The Shifting Paradigm of Quantum Computing

Presented at the Nov 2005

Annual Dallas Mensa Gathering

By Douglas Matzke, Ph.D.

doug@QuantumDoug.com

http://www.QuantumDoug.com

Abstract

Quantum computing has shown to efficiently solve problems that classical computers are unable to solve. Quantum computers represent information using phase states in high dimensional spaces, which produces the two fundamental quantum properties of superposition and entanglement.

This talk introduces these concepts in plain-speak and discusses how this leads to a paradigm shift of thinking "outside the classical computing box".

Biography

Doug Matzke has been researching the limits of computing for over twenty years. These interests led him to investigating the area of quantum computing and earning a Ph.D. in May 2001. In his thirty year career, he has hosted two workshops on physics and computation (PhysComp92 and (PhysComp94), he has contributed to 15 patent disclosures and over thirty papers/talks (see his papers on QuantumDoug.com). He is an enthusiastic and thought provoking speaker.

Outline

- Classical Bits
  - Distinguishability, Mutual Exclusion, co-occurrence, co-exclusion
  - Reversibility and unitary operators
- Quantum Bits – Qubits
  - Orthogonal Phase States
  - Superposition
  - Measurement and singular operators
  - Noise – Pauli Spin Matrices
- Quantum Registers
  - Entanglement and coherence
- Entangled Bits – Ebits
  - Bell and Magic States
  - Bell Operator
- Quantum Algorithms
  - Shor's algorithm
  - Grover's Algorithm
- Quantum Communication
  - Quantum Cryptography
- Summary

Classical Bits

A single coin with two sides or states.			
	$= 1$ $= \text{On}$		$= 0$ $= \text{Off}$
Coin #1 Heads state		Coin #1 Tails state	

$\uparrow^{+}$ $\rightarrow^{+}$	$= +1 = +$	$\downarrow_{-}$ $\overset{-}{\leftarrow}$	$= -1 = -$

Alternate vector notations for multiple coins!!!

Classical Information

Distinguishability

- **Definition:** Individual items are identifiable
  - Coins, photons, electrons etc are *not* distinguishable
  - Groups of objects described using statistics

Mutual Exclusion (mutex)

- **Definition:** Some state excludes another state
  - Coin lands on heads or tails but not both
  - Faces point in opposite directions in vector notation

Coin Demonstration: Act I

Setup:

Person stands with both hands behind back

Act I part A:

Person shows hand containing a coin then hides it again

Act I part B:

Person again shows a coin (indistinguishable from 1^{st})

Act I part C:

Person asks: “How many coins do I have?”

Represents one bit: either has 1 coin or has >1 coin

Coin Demonstration (cont)

Act II:

Person holds out hand showing two identical coins

Received one bit since ambiguity resolved!

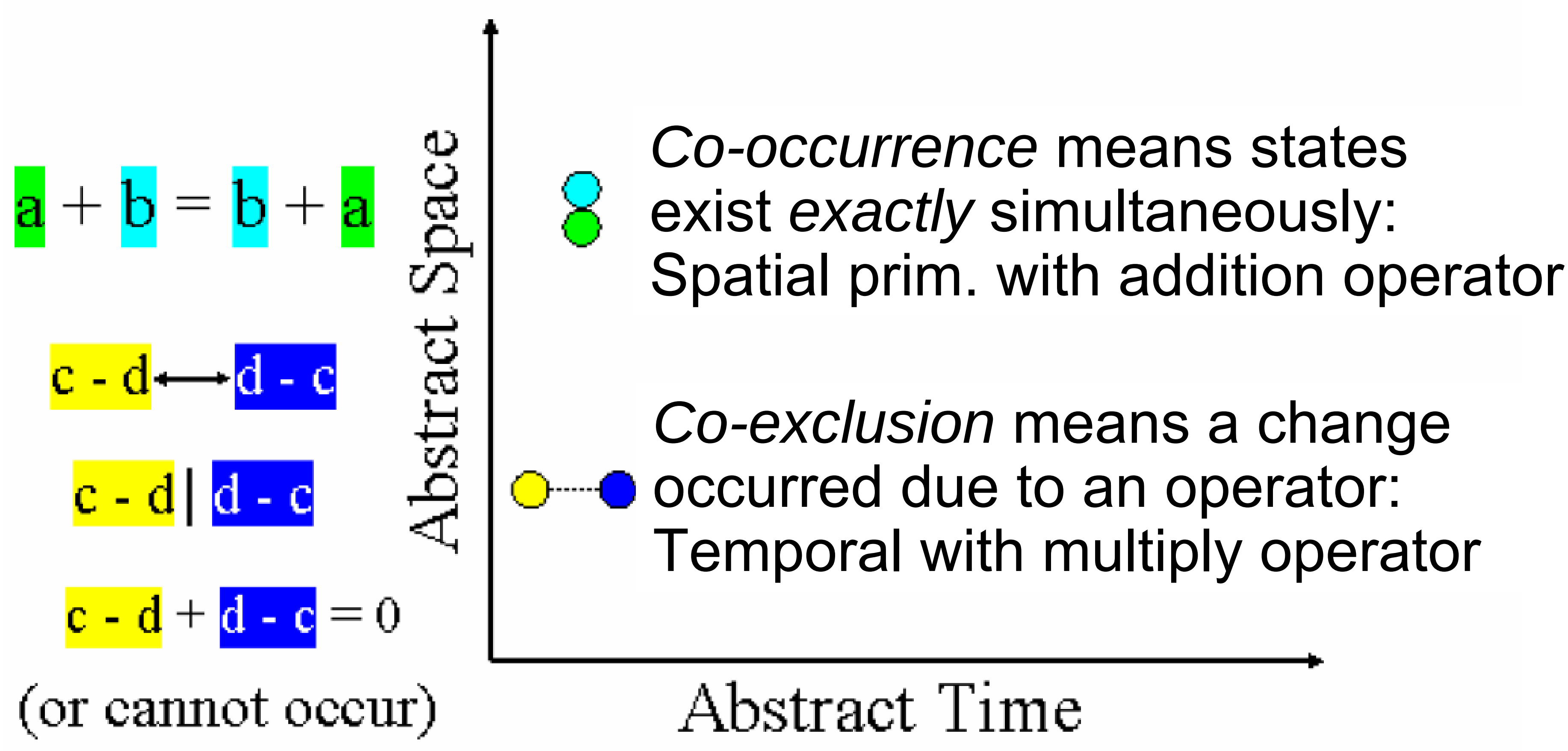
Act III:

Asks: "*Where* did the bit of information come from?"

