

Quantum Computing

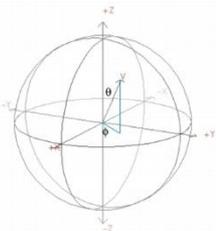
Bob Senser

CSC 4034

Fall 2014

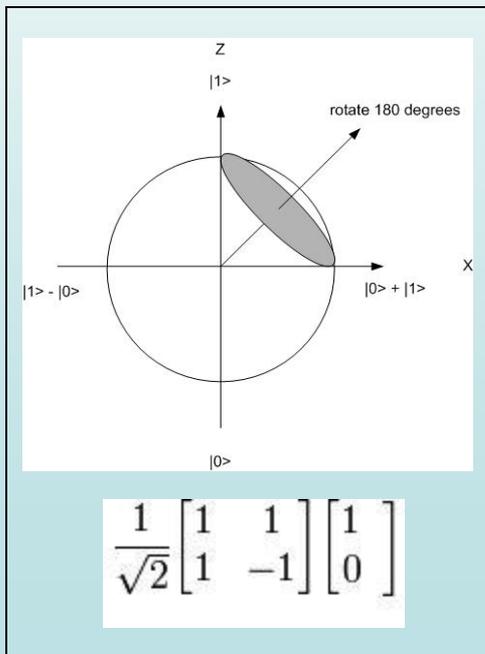
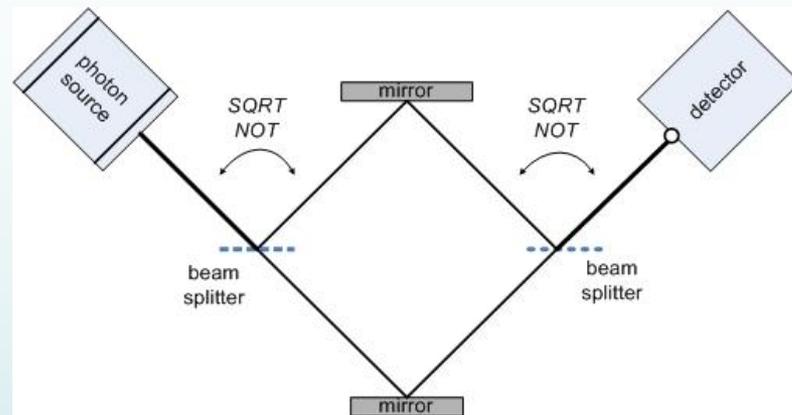
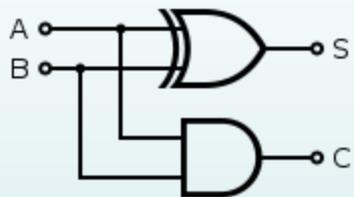
Quantum Computing

Overview of Presentation Topics



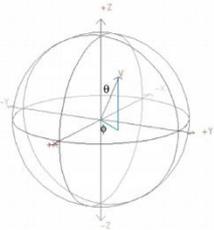
Terms:

Measurement
Qubit
Superposition
etc.



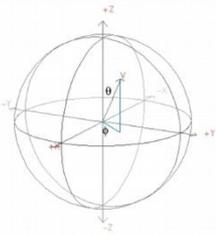
Init_state(2)
H(1)
 $m = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
U(m, 1)
cnot(1, 2)
.....

Look at quantum computing from C.S.
theory point of view:
Change halting problem?
Answer to "P versus NP?"
Impact NP-Complete?



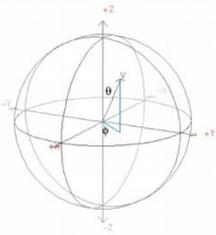
Quantum Computing

- Presentation topics:
 - Terminology of Quantum Computing (“QC”)
 - Quick comparison of the digital, analog and QC technologies
 - List of QC algorithms, and a look at one algorithm
 - QC “reality check”
 - QC impact on Computer Science Theory
 - Wrap up and questions
- Presentation omissions:
 - Quantum encryption/security, teleportation
 - Universal quantum logic gates
 - Higher-level mathematics of quantum physics
 - Quantum error detection/correction
 - Quantum annealing



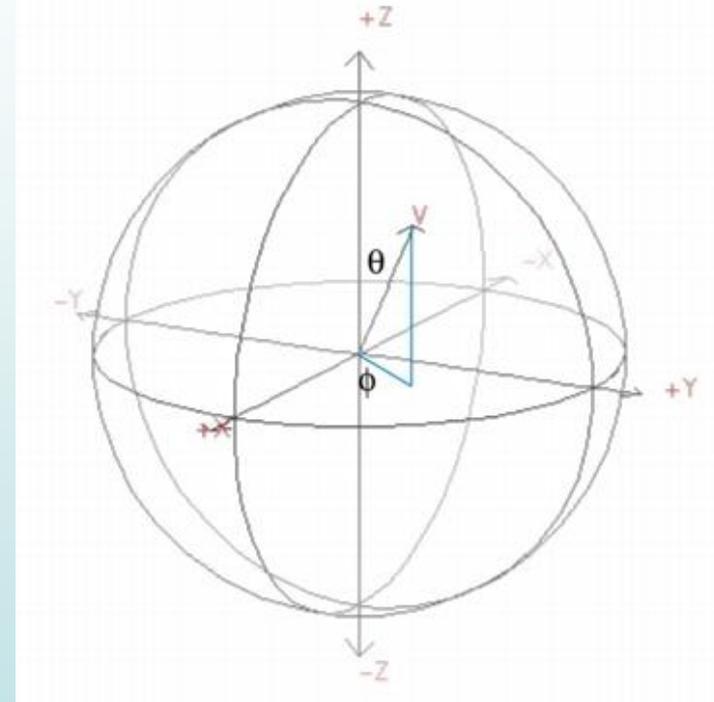
Quantum Computing, Some Basic Questions

- In the abstract, can Quantum Computing (“QC”) perform processing/computations?
- Is QC viable? Similar questions: Is QC useful? Does the use of QC ‘make sense?’
- Are there quantum computers available today?
- Does QC have a significant impact on C.S. with the “P versus NP” problem or with the solution of “NP-Complete” problems?

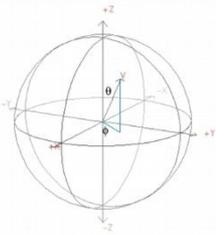


← This is a “Bloch Sphere.”

- The Bloch Sphere is a QC presentation showing the “the pure state space of a 1 qubit quantum register.”
- A qubit is a quantum bit.
- The vector to V is length 1 and its X , Y , Z coordinates provide the ‘probability amplitudes’ for the qubit.
- Qubit also shown in $[0 \ 1]^T$ or $|1\rangle$ format.

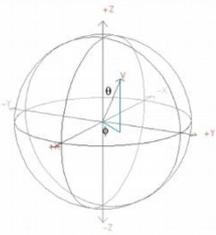


Note: We will cover QC terms, like “qubit,” in just a few more slides.



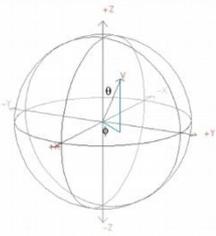
Quantum Computing

- What is Quantum Computing?
 - It is computation done using quantum hardware components.
 - The Heisenberg Uncertainty Principle applies:
 - Certain pairs of physical properties, like position and momentum, cannot both be known to arbitrary precision.
 - Measurement can cause state changes, for example the collapse of a wave function.
 - Before measurement we speak of probabilities, after measurement we speak of binary values: $|0\rangle$ and $|1\rangle$. The QC behavior is “irreducibly random.”



Some Key People in QC

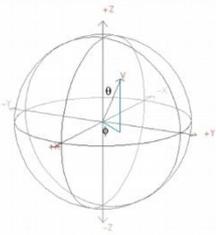
- Richard Feynman - Physicist
 - Presented a solid justification for QC in his 1981 paper.
 - Saw that the simulation of quantum mechanics could be a high-value use of QC.
- David Deutsch - Physicist
 - Championed the *multiverse* (multiple universe, many-worlds) view of *superposition*.
 - Produced some of the first significant QC algorithms. We will briefly look at his first algorithm.



