Introduction to Computer Science

Introduction (again)

Ryan Stansifer

Department of Computer Sciences
Florida Institute of Technology
Melbourne, Florida USA 32901

http://www.cs.fit.edu/~ryan/

8 January 2012

Overview of Course

- Introduction. What is CS? What is a computer?
- Java review. Data, control constructs, static methods
- Classes. Incorporation, instantiation, inheritance
- Generics. Code reuse
- Data structures. Lists, stacks, queue

Course Goals

- Programming
  - exciting to translate ideas into reality
  - basics are simple, yet programming well is difficult; do not underestimate the challenge
  - problem solving is hard and difficult to teach
- Computer Science
  - Computer Science is not just programming
  - It is easy to lose sight of the big picture, so we have a general introduction
  - Other (non-programming) topics from time to time: architecture, Monte Carlo methods, $O(N)$, invariants, and so on

Outline of Introduction

- What is Computer Science? Architecture, OS, networking, ...
- What is a computer? Architecture, CPU, memory hierarchy
- Interface layers: hardware, operating system, application
- The Java platform
  - JVM and a million other pieces
  - Java history, pragmatics
- Programming languages — not just Java
- Program development; debuggers and so on
- Program style. A program is a text file
- I/O, streams

Outline

What is Computer Science?

What is Computer Science?

computer science. *The study of information, protocols and algorithms for idealized and real automata.*

What is Computer Science?

computer science. *The study of information, protocols and algorithms for idealized and real automata.*

- automaton: “self moving” – in our context, self “deciding” or autonomous mechanism

What is Computer Science?

> **computer science**. *The study of information, protocols and algorithms for idealized and real automata.*

- automaton: “self moving” – in our context, self “deciding” or autonomous mechanism
- information: knowledge represented in a form suitable for transmission, manipulation, etc.

What is Computer Science?

> **computer science**. *The study of information, protocols and algorithms for idealized and real automata.*

- automaton: “self moving” – in our context, self “deciding” or autonomous mechanism
- information: knowledge represented in a form suitable for transmission, manipulation, etc.
- protocol: rules for exchanging information

What is Computer Science?

computer science. *The study of information, protocols and algorithms for idealized and real automata.*

- automaton: “self moving” – in our context, self “deciding” or autonomous mechanism
- information: knowledge represented in a form suitable for transmission, manipulation, etc.
- protocol: rules for exchanging information
- algorithm: an unambiguous, finite description in simple steps of actions

What is Computer Science?

computer science. *The study of information, protocols and algorithms for idealized and real automata.*

- automaton: “self moving” – in our context, self “deciding” or autonomous mechanism
- information: knowledge represented in a form suitable for transmission, manipulation, etc.
- protocol: rules for exchanging information
- algorithm: an unambiguous, finite description in simple steps of actions

What is Computer Science?

> **computer science**. *The study of information, protocols and algorithms for idealized and real automata.*

- automaton: “self moving” – in our context, self “deciding” or autonomous mechanism
- information: knowledge represented in a form suitable for transmission, manipulation, etc.
- protocol: rules for exchanging information
- algorithm: an unambiguous, finite description in simple steps of actions

Computer Science is not the study of computers, nor is it the practice of their use.

Mathematics, science, or engineering?

Mathematics. *The science of numbers, interrelations, and abstractions.*

Science. *Systematic knowledge or practice. Acquiring knowledge through the scientific method of natural phenomena (natural sciences) or human or social behavior (social sciences).*

Engineering. *The applied science of acquiring and applying knowledge to design, or construct works for practical purposes.*

What is CS?

- Engineering? Application of science?
- Natural science? Observable phenomena?
- Mathematics? Invisible abstractions?
- Social science? Functioning of human society?

CS is exciting and difficult as it is all these things.

Mathematics is the Queen of Science, and Arithmetic the Queen of Mathematics. - C. F. Gauss

> *Philosophy is written in this grand book, the universe which stands continually open to our gaze. But the book cannot be understood unless one first learns to comprehend the language and read the letters in which it is composed. It is written in the language of mathematics, and its characters are triangles, circles and other geometric figures without which it is humanly impossible to understand a single word of it; without these, one wanders about in a dark labyrinth.*

Galileo Galilee in Assayer

We are at the dawn of new era. The, as yet unfinished, language of computation is the language of science and engineering.

Existential Angst

The Scream by the Norwegian artist Edvard Munch, painted in 1893.

What Does A Computer Scientist Do?

Just like mathematics, everyone in modern society uses computing. So getting a computer science degree prepares you for everything and nothing.

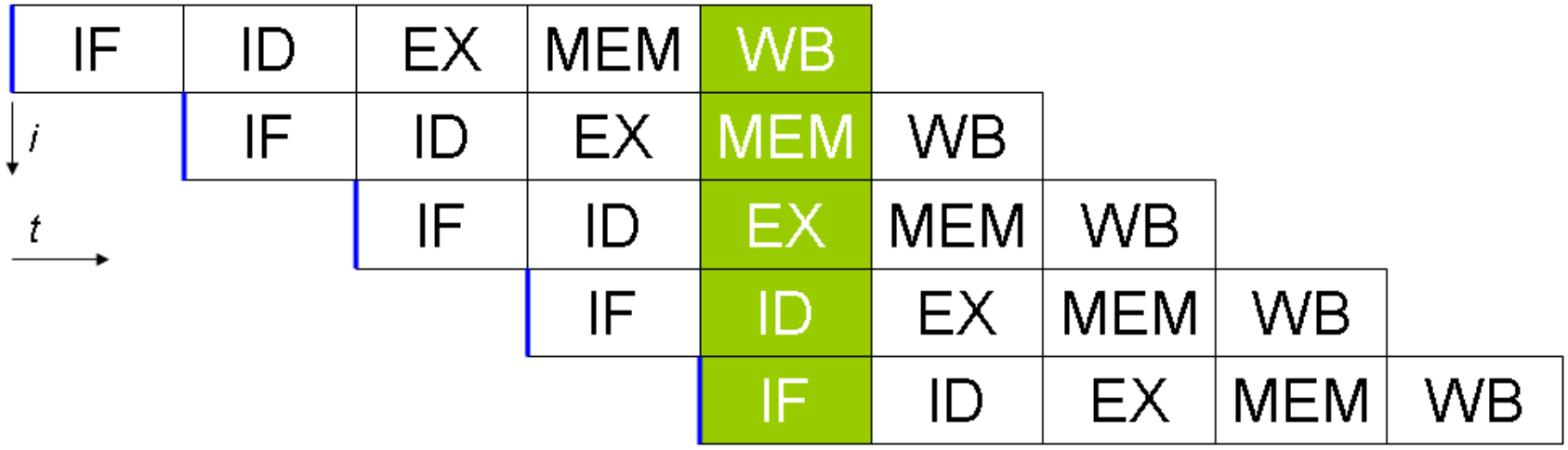
The most visible activity is commanding computers to do our bidding, i.e., programming.

What do you want to do?

Fields

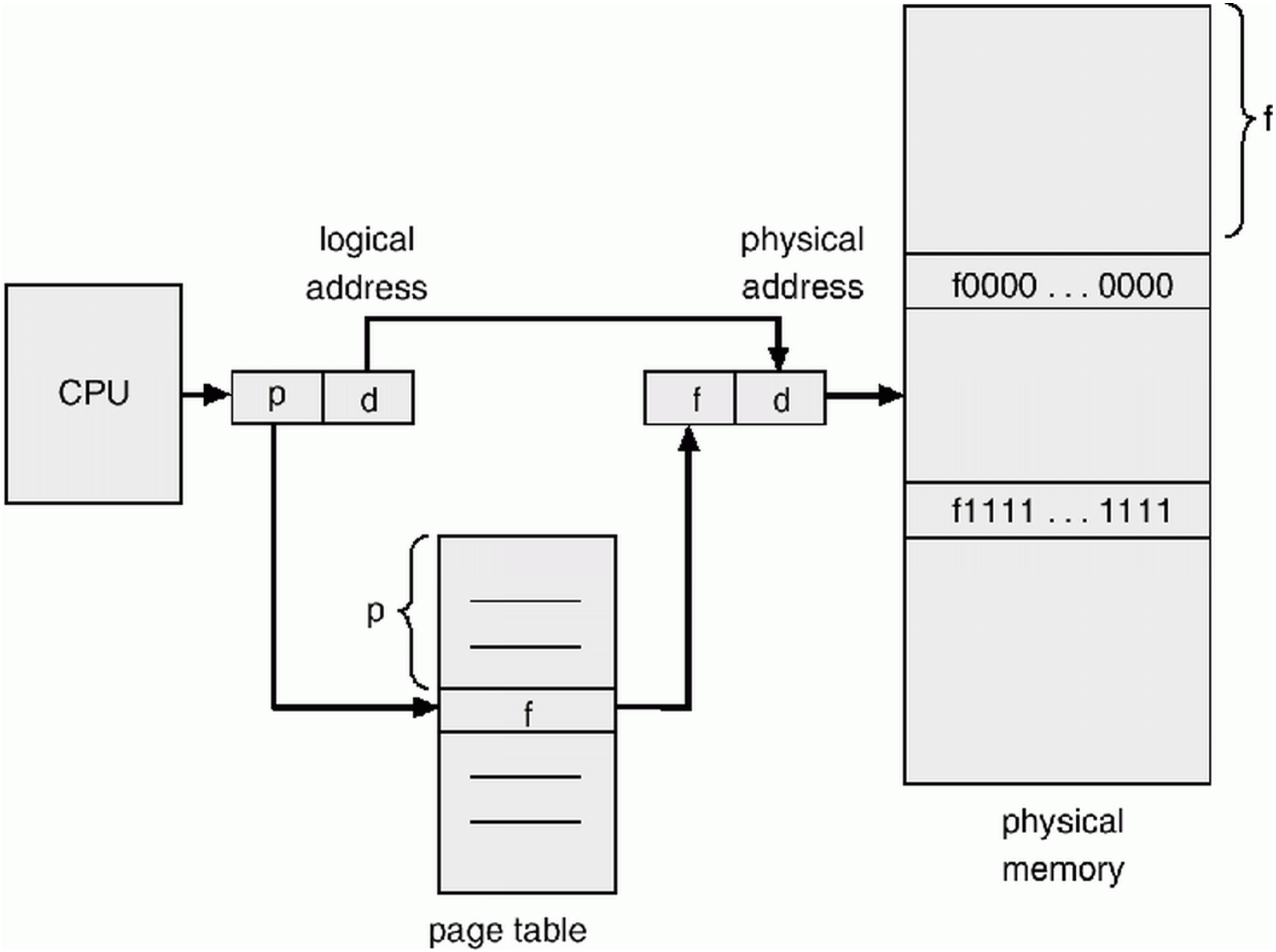
- Computer architecture
- Operating systems
- Programming languages and compilers
- Algorithms, data structures, complexity
- Computability theory
- Numerical analysis
- Networking and distributed computing
- Parallel computing
- Information Management/Database systems
- Software development (aka Software Engineering)
- Human-computer communication/interaction
- Graphics and Visual Computing
- Intelligent Systems (aka Artificial Intelligence)

Architecture

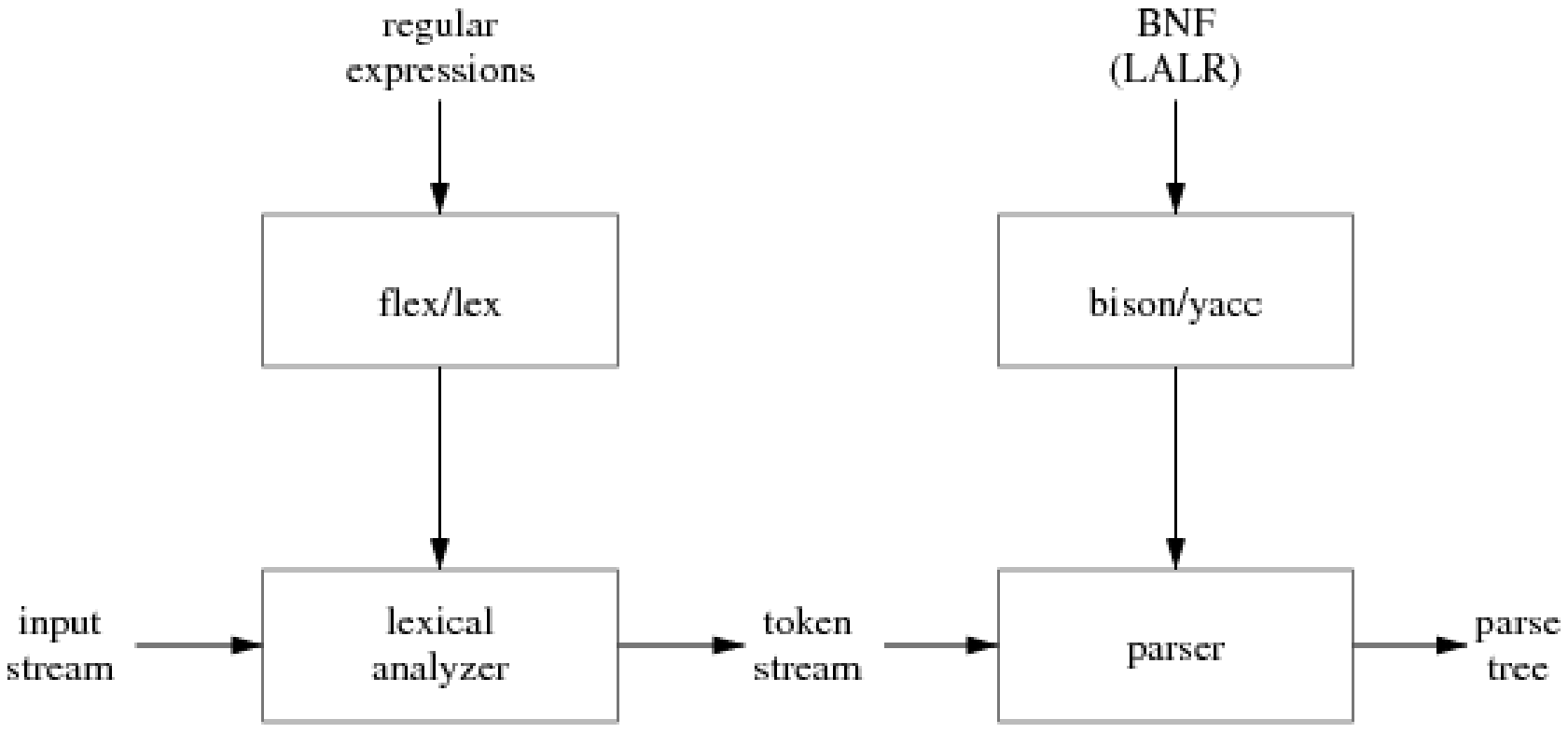


Basic five-stage pipeline in a RISC machine: instruction fetch, instruction decode, execute, memory access, register write back.