Answer: *Simultaneous* presence of the 2 coins!

Related to simultaneity and synchronization!

Space and Time Ideas

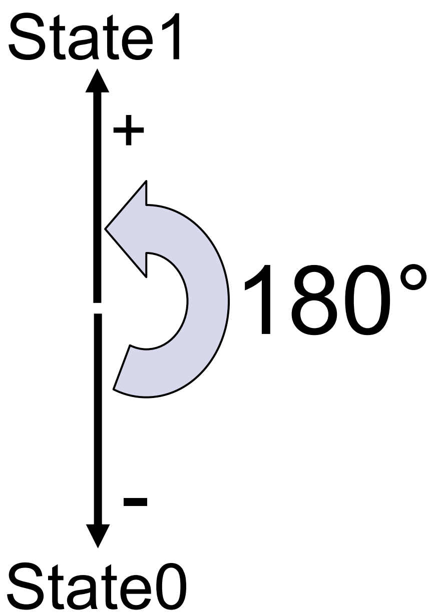


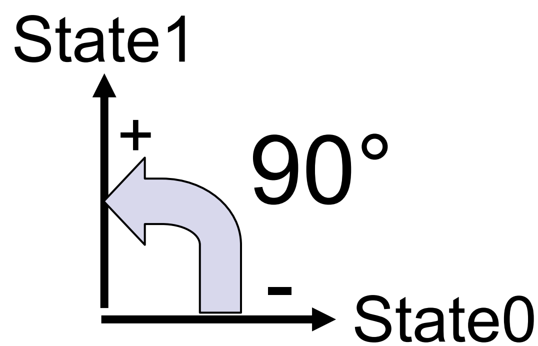
* see definitions in my dissertation but originated with Manthey

Quantum Bits – Qubits

Classical bit states: Mutual Exclusive

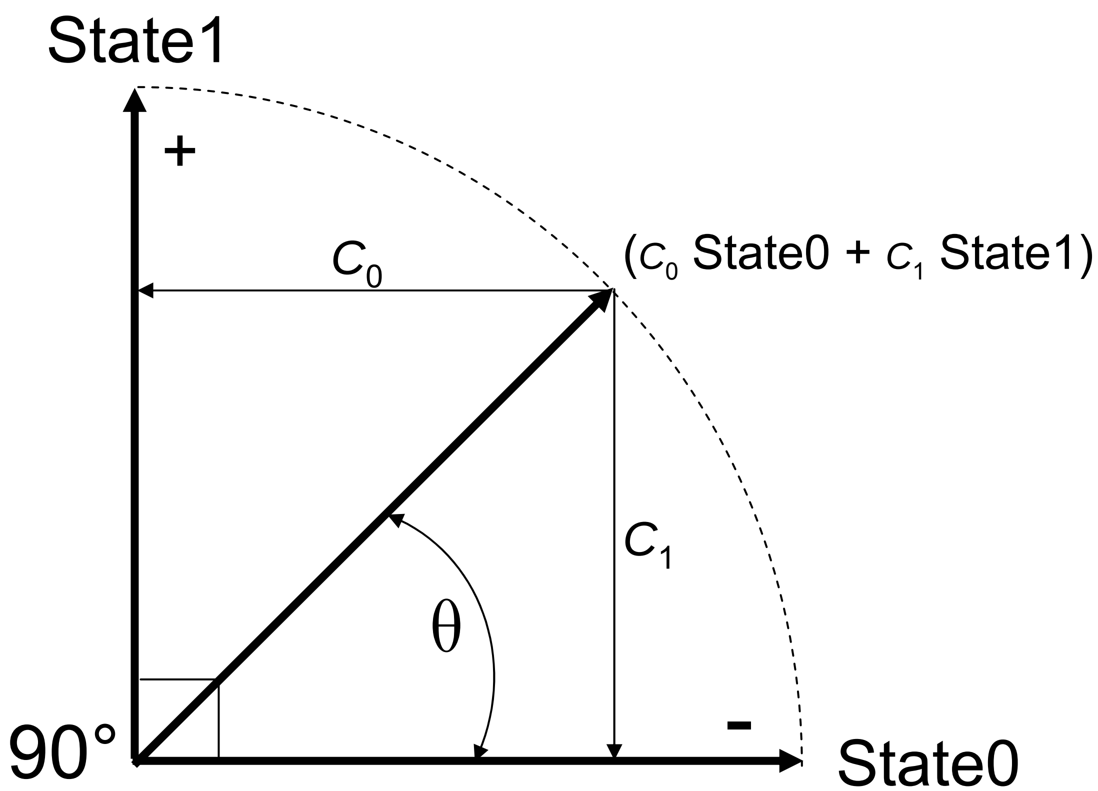
Quantum bit states: Orthogonal





Qubits states are called spin ½

Phases & Superposition



$$state0 = |0\rangle = \begin{bmatrix}1\\0\end{bmatrix}$$

$$state1 = |1\rangle = \begin{bmatrix}0\\1\end{bmatrix}$$

For θ = 45°

$$c_0 = c_1 = \sqrt{\frac{1}{2}}$$

Unitarity Constraint is $1 = \sum c_i^2 = \sum p_i$

Classical vs. Quantum

Topic	Classical	Quantum
Bits	Binary values 0/1	Qubits $c_0\|0\rangle + c_1\|1\rangle$
States	Mutually exclusive	Linearly independ.
Operators	Nand/Nor gates	Matrix Multiply
Reversibility	Toffoli/Fredkin gate	Qubits are unitary
Measurement	Deterministic	Probabilistic
Superposition	*Code division mlpx*	Mixtures of $\|0\rangle$ & $\|1\rangle$
Entanglement	*none*	Ebits $c_0\|00\rangle + c_1\|11\rangle$