Terminology of QC

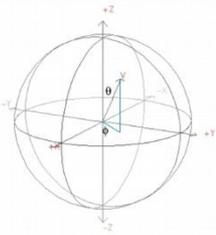
(and some basic quantum mechanics)

- Qubit
 - A quantum “bit” of information.
 - Often based on particle’s polarization or spin.
 - When measured, the qubit will have one of two values.
 - Before measurement, qubit state is viewed as a complex number, a “probability amplitude.”
 - Common ways to express or view a qubit’s state:
 - Bloch sphere
 - 2 x 1 matrix view; examples: $[0, 1]^T$, $[1, 0]^T$, $[\text{SQRT}(2)/2, \text{SQRT}(2)/2]^T$
 - Dirac “bra-ket” notion; “ket” examples: $|1\rangle$, $|0\rangle$, $\alpha|0\rangle + \beta|1\rangle$
 - Note: one particle can represent two qubits by utilizing both polarization and spin.



Describing Qubit Values

- With Bloch Sphere
 - Value $|1\rangle$ is triplet: X: 0, Y: 0, Z: -1
 - Value $|0\rangle$ is triplet: X: 0, Y: 0, Z: 1
 - Note: These X, Y, Z values are *probability amplitude* components.
- With Matrices
 - $|0\rangle$ is $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$
 - $|1\rangle$ is $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$
 - $H(|1\rangle)$ is $\begin{pmatrix} .5 & -.5 \\ -.5 & .5 \end{pmatrix}$ Note: H() is a Hadamard gate and this value is in “superposition.”



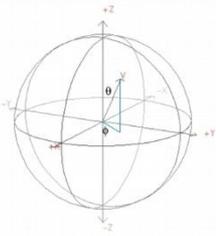
Terminology of QC

(and some basic quantum mechanics)

Needed: “*A willing suspension of disbelief.*”

This is especially true for *Superposition* and *Entanglement*.

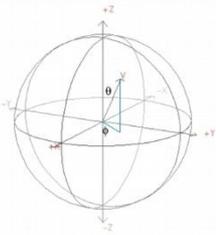
- Quantum Behaviors
 - No-Cloning Theorem
 - Probability Amplitudes
 - Reversibility
- Qubit States
 - Measurement
 - Transformations
 - *Superposition*
 - *Entanglement*
 - Decoherence



Terminology of QC

(and some basic quantum mechanics)

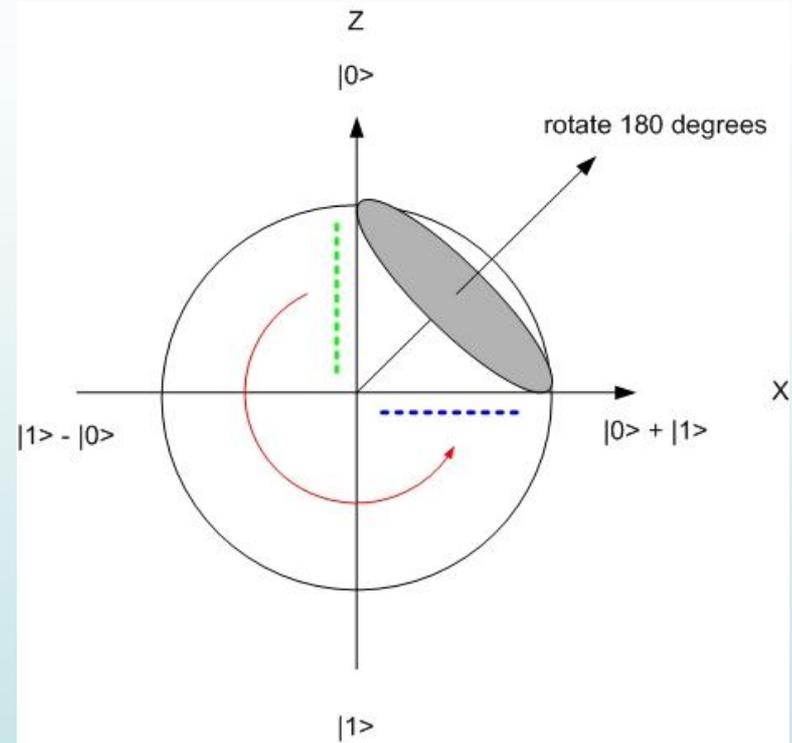
- Measurement
 - Observing the state of the qubit.
 - Measurement always results in one of two results: $|0\rangle$ or $|1\rangle$.
 - Result depends on the probability amplitudes.
 - Measurement might change the state of the qubit.
- Probability Amplitudes
 - Complex number associated with a qubit.
 - These amplitudes can be negative!
 - Summing the squares of the absolute values = 1.
 - In simple terms: Probability amplitudes determine the behavior/value of the qubit.



Terminology of QC

(and some basic quantum mechanics)

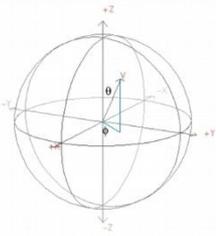
- Transformations/Evolutions
 - Application of a “rotation” or phase shift to a qubit.
 - This is not measurement!
 - Can be viewed as matrix multiplication.
- Quantum Programming is done with these transformations!



“Hadamard” Transformation.

Const.	Trans	Qubit
Value	Matrix	Value

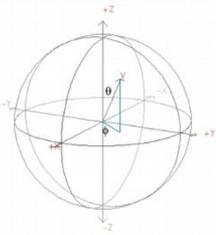
$$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$



Terminology of QC

(and some basic quantum mechanics)

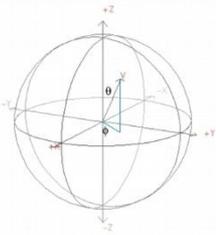
- Superposition (“multiverse”)
 - A phenomenon where an object exists in more than one state simultaneously.
 - Enables qubits to have simultaneous values.
 - In simple terms: In this state, a qubit can be $|0\rangle$ and $|1\rangle$ at the same time (but we cannot view this).
- Entanglement
 - The quantum states of the involved objects are linked together so that one object can no longer be adequately described without full mention of its counterpart.
 - In simple terms: Changing one object changes the other; they are “linked” even if physically separated.



Terminology of QC

(and some basic quantum mechanics)

- Decoherence
 - Untangling of quantum states to produce a single reality.
 - This “untangling” or collapse may occur prematurely.
 - In QC, decoherence may require error correction.
 - In simple terms: Quantum state collapses to one value. Can be viewed as premature measurement.

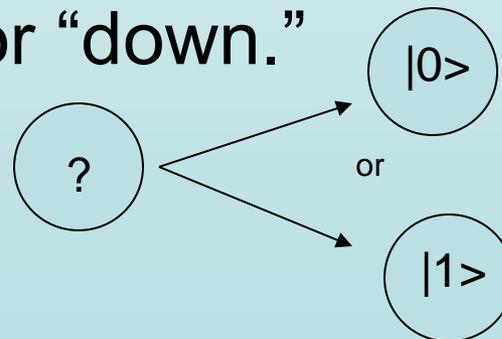


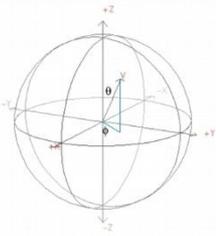
Terminology of QC

(and some basic quantum mechanics)

- Polarization and Spin

- These are two, of many, quantum characteristics that can be used to encode information.
- Polarization refers to the polarity of light.
- Spin refers to a measurable characteristic of quantum particles/waves, usually expressed, at measurement, as “up” or “down.”

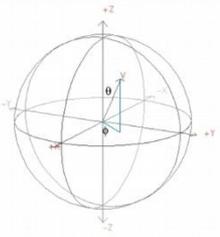




Terminology of QC

(and some basic quantum mechanics)

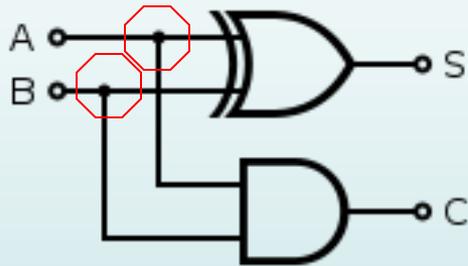
- No-Cloning Theorem
 - Qubits cannot be directly copied.
 - In simple terms: cannot code “qubit1 = qubit2;” in a QC environment.
 - How to debug errors, if can’t copy or measure intermediate results??
- Reversibility (Landauer’s principle)
 - Quantum actions are reversible.
 - In simple terms: Quantum logic gates have an equal number of inputs and outputs.
 - Note: Measurement is not reversible.



