

Epilogue: The Future of Computing

15110 Principles of Computing, Carnegie
Mellon University - CORTINA

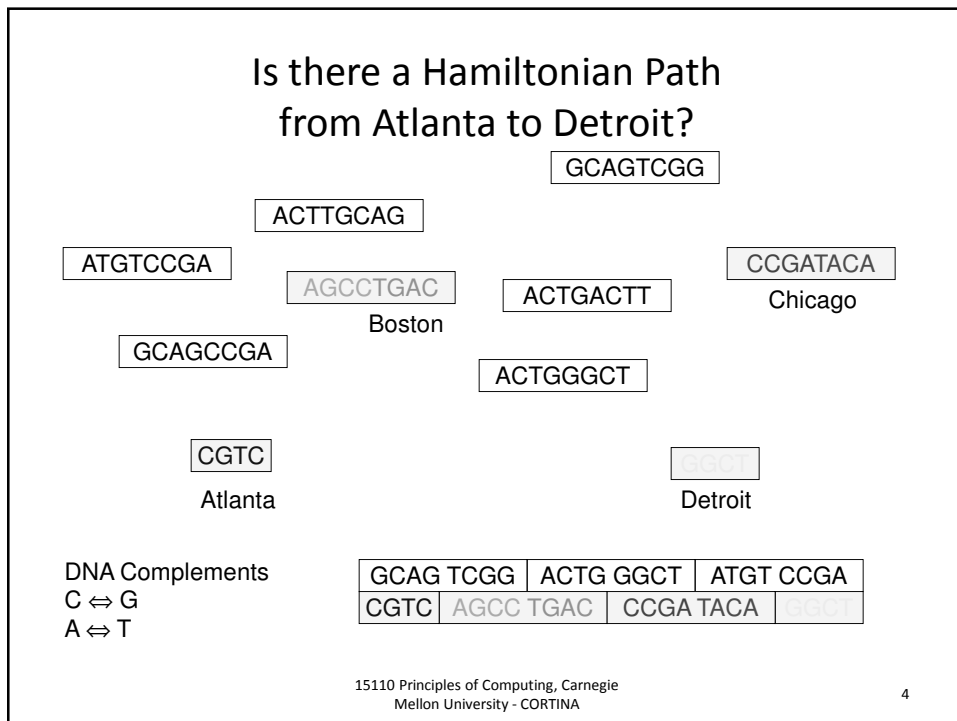
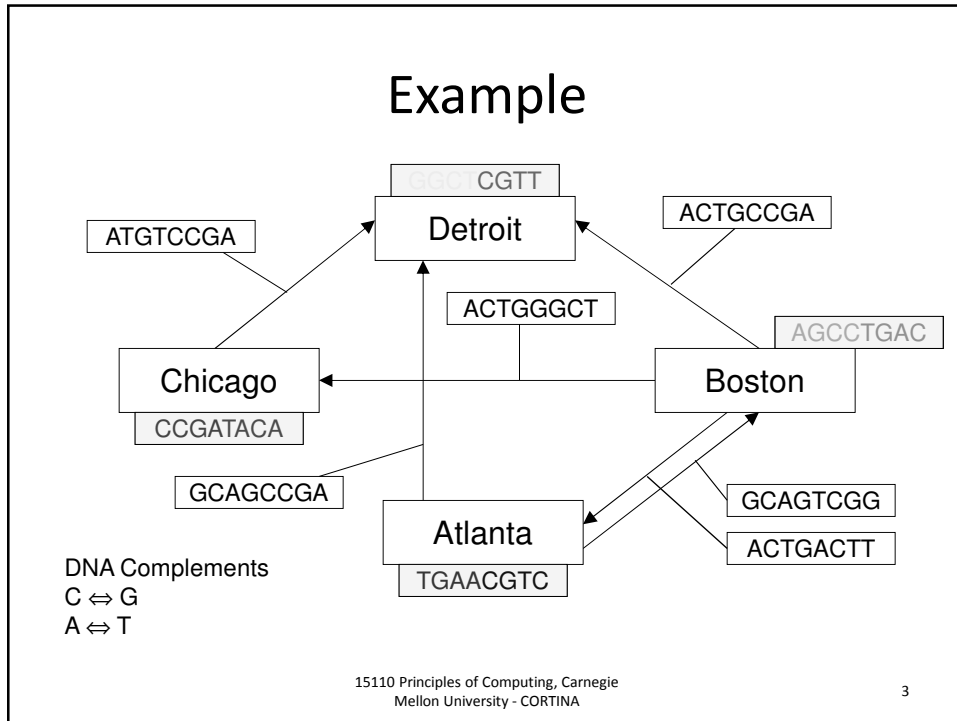
1