Hilbert Space Notation

- Qubit

q0 $\qquad$ q1

$c_0\,|0\rangle + c_1\,|1\rangle \qquad c_0\,|0\rangle + c_1\,|1\rangle$

not * q0
phase * q1

- Qureg

q0 | q1 | q2

$$q0 \otimes q1 \otimes q2$$

$$c_0|000\rangle + c_1|001\rangle + c_2|010\rangle + c_3|011\rangle + c_4|100\rangle + c_5|101\rangle + c_6|110\rangle + c_7|111\rangle$$

- Ebit

q0 | q1

$$\mathrm{bell} * (q0 \otimes q1)$$

$c_0\,|00\rangle + c_1\,|11\rangle$ or $c_0\,|01\rangle + c_1\,|10\rangle$

$\otimes$=tensor product

Unitary Qubit Operators

Gate	Symbolic	Matrix	Circuit	Exists
Identity	$\sigma_0 * \psi$	$\sigma_0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	ψ ———	$1/\sigma_0$
Not (Pauli-X)	$\sigma_1 * \psi$	$\sigma_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$	ψ —$\boxed{\mathrm{X}}$—	$1/\sigma_1$
Shift (Pauli-Z)	$\sigma_3 * \psi$	$\sigma_3 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$	ψ —$\boxed{\mathrm{Z}}$—	$1/\sigma_3$
Rotate	$\theta * \psi$	$\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$	ψ —$\boxed{\theta}$—	$1/\theta$
Hadamard - Superposition	$H * \psi$	$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$	ψ —$\boxed{\mathrm{H}}$—	$1/H$

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

Matrices 101

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

$$\Psi = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

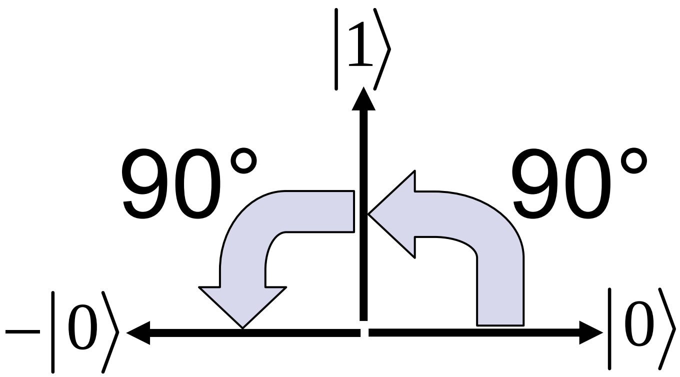
$$c_0 = 1/\sqrt{2} = 0.707$$

$$\sigma * \Psi = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} a\alpha + b\beta \\ c\alpha + d\beta \end{bmatrix}$$

$$\sigma_1 * |0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0*1+1*0 \\ 1*1+0*0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$H * |0\rangle = c_0 \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = c_0 \begin{bmatrix} 1*1+1*0 \\ 1*1+-1*0 \end{bmatrix} = c_0 \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \begin{bmatrix} c_0 \\ c_0 \end{bmatrix}$$

$\sqrt{Not}$ and Trine States



$$Not^2 = \theta_{90}{}^2 = -1$$

$$Not = \sqrt{-1} = i$$

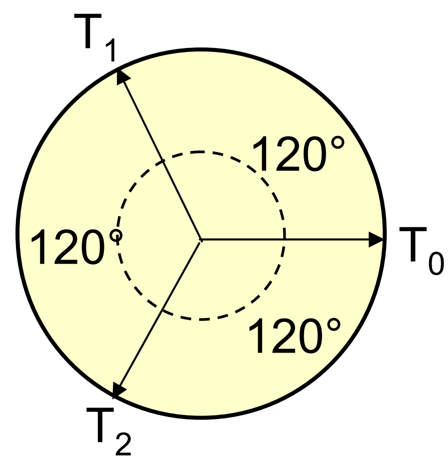
$$\sqrt{Not} = \theta_{45} = \sqrt{i}$$

$$Tr^3 = \theta_{120}{}^3 = 1$$

$$Tr|0\rangle \rightarrow c_0|0\rangle + c_1|1\rangle = T_1$$

$$Tr\left(c_0|0\rangle + c_1|1\rangle\right) = c_0|0\rangle - c_1|1\rangle = T_2$$