Computer Hardware/Circuits

(Digital and Analog Examples)

Digital Computer Circuit

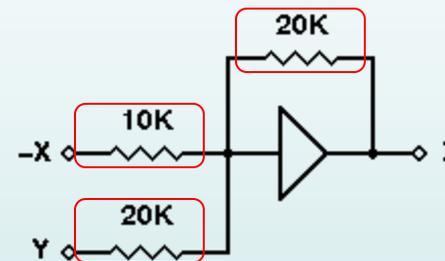


Half Adder:

$$S = A \text{ xor } B$$

$$C = A \text{ and } B$$

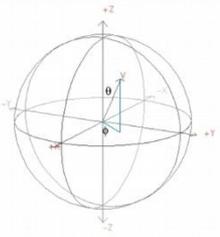
Analog Computer Circuit



$$\text{Voltage: } Z = 2X - Y$$

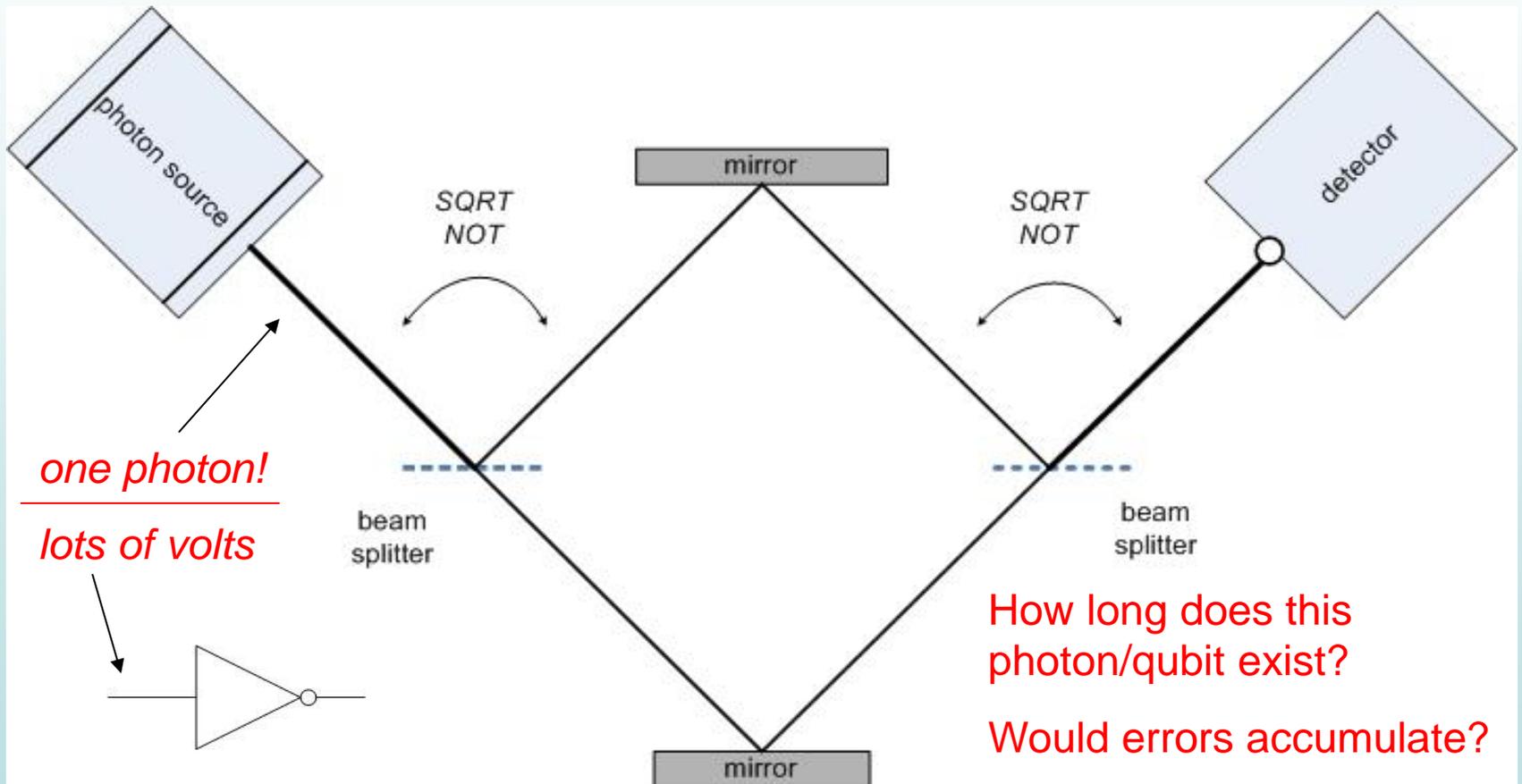
Comments:

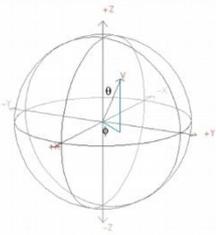
- Half Adder clones the values of pin A and pin B.
- Analog circuits tend to accumulate errors.



Computer Hardware/Circuits

QC Hardware: NOT "Gate" (Pauli-X)





Values in Bits and Qubits

3-Bit Register

value	likelihood
000	0
001	0
010	1
011	0
100	0
101	0
110	0
111	0

3-Qubit Register

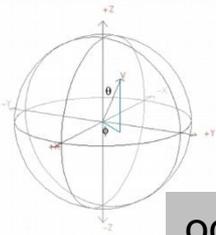
value	likelihood
000	C_0
001	C_1
010	C_2
011	C_3
100	C_4
101	C_5
110	C_6
111	C_7

Feynman's Point: Quantum values use huge amounts of "digital" resources:

- 64-bits: ~ 8 bytes
- 64-qubits: $\sim 2^{64}$ complex numbers.
- A digital calculation on two 64-qubit values in superposition is 2^{128} calculations!

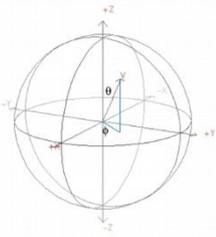
value is 010;
bit fits in < one
byte

probability of any pattern is C_p ;
qubit fits in 8 complex numbers
(~64 bytes)



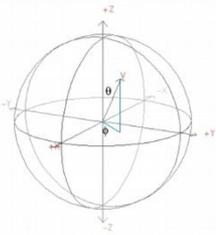
Describing Qubit Values

```
octave-3.2.3.exe:3:C:\Octave\3.2.3_gcc-4.4.0\bin\Quack!  
> init_state(1)  
octave-3.2.3.exe:4:C:\Octave\3.2.3_gcc-4.4.0\bin\Quack!  
> print_dm(1)  
  1  0  
  0  0  
octave-3.2.3.exe:5:C:\Octave\3.2.3_gcc-4.4.0\bin\Quack!  
> init_state(3)  
octave-3.2.3.exe:6:C:\Octave\3.2.3_gcc-4.4.0\bin\Quack!  
> print_dm(3)  
  1  0  0  0  0  0  0  0  
  0  0  0  0  0  0  0  0  
  0  0  0  0  0  0  0  0  
  0  0  0  0  0  0  0  0  
  0  0  0  0  0  0  0  0  
  0  0  0  0  0  0  0  0  
  0  0  0  0  0  0  0  0  
  0  0  0  0  0  0  0  0  
octave-3.2.3.exe:7:C:\Octave\3.2.3_gcc-4.4.0\bin\Quack!  
>
```



Quantum Hardware

- The quantum hardware qubits are maintained in different ways, here are two:
 - Particle stream
 - Particle moves through quantum gates between a source and detector.
 - Qubit is a characteristic of the particle: polarization or spin.
 - Quantum dot
 - Particle is stationary.
 - Qubit is represented by a characteristic of the particle: polarization, electron orbit or spin.



