15110 in a Nutshell

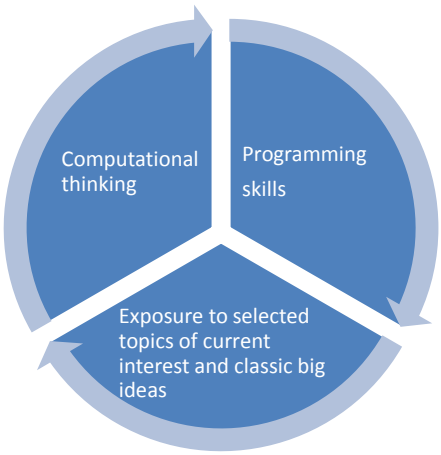
Computer Science for Non-majors

- Fine Arts
- Basic Sciences
- Engineering
- Psychology
- Business
- Modern Languages
- Others ...

Why Were You Here?

- Curiosity: find out about computing technology and its many effects on society.
- Professional development: computing skills can make you more successful at work.
- Academic requirement: a computing course is required for your major.
- Intellectual growth

Course Objectives



WHAT DID WE DO?

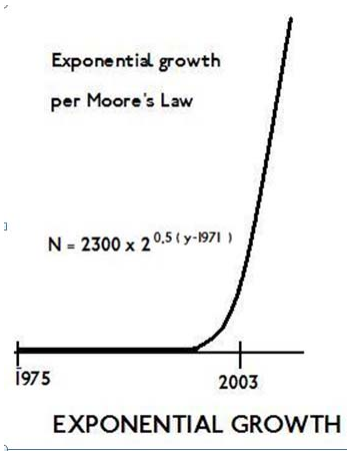
Computers Getting Faster and Smaller

- Purely mechanical (Leibniz, Babbage)
- Electro-mechanical (Aiken's Harvard Mark I)
- Purely electronic (vacuum tubes)
  - 1000 times faster than electro-mechanical
- Stored-program digital computers
- Integrated circuits
- Microprocessors
- Quantum computers (in development)

Units of Memory

• Byte	B	8 bits (8b)		
• Kilobyte	KB	1024 B	= 2^{10} bytes	≈ 10^3 bytes
• Megabyte	MB	1024 KB	= 2^{20} bytes	≈ 10^6 bytes
• Gigabyte	GB	1024 MB	= 2^{30} bytes	≈ 10^9 bytes
• Terabyte	TB	1024 GB	= 2^{40} bytes	≈ 10^{12} bytes
• Petabyte	PB	1024 TB	= 2^{50} bytes	≈ 10^{15} bytes

Moore's Law



Growth of number of transistors on an integrated circuit

Algorithmic Thinking and Programming

- Process of moving from a problem statement to a formulation of the problem in a way that can be solved using computers
- Learned Ruby -- a language for expressing computations
- Systematic approach to organizing, writing and debugging small programs

These skills will translate to other languages
Python, Java, MatLab, Perl

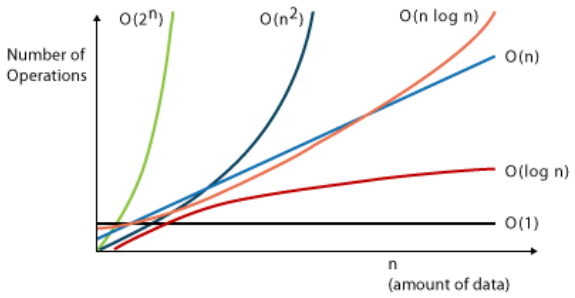
9

Reasoning About Programs

- How much work does my program to accomplish a certain task, given a certain input?
- How does my program scale as I use it on larger inputs?