$$Tr\left(c_0|0\rangle - c_1|1\rangle\right) = |0\rangle = T_0$$



$$c_0 = 1/2 \qquad p_0 = 1/4$$

$$c_1 = \sqrt{3}/2 \qquad p_1 = 3/4$$

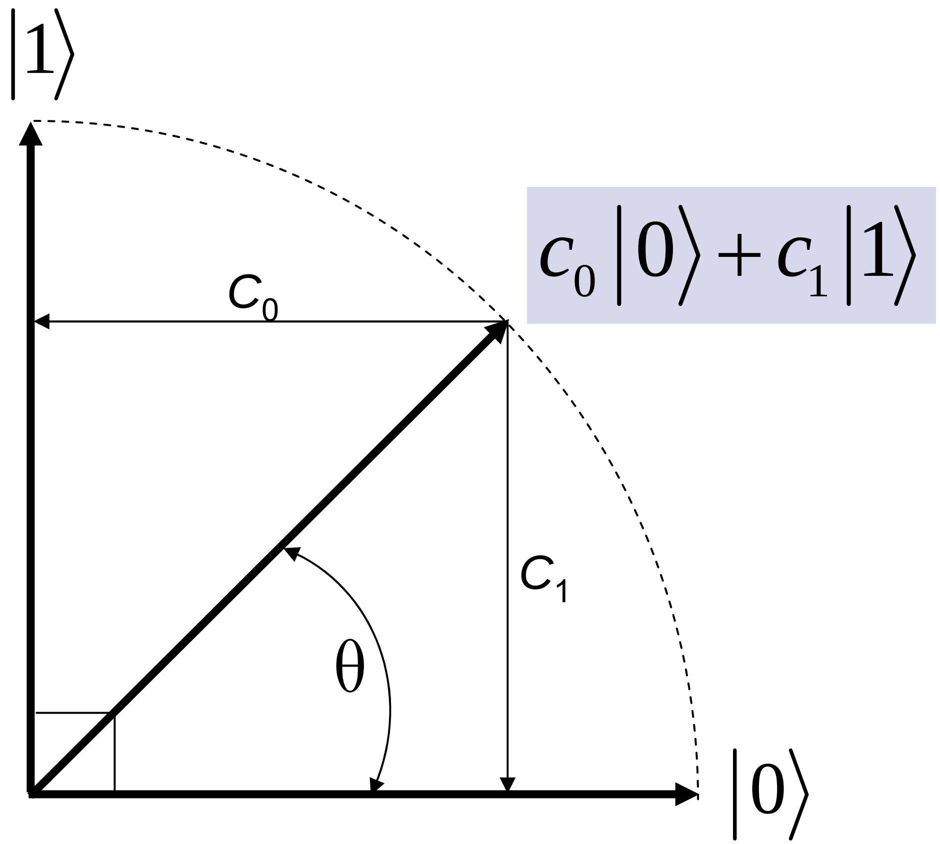
Quantum Noise

- Pauli Spin Matrices

Label	Symbolic	Matrix	Description
Identity	$\sigma_0 * \psi$	$\sigma_0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = 1$	$\sigma_0 \lvert 0\rangle \rightarrow \lvert 0\rangle$
Bit Flip	$\sigma_1 * \psi$	$\sigma_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$	$\sigma_1 \lvert 0\rangle \rightarrow \lvert 1\rangle$ $\sigma_1 \lvert 1\rangle \rightarrow \lvert 0\rangle$
Phase Flip	$\sigma_3 * \psi$	$\sigma_3 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$	$\sigma_3 \lvert 1\rangle \rightarrow -\lvert 1\rangle$
Both Flips	$\sigma_2 * \psi$	$\sigma_2 = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$	$\sigma_2 \lvert 0\rangle \rightarrow i\lvert 1\rangle$ $\sigma_2 \lvert 1\rangle \rightarrow -i\lvert 0\rangle$

Quantum Measurement

Probability of state $c_i\left|i\right\rangle$ is $p_i = c_i^2$ and $p_1 = 1 - p_0$



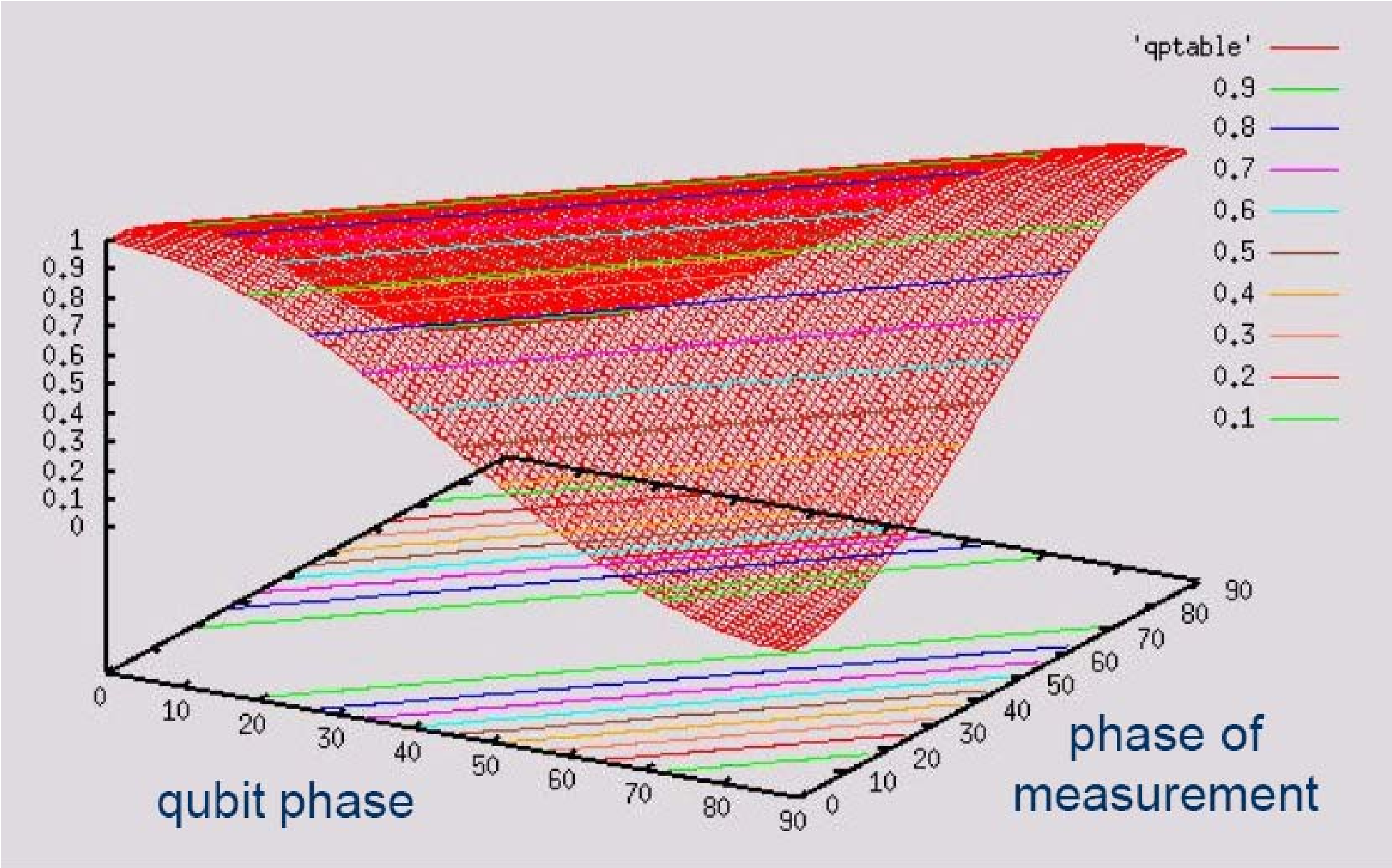
Destructive and Probabilistic!!