Quantum Logic Gates

- SQUARE-ROOT-OF-NOT

- We saw this earlier: QC Hardware: NOT “Gate.”

- Evolution: $1/(2^{1/2}) \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$

- Done twice is a NOT operation.

- Hadamard (“H gate”), symbol:

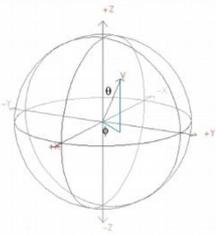


- We will see this used.

- Puts a qubit into a state of superposition.

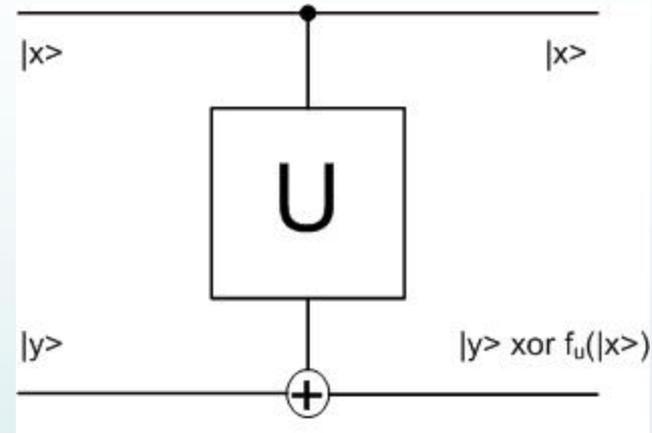
- Evolution: $1/(2^{1/2}) \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

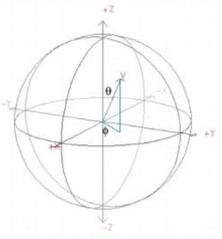
- Done twice returns original state.



Quantum Logic Gates

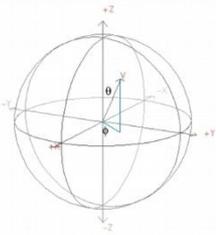
- C-NOT, symbol:
 - We will see this used.
 - $|x\rangle$ controls behavior of the output.
 - Observation: If $|y\rangle$ is zero then output is $f_u(|x\rangle)$; ‘xor’ operation acts like a copy.
 - But wait, what about the *No-Cloning Theorem*?
 - This is not actually a clone or copy.
 - $|x\rangle$ output is now entangled with $|y\rangle$!!





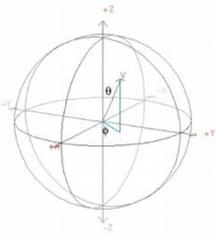
Quantum Logic Gates

- Some other common quantum gates:
 - Toffoli:
 - Similar to C-NOT, but with two control inputs
 - 3 input and 3 outputs
 - outputs: $|x\rangle$, $|y\rangle$, and $(|(z \text{ xor } (x \text{ and } y))\rangle$
 - Pauli-X, Pauli-Y, Pauli-Z:
 - Rotations about X, Y, or Z axis.
 - Pauli-X is a “NOT” operation.



Famous QC Algorithms

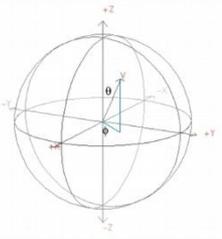
- Deutsch's Algorithm (1985/1992)
 - First “useful” QC algorithm.
 - Very contrived financial problem.
 - We will see this algorithm digitally simulated.
- Grover's Search Algorithm (1997)
 - Searches an unordered list in $O(N^{1/2})$ time.
 - Non-quantum algorithm takes $O(N/2)$ time.
- Shor's Factoring Algorithm (1994)
 - Integer factoring of numbers.
 - Uses periodicity (“mod”) and Fourier Transform.
 - In 2001, demonstrated by IBM researchers using NMR-based hardware with 7 qubits.



Deutsch's Algorithm

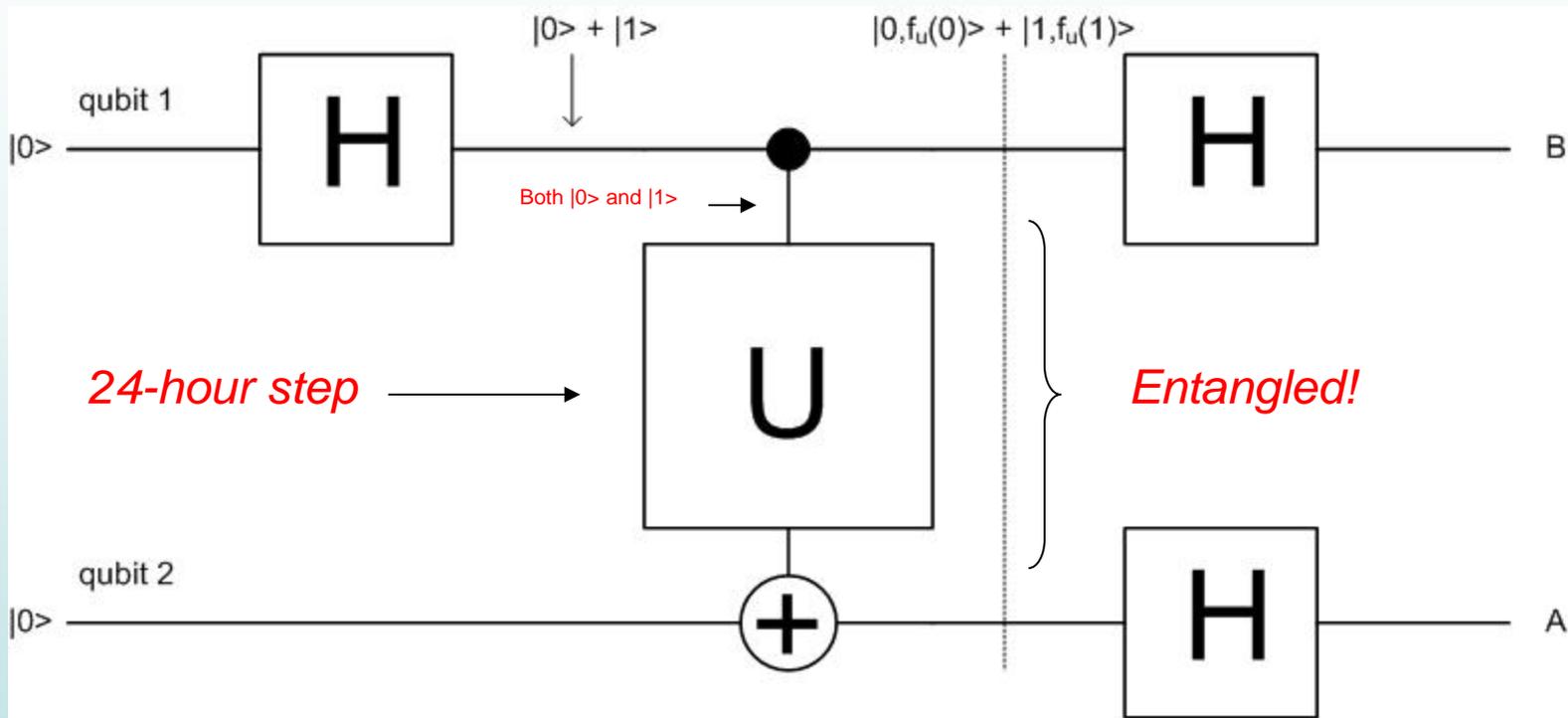
(Briefly look at and simulate Deutsch's Algorithm)

- The contrived problem:
 - Have a financial “algorithm” that runs for 24 hours; run it twice to get a recommendation.
 - The final result is Exclusive-OR (XOR) of the two runs, each with a different input.
 - A digital computer needs 48 ($2 * 24$) hours.
 - Results are needed in 24 hours.
 - If the binary results of each run match, we act.
 - “Act” could be buy stock, sell stock, etc.