Informal understanding of computational complexity

Some Complexity Classes



Superpolynomial (for example exponential) complexity is considered intractable

11

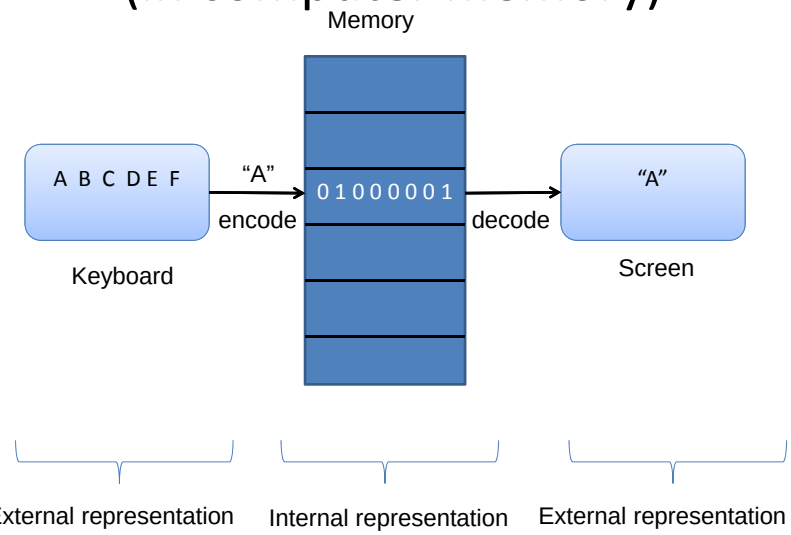
Organizing Data (mental model)

- Simple arrays, multi-dimensional arrays, hash tables, trees, graphs
- What data structure is most natural for your computational task?
- How does using one data structure fare against using another one in terms of time and space complexity?

We only scratched the surface.

12

Representing Data (in computer memory)

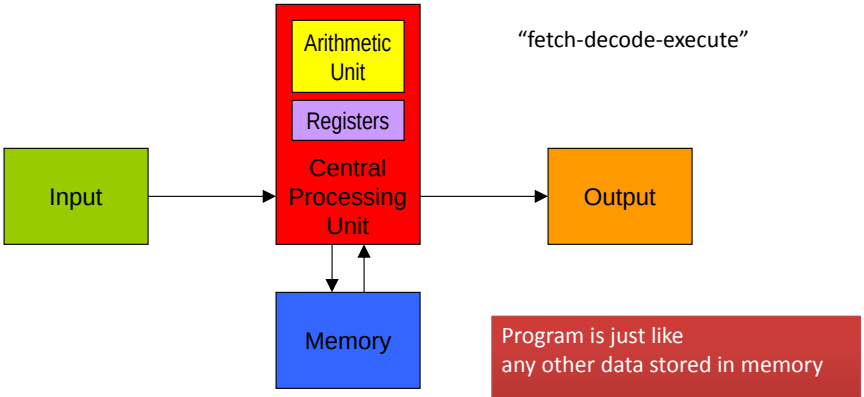


13

- Encoding schemes for numbers, text, images
- How many distinct values can we represent using *n* bits within a given encoding scheme?
- How can we compress encodings to save space? For example, Huffman encoding.

Base 2 and 16 arithmetic are our friends in reasoning about representation in digital computers.

Computer Organization



Randomness

- Many aspects of the real-world can be modeled only by using randomness.
  - Maybe there is true randomness – we cannot determine a cause for not everything that happens.
  - Maybe there is a cause for everything but our knowledge of the world is not enough to determine that
- How can we use deterministic computers to exhibit "random-like" behavior?

Stochastic Simulations

- Given some primitive functions that yield "random-like" values, how can we do simulations to make predictions? For example, forest fire simulation, game simulations.
- Randomness can also be used in estimating outcomes that are not inherently random. For example, using Monte Carlo simulation to estimate π.

Deterministic Simulations

- Simulations are also useful when the system being modeled is too complex for analytic methods
  - Solar system simulation, performance analysis of processor chips

Concurrency

- Concurrency is the process of performing more than one process at a time.
  - Some computations require concurrency by their nature. Some computations can be sped up if we can figure out how to decompose computation
  - Many flavors: parallel processing, multitasking on a single processor, pipelining, distributed computing

In general it is harder to think about concurrent computation because of the coordination required in sharing resources and the large number of possibilities for the execution to evolve.

19

Internet

- An open network of networks based on a stack of standardized protocols
- Glued by the Internet protocol (IP)
  - IP addresses for individual devices, routers switching packets
- Provides the infrastructure for many services that we take for granted.

The Internet is a complex system that is studied from many perspectives, communication technologies, networking technologies, algorithms, cyber law, societal concerns.

