# Quantum vs. DNA Computing

In search for new computing methods

# What Is this all about?

- Rise of the machines.
  - 1947 – “Six electronic computers would be enough for the computing needs of the U.S.A.”
- Need for more computing power.
  - Science, Education, etc
- Search for a new computing medium.
  - DNA or Quantum Computing
- Is this feasible?

# An overview.

- Quantum Computing in a nutshell
- DNA Computing review.
- Theories & Applications for both methods
- A comparison
- Some thoughts
- Parting words.
- Maybe Q&A

# Quantum Computing

" A quantum computer is any device that exploits quantum mechanical phenomena to run algorithms"

- Geekwise.com

# Quantum Computing: History

- 1981 - Paul Benioff, the first

- 1982 - Richard Feynman, realized that some quantum mechanic simulations can not be performed efficiently on a regular computer



- 1985 - David Deutsch. Description of a universal quantum machine

# Quantum Computing: History (2)

- 1994 - Peter Shor, achieving polynomial time in factorization of integers made possible.
- 1996 - Lov Grover and quantum database search algorithm
- 1998 - 2001 - 2q, 3q, 5q, 7qbit computers, and execution of Shors’ factoring algorithm
- 2005 - 2006 - More Innovations.

# Quantum Computing: Intro

- Quantum phenomena?
  - Superposition
    - Bits vs Qubits
      - (0 or 1) vs (0 or 1) or (0 and 1)
  - Quantum parallelism: result of superposition
  - Entanglement: allows us to know the spin of the opposite particle upon measurement.

# Intro(2): Interference

- Interference: results can interfere since quantum computing can calculate multiple inputs at same time.
- Interference is utilized by quantum algorithms
- The result from each calculation of a universe will constructively and destructively interfere to give measurable result
- Different significance for different algorithms

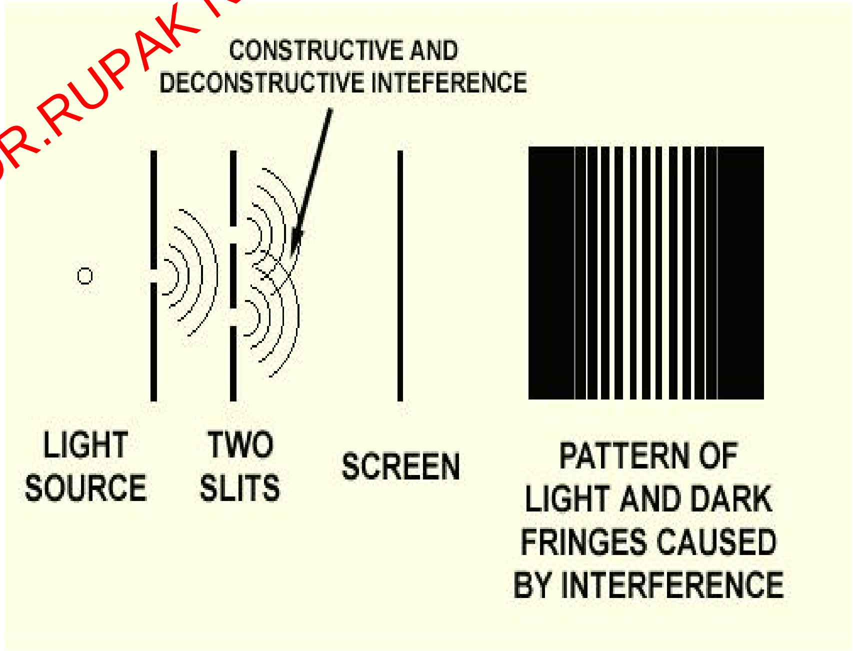



*Figure 1* - Young's two slit experiment demonstrates interference of photons.

# Intro(3): Decoherence

- Tendency for qubit to fall back to one of either 0 or 1 state
- This happens upon measurement, making solutions really hard to extract.
- Why?