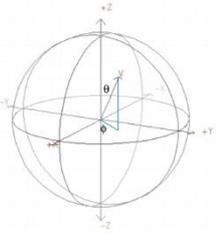
Deutsch's Algorithm

(Perhaps better titled: Deutsch's Circuit)



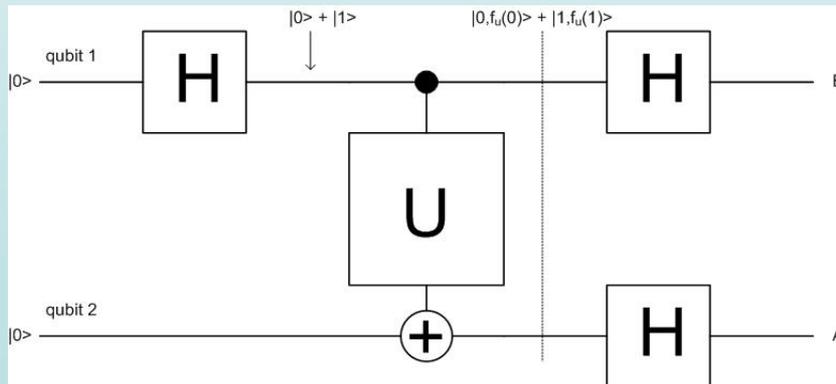
A: Measure first; if zero then inconclusive else measure B.

B: Measure second; if 0 then f is same; if 1 then f is different.



Deutsch's Algorithm

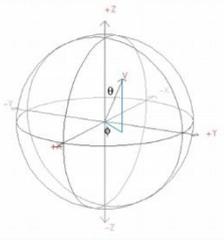
- My goal: To simulate the execution of Deutsch's algorithm. /* my quantum "Hello world" program... */
- Done using MatLab (Octave) and "Quack!"
- Quack! is a quantum computer simulator for MATLAB, by Peter P. Rohde, University of Queensland, Brisbane, Australia.
- This simulator made it possible to get some "hands on" experience with quantum computer programming.



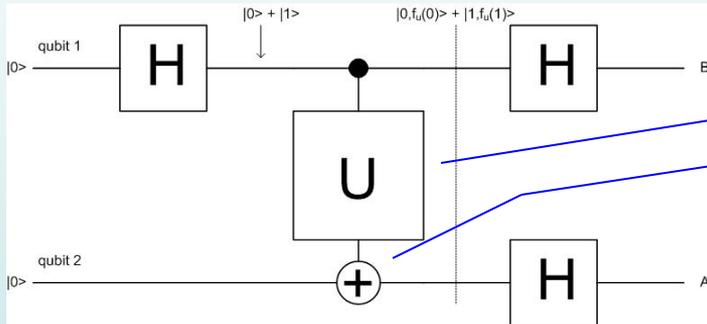
```

Init_state(2)
H(1)
m=[1 0; 0 -1]
U(m,1)
cnot(1,2)
.....

```

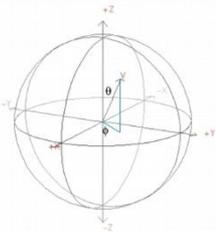


Quack! & Deutsch Algorithm



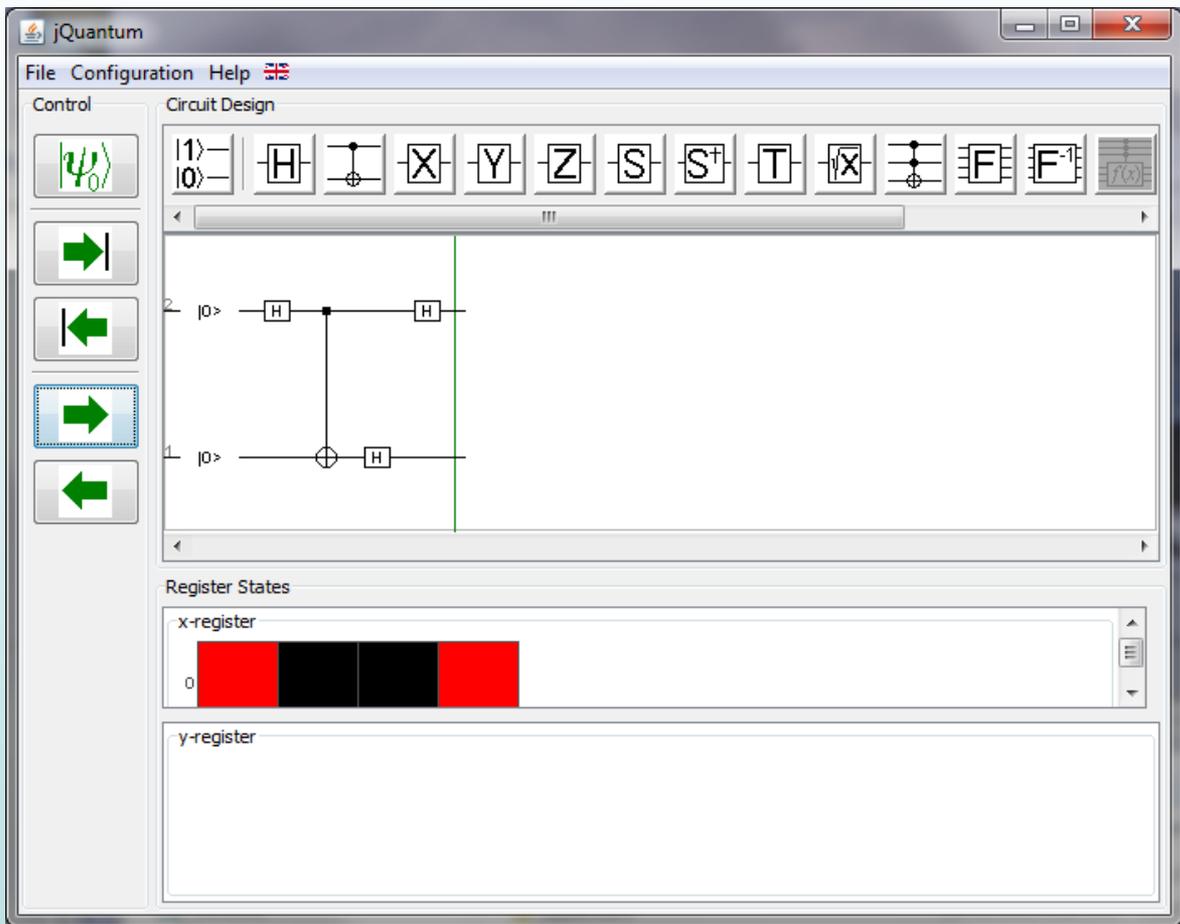
```
# Dcase3.m:
init_state(2)
H(1)
# f(i) = 0
m=[1 0 ; 0 -1]
U(m,1)
cnot(1,2)
H(1)
H(2)
disp('bit2:')
Z_measure(2)
disp('bit1:')
Z_measure(1)
```

```
> source Dcase3.m
m =
     1     0
     0    -1
bit2:
ans = 1    is: |0>
bit1:
ans = -1   is: |1>
```

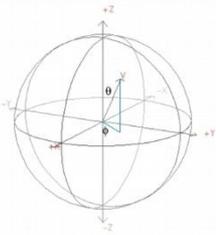


jQuantum

<http://jqquantum.sourceforge.net/>

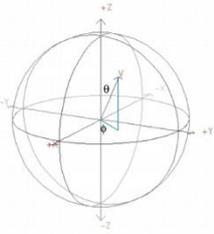


*As of 2014, “Quack!”
is no longer available,
here is a look at:
“jQuantum”*



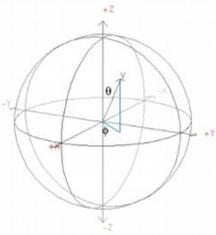
Feynman's QC Vision

- Solving Quantum Mechanics problems with Quantum Computing.
- What's the problem? The “tensor product;” the explosion of terms.
- In Octave (like MATLAB), using “Quack!”
 - `init_state(12)` creates 12 qubits.
 - `init_state(16)` exhausts memory!
- But how much measurable “information” is there in N qubits? Exactly N bits!