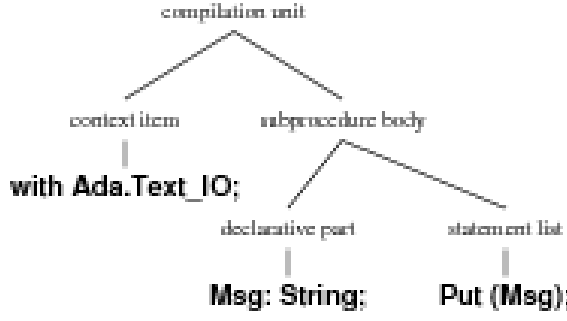
Operating Systems — paging

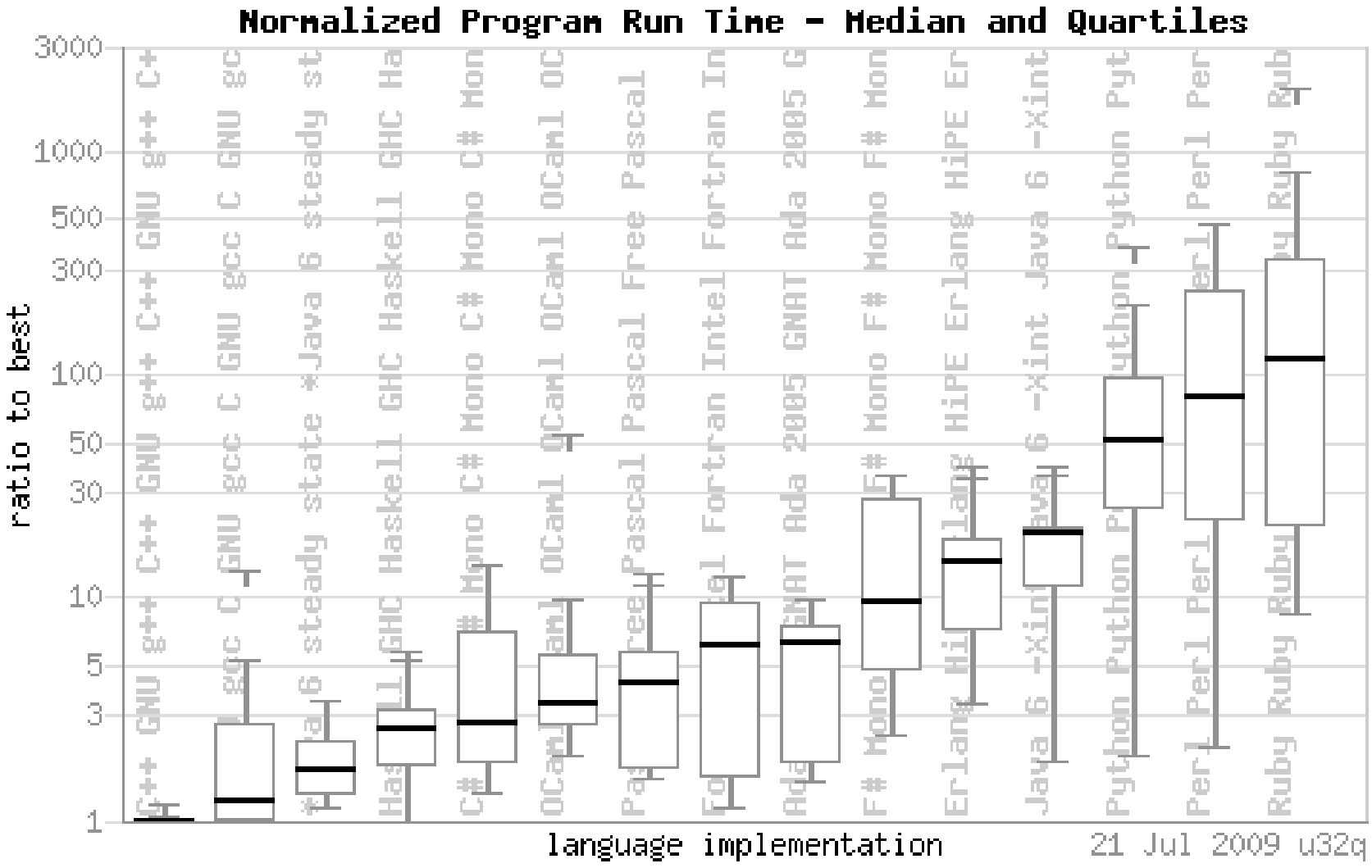


Programming Languages and Compilers

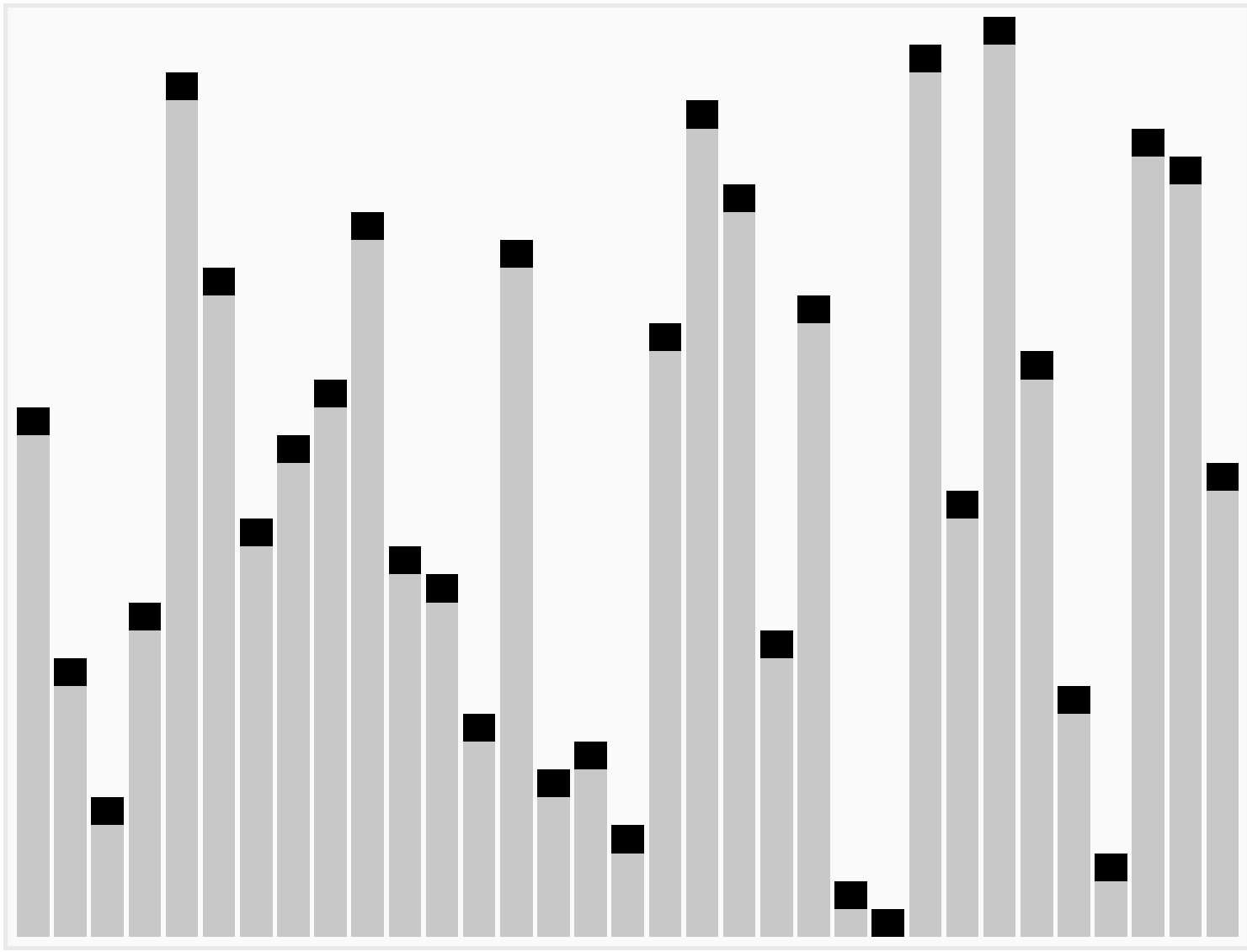



```
w i t h   b e g i n  2 * x ;
```

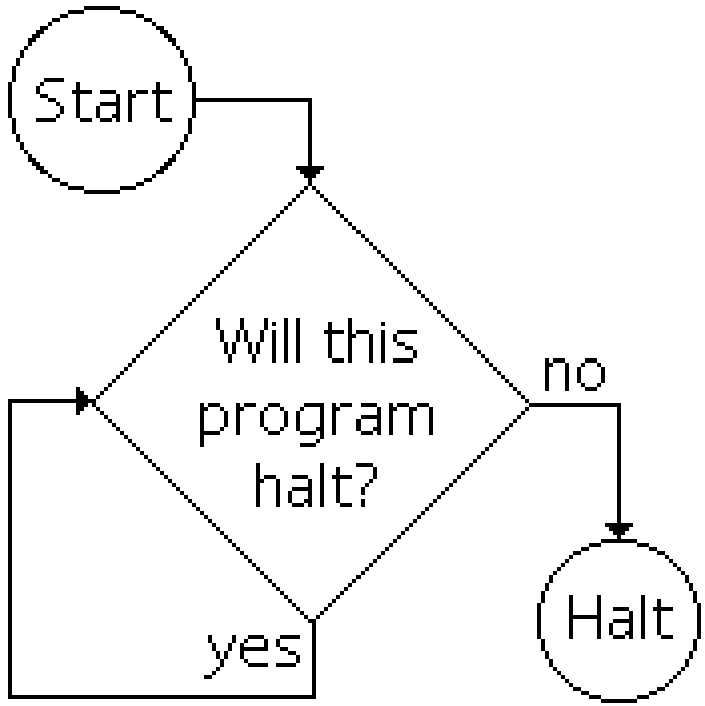



Normalized Program Run Time - Median and Quartiles
ratio to best
3000
1000
500
300
100
50
30
10
5
3
1
language implementation
21 Jul 2009 u32q

Algorithms and Data Structures — Sorting



Theory of Computation — halting problem



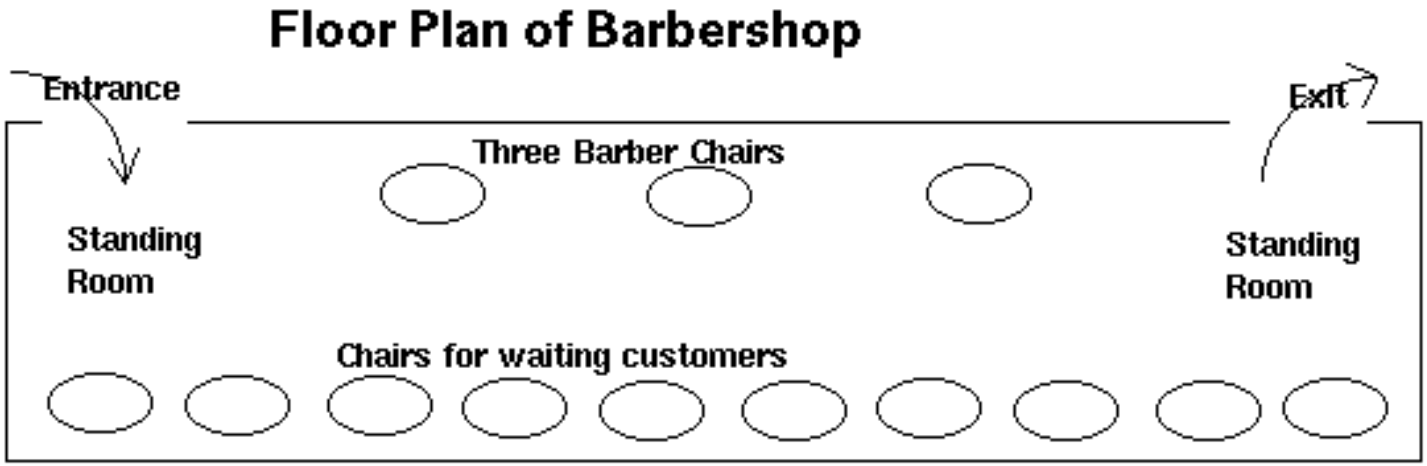
Numerical Analysis

> *A report from the United States General Accounting Office begins "On February 25, 1991, a Patriot missile defense system operating at Dhahran, Saudi Arabia, during Operation Desert Storm failed to track and intercept an incoming Scud. This Scud subsequently hit an Army barracks, killing 28 Americans." The report finds the failure to track the Scud missile was caused by a precision problem in the software.*

Nicholas J. Higham, *Accuracy and Stability of Numerical Algorithms*, SIAM, 1996, ISBN13 9780898713558. Page 505.

`http://www.ima.umn.edu/~arnold/disasters/disaster.html`

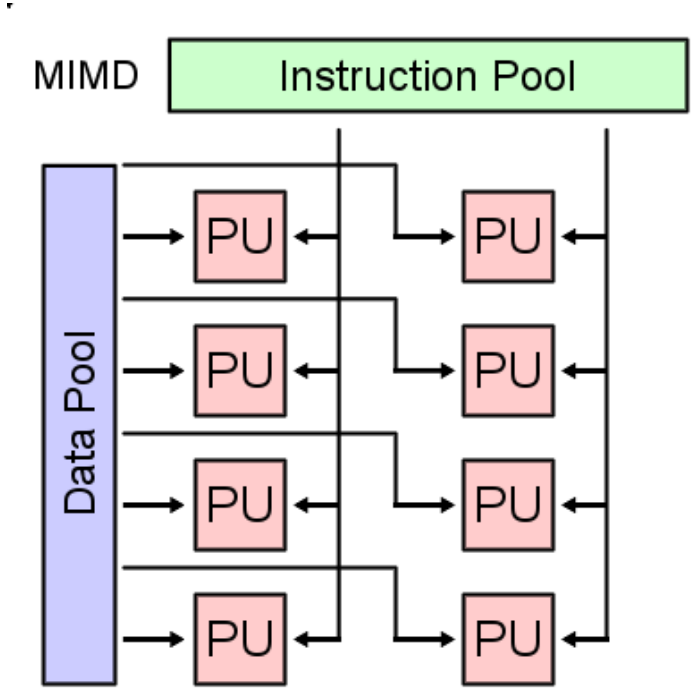
Distributed Computing — barber shop problem