When $c_0 = c_1 = \sqrt{\frac{1}{2}}$

then $p_0 = p_1 = \frac{1}{2}$

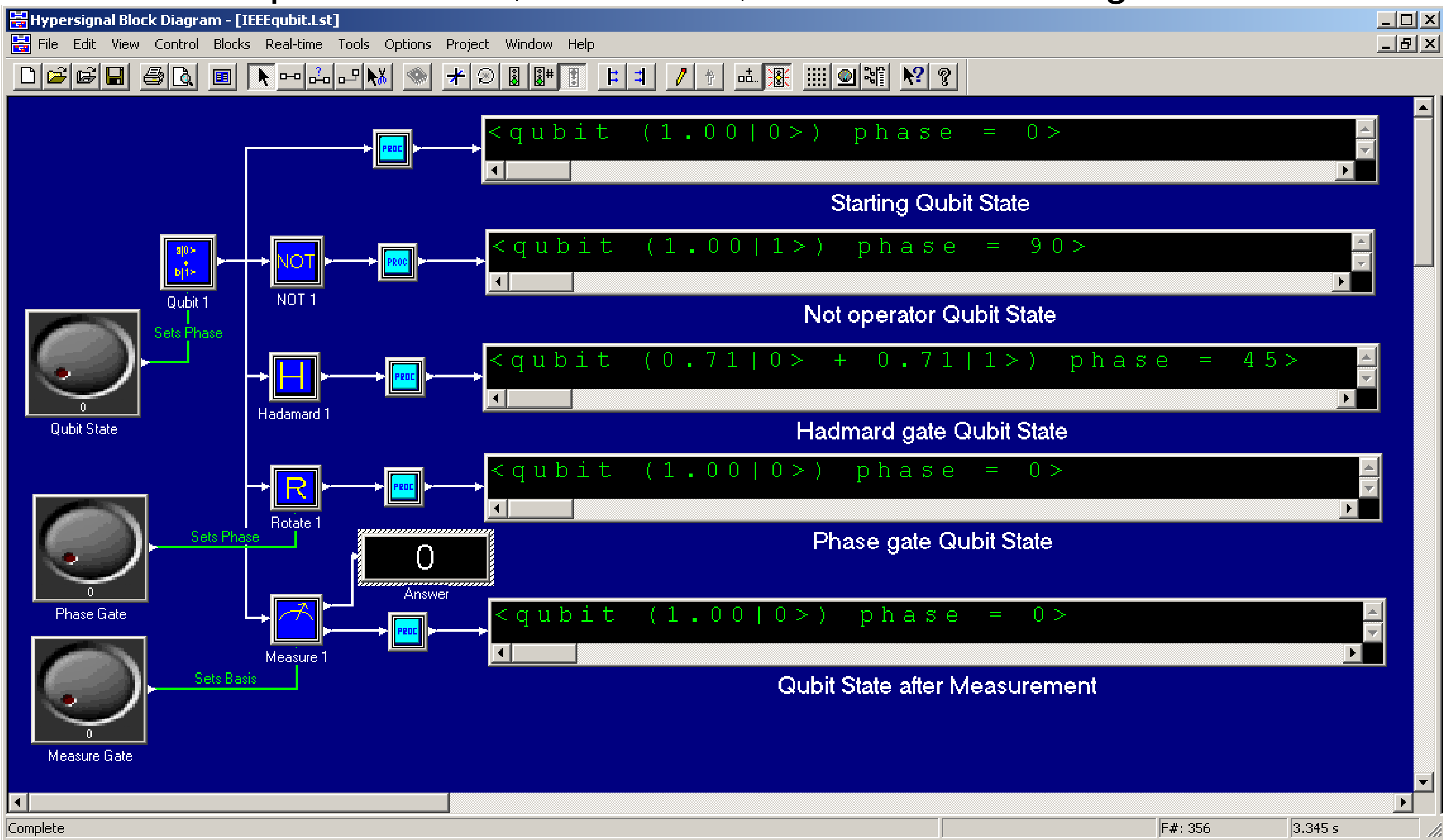
or 50/50 random!