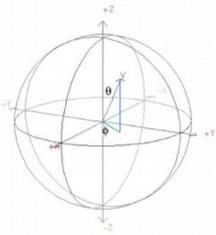
QC Personal Observations

- Before we talk about QC and Computer Science, here are my personal observations:
 - QC algorithms are not easy to understand and produce.
 - QC does not appear to scale well.
 - Scaling from 4 to 32 qubits is not easily done.
 - Quantum gates in serial might accumulate errors.
 - QC is probability-based, so it may not be sufficiently precise.
 - QC appears useful mainly in very specialized cases.
 - Creation of “Oracles.”
 - Simulation of quantum systems.
 - QC is likely to become real – but not anytime soon.
 - ENIAC, early digital computer (1946), vacuum tube-based, estimated MTF: 10 minutes; reality: nonfunctional about half the time. The invention of the transistor enabled the practical digital computer.
 - Observation: NSA, RSA, etc. do not appear concerned about QC breaking current security schemes.



“Hype” associated with QC

- There is ample “hype” associated with QC.
 - The notion of qubit registers holding “infinite information” is expressed, common in the popular press. This notion is wrong! N qubits hold N bits.
 - The multiverse concept appears in movies and TV, for example as parallel universes in *Star Trek, etc.*
 - Superposition is on a very small scale.
 - Decoherence tends to occur with any environmental interactions.
 - Some people suggest that QC will show $P=NP$ or solve NP-Complete problems. This is our next topic.



Halting Problem

- Nothing to do with QC: Will these halt?

$n = 2$

```
for i=1 to infinity;
  for j=1 to infinity;
    for k=1 to infinity;
      if ( $i^n == j^n + k^n$ ) exit;
```

$n = 3$

```
for i=1 to infinity;
  for j=1 to infinity;
    for k=1 to infinity;
      if ( $i^n == j^n + k^n$ ) exit;
```

Assume all i, j, k : first 1,000 values are tried, then values $< 10^6$ are tried, etc. What problem/theorem are these related to?

Fermat's Last Theorem!

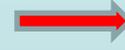
$n = 3$

```
for i=1 to 1000;
  for j=1 to 1000;
    for k=1 to 1000;
      if ( $i^n == j^n + k^n$ ) exit;
```



$n = 3$

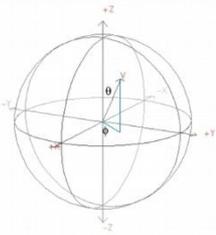
```
for i=1 to 1000000;
  for j=1 to 1000000;
    for k=1 to 1000000;
      if ( $i^n == j^n + k^n$ ) exit;
```



$n = 3$

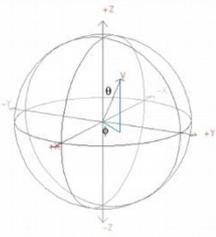
```
for i=1 to  $10^9$ ;
  for j=1 to  $10^9$ ;
    for k=1 to  $10^9$ ;
      if ( $i^n == j^n + k^n$ ) exit;
```





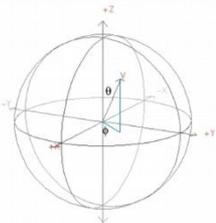
QC in 2014

- What has changed recently with QC?
 - When I walk through *Best Buy*, I do not see any quantum computers.
 - To the best of my knowledge, no new major quantum computer companies have formed.
 - But, progress has occurred.
 - Let's review 2010, 2012, and then look at 2014.



QC Realities

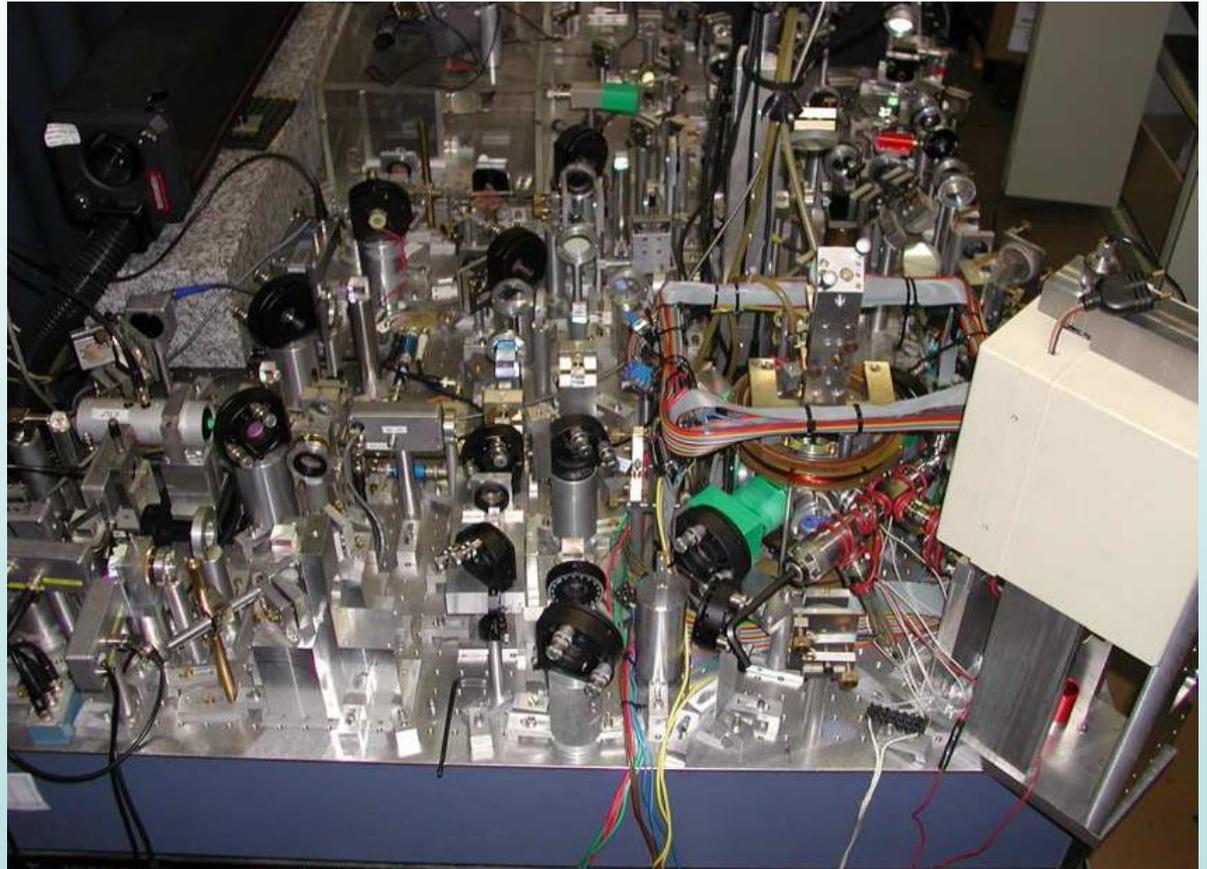
- 2010 Status
 - Commercial QC computer attempt in 2007
 - D-Wave Company, claimed 16 qubits.
 - A register of 8 to 12 qubits is “noteworthy.”
 - Shor actually factored 15 into 3 and 5!
 - Losing coherence at 1.2 seconds is news.
- 2012 Status
 - Factored 143 ($11 \cdot 13$) using quantum computing.
 - D-wave: claims 84 qubits. Sells a 128-qubit for \$10M.
 - IBM has produced a three-qubit chip.
 - Single atom transistor, has quantum behaviors.

