8} + \frac{3}{8} + \frac{3}{8} = \frac{9}{8} > 1$

Can you Explain? Come back in 3 weeks, March 27

Will review basics – accessible if missed today – also post slides

Further Reading

- N .D. Mermin *Boojums All the Way Through* (Cambridge, 1990)

delightful collection of essays, including some on Q.M.

- D. Wick *The Infamous Boundary* (Birkhaüser, 1995)

history of Bell ineq. with Appendix on Probability by W. Faris

- N .D. Mermin *Quantum Information Science* (Cambridge, 2007)

- B. Schumacher and M. Westmoreland *Quantum Processes, Systems, and Information* (Cambridge, 2010)

excellent introductory text written for undergraduates