# Intro(4): Strengths

- Massive parallelism
  - Because of coherent superposition
  - 2^(#of qubit) calculations at the same time!
- Faster than the speed of light
  - Entanglement: setting the spin of one particle instantaneously allows us to know spin of other.
- Great for storage!

# Quantum Computing: Future

- David DiVincenzo, of IBM, listed the following requirements for a practical quantum computer:
  - scalable physically to increase the number of qubits
  - qubits can be initialized to arbitrary values
  - quantum gates faster than decoherence time
  - Turing-complete gate set
  - qubits can be read easily

# DNA Computing

“ **DNA computing** is a form of computing which uses DNA and molecular biology, instead of the traditional silicon-based computer technologies”

-Wikipedia.com

# DNA Computing: History

- 1994 – L. Adleman solves Hamiltonian Path Problem
- 1995 – Boneh et al. paper on cracking DES using molecular computer
- 1997 – Rochester U. Team developed logic gates using DNA.
- Many researchers have tried to follow Adlemans example.

# DNA Computing: Intro

- Deoxyribonucleic Acid
  - Contains four different bases A, T, G, C
  - Bases are complimentary and are responsible for the formation of the double helix.
- Strengths
  - Faster than classical computer systems
  - Greater storage capacity
  - Massive parallelism
  - Lightweight
    - 1Lb gives us more computing power than all the computers ever made.

# DNA Computing: Future

- Many promising algorithms.
- Lack of knowledge hinders progression
- However, small and encouraging steps are being made
  - 2000 – development of gold plate applied with DNA

# Theories

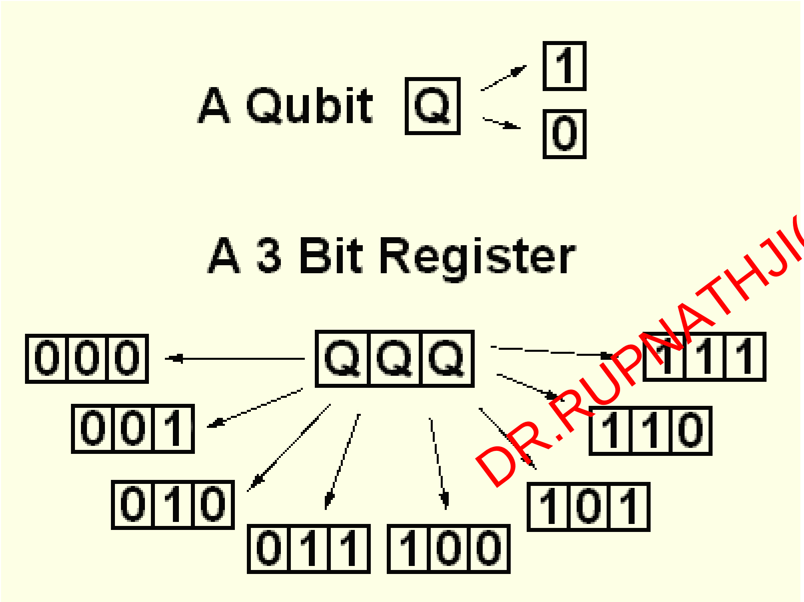
- We will be looking at two algorithms dealing with:
  - Cryptography
  - Data storage searching ( databases )

# Quantum Computing

- Cryptography: breaking RSA (Shor, P. 1995).

- Example: factor of number 15.

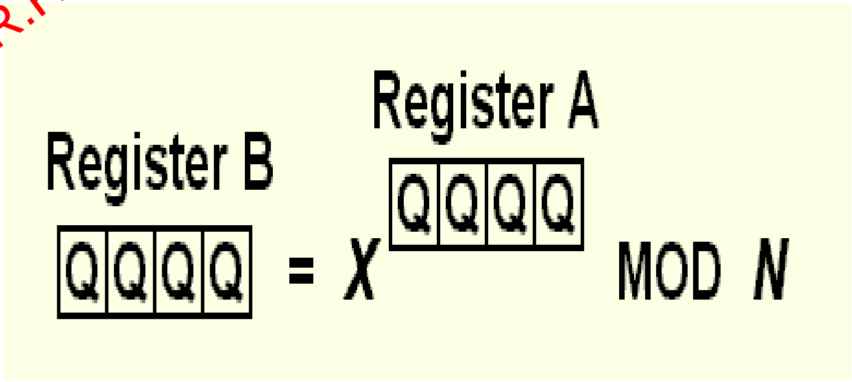
# Cryptography – Shor – stage 1




- 8 different universes
- All calculations are performed in parallel, one in each universe