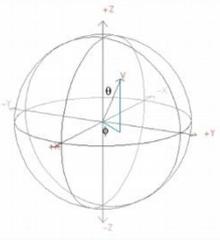


QC 2010 Realities

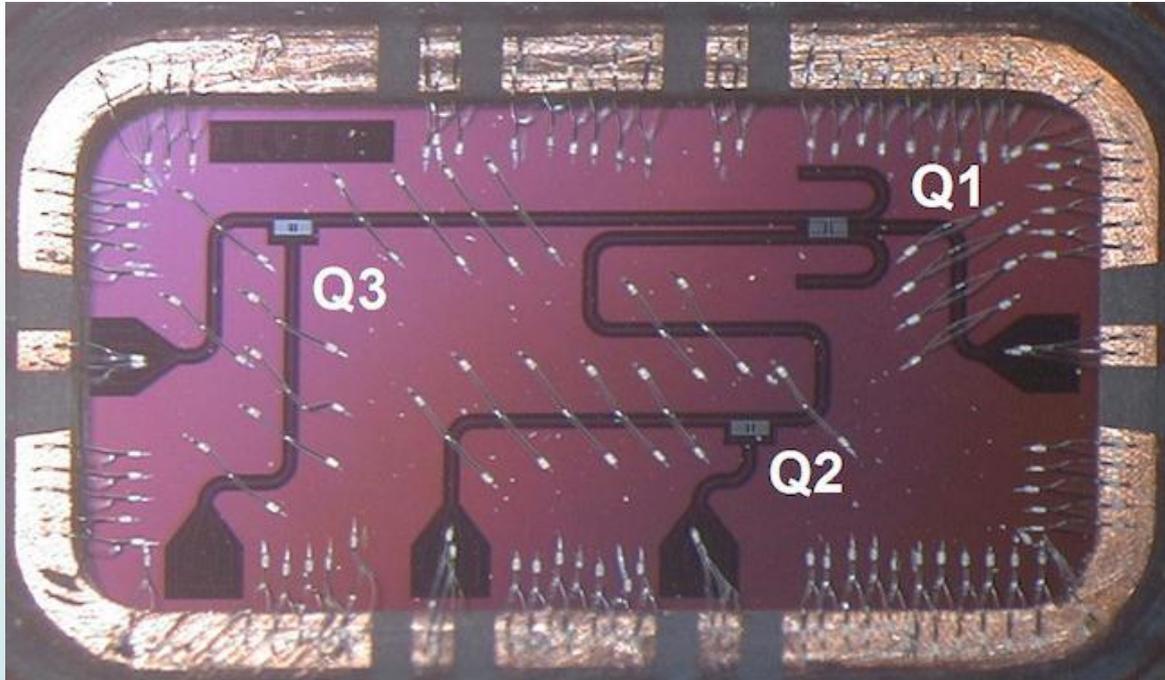
- No commercial QC computers existed!

2010 lab picture of a large quantum circuit using laser-beam based gates:



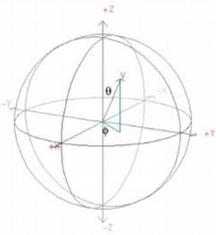


IBM 3-qubit Chip



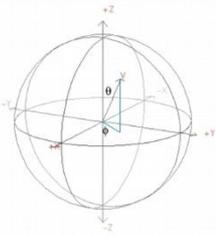
“IBM’s team has also built a “controlled NOT gate” with traditional two-dimensional qubits, meaning they can flip the state of one qubit depending on the state of the other. This too is essential to building a practical quantum computer, and Steffen says his team can successfully flip that state 95 percent of the time — thanks to a decoherence time of about 10 microseconds.”

source: <http://www.wired.com/wiredenterprise/2012/02/ibm-quantum-milestone/>



QC 2014 Realities

- Commercial QC computer 2014
 - D-Wave Company, claims 128 qubits.
 - Working with Lockheed Martin and more recently NASE and Google.
 - Direct quote: “D-Wave's architecture differs from traditional quantum computers (none of which exist in practice as of today) in that it has noisy, high error-rate qubits. It is unable to simulate a universal quantum computer and, in particular, cannot execute [Shor's algorithm](#).”
- But: uses “quantum annealing”.



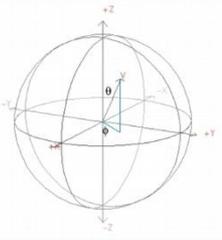
D-Wave Background

- The D-Wave company is controversial.
 - Geordie Rose is CEO.
 - Canadian company; in past, Google invested money.

“Geordie Rose has a Ph.D. in quantum physics, but he’s also a world champion in Brazilian jiu-jitsu and a Canadian national champion wrestler. That may seem like an odd combination, but this dual background makes him the perfect fit for his chosen profession.”

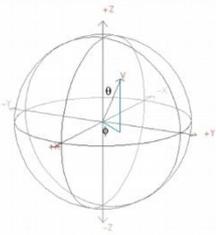
“But Rose keeps fighting. In May, D-Wave published a [paper](#) in the influential journal *Nature* that backed up at least some of its claims. And more importantly, it landed a customer. That same month, mega defense contractor Lockheed Martin bought a D-Wave quantum computer and a support contract for \$10 million.”

source: <http://www.wired.com/wiredenterprise/2012/02/dwave-quantum-cloud/>



QC Realities

- Again, Shor actually factored 15 into 3 and 5!
- A qubit taking 1.2 seconds to lose coherence makes for a significant journal article.
- Due to decoherence, error correction remains a major issue.



Wrap Up

(Thoughts about Basic Questions)

1. In the abstract, can Quantum Computing ('QC') perform processing/computations?

Yes

2. Is QC viable? Similar questions: Is QC useful? Does the use of QC 'make sense?'

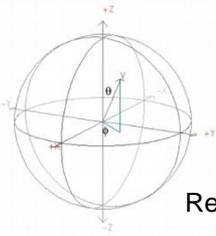
Perhaps

3. Are there quantum computers available today?

No (2010); Yes (2012), Bigger (2014), but....

4. Does QC have a significant impact on C.S. such as the "halting" problem?

What do you think?



QC References

References:

- [] Aaronson, S "The Limits of Quantum", *Scientific American*, pp 62-69, March 2008.

- [] Bacon, D., Van Dam, W. "Recent Progress in Quantum Algorithms," *Communications of the ACM*, vol 53, no 2, pp. 84-93, February 2010.

- [] Bigelow, K. Analog Addition [Internet]. www.play-hookey.com; 3/8/2010. Available from: http://www.play-hookey.com/analog/analog_addition.html.

- [] Brown, J. *The Quest for the Quantum Computer*, New York: Touchtone/Simon and Schuster, 2001.

- [] Feynman, R. "Simulating Physics with Computers," *International Journal of Theoretical Physics*, vol 21, no 6/7, 467-488, 1982.

- [] Fortnow, L. "The Status of the P versus NP Problem," *Communications of the ACM*, vol 52, number 9, pp. 78-86, September 2009.

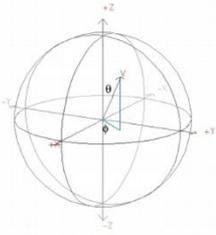
- [] Morton, J and others "Solid-state quantum memory using the ^{31}P nuclear spin," *Nature*, vol 455, pp 1085-1087, October 2008.

- [] Milburn, G. *The Feynman Processor*, New York: Helix Books, 1998.

- [] Yanofsky, N., Mannucci, M. *Quantum Computing for Computer Scientists*, Cambridge: Cambridge University Press, 2008.

- [] Wikipedia contributors, Adder (electronics) [Internet]. Wikipedia, The Free Encyclopedia; 4/1/2010. Available from: http://en.wikipedia.org/wiki/Adder_%28electronics%29.

- [] Wikipedia contributors, D-Wave (electronics) [Internet]. Wikipedia, The Free Encyclopedia; 10/22/2014. Available from: http://en.wikipedia.org/wiki/D-Wave_Systems.



QC References

Picture and Graphic Credits:

Bloch Sphere: <http://comp.uark.edu/~jgeabana/blochapps/sphere2.jpg>

Hadamard Transformation: derived from Brown, Figure 4.4, page 131.

Hadamard Matrix: derived from "Automatic Quantum Computer Programming", Lee Spector, 2007, Springer, ISBN: 978-0-387-36496-4, Sample pages:
http://www.springer.com/cda/content/document/cda_downloadaddocument/9780387364964-c2.pdf?SGWID=0-0-45-346665-p173670367_fulltextQCsim.pdf.

Digital Half Adder: http://en.wikipedia.org/wiki/Adder_%28electronics%29

Analog Computer Circuit: http://www.play-hookey.com/analog/analog_addition.html.

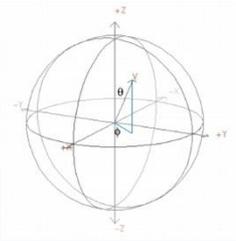
Quantum Hardware, NOT Gate (Pauli-x): derived from: Milburn, Figure 5.6, page 138.