Parallel Computing

single data	SISD	MISD
multiple data	SIMD	MIMD

Flynn's taxonomy



Information Management/Database Systems

Name

A	B
Dot	cat
Sue	dog
Zan	cat
Bip	bird

Have

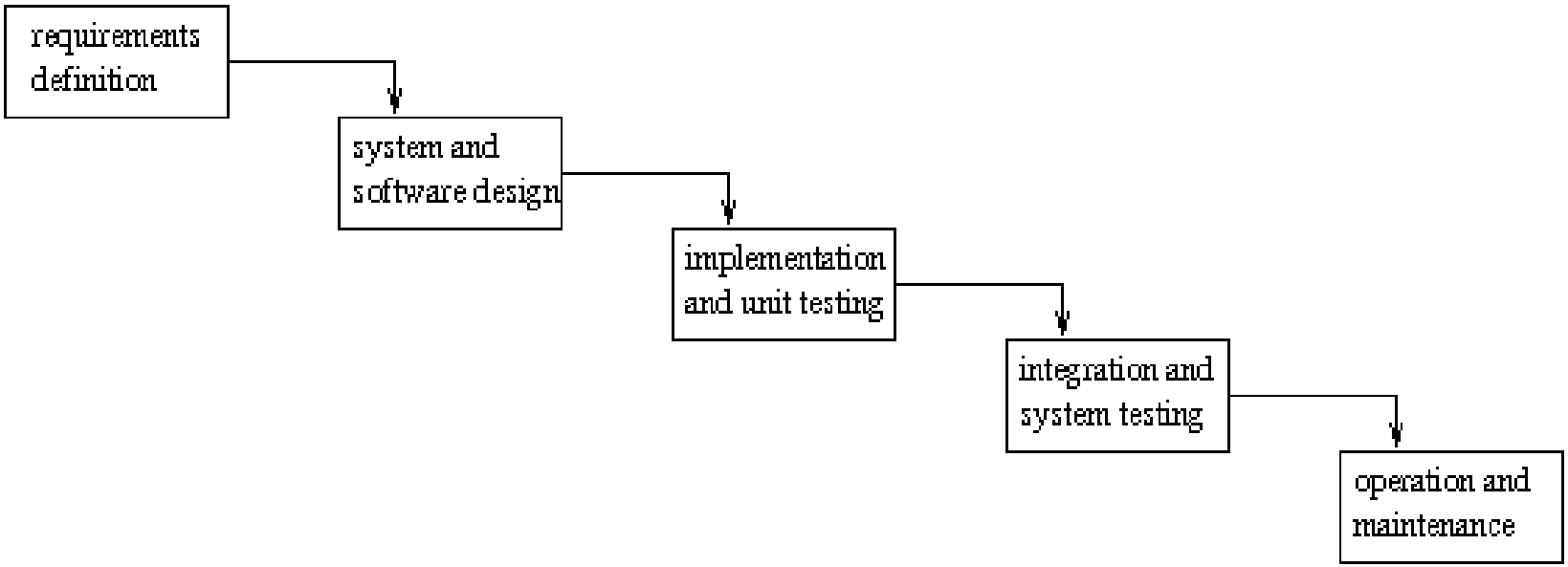
B	C
cat	shots
dog	shots
dog	leash

Result of Join

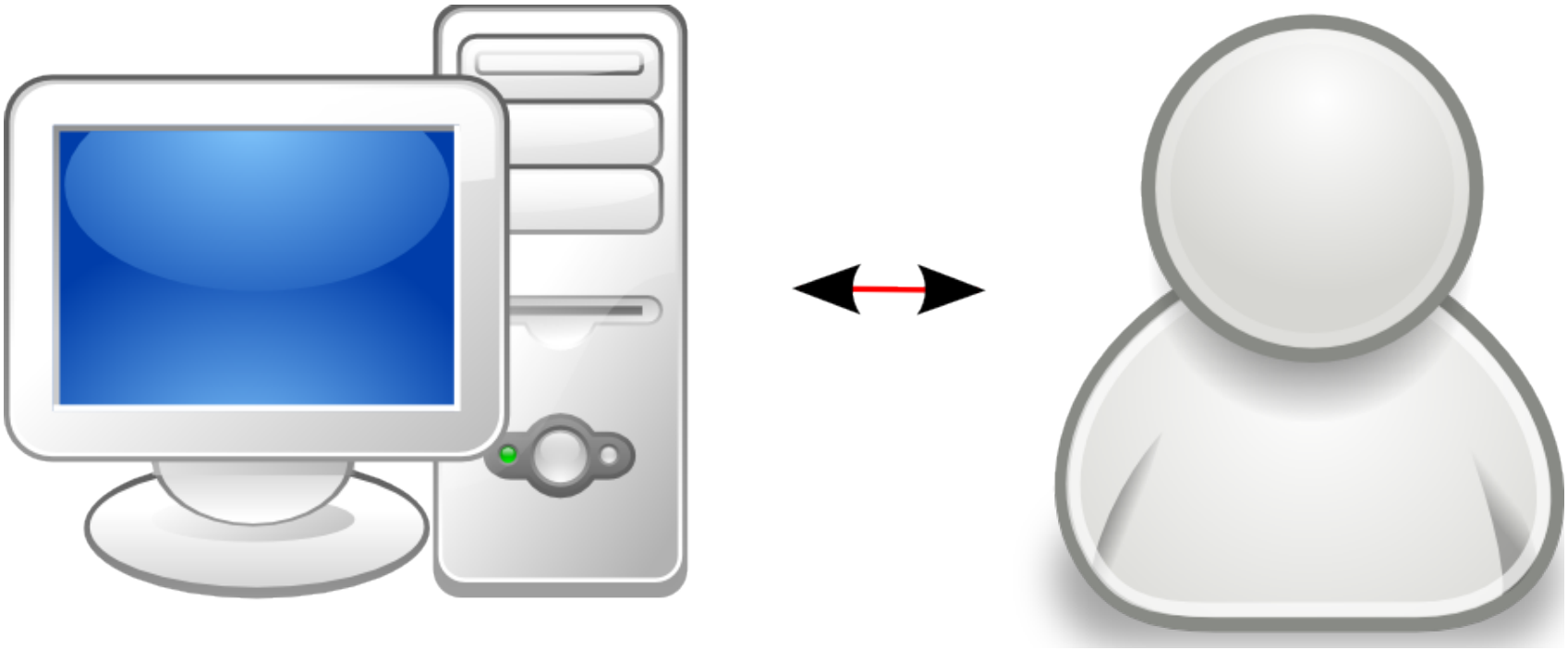
A	B	C
Dot	cat	shots
Sue	dog	shots
Sue	dog	leash
Zan	cat	shots

The join of two relational tables

Software Engineering — waterfall model



Human-Computer Communication/Interaction



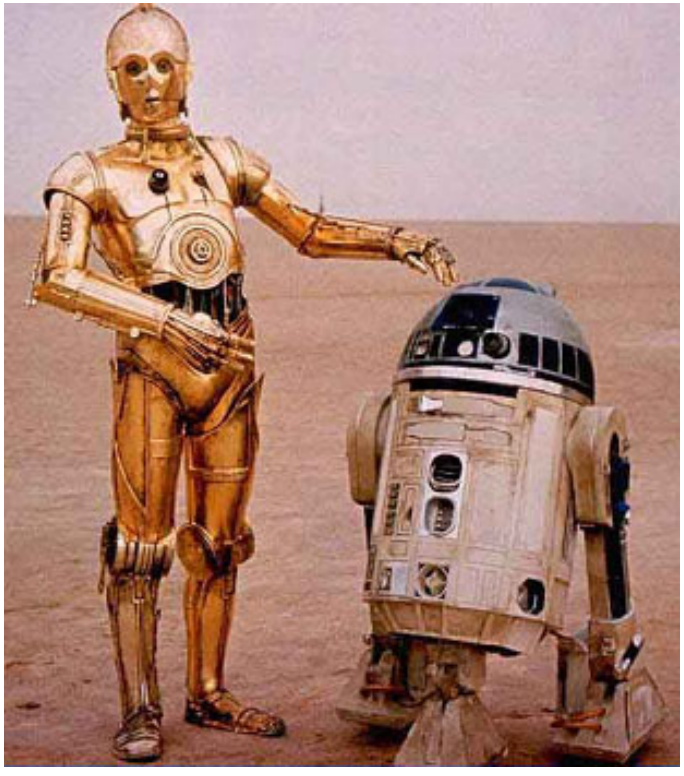
Cue `Macintosh_Plus_in_StarTrek`

Graphics and Visual Computing

Frozen Fire

- 37 hours to render
- POV ray uses a C-like programming language

Intelligent Systems

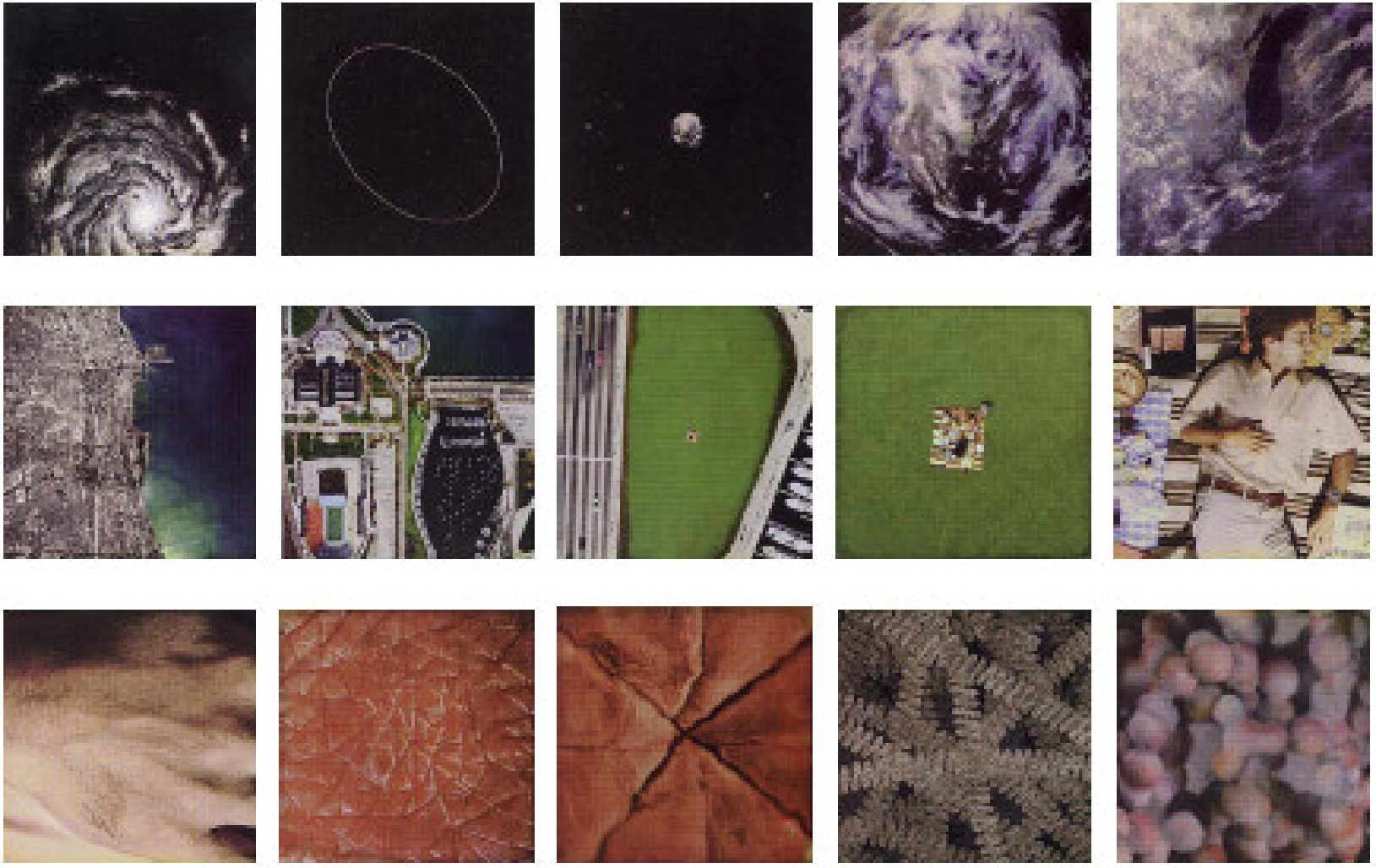


C3PO and R2D2 are fantasy robots from the movie Star Wars, while Kiva's industrial robots can efficiently and intelligently move shelves in a warehouse.


THINK
ДУМАЙ
सोचिए
$0
$1,200
$0
KEN
WATSON
BRAD

End of the overview of different fields of study in computer science

Computing is complex. There are many layers of interesting stuff between the person and the automaton.



The vastness and minuteness of time and space is a challenge to comprehend.

From Wikipedia, the free encyclopedia

Section	Range (m)		Unit	Example Items
	≥	<		
Subatomic	0	10^{-15}	am	electron, quark, string
Atomic to Cellular	10^{-15}	10^{-12}	fm	proton, neutron
	10^{-12}	10^{-9}	pm	wavelength of gamma rays and X-rays, hydrogen atom
	10^{-9}	10^{-6}	nm	DNA helix, virus, wavelength of optical spectrum
Human Scale	10^{-6}	10^{-3}	µm	bacterium, fog water droplet, human hair[1]
	10^{-3}	10^{0}	mm	mosquito, golf ball, soccer ball,
	10^{0}	10^{3}	m	human being, American football field, Eiffel Tower
	10^{3}	10^{6}	km	Mount Everest, length of Panama Canal, asteroid
Astronomical	10^{6}	10^{9}	Mm	the Moon, Earth, one light-second
	10^{9}	10^{12}	Gm	Sun, one light-minute, Earth's orbit
	10^{12}	10^{15}	Tm	orbits of outer planets, Solar System,
	10^{15}	10^{18}	Pm	one light-year; distance to Proxima Centauri
	10^{18}	10^{21}	Em	galactic arm
	10^{21}	10^{24}	Zm	Milky Way, distance to Andromeda Galaxy
	10^{24}	∞	Ym	visible universe

SI Prefixes

10^{12}	tera	T	trillion	1 000 000 000 000
10^{9}	giga	G	billion	1 000 000 000
10^{6}	mega	M	million	1 000 000
10^{3}	kilo	k	thousand	1 000
10^{2}	hecto	h	hundred	100
10^{1}	deca	da	ten	10
10^{0}	(none)		one	1
10^{-1}	deci	d	tenth	0.1
10^{-2}	centi	c	hundredth	0.01
10^{-3}	milli	m	thousandth	0.001
10^{-6}	micro	ν	millionth	0.000 001
10^{-9}	nano	n	billionth	0.000 000 001
10^{-12}	pico	p	trillionth	0.000 000 000 001

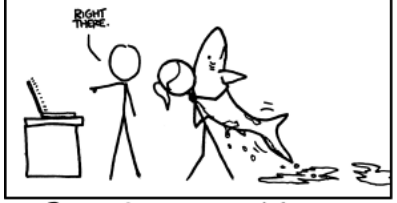
XKCD PRESENTS:

SOME NEW SCIENCE MNEMONICS

ORDER OF OPERATIONS

PARENTHESES, EXPONENTS, DIVISION & MULTIPLICATION, ADDITION & SUBTRACTION

TRADITIONAL: PLEASE EXCUSE MY DEAR AUNT SALLY



PLEASE EMAIL MY DAD A SHARK

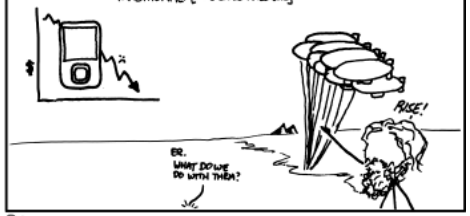
OR: PEOPLE EXPECT MORE DRUGS AND SEX

SI PREFIXES

KILO, MEGA, GIGA, TERA, PETA, EXA, ZETTA, YOTTA

MILLI, MICRO, NANO, PICO, FEMTO, ATTO, ZEPTO, YOCTO

TRADITIONAL: [I NEVER LEARNED ONE]



BIG:

KARL MARX GAVE THE PROLETARIAT ELEVEN ZEPPELINS, YO.