20

Security

- Communication over the Internet takes place in the presence of adversaries that can intercept and modify messages.
- Cryptography is an old art that we use for secrecy, integrity, authentication.

Privacy is a related concept that concerns how personal information is handled. We could not spend enough time on it.
Blown to Bits offers insightful readings!

Encryption

- Symmetric and asymmetric schemes for encryption
  - Exploit computational hardness (intractability) of certain problems. For example, RSA relies on the intractability of factoring.
- One-way hash functions, digital signatures

Artificial Intelligence

- Can computers perform computational processes normally associated with human intellect and skill?
  - Game playing, natural language processing, machine learning, robotics
  - Computers play chess, win Jeopardy, drive cars, but are they intelligent?

We identified challenges. We asked questions rather than answering them.

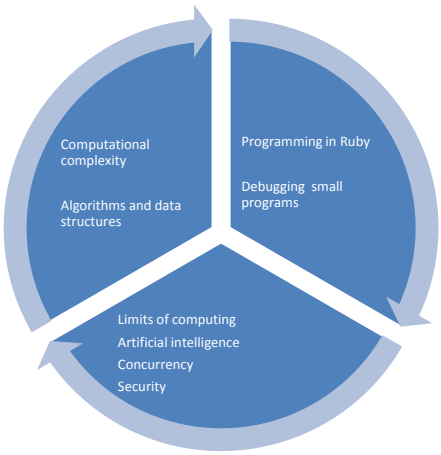
23

Limits of Computing

- Tractable Problems (polynomial time-complexity), intractable problems (super-polynomial time-complexity), uncomputable problems
- Open question: Is P = NP?
  - Are some problems that are believed to be intractable in fact tractable?

24

Course Coverage



WHAT IS NEXT FOR YOU?

Where to Go From Here

- Done with computer science. You will be involved in computing only as needed in your own discipline?
  - We believe you are leaving this course with useful skills.
- Grew an interest in computing. You want to explore more?
  - 15-112 is taken by many who feel this way. It primarily focuses on software construction.
- Considering adding computer science as a minor or major?
  - Great! We are happy to have been instrumental in this decision.

WHAT IS NEXT FOR COMPUTER SCIENCE?

- Will we eventually prove that P = NP or P ≠ NP?
- Will the computers for the next generation be made up of quantum particles rather than silicon?
  - Star Trek computers already use qubits!
- Will humans become more and more robotic as they evolve?
  - Smartphones today; Google glasses tomorrow; cyborgs in 50 years?
- Will robots eventually replace humans as the dominant race due to their superior intelligence?

Quantum Computing

- A nice video from our Resources page:
  http://www.youtube.com/watch?v=VyX8E4KUkWw

Thanks

15110 Staff for Spring 2013

Missing: Guna, Eshan, Heidi, Jack, and Vishal

Thanks also to Tom Cortina, Dave Touretzky, and Jim Morris

31

From Dave Touretzky's Fall 2012 lecture

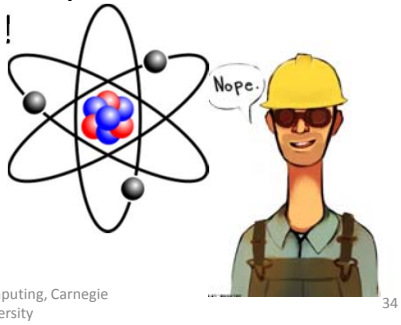
NOTES ON QUANTUM COMPUTING FOR THE ENTHUSIAST

Promise of Quantum Computation

- Classical computers have their limitations:
  - Factoring large numbers takes exponential time.
    - No faster algorithm is known.
  - Searching an unordered list takes O(n) time.
    - No faster algorithm is possible.
- Quantum computers can solve some problems more efficiently than classical computers.
  - Prime factoring: could break RSA encryption.

What Is Quantum Mechanics?

- Objects at the subatomic level behave in ways that have no analog at the macroscopic level.
- Protons, neutrons, and electrons are not little billiard balls. They are both *particles* and *waves* at the same time!
- Quantum mechanics describes how these objects really behave. It's quite weird.