Quantum Measurement



Qubit Modeling

Qubit Operators: not, Hadamard, rotate & measure gates



Our library in Block Diagram tool by Hyperception

Quantum Registers

- Entanglement
  - Tensor Product $\otimes$ is mathematical operator
  - Creates 2^q orthogonal dimensions from q qubits: $q_0 \otimes q_1 \otimes \ldots$
  - Unitarity constraint for entire qureg
- Separable states
  - Can be created by tensor product
  - Maintained by “coherence” and no noise.
- Inseparable states
  - Can’t be directly created by tensor product
  - Concept of Ebit (pieces act as whole)
  - EPR and Bell/Magic states (spooky action at distance)
  - Non-locality/a-temporal quantum phenomena proven as valid

Qureg Dimensions

$$state0_0 = |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$state1_0 = |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

q_0

$\otimes$

$$state0_1 = |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$state1_1 = |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

q_1

=

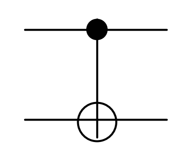
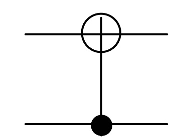
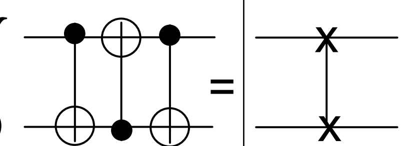
$q_0 \otimes q_1$

$$state0 = |00\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad state1 = |01\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

$$state2 = |10\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \quad state3 = |11\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

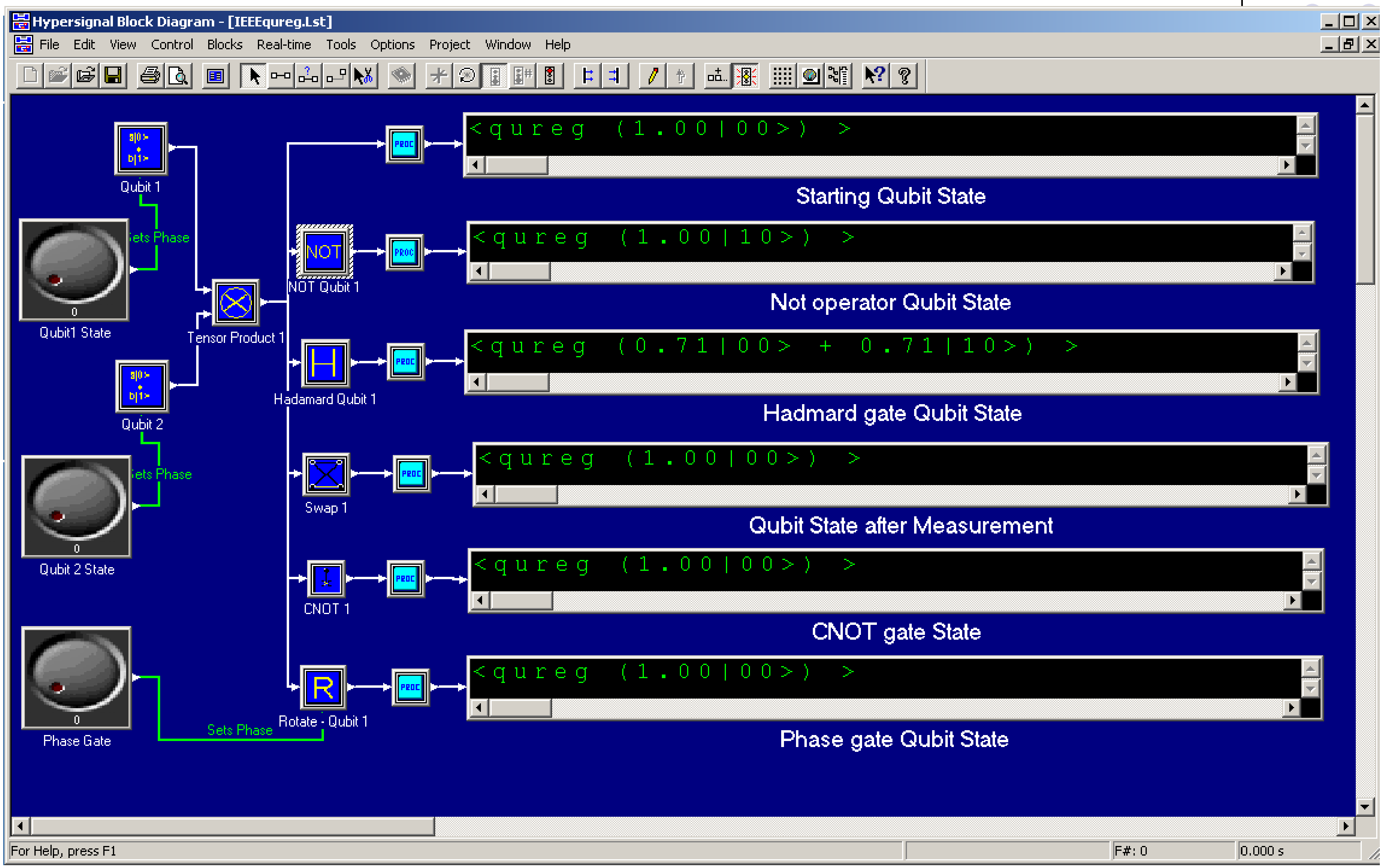
Special kind of linear transformations

Unitary QuReg Operators

Gate	Symbolic	Matrix	Circuit
cnot = XOR Control-not	$cnot * \psi$	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$	ψ Φ 
cnot2	$cnot2 * \psi$	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$	ψ Φ 
swap = cnot*cnot2*cnot	$swap * \psi$	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$	ψ Φ 

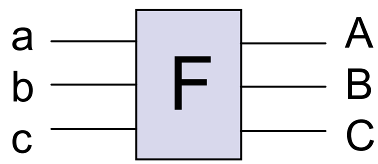
$$\begin{bmatrix} \|00\rangle & \|01\rangle & \|10\rangle & \|11\rangle \end{bmatrix}$$