H Gate Graphic: derived from Milburn, Figure 5.8, page 144.

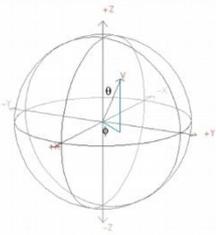
C-NOT Gate Graphic: derived from Yanofsky, Figure (6.6), page 172.

Deutsch's Algorithm Graphic: derived from Brown, Figure D-2, page 351.

Quantum Circuit Picture: <http://almaak.usc.edu/~tbrun/Course/lecture05.pdf>



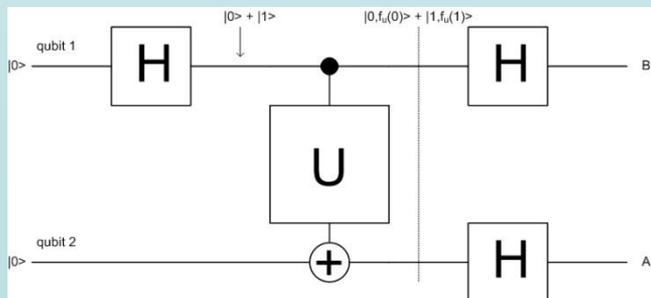
Slides Omitted for 4034



Quack! & Deutsch Algorithm

- There are 4 cases with 2 qubits: $|10\rangle$, $|01\rangle$, $|00\rangle$, $|11\rangle$.
- Each of these was run with Dcase1.m .. Dcase4.m.
- Results:

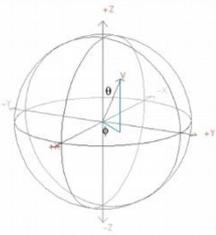
	qbits <>		qbits <>		qbits =		qbits =	
	Dcase1.m		Dcase2.m		Dcase3.m		Dcase4.m	
raw:								
bit 2	-1	1	-1	1	-1	1	-1	1
bit 1	-1	1	-1	1	1	-1	1	-1
formatted:		inconclusive		inconclusive		inconclusive		inconclusive
bit 2	$ 1\rangle$	$ 0\rangle$						
bit 1	$ 1\rangle$	$ 0\rangle$	$ 1\rangle$	$ 0\rangle$	$ 0\rangle$	$ 1\rangle$	$ 0\rangle$	$ 1\rangle$



A: Measure first; if zero then inconclusive else measure B.

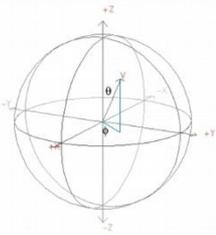
B: Measure second; if 0 then f values are the equal; if 1 then f values are not equal.

Note: We never get to see the actual $f(\text{qubit})$ results!



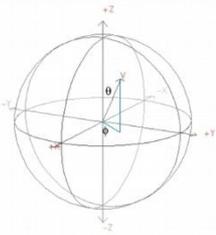
QC Impact on CS Theory

- Does quantum computing impact Computer Science theory?
 - Change the “halting problem?”
 - Have impact on the “P versus NP” problem?
 - Make NP-Complete problems “easy” to solve?
- Before looking into these questions, a review of some basic CS theory.



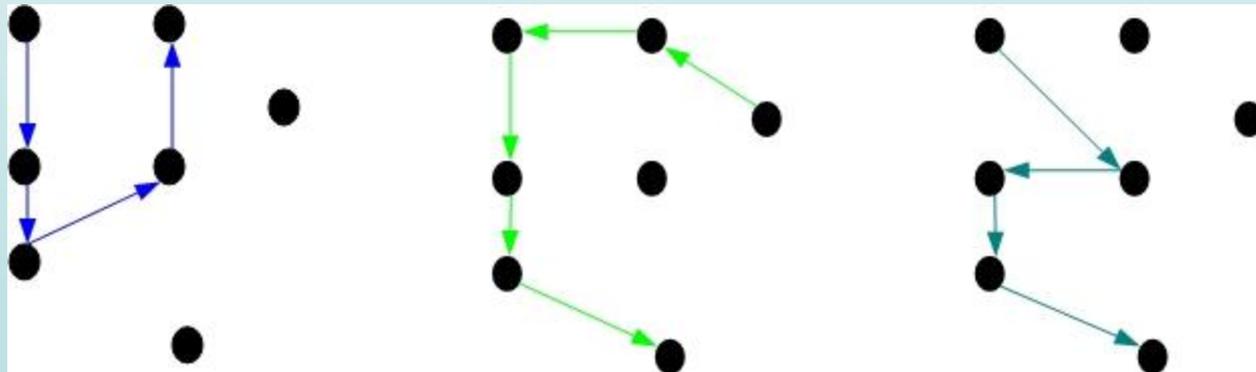
P and NP Problems

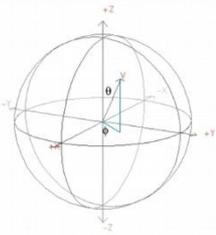
- Problems in class P (Polynomial time)
 - The class of problems with efficient solutions.
 - Solvable in polynomial time, (run time “ N^2 ” -- not “ 2^N ”).
 - Example: Find a integer in an un-ordered list of integers.
- Problems in class NP (Nondeterministic Polynomial time)
 - The class of problems that have efficiently verifiable solutions.
 - Finding solutions is not polynomial, verifying the solution is.
 - Example: “subset-sum” problem.
 - Given a set of integers, does some subset add up to zero?
 - Example data: (-2, -3, 15, 14, 7, -10)
- “P=NP” means: For problems with efficiently verifiable solutions we can also find efficient solutions. No one has yet proven this notion, “P=NP”, to be true or false.



NP-Complete Problems

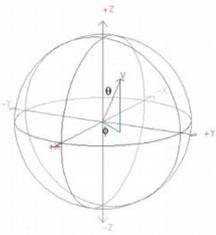
- NP-Complete problems
 - NP-Complete problems are NP problems (easy to verify, hard to solve) and are transformable into each other.
 - The satisfiability (SAT) logic problem can be transformed into any NP-Complete problem. The satisfiability problem is at least as hard as any other problem in NP.
 - If a NP-Complete problem can be solved quickly then so can every problem in class NP!
- Example: Traveling salesperson
 - Asks for the shortest distance through a set of cities.
 - Here are 3 possible solutions, each with 7 cities. Imagine 10,000 cities!





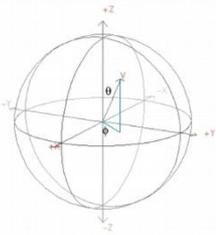
QC & P/NP/NP-Complete

- “Halting Problem” and QC
 - HP is not a constraint because of limited computational speed; it is due to a basic limit in the nature of computation itself.
 - My view: No impact.
- QC impact on “P = NP?”
 - Shor’s Factoring Algorithm does appear to break into the class of NP problems.
 - For some classes of problems, like Feynman’s quantum mechanics issues, it appears that QC can drastically increase computational speed.



QC & P/NP/NP-Complete

- Impact on solving NP-Complete problems.
 - Many NP-Complete problems are non-optimally solved today using heuristics & hybrid solutions based on statistics, trial and error, and brute force. Today there often exist “good enough,” non-optimal solutions.
 - My view:
 - It is not clear that QC brings forth something new for solving the NP-Complete problems.
 - In addition, solving problems in terms of manipulating probability amplitudes makes for very complex algorithms.
 - Trying to use classic digital gates, circuits, and algorithms causes an “explosion” in the number qubits, due to non-cloning and reversibility, and this makes classic digital processing in QC impractical. Likely that practical quantum computers will be linked with digital computers.



Wrap Up

(Thoughts about Basic Questions)

1. In the abstract, can Quantum Computing ('QC') perform processing/computations?

Yes

2. Is QC viable? Similar questions: Is QC useful? Does the use of QC 'make sense?'

Perhaps

3. Are there quantum computers available today?

No (2010); Yes (2012), Bigger (2014), but....

4. Does QC have a significant impact on C.S. such as the "P versus NP" question or the solution of "NP-Complete" problems?

What do you think?