Superposition, Entanglement, and Quantum Computation

Aditya Prasad
3/31/02

Introduction - Feynman

- An N-particle quantum system can't be simulated on a classical machine whose resources don't grow exp with N.
- *Would* be possible on a 'quantum computer'
  - *Not* a Turing machine

Both have been proven true

Introduction, cont'd

- Quantum parallelism – quantum superposition of distinct states
  - Doesn't immediately lead to speedup
- Shor showed how info could be extracted usefully
  - Polynomial factoring algo.

Intro to 

- On a classical computer, unsorted database search takes O(n) time
- In 1997, Grover showed a quantum algo that takes O(sqrt N)

Superposition and entaglement

- Quantum systems can exhibit superpositions of eigensolutions
  - Not specifically quantum – classical too
- Ekert and Josza consider a multi-qubit system: apply gate U to qubits (i,j) n times
  - Quantum system: measurement in O(n)
  - Classical system: measurement in $O(2^n)$

Classical and quantum: a difference

- Classical waves allow superposition
  - Qubit could be represented by classical strings?
- Superposition can always be described by Cartesian product of states
- Quantum superposition may be ‘entangled’
  - ½(|0> + |1> + |2> + |3>) can be factored
  - 1/sqrt2(|0> + |1>) cannot be: it is entangled
- Difference is Cartesian vs. tensor products

Entanglement, cont’d

- Schroedinger says quantum entanglement is defining characteristic
- Entanglement depends on basis
  - ½(|0> + |1> - |2> + |3>) is entangled wrt C_2 x C_2, but not wrt C_4
- State of n qubits is 2^n-dim, isomorphic to 1 particle with 2^n levels.
  - Not useful for complexity consideration, as the 1 particle requires energy resources in O(2^n)

Back to Grover

- Search through a phone book for name, only knowing telephone number
  - Takes O(n) time classically
  - O(sqrt n) time by Grover’s algo

Basics

- There are $N = 2^L$ states labelled S_0, S_1, S_2 … S_{N-1}
  - Only one fulfills the condition C_J so that $C_J(S_J) = 1$ and $C_J(S_K) = 0$, K != J
- Goal is to find the solution S_J in the fewest evaluations of C_J

Grover's solution

- Start with an L-qubit register in state |0>
- Apply an L-qubit Hadamard gate, yields an equal superposition
- Perform the following two operations on the wires, O(sqrt N) times:

Grover's operations

- 1) Apply oracle U_J defined by:
  - U_J |J> = -|J>
  - U_J |K> = |K>, K != J
- 2) Apply diffusion operator D:
  - D = H U_0 H
  - U_0|0> = -|0>
  - U_0|K> = -|K>, K != 0

Result

- After O(sqrt N) iterations, the outcome is the state |J> with high probability
- Grover explains D to be an 'inversion about the average' of the coefficients

Example

- Apply Hadamard to get
  - |M> = ½(|0> + |1> + |2> + |3>)
- Now apply the oracle U_J
  - UJ|M> = |M> - 2<J| |M> |J>
- Apply Grover's diffusion operator:
  - D U_J H|)> = -|J>
  - Found in one pass!

Classical implementation

- We map each integer 0…2^L-1 into another integer in the same range:
  - Define L qubits to be a 'control' register |J> and another L to be the 'target' register |K>
  - Let |J> x |K> → |J> x |K x f(J)>
  - Starting with |K> = 0, we get |f(J)>

Classical, cont'd

- Consider an f(M) that maps an integer M to an integer F = f(M) (bijective)
- Want to force init state into |M> x |F(M)> so that we can measure f^{-1}(F) = M
  - Define W = V_f H_c
  - Let U_f be an oracle that flips the sign of the state iff it is |F>

An Electronic approach

- Use 2^n signal paths, one for each base state
- L-qubit Hadamard device uses op-amps with 2^n inputs and ouputs
- (Description of how they used motherboards with what color LEDs here)

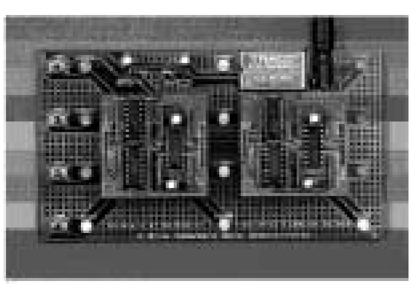
Hadamard implementation

- A general L-qubit Hadamard operator can be written as a $2^L \times 2^L$ matrix
- Split each of the 2^L input signals into 2^L separate signals, each with amplitude $1/\mathrm{sqrt}(2^L)$
- Use an inverting op-amp for phase-shift

Electronic Hadamard

Fig. 1. Schematic diagram for the single qubit Hadamard gate.

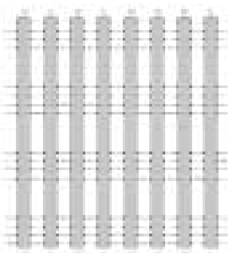
A *photograph*



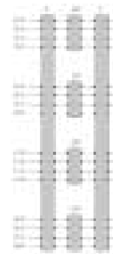
Hadamard conclusion

- Is reversible: two applications always restores input
- Is not *physically* reversible
- Use of op-amps and resistors ensures correct operation with AC signals
- Requires 2^{2L} signals (analogous to Deutsch's 'extra universes')
- *This is just a demonstration*

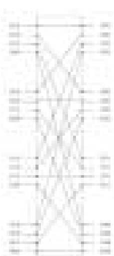
Grover schematic



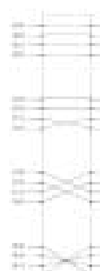
Hc schematic



T matrix



V_f for f(I) = 3-I



Oracle for ex. f(I) = 2

Conclusions

- Entanglement depends on the representation
- Their electronic implementation shows that any implementation without multi-particle entanglement requires exp. resources (refer to Ekert and Josza)

Final conclusion

- "The number of signal paths increases exponentially and makes electronic implementations of large numbers of qubits impracticable"
- Therefore, multi-particle entanglement is the key property of quantum systems that gives rise to the remarkable power of quantum computers