Quantum Register Modeling

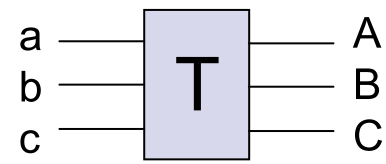


Qureg Operators: tensor product, CNOT, SWAP & qu-ops

Reversible Computing



3 in & 3 out



c	b	a	C	B	A
0	0	0	0	0	0
0	0	1	0	1	0
0	1	0	0	0	1
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	0
1	1	1	1	1	1

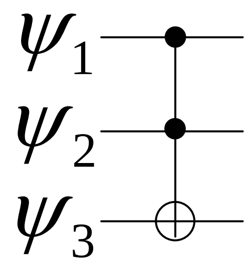
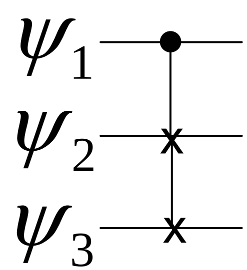
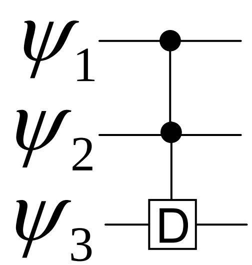
Fredkin Gate c=control

c	b	a	C	B	A
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

Toffoli Gate c=b=control

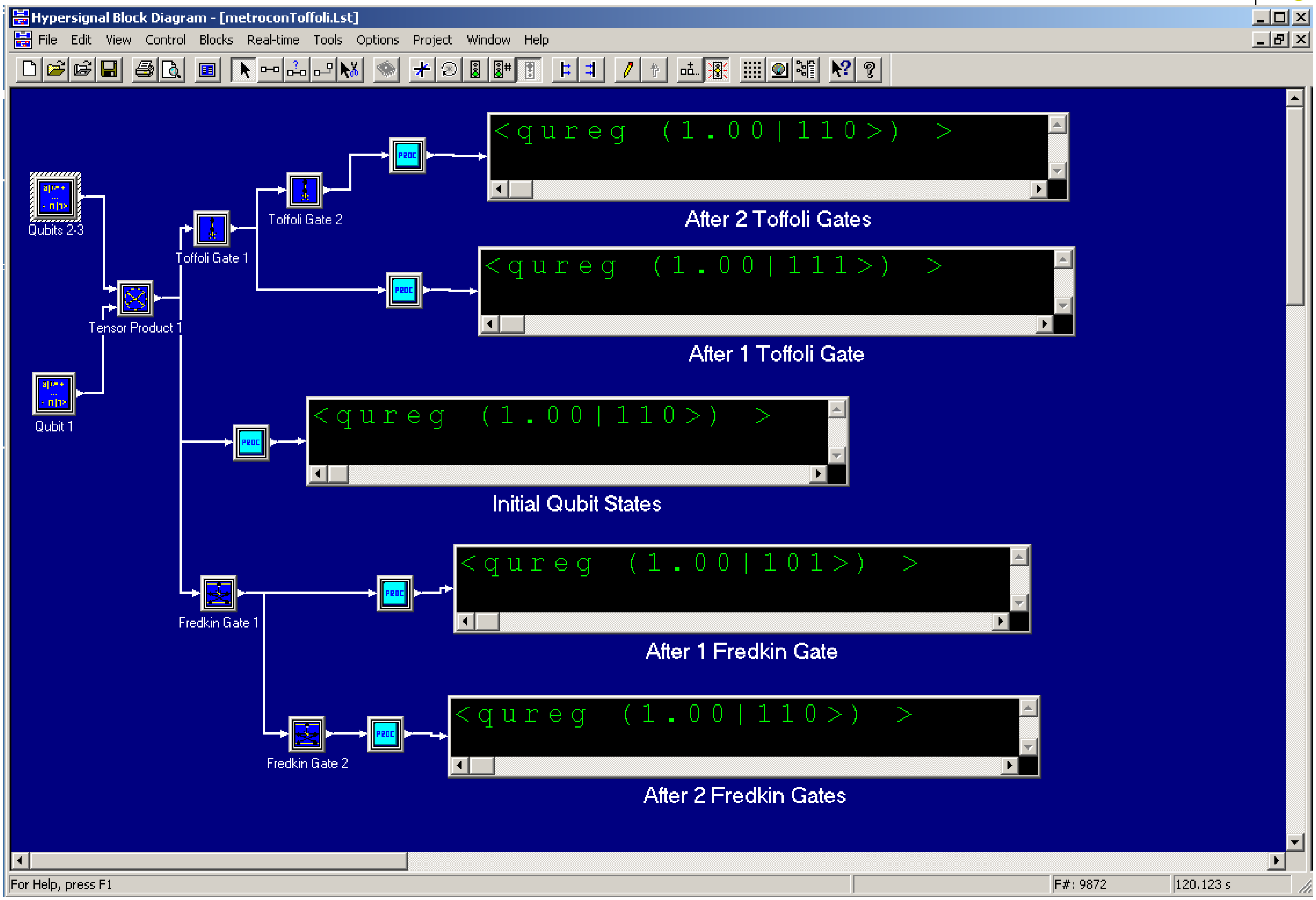
2 gates back-to-back gives unity gate: T*T = 1 and F*F = 1

Reversible Quantum Circuits

Gate	Symbolic	Matrix	Circuit
Toffoli = control-control-not	$T*\psi$	$\begin{bmatrix} 1 & & & & & & & \\ & 1 & & & & & 0 & \\ & & 1 & & & & & \\ & & & 1 & & & & \\ & & & & 1 & & & \\ & & & & & 1 & & \\ & 0 & & & & & 0 & 1 \\ & & & & & & 1 & 0 \end{bmatrix}$	
Fredkin= control-swap	$F*\psi$	$\begin{bmatrix} 1 & & & & & & & \\ & 1 & & & & & 0 & \\ & & 1 & & & & & \\ & & & 1 & & & & \\ & & & & 1 & & & \\ & & & & & 0 & 1 & \\ & 0 & & & & 1 & 0 & \\ & & & & & & & 1 \end{bmatrix}$	
Deutsch	$D*\psi$	$\begin{bmatrix} 1 & & & & & & & \\ & 1 & & & & 0 & & \\ & & 1 & & & & & \\ & & & 1 & & & & \\ & & & & 1 & & & \\ & & & & & 1 & & \\ & 0 & & & & & i\cos\theta & \sin\theta \\ & & & & & & \sin & i\cos\theta \end{bmatrix}$	