# Cryptography – Shor – stage 2

- *N* is the number we wish to factorise, *N* = 15
- *X* is randomly chosen, where $1 < X < N-1$
- *X* is raised to the power contained in the register (register A) and then divided by *N*
- The remainder from this operation is placed in a second 4 bit register (register B).



# Cryptography – Shor – stage 2

- Repeating values of 1, 2, 4, 8, all with frequency f = 4.

| | |
|---|---|
| 0 | 1 |
| 1 | 2 |
| 2 | 4 |
| 3 | 8 |
| 4 | 1 |
| 5 | 2 |
| 6 | 4 |
| 7 | 8 |
| 8 | 1 |
| 9 | 2 |
| 10 | 4 |
| 11 | 8 |
| 12 | 1 |
| 13 | 2 |
| 14 | 4 |
| 15 | 8 |

# Cryptography – Shor – stage 3

$$\text{Factor } P = X^{\frac{f}{2}} - 1$$

- *f*, can be found using a quantum computer.
- We use interference to dispose cancel out values
- Equation calculates *possible* value.

# Grover’s Search algorithm

- Similar to Shors’ algorithm

- The information is in a register under superposition.

- Interference cancels out wrong answers

- Grover: “It’s like throwing stones in water, and let the ripples cancel out”.

# Grover’s Search algorithm (2)

- Possible to perform search in root N searches
- The speed up that this algorithm provides is a result of quantum parallelism.
- The database is effectively distributed over a multitude of universes, allowing a single search to locate the required entry.

# Grover’s Search algorithm (3)

- Application in cryptography as well.
- Theoretically possible to break DES
- Approximately 185 search cases vs. 2^55 on a regular computer.

# Problems

- Shors' algorithm is probabilistic
- Grovers' algorithm is theoretically applicable to breaking DES
- Technological issues:
  - laser that manipulates qubit, fluctuates.
  - dealing with decoherence.

# DNA Computing

- Following Joshs' presentation in class it was said that RSA was on a "Provable security" level.

- Algorithm for breaking DES with DNA computing.
- Plan of attack [ Joshs' presentation ]
  - Oscar chooses some plaintext P and encrypts it using the DES circuit to obtain ciphertext C0
  - Oscar wants to find the key k0 used in the circuit
  - For every possible key ki (256 possibilities) Oscar creates a strand kiCi, where Ci is the ciphertext resulting from performing the encryption on P with potential key ki
  - Similar to traveling salesman problem where Adleman generated all possible paths [Adleman 1994]
  - Oscar now has a soup Tf containing 256 strands
  - The strand for which Ci = C0 has the correct key ki

# Problems

- DNA computing is mostly theoretical
- No killer app has been found.
- DNA can solve most problems a typical computer can solve, not always more efficiently though ☹

# Solutions

- It seems that we are waiting for some advances in technology.
- Increase of knowledge on biological field, and of biological operations, would aid progression.
- Funding wouldn’t be bad either ☺

# Problems: A Comparison

- Quantum Computing is not as theoretical
- Quantum Computing does have a killer app. “factorization of large numbers in polynomial time”
- We have more knowledge on how quantum mechanics work, rather than how biological operation work.
- In all fairness, quantum gets more funding.

# Some thoughts (my own)

- There is a need for more computational power
- Both are excellent means of computation
  - Viable alternatives to todays electronic computers
- Don’t see them as competitive disciplines
  - They compliment each other
    - DNA focuses on storage capacity
    - Quantum on speed
- Future would be interesting to see!