SMALL:

MICROSOFT MADE NO PROFIT FROM ANYONE'S ZUNES, YO.

TAXONOMY

KINGDOM, PHYLUM, CLASS, ORDER, FAMILY, GENUS, SPECIES

TRADITIONAL: KING PHILIP CAME OVER FOR GOOD SEX

KATY PERRY CLAIMS ORGASMS FEEL GOOD SOMETIMES

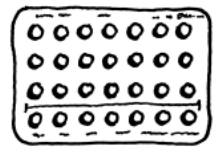
OR:

KERNEL PANICS CRASH OUR FAMILY GAME SYSTEM.

GEOLOGIC PERIODS

(PRECAMBRIAN) CAMBRIAN ORDOVICIAN SILURIAN DEVONIAN CARBONIFEROUS PERMIAN TRIASSIC JURASSIC CRETACEOUS PALEOGENE NEOGENE

TRADITIONAL: [I NEVER LEARNED ONE]



POLYCYSTIC OVARIAN SYNDROME DOES CAUSE PROBLEMS THAT JUDICIOUS CONTRACEPTIVES PARTIALLY NEGATE.

RESISTOR COLOR CODES

BLACK BROWN, RED, ORANGE, YELLOW, GREEN, BLUE, VIOLET, GRAY, WHITE

TRADITIONAL: [NONE I CARE FOR]

"BIG BROTHER REPTILIAN OVERLORDS," YELLED GLENN, "BRAINWASHING VIA GROUND WATER!!"

OR: BE BOLD, RESPECT OTHERS; YOU'LL GRADUALLY BECOME VERSATILE, GREAT WIKIPEDIANS!

PLANETS

MERCURY VENUS EARTH MARS JUPITER SATURN URANUS NEPTUNE

TRADITIONAL: MY VERY EXCELLENT MOTHER JUST SERVED US NACHOS

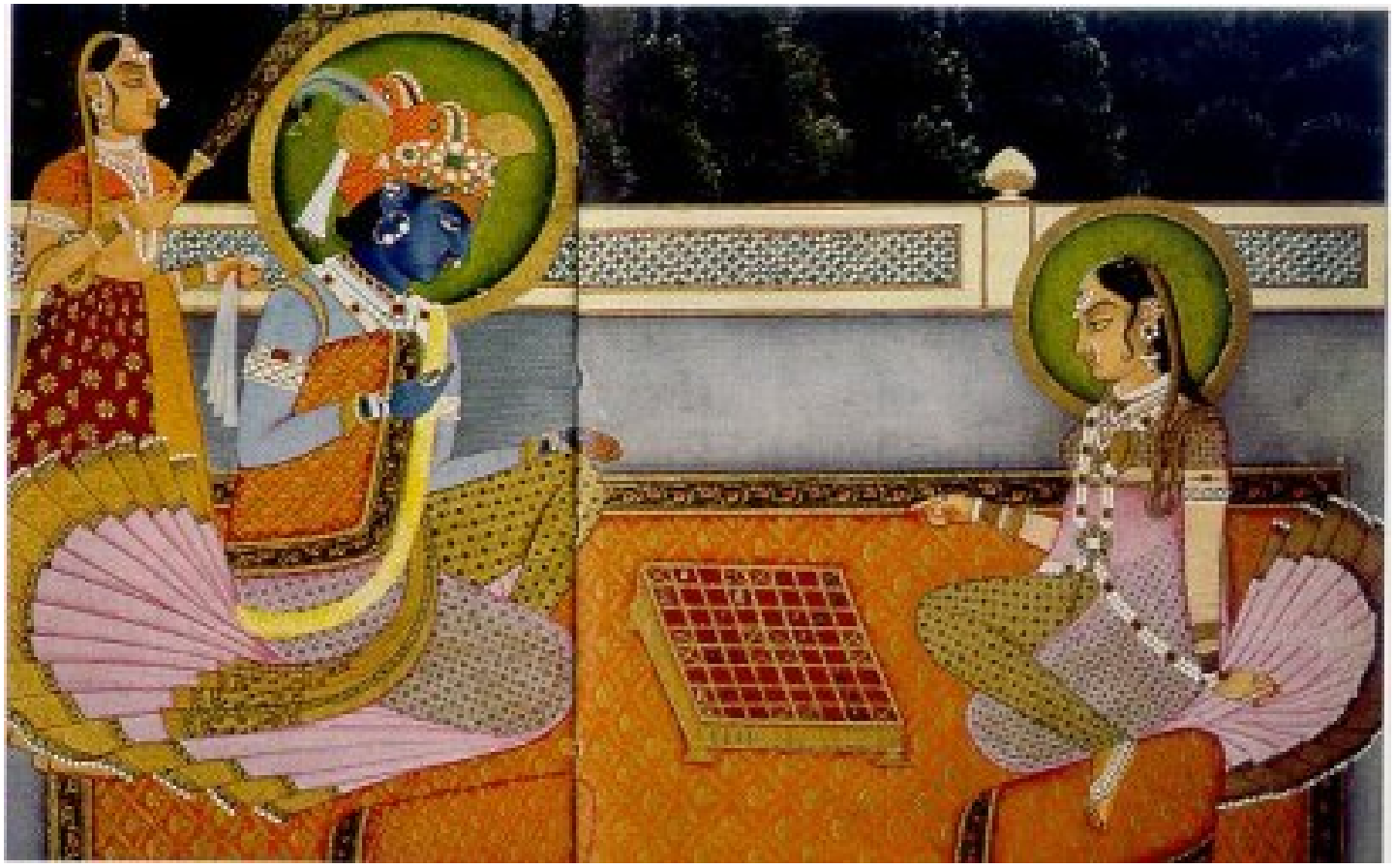
MARY'S "VIRGIN" EXPLANATION MADE JOSEPH SUSPECT UPSTAIRS NEIGHBOR

kilo, mega, giga, tera, peta, exa, zetta
Karl Marx gave the proletariat eleven zeppelins.
milli, micro, nano, pico, femto, atto, zepto
MicroSoft made no profit from anyone's zunes.
Every Player That Gets Mangled May Never Play Football Again
Exa Peta Tera Giga Mega Micro Nano Pico Femto Atto

Powers of Two

Because computers represent information in binary form, it is important to know how many pieces of information can be represented in n bits. 2^n pieces of information can be store in n bits, and so is it necessary to be familiar with powers of two.
It should be immediately obvious that $\lceil \log_2 n \rceil$ bits of are required to represent n things.

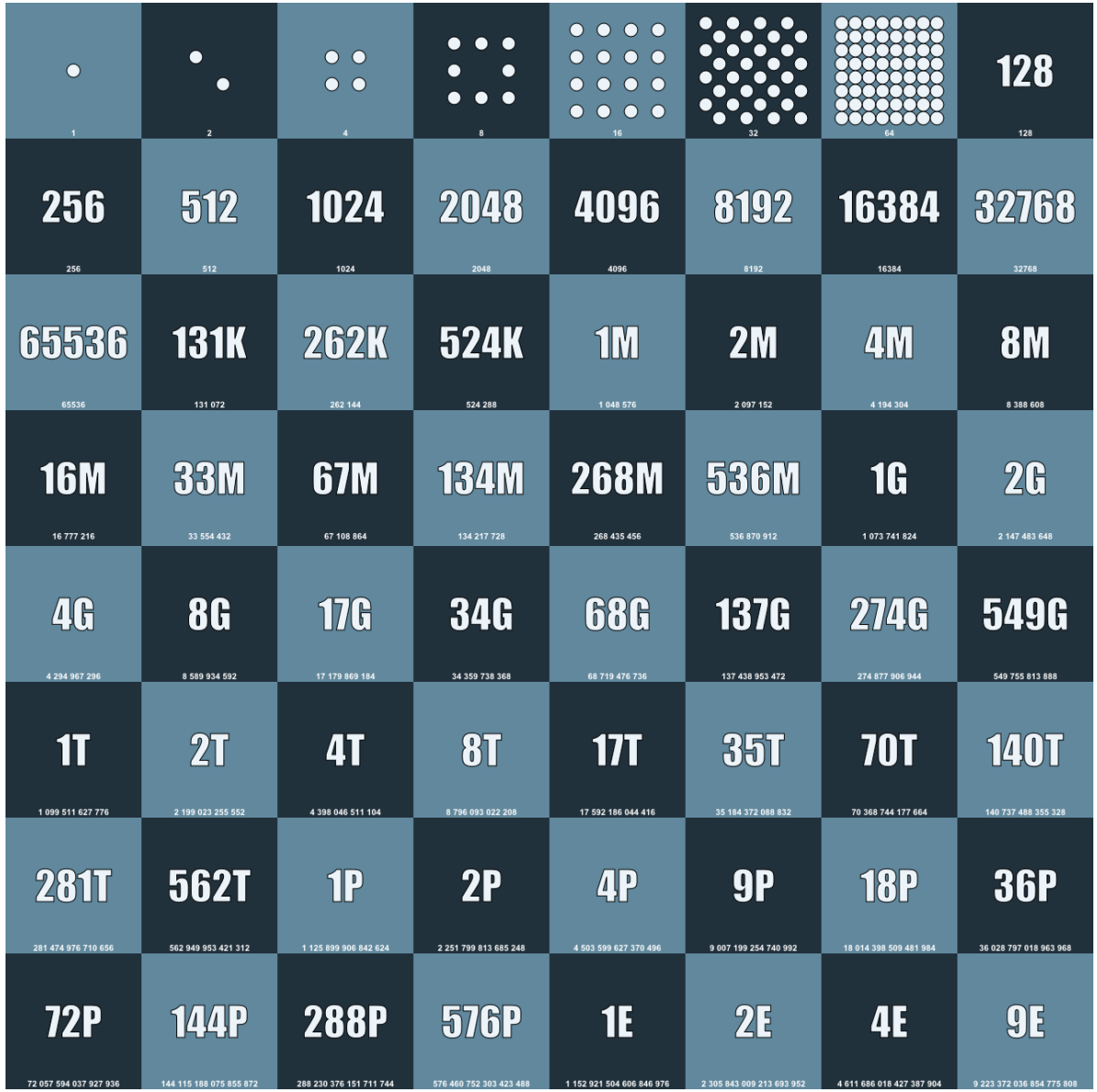
Because information is represented in ones and twos, doubling (exponential growth) is an important concept in computing.
To grasp it better we use an ancient Indian chess legend.



A picture of Krishna playing Chess from the National Museum, New Delhi

Legend of the Ambalappuzha Paal Payasam

According to the legend, Lord Krishna once appeared in the form of a sage in the court of the king who ruled the region and challenged him for a game of chess (or chaturanga).
The sage told the king that he would play for grains of rice—one grain of rice in the first square, two grains in the second square, four in the third square, eight in the fourth square, and so on. Every square would have double the number of grains of its predecessor. The king lost the game and soon realized that even if he provided all the rice in his kingdom, he would never be able to fulfill the promised reward. The sage appeared to the king in his true form, that of lord Krishna. and said he could serve paal-payasam (sweet pudding made of milk and rice) in the temple freely to the pilgrims every day until the debt was paid off.


1
2
4
8
16
32
64
128
256
512
1024
2048
4096
8192
16384
32768
65536
131K
262K
524K
1M
2M
4M
8M
16M
33M
67M
134M
268M
536M
1G
2G
4G
8G
17G
34G
68G
137G
274G
549G
1T
2T
4T
8T
17T
35T
70T
140T
281T
562T
1P
2P
4P
9P
18P
36P
72P
144P
288P
576P
1E
2E
4E
9E

We might try gains of sand instead of wheat. How much does a gain of sand weight? One grain of sand weighs about 0.01 grams.

Powers of Two

Suppose we double that one grain of sand and double that amount of sand again. And we do this again and again.

0	1	0.01g
1	2	0.02g
2	4	0.04g
3	8	0.08g
4	16	0.16g
5	32	0.32g
6	64	0.64g
7	128	1.28g
8	256	2.56g
9	512	5.12g

Powers of Two

10	1 024	10.24g	
11	2 048	20.48g	
12	4 096	40.96g	an ounce
⋮			
18	262 144	2.6kg	
19	524 288	5.2kg	a pound
20	1 048 576	10kg	two pounds
21	2 097 152	21kg	three pounds
30	1 073 741 824	1073kg	one ton
⋮			
40	1 099 511 627 776		12,000 tons

Powers of Two

Suppose we double 1 second and double that amount of time again. And we do this again and again.

0	1	1 second
1	2	2 seconds
2	4	4 seconds
3	8	8 seconds
4	16	16 seconds
5	32	32 seconds
6	64	a minute
7	128	2 minutes
8	256	4 minutes
9	512	8 minutes

Powers of Two

10	kilo	1 024	17 minutes
⋮			
19		524 288	one week
20	mega	1 048 576	two weeks
⋮			
25		33 554 432	a year
⋮			
30	giga	1 073 741 824	34 years
40	tera	1 099 511 627 776	37 millennia
50	peta	125 899 906 842 624	
60	exa	1 152 921 504 606 846 976	age of universe

Powers of Two

Notice that $2^{10} \approx 10^3$, so these powers have significance:

10	kilo	1 024	17 minutes
20	mega	1 048 576	two weeks
30	giga	1 073 741 824	34 years
40	tera	1 099 511 627 776	37 millennia
50	peta	125 899 906 842 624	
60	exa	1 152 921 504 606 846 976	age of universe
70	zetta	1 180 591 620 717 411 303 424	

One ought not to use SI prefixes for power of 2 (just powers of 10).