Examples of Quantum Weirdness

- A particle (or an atom) can:
  - Be in two different states at the same time.
  - Be in several places at the same time.
  - Move from A to B without ever occupying the space between them (tunneling).
  - Communicate information to another distant particle instantly (quantum teleportation).

Quantum Computers

- We can exploit 3 weird quantum phenomena to build a new kind of computer.

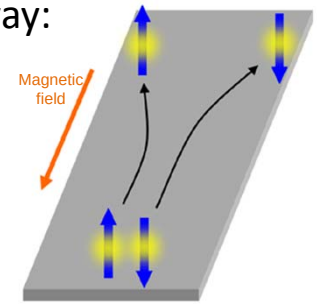
Intrinsic Angular Momentum

- Particles have a property (intrinsic angular momentum) that has two distinct values.
- Call the values "up" and "down".
- Or +½ and -½.
- Or |1> and |0>.

- Intrinsic angular momentum is called "spin" but that is misleading. Nothing is spinning.

Measurement

- We can measure a particle's state and we will always get one of two results: |0> or |1>.
  - There are no intermediate values. Spin is quantized.
- How do we measure? One way:
  - Pass the particle through a magnetic field.
  - It will go left if its state is |0> and right if |1>.
  - Put a detector on each side.



Q Weirdness 1: Mixtures of States

- Before we measure, a particle's state can be a mixture of "up" and "down".
- Suppose it's ¾ "up" and ¼ "down".
- When we measure the state, we will get:
  - "Up" with probability 0.75
  - "Down" with probability 0.25
- Once we measure, the state is fixed; it's either "up" or "down". No more mixture.

Bits vs. Qubits

- Conventional computers use bits:
  - Value is either 0 or 1. Might be encoded by a voltage, e.g., "0" = 0 volts, "1" = +5 volts.
  - There are no mixture states. A value of +2 volts would indicate a broken computer.
- Quantum computers use qubits instead of bits. Qubits can have mixture states.

Qubits in Mixture States

- Let |0> denote the 100%"down" state and |1> the 100% "up" state. These are *basis* states.
- Any qubit's state can be expressed in terms of the basis states using two coefficients *a* and *b*:

  $a|0\rangle + b|1\rangle$

  where $|a|^2 + |b|^2 = 1$.

Mixture States (cont.)

- Mixture state is: $a|0\rangle + b|1\rangle$
- So the 100% "down" state is a=1,b=0
  The 100% "up" state is a=0,b=1
- Equal mixture of "up" and "down" would be:

  $a = b = \frac{1}{\sqrt{2}}$

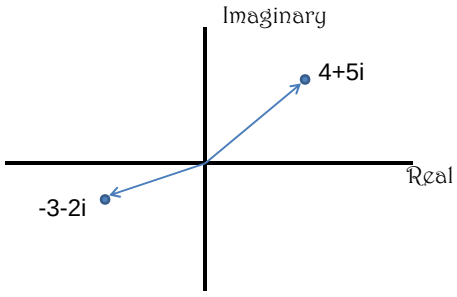
  because we must have: $a^2 + b^2 = \frac{1}{2} + \frac{1}{2} = 1$

Q Weird. 2: Complex Amplitudes

- "Normal" mixture coefficients: $0 \leq x \leq 1$.
- Combine by simple addition: $a + b = 1$.
- Negative values would make no sense.
  - Can you have a dog that is 4/3 golden retriever and -1/3 german shepherd? No!
- But in quantum mechanics, the mixture coefficients are *complex numbers*!
- That's why the mixture rule is $|a|^2 + |b|^2 = 1$.

Complex Numbers: Cartesian Form

- Define *i* as $\sqrt{-1}$
- Complex numbers: p = a + b*i,* q = c + d*i*

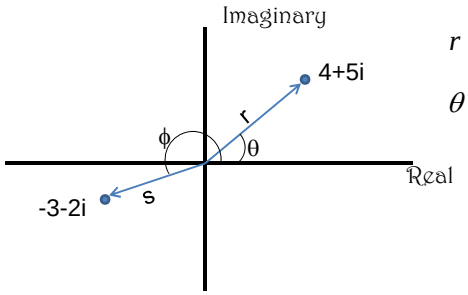


Complex Arithmetic

- Complex numbers: p = a + b*i*, q = c + d*i*
- p+q = (a+b*i*) + (c+d*i*) = (a+c) + (b+d)*i*
- p×q = (a+b*i*) × (c+d*i*)
  = a×c + a×d*i* + b*i*×c + b*i*×d*i*
  = (ac-bd) + (ad+bc)*i*