$\begin{bmatrix} \|000\rangle & \|001\rangle & \|010\rangle & \|011\rangle & \|100\rangle & \|101\rangle & \|110\rangle & \|111\rangle \end{bmatrix}$

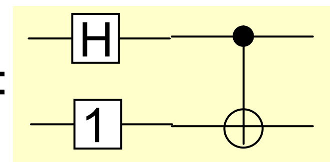
Toffoli and Fredkin Gates



Ebits – Entangled Bits

- EPR (Einstein, Podolsky, Rosen) operator

$$\boldsymbol{B} =$$



$$= \begin{bmatrix} c_0 & 0 & 0 & c_0 \\ 0 & c_0 & c_0 & 0 \\ c_0 & 0 & 0 & -c_0 \\ 0 & c_0 & -c_0 & 0 \end{bmatrix}$$

- Bell States

$$B_0 = \Phi^+ = c_0\left(\left|00\right\rangle + \left|11\right\rangle\right), \quad B_1 = \Phi^- = c_0\left(\left|00\right\rangle - \left|11\right\rangle\right)$$

$$B_2 = \Psi^+ = c_0\left(\left|01\right\rangle + \left|10\right\rangle\right), \quad B_3 = \Psi^- = c_0\left(\left|01\right\rangle - \left|10\right\rangle\right)$$

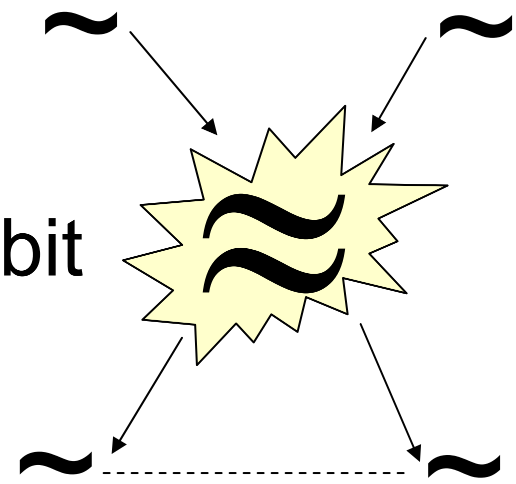
- Magic States

$$M_0 = c_0\left(\left|00\right\rangle + \left|11\right\rangle\right), \quad M_1 = c_1\left(\left|00\right\rangle - \left|11\right\rangle\right) \quad c_0 = 1\big/\sqrt{2}$$

$$M_2 = c_1\left(\left|01\right\rangle + \left|10\right\rangle\right), \quad M_3 = c_0\left(\left|01\right\rangle - \left|10\right\rangle\right) \quad c_1 = i\big/\sqrt{2}$$

EPR: Non-local connection

- Step1: Two qubits
- Step2: Entangle →Ebit
- Step3: Separate
- Step4: Measure a qubit
  - Other is same if $\Phi^{\pm}$
  - Other is opposite if $\Psi^{\pm}$



$$\left|0_0\right\rangle, \left|0_1\right\rangle$$

$$\Phi^{\pm} = \left|00\right\rangle \pm \left|11\right\rangle$$
$$\Psi^{\pm} = \left|01\right\rangle \pm \left|10\right\rangle$$

$$\left|?\right\rangle, \left|?\right\rangle$$

$$answer = 1, other = 1$$
$$answer = 1, other = 0$$

Linked coins analogy

Quantum Algorithms

- Speedup over classical algorithms
  - Complexity Class: Quantum Polynomial Time
  - Reversible logic gates just mimics classical logic
- Requires quantum computer with q>100 qubits
  - Largest quantum computer to date has 7 qubits
  - Problems with decoherence and scalability
- Known Quantum Algorithms
  - Shor’s Algorithm – prime factors using QFT
  - Grover’s Algorithm – Search that scales as sqrt(N)
  - No other algorithms found to date after much research

Quantum Communication

- Quantum Encryption
  - Uses fact that measuring qubit destroys state
  - Can be setup to detect intrusion
- Quantum Key Distribution
  - Uses quantum encryption to distribute fresh keys
  - Can be setup to detect intrusion
- Fastest growing quantum product area
  - Many companies and products
  - In enclosed fiber networks and also open air

Quantum Mind?

- Did biology to tap into Quantum Computing?
  - Survival value using fast search
  - We might be extinct if not for quantum mind
- Research with random phase ensembles
  - Ensemble states survive random measurements
  - See paper “Math over Mind and Matter”
- Relationship to quantum and consciousness?
  - Movie: “What the Bleep do we know anyhow?
  - Conferences and books

Summary and Conclusions

- Quantum concepts extend classical ways of thinking
  - High dimensional spaces and simultaneity
  - Distinguishability, mutual exclusion, co-occurrence and co-exclusion
  - Reversible computing and unitary transforms
  - Qubits superposition, phase states, probabilities & unitarity constraint
  - Measurement and singular operators
  - Entanglement, coherence and noise
  - Ebits, EPR, Non-locality and Bell/Magic States
  - Quantum speedup for algorithms
  - Quantum ensembles have most properties of qubits

- Quantum systems are ubiquitous
  - Quantum computing may also be ubiquitous
  - Biology may have tapped into quantum ensemble computing
  - Quantum computing and consciousness may be related