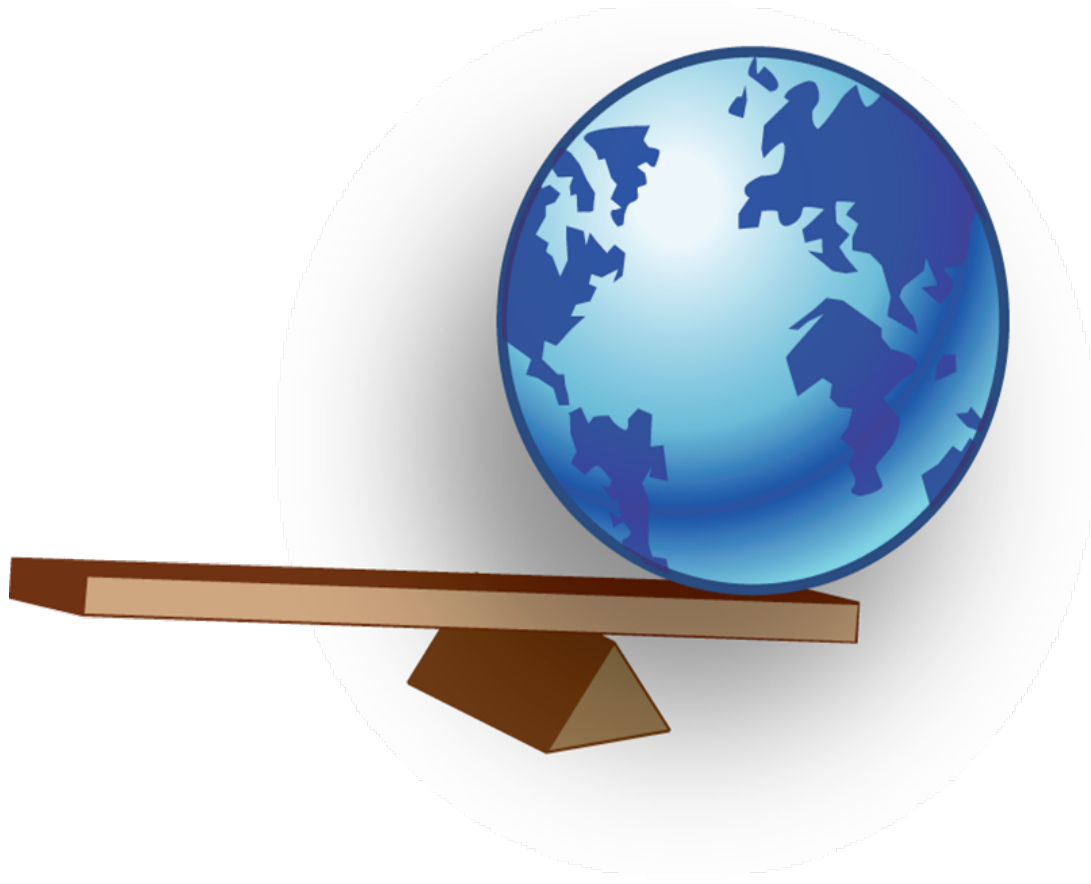
Powers of Two

Some other powers have special significance in computing.

7	128	size of ASCII char
8	256	size of Latin-1 char
16	65 536	size of Java **`short`**
31	2 147 483 648	no. of neg **`int`**
33	4 294 967 296	size of Java **`int`**
63	9 233 372 036 854 775 808	no. of neg **`long`**
64	18 446 744 073 709 551 616	size of Java **`long`**

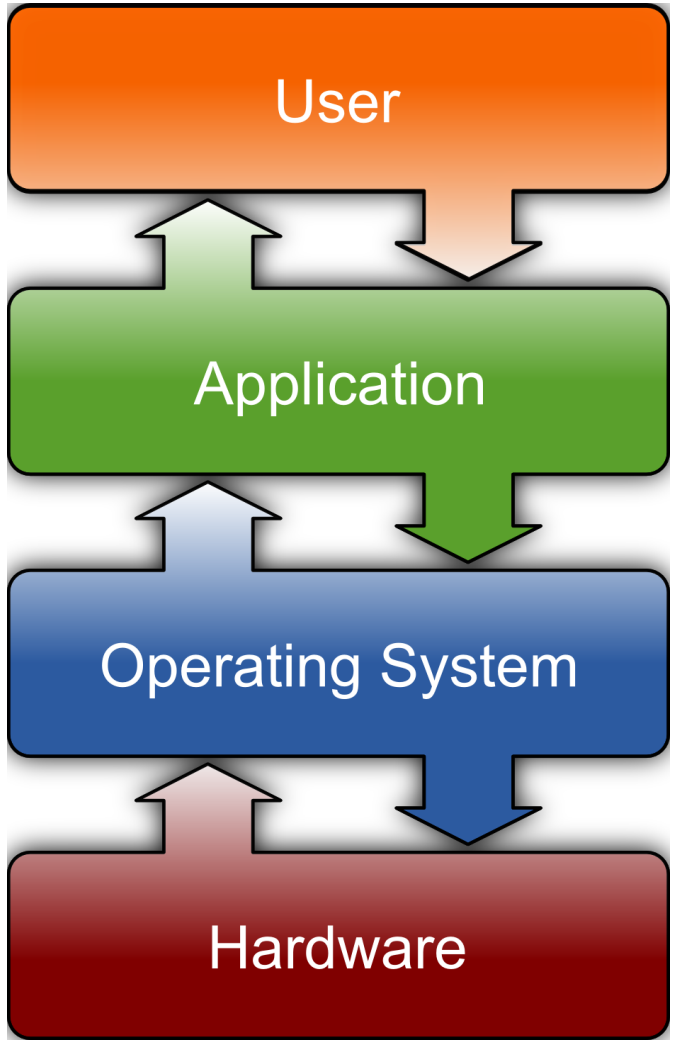
One challenge in computer science is the vast scale of computing devices.
A computer may have a terabyte (10^{12} bytes) worth of storage. A computer may execute ten instructions every nanosecond (10^{-9} seconds).

Software is a tool the enables us do things more efficiently and quicker than ever thought possible.



Everyone wants to be the person causing the earth to move. But the lever is really important.

Interface Layers



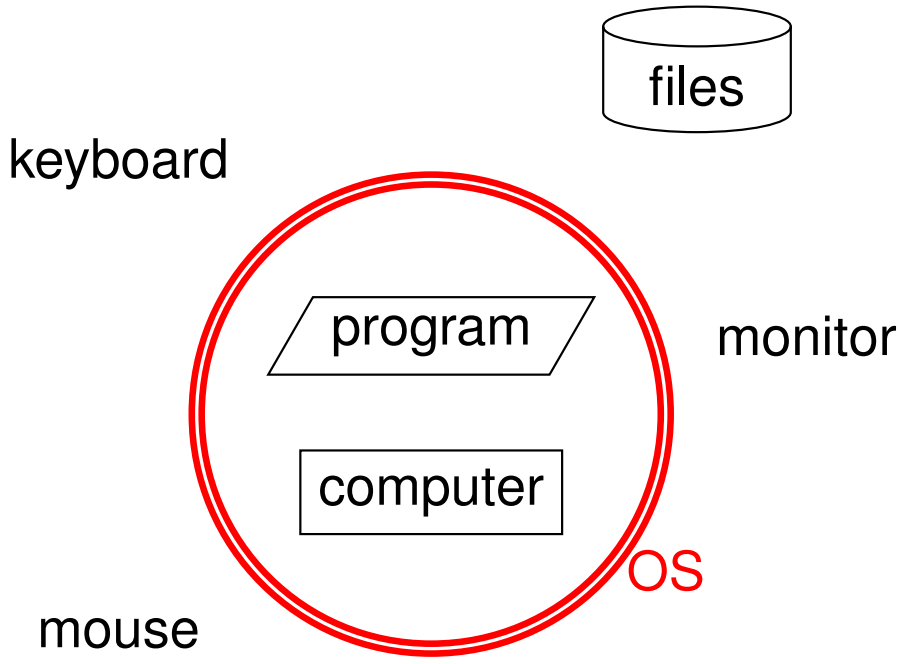
Computing is complex. There are many layers of interesting stuff between the person and the automaton.

- person (user)
- user-interface (mouse, etc)
- application (program)
- high-level programming language
- machine language
- operating system (OS)
- hardware
- logical devices
- physics

Definitions

- interface — An *interface* defines the communication boundary between two entities, such as a piece of software, a hardware device, or a user. It generally refers to an abstraction that an entity provides of itself to the outside.
- API — An *application programming interface (API)* is a set of procedures that an operating system, library, or service provides to support requests made by computer programs.
- IDE — In computing, an *Integrated development environment (IDE)* is a software application that provides facilities to computer programmers of a source code editor, a compiler and/or interpreter, build automation tools, and usually a debugger.

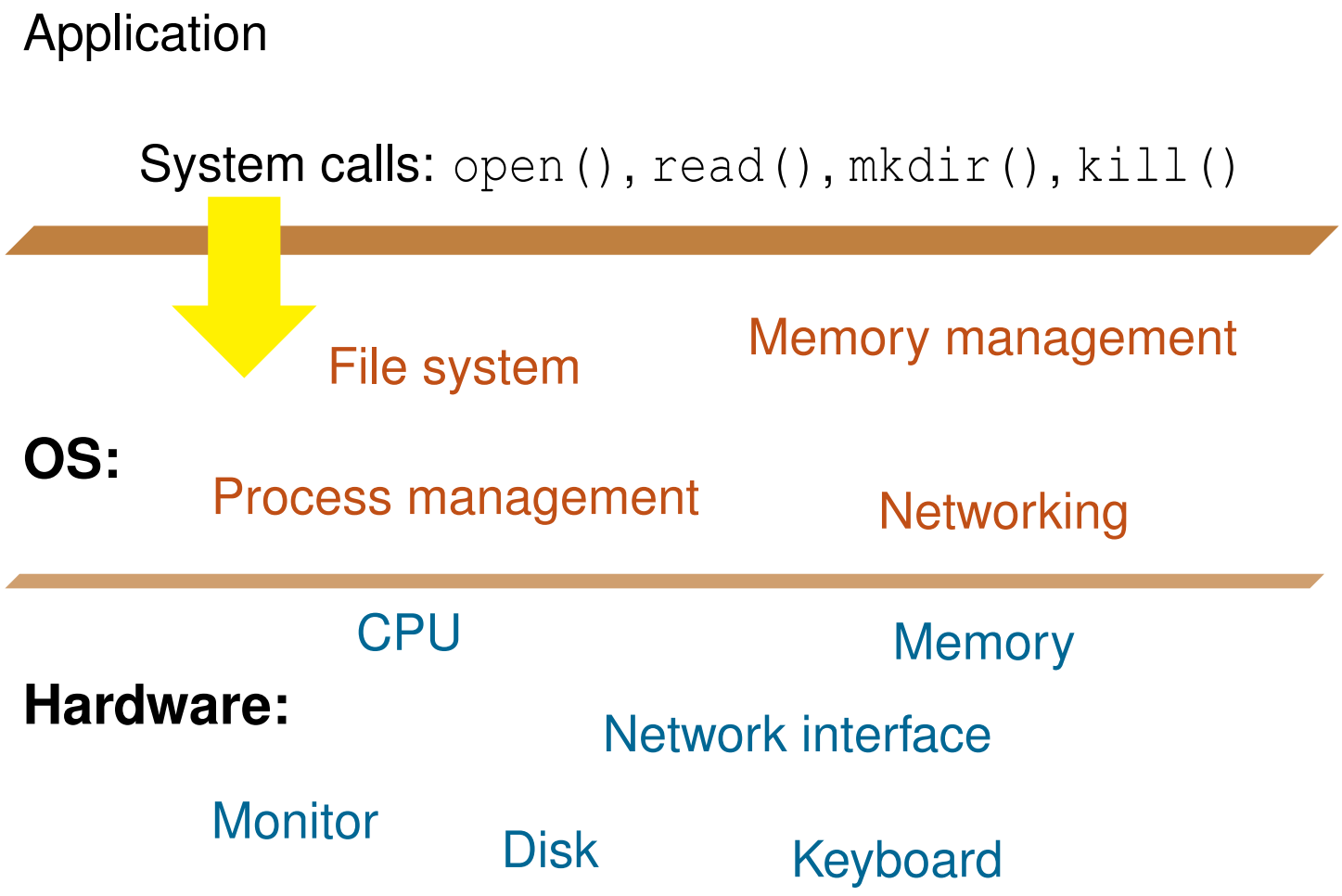
Simple View of Programming



The program controls the computer, yet it needs critical assistance (from the operating system) to communicate with the outside environment and even to run effectively.

For a deeper appreciation of programming a computer, we should examine briefly the many layers upon which the user depends.
An important lesson in organizing these complex systems is that the boundaries should be well chosen. Rapidly changing technology, competing business interests, and new insights make it impossible to settle these boundaries once and for all.
Whole college classes like computer architecture, operating systems, compiler construction, and programming languages go into the subjects more deeply.

Hardware and Operating System Platform



Example Platforms

- Hardware: IBM PowerPC, Intel x86, Sun Ultra-SPARC II
- OS: Microsoft Windows XP, Mac OS X v10.5 “Leopard”, Linux, Solaris 10

Try:

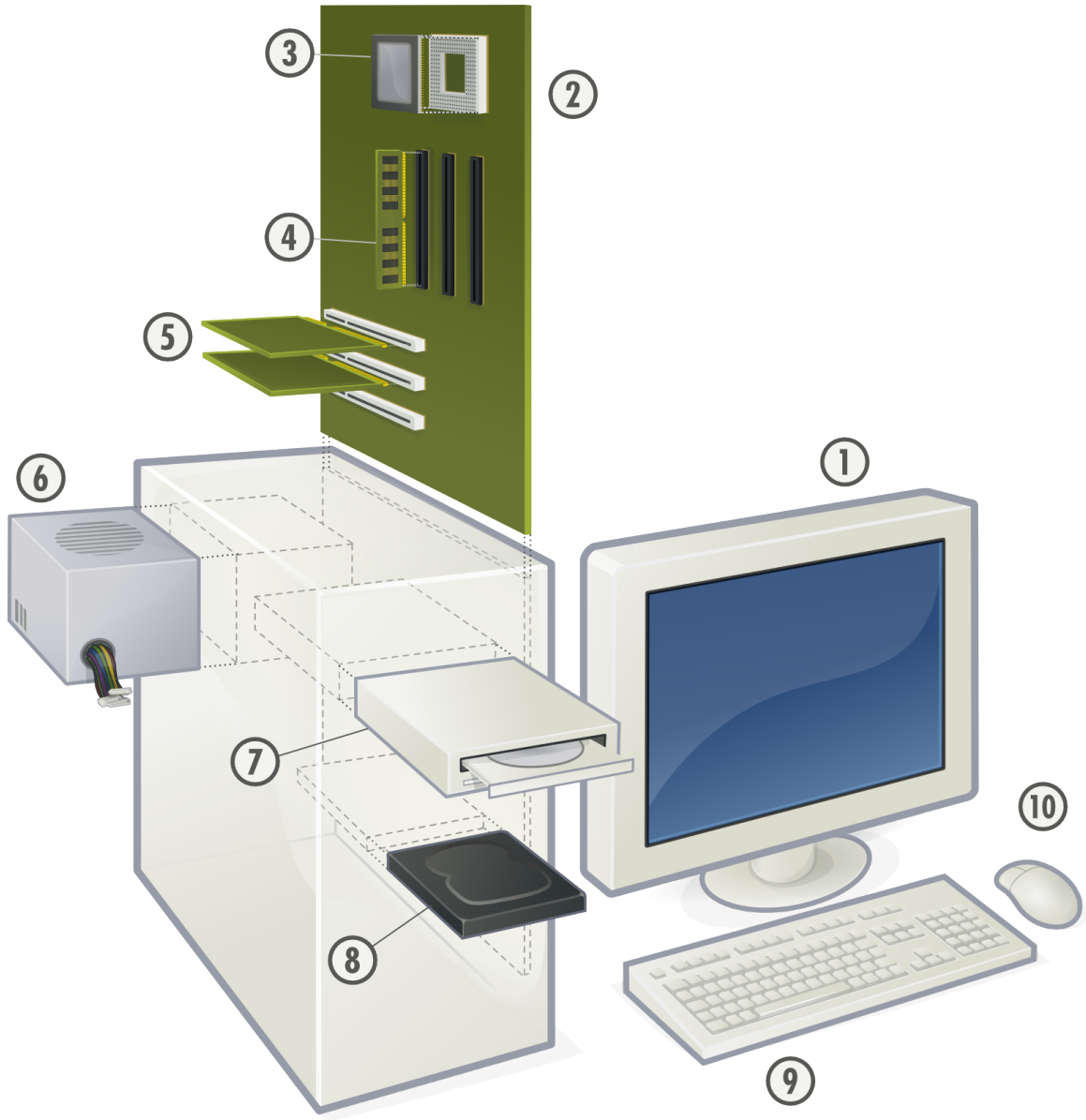
```
cs> uname -io
RackMac3, 1 Darwin

olin> uname -io
X86_64 GNU/Linux
```

Good interfaces mean you don't have to understand the lower layers.
You don't have to understand flip-flops to programs.
The point is:

- Many interfaces are software and software interfaces are an important design problem for programmers
- Many existing interfaces are in flux requiring an understanding of the lower layers.