Complex Numbers: Polar Form

- Defined in terms of a magnitude and phase.
- Complex numbers: p = <r,θ>, q = <s,ϕ>



$$r = \sqrt{4^2 + 5^2}$$

$$\theta = \arctan\frac{5}{4}$$

Complex Arithmetic (Polar)

- Complex numbers: p = <r,θ>, q = <s,ϕ>
- p+q = <r,θ> + <s,ϕ> = *something messy*
- p×q = <r,θ> × <s,ϕ> = <r·s, θ+ϕ>
- Some common constants:

  1 = <1, 0°> -1 = <1, 180°>

  i = <1, 90°> -i = <1, 270°>

  So i × i = <1·1, 90°+90°> = <1, 180°> = -1
- Multiplication is just scaling plus rotation!

Complex Magnitude

- In polar form:

  p = <r,θ> so |p| = r
- In rectangular form:

  p = a + bi, so $|p| = \sqrt{a^2 + b^2}$
- In quantum mechanics, probability is the square of the complex coefficient: $|p|^2$

Quantum Weirdness 2a: Phase

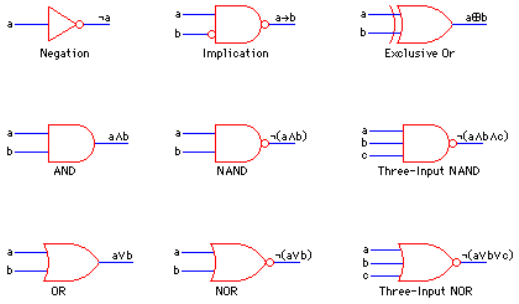
- Consider a photon in state a|0> + b|1>.
- The complex coefficients ("amplitudes") *a* and *b* have both magnitude and phase.
- Photons have *polarization* determined by the relative phases of *a* and *b*.
  - Vertically polarized, horizontally polarized, left or right circularly polarized, elliptically polarized, etc.
- Polarized sunglasses filter out photons based on phase to reduce glare.

Logic Gates

Conventional Boolean logic gates:

1-input: the NOT gate

2-input: AND, OR, NAND, NOR, XOR, EQV, …

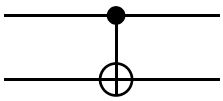


Quantum Gates

- 1-input quantum gates change the magnitudes and/or phases of *a* and *b*. Assume state is: a|0> + b|1>.
- Pauli-X gate: (a,b) → (b,a) quantum NOT
- Pauli-Y gate: (a,b) → (b*i*,-a*i*)
- Pauli-Z gate: (a,b) → (a,-b) phase flip
- Hadamard: (a,b) → (a+b,a-b) /$\sqrt{2}$

Quantum Gates

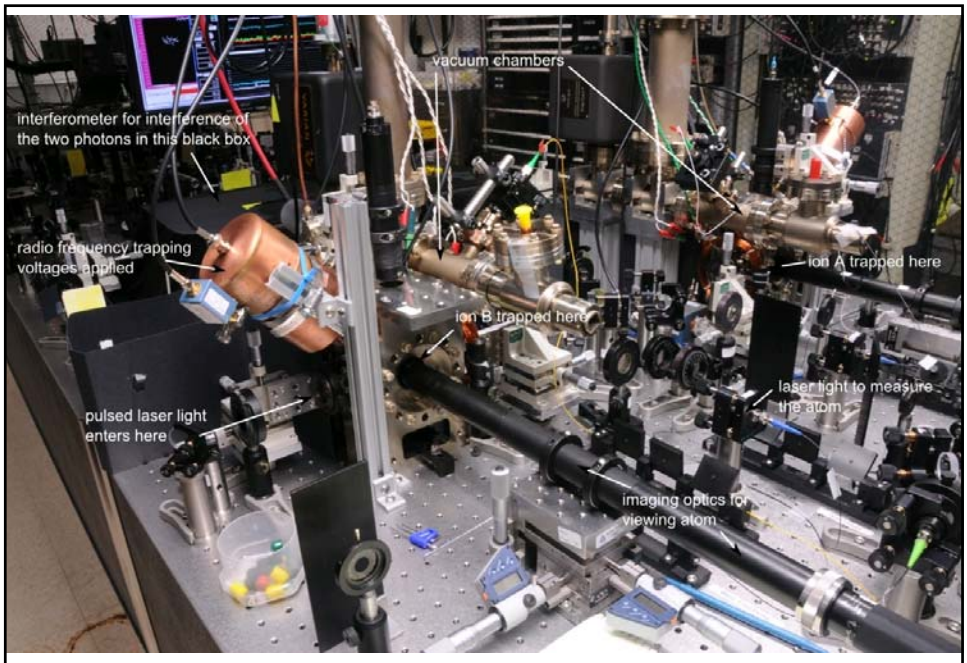
- 2- and 3-input quantum gates perform operations on one qubit based on the values of one or two other qubits.
- Controlled-NOT gate performs NOT on second qubit when first qubit is |1>.