DNA Computing

- Use of DNA strands to compute solutions quickly.
- Computing with DNA
by Leonard Adleman (UC Berkeley)
 - Demonstrated the use of DNA to solve a small instance of the Hamiltonian path problem.
 - DNA sequences consist of the letters A,C,T,G representing the bases adenine, thymine, guanine, and cytosine.
- Adleman demonstrated the use of DNA to solve a Hamiltonian Path problem with 7 cities in 1998.
 - The Hamiltonian Path problem is NP Complete.

15110 Principles of Computing, Carnegie
Mellon University - CORTINA

2



Is there a Hamiltonian Path from Detroit to Atlanta?

DNA Complements
 $C \leftrightarrow G$
 $A \leftrightarrow T$

NO SOLUTION

15110 Principles of Computing, Carnegie Mellon University - CORTINA

5

Quantum Computing

- A subatomic particle has spin (up or down). In quantum physics, particles can be in a state defined by *superposition* (up and down).
 - Using quantum mechanics, a quantum computer can do computations simultaneously since particles can be in two states at once.
 - This only holds as long as we don't interfere or observe these particles.
 - If we do, then the particles will make a random decision and choose one of the two states. (*decoherence*)

15110 Principles of Computing, Carnegie Mellon University - CORTINA

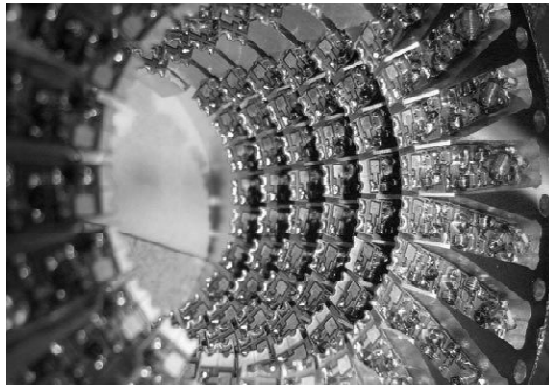
6

Qubits

- In a classic computer, basic information is stored in bit form. A bit can only be in one of two states at any given time.
- In a quantum computer, basic information is stored in a qubit which can be in the states 0 and 1 at the same time (with some probability for each).
- A 4-qubit quantum computer can store 16 separate computations at the same time.
 - This improvement grows exponentially as the size of the quantum computer grows.

Quantum Computing and RSA

- Peter Shor (at AT&T Bell Labs in 1994) described an algorithm that could factor a number that was the product of two prime numbers in polynomial time using a quantum computing model.
- This algorithm could be used with a quantum computer (once developed) to crack the RSA encryption algorithm.
- In 2001, IBM demonstrated a 7-qubit quantum computer to factor the number 15 into the prime values 3 and 5.



D-Wave Systems “demonstrated” a 28-qubit quantum computer in November 2007 at a SC07 (a supercomputing conference).

What's Next?

- Will we eventually prove that $P = NP$ or $P \neq NP$?
- Will the computers for the next generation be made up of DNA or quantum particles rather than silicon?
- Will robots eventually replace humans as the dominant race due to their superior intelligence?
- Will humans become more and more robotic as they evolve?