Outline

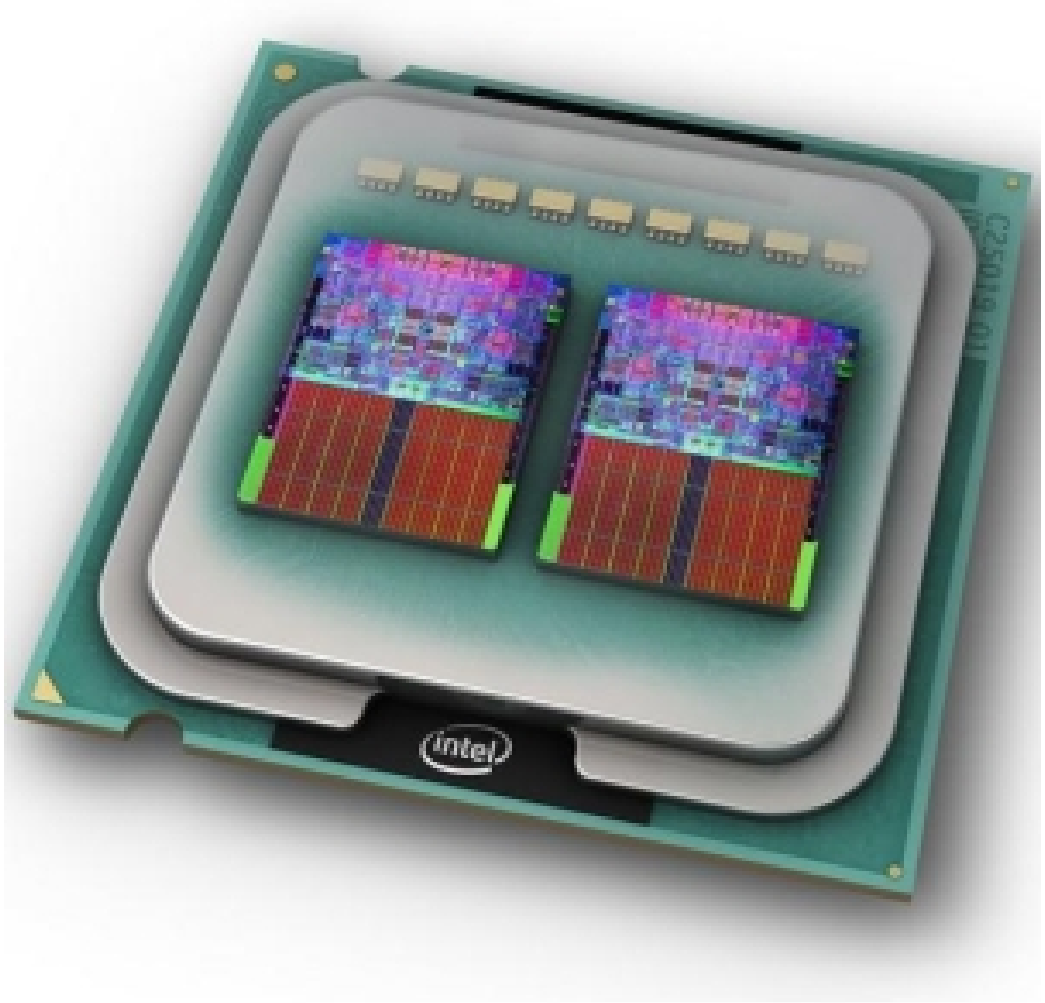
Computer Hardware



Computer Hardware

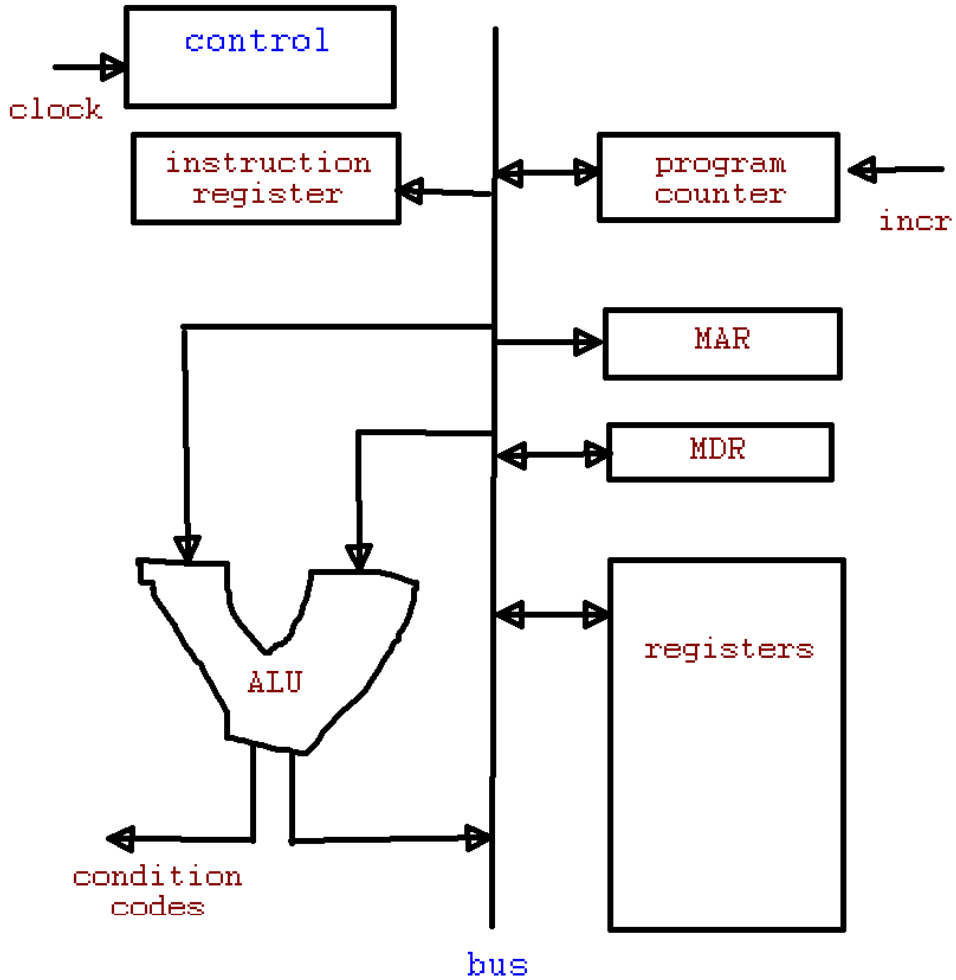
AMD 64X2 dual core

Computer Hardware



Intel quad

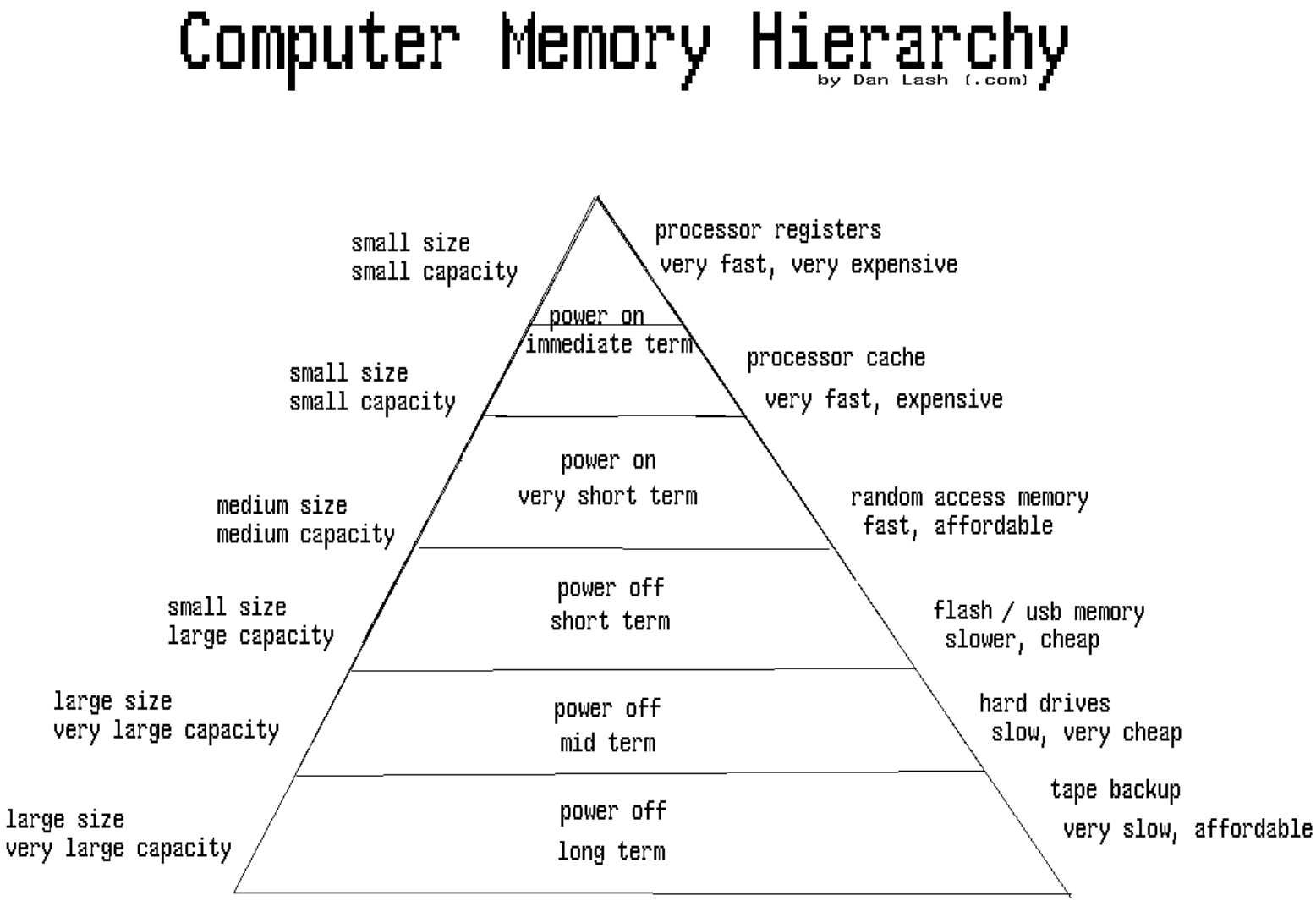
Computer Architecture—CPU



Computer Architecture—CPU

control unit is the part of the cpu that controls all the internal actions of the cpu, especially the fetch/execute cycle.
arithmetic/logic unit (ALU) is the part of the cpu that does operations: addition, multiplication, etc.
memory data register (MDR) is the register of the cpu that contains the data to be stored in the computer's main storage, or the data after a fetch from the storage. It acts like a buffer keeping the contents of storage ready for immediate use by the cpu.

Computer Architecture



Memory Hierarchy

type	access	size	cost
registers	5ns	1e2	
caches (SRAM)	10ns	1e6	100.00 $/MB
main memory (DRAM)	100ns	1e9	1.00 $/MB
hard disk	5000ns	1e11	.05 $/MB

As the technology improves and the costs go down over time, the typical size of each layer goes up. The ratio in access time between two layers influences the design of the computer hardware. When the ratio changes significantly a different design may achieve better performance.

Cloud Computing

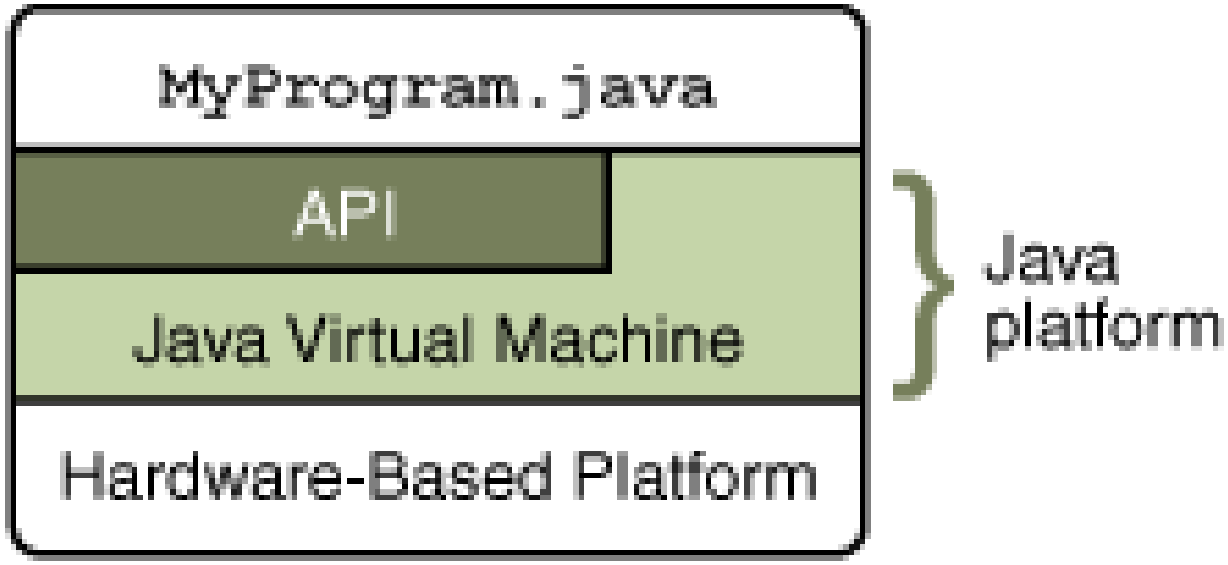
A final note about computers. The computing platform today is less concerned about the individual computer and more concerned about the network of interconnected computers on the Internet.