- More gates: Toffoli, Fredkin, etc.

How to Make a Quantum Gate

- Use trapped ions for qubits.
  - Trap them in a vacuum using magnetic fields.
- Zap the ions with:
  - Magnetic fields
  - Lasers
  - Radio waves



QW3: Entanglement (Big Payoff)

- Suppose we have two independent qubits:
  $q_1 = a_1|0> + b_1|1>$
  $q_2 = a_2|0> + b_2|1>$
- If we measure them, we find that:
  q_1 is "down" with probability $|a_1|^2$
  q_2 is "down" with probability $|a_2|^2$
- For n qubits, we have 2n amplitudes.
- But qubits don't have to be independent…

Entanglement

- We can "hook up" two qubits so that their states are bound together, or "entangled".
- Now they have a joint state space:

  $a|00> + b|01> + c|10> + d|11>$

  where a, b, c, d can all vary freely,
  subject to $|a|^2+|b|^2+|c|^2+|d|^2 = 1$.
- If a=d=0 then q_1 and q_2 have opposite states.

Implications of Entanglement

- If we entangle *n* entangled qubits, the resulting system has 2^n independent coefficients.
- You can operate on all 2^n coefficients *in parallel* by applying quantum gates.
- 50 entangled qubits give $2^{50} = 10^{15}$ coefficients: more memory than in any computer!

Quantum Algorithms

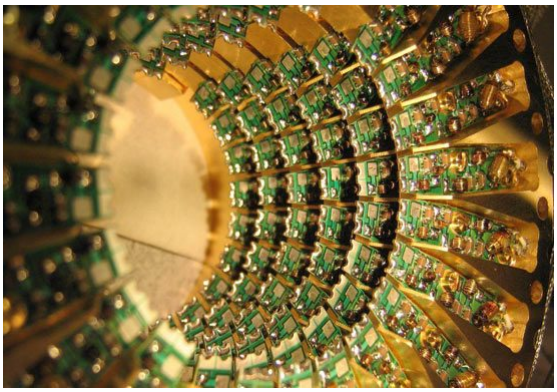
- Shor's algorithm can factor numbers.
  - Runs in time polynomial in # of digits.
  - Exponentially faster than conventional computer.
  - Might break RSA encryption.
- In 2001 IBM demonstrated factorization of 15 into 3 and 5 using a 7-qubit quantum computer.
- Another group has factored 21 into 3 and 7.

Quantum Algorithms

- Grover's algorithm for searching unordered lists (or inverting a function).
  - Runs in time O(sqrt(N)) where N = # of items
  - Conventional computer requires O(N) time.
- Works by exploiting the fact that coefficients have phases that can amplify (if in phase) or attenuate (if out of phase) when added.
- Google wants to use quantum algorithms for fast, sophisticated searching.

Obstacles to Quantum Computers

- Qubits don't last very long (decoherence).
  - Must keep them isolated to preserve their states.
  - Atoms cooled to almost absolute zero.
  - Any collision is a "measurement" that will "collapse the wave function": no more mixture.
- Entanglement is tricky to achieve.
  - Gets harder as the number of qubits goes up.



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