> *The computer is the network*
>
> Slogan of Sun Microsystems

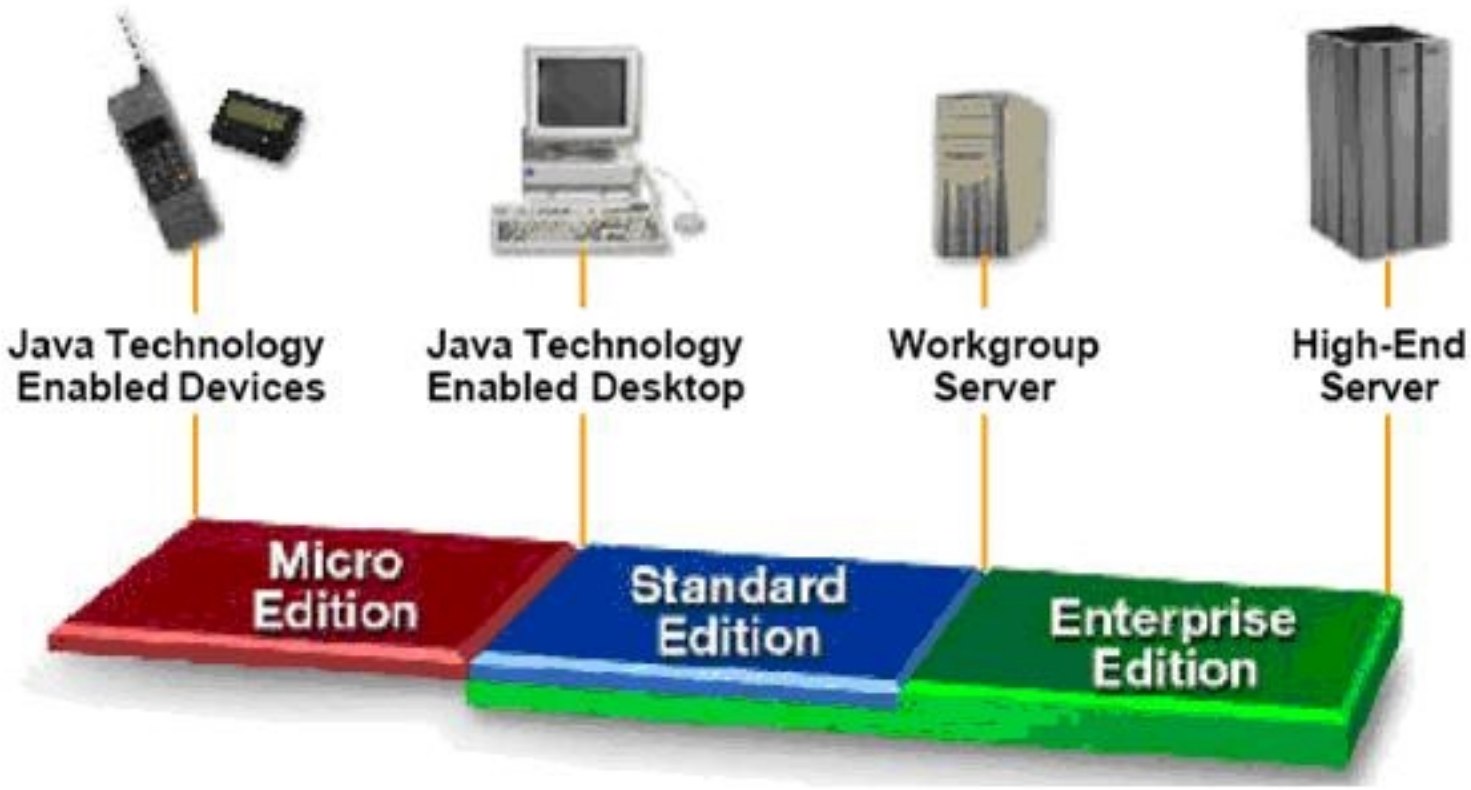
Cue `The Network is the Computer`

Outline

- 1991: a small group led by James Gosling at Sun Microsystems rejected C/C++ as the basis for digital consumer devices.
- 1993: Failed in win the contract from Time-Warner for the interactive cable television trial in Orlando, Florida.
- 1995: WWW, browsers, Java, applets
- 2009: Oracle buys Sun
- 2010: Oracle sues Google over Java use in Android Java. "The lawsuit is one battle in a whole war of the mobile industry. Virtually every major player is locked in courtroom battles with another – many fighting on multiple fronts. Software patents, which tend to be broad and subject to multiple interpretations, make for useful tools to bludgeon competitors."


MyProgram.java
API
Java Virtual Machine
Hardware-Based Platform
Java
platform

The Java™ Platform



enterprise computing

networking

telecommunications

programs

WWW applications

databases

Java Platform

Some of the major components surrounding Java:

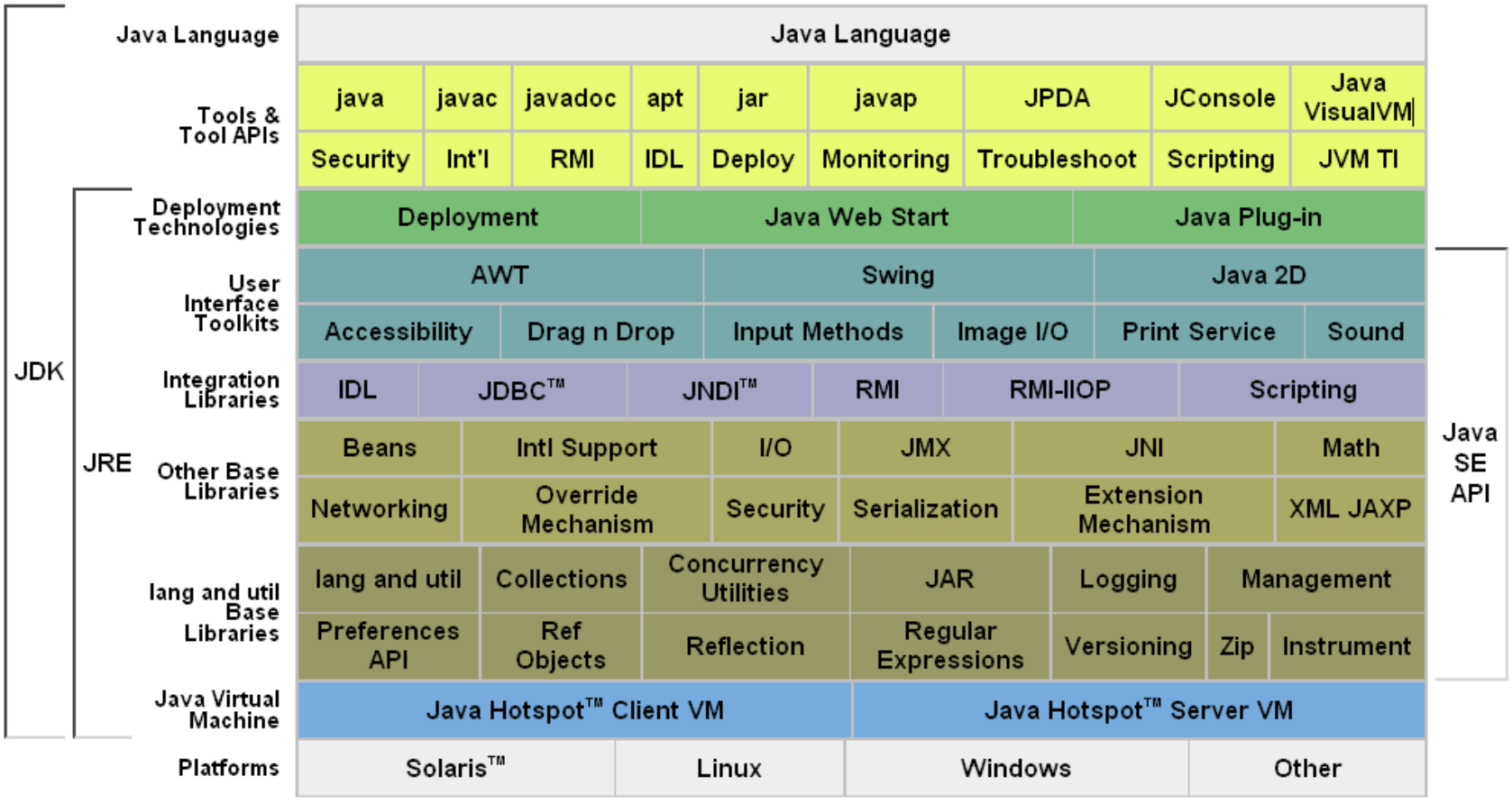
- Java virtual machine (JVM) specification
- Virtual machine implementation (for Solaris, Window, and Linux), translation tools (`java` and `javac`), and development tools
- Java programming language specification
- A core library (the package `java.lang`), extensive libraries (APIs) for networking, graphics, etc., and additional APIs for special purposes (e.g., telephony)

Java Platform

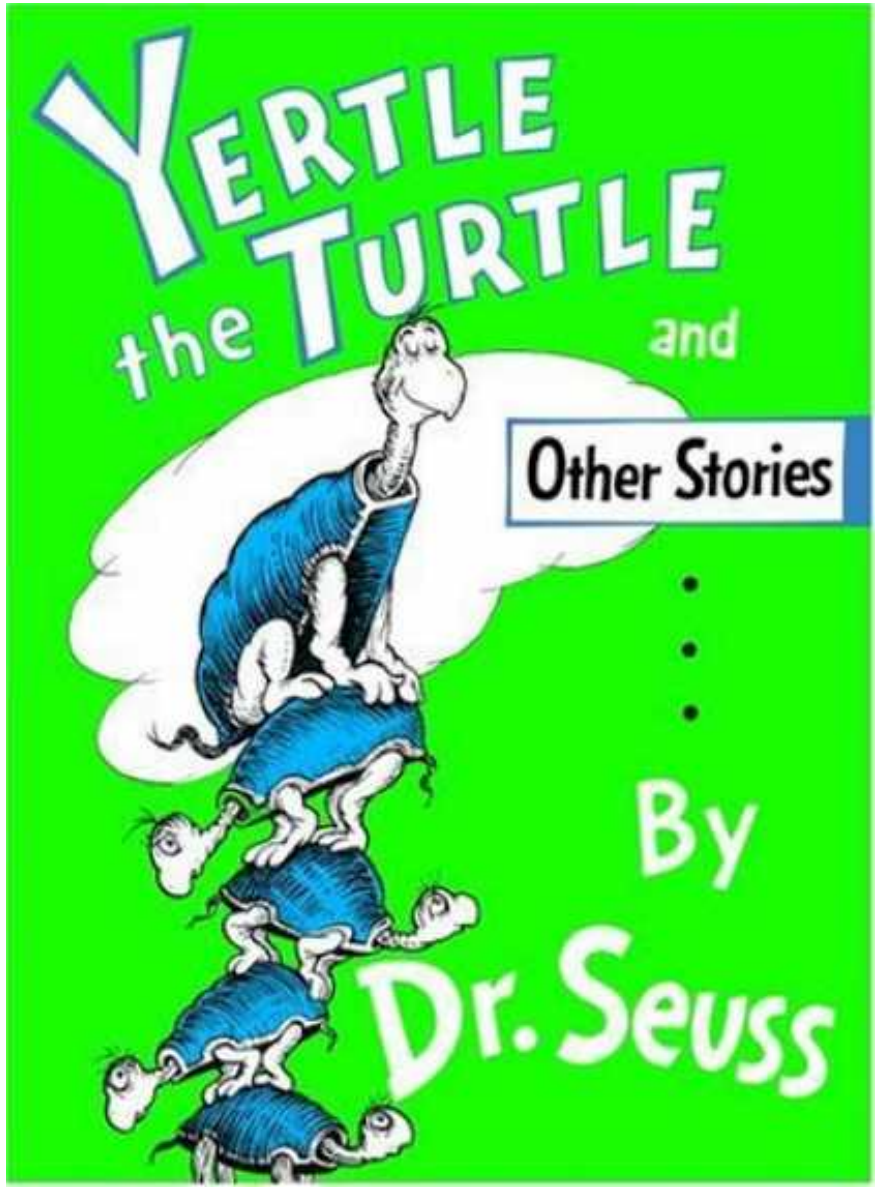
Additional components surrounding Java:

- API documentation
  (No reference material will be given to you. We expect you to go out on the Internet, find it, and know some parts of it in detail.)
- An IDE for developing Java programs and GUIs: Netbeans
  (We expect you to be able to develop Java programs; we don't explicitly teach using an IDE.)

(In lab and lecture we have other priorities and we expect a lot from you. However, don't be reluctant to ask your classmates, instructors, the help desk, etc., if you have questions. Asking knowledgeable people is still the fastest way to learn.)



Sun Java SE 6 platform overview



Precarious pyramid

Outline

International Olympiad in Informatics (IOI)

World-wide competitions for pre-college students exist in many subjects. In addition to computer science, competitions are held in math, physics, chemistry, biology linguistics, geography, *inter alia*.

The national organization of the US, USA Computing Olympiad (USACO), trains and selects the team representing the USA.

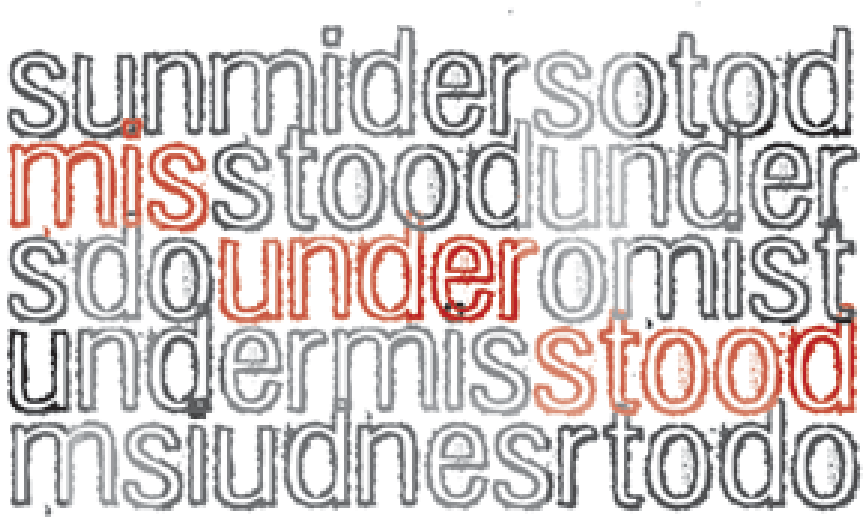
Unlike the other subjects, it is easy to participate with USACO. They offer on-line practicing, and exciting world-wide contests every month.

usaco.org

Outline

Computers Are Misunderstood

- Buffer overruns in old languages like C/C++ cause risks
- Intellectual property, copyrights
- Computer voting, computer money
- Free software works better
- Correct software is hard

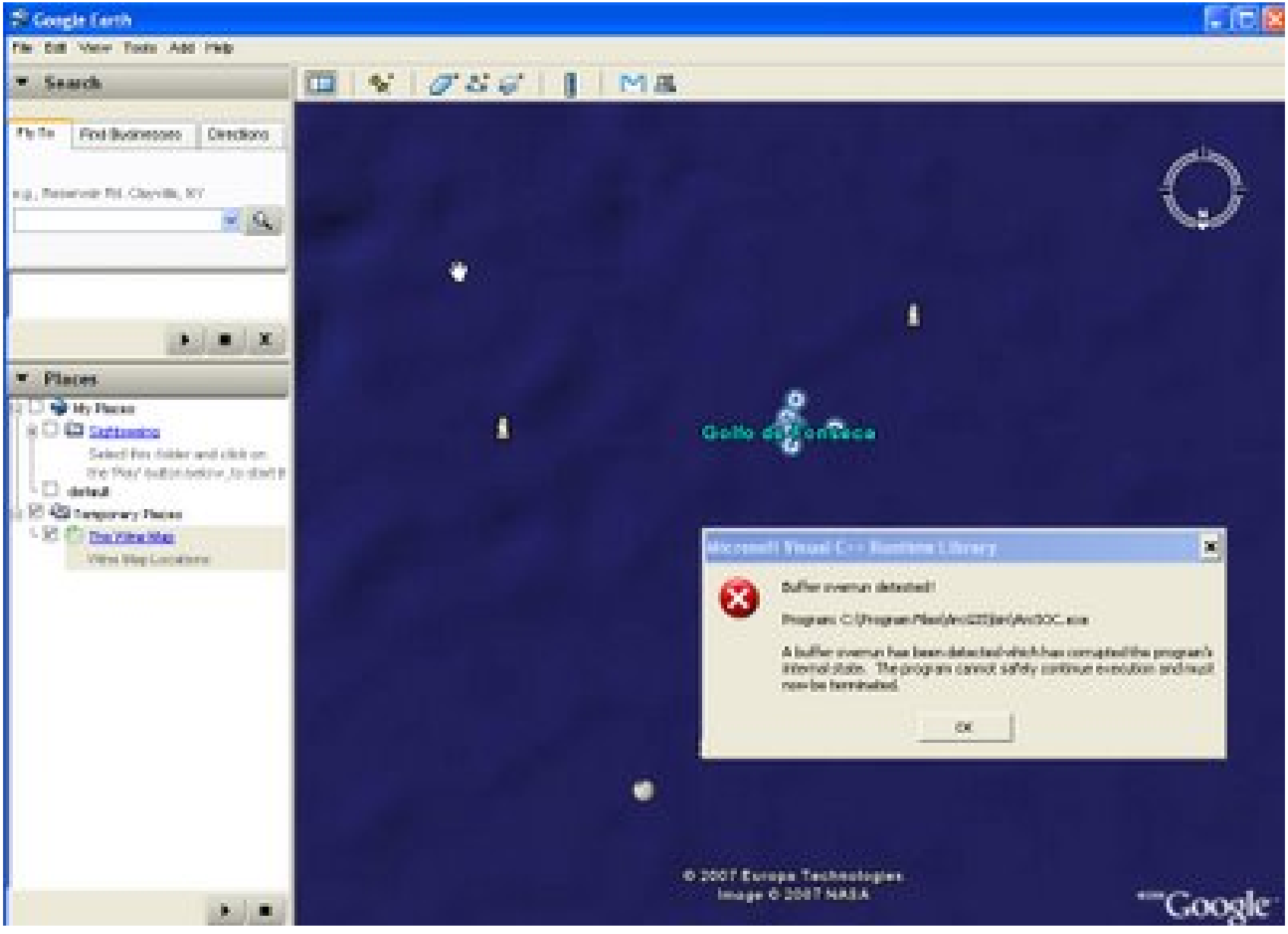


Computer Experts Needed

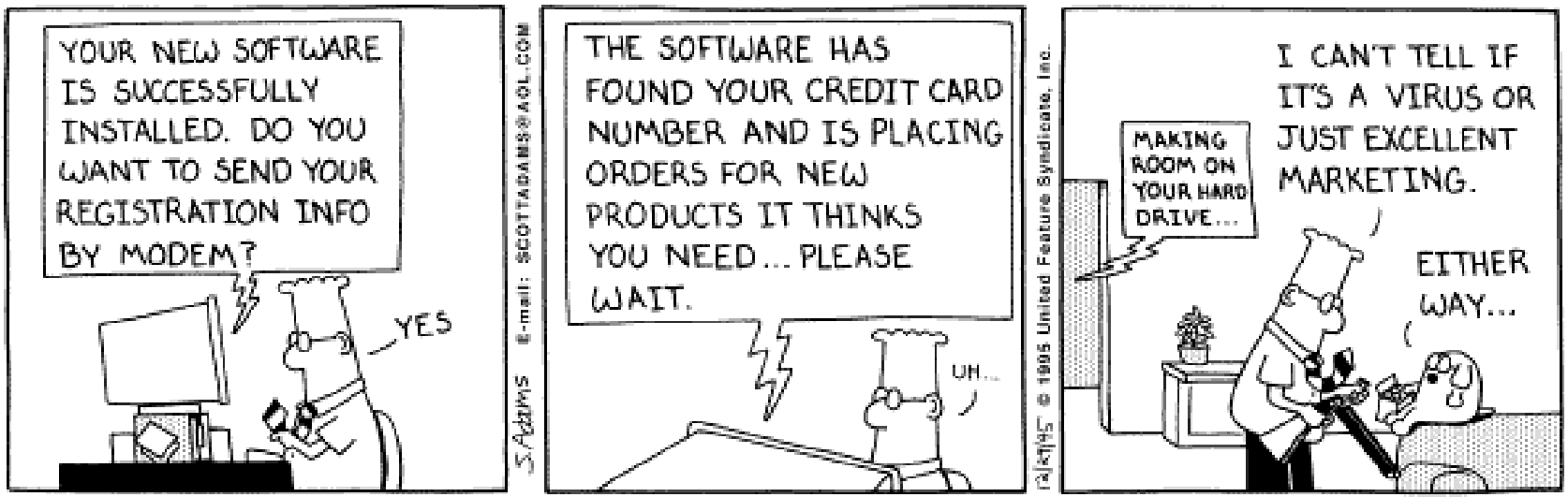
WASHINGTON – Federal agencies are facing a severe shortage of computer specialists, even as a growing wave of coordinated cyberattacks against the government poses potential national security risks, a private study found.

Wed, 22 July 2009, Associated Press

Buffer Overrun



Society has not found the right incentive for the creation of useful and correct software.



Outline

The greedy algorithm used to give change.
Amount owed: 41 cents.

Subtract Quarter
41 - 25 = 16

Subtract Dime
16 - 10 = 6

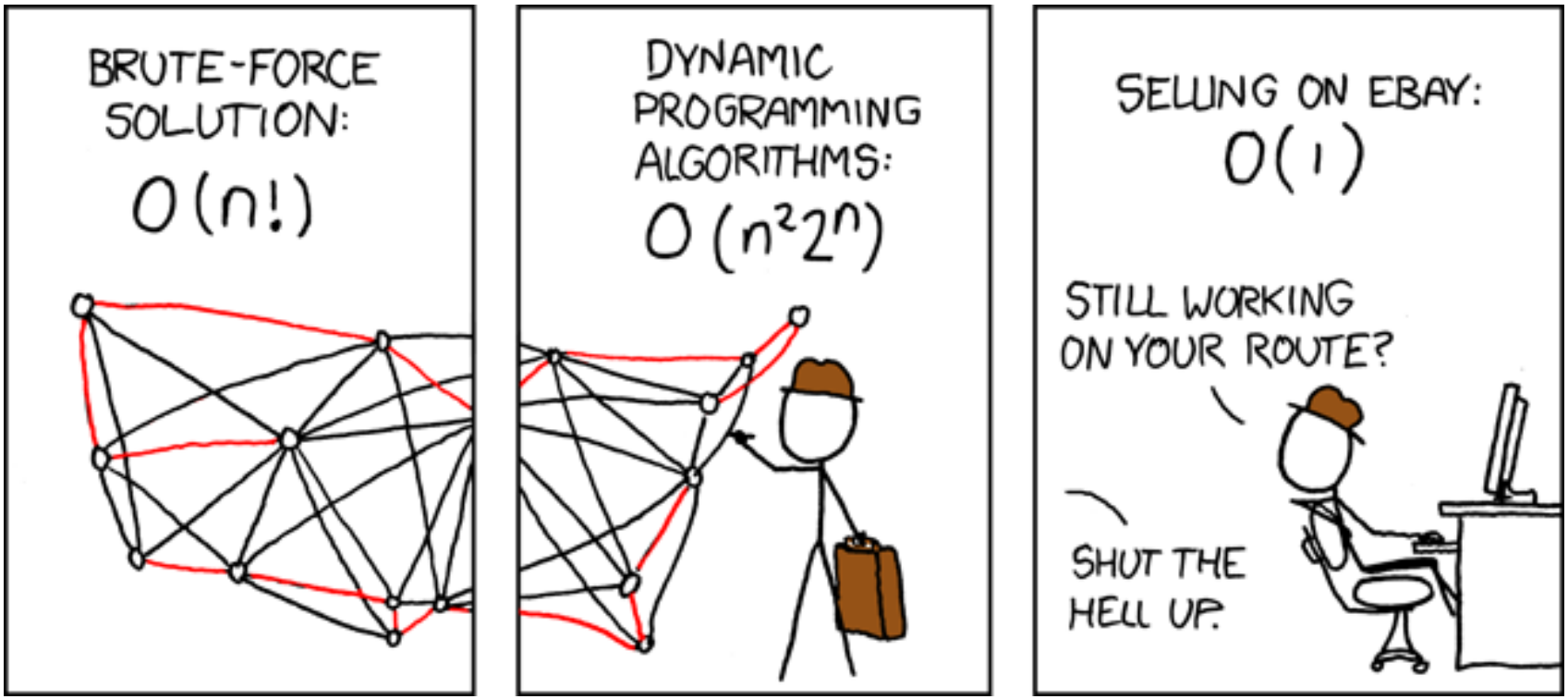
Subtract Nickel
6 - 5 = 1

Subtract Penny
1 - 1 = 0

Change Counting

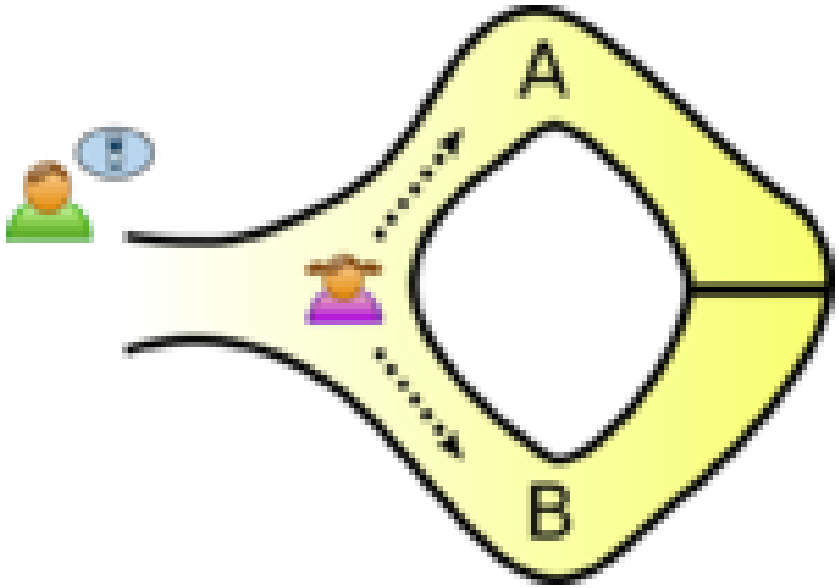
Imagine the coin example with only 25-cent, 10-cent, and 4-cent coins. We could make 41 cents change with one 25-cent coin and four 4-cent coins, but the greedy algorithm could only make change for 39 or 43 cents, as it would have committed to using one 10-cent coin.
Imagine the coin example with only 25-cent, 10-cent, 6-cent, and 1-cent coins. We could make 25+18 cents change with one 25-cent coin and three 6-cent coins (four coins total), but the greedy algorithm would make change for 43 cents using one 25-cent coin, one 10-cent coin, one 6-cent coins, and two 1-cent coins (five coins total), as it would have committed to using one 10-cent coin.
It would appear to be necessary to try *all* possibilities, and this would take a very long time. Fortunately, a clever algorithm exists for making change that does something unexpected. It computes the change for all amounts (not just one), this turns out to be much faster.

Traveling Salesman Problem



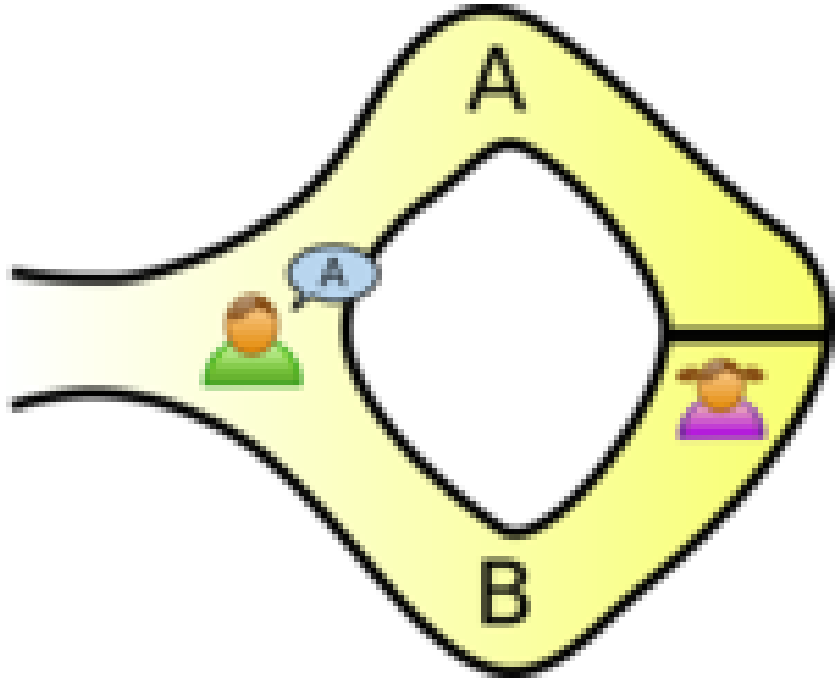
Zero Knowledge Proof

Peggy has a secret word used to open a door in a cave shaped like a circle. Victors says he'll pay her for the secret, but not until he's sure she really knows it. Peggy says she'll tell him the secret, but not until she receives the money. They devise a scheme by which Peggy can prove that she knows the word without telling to Victor.
First, Victor waits outside while Peggy goes out of sight and stands at one side or the other of the door. Victor does not see which way she goes, nor can he hear or watch Peggy if she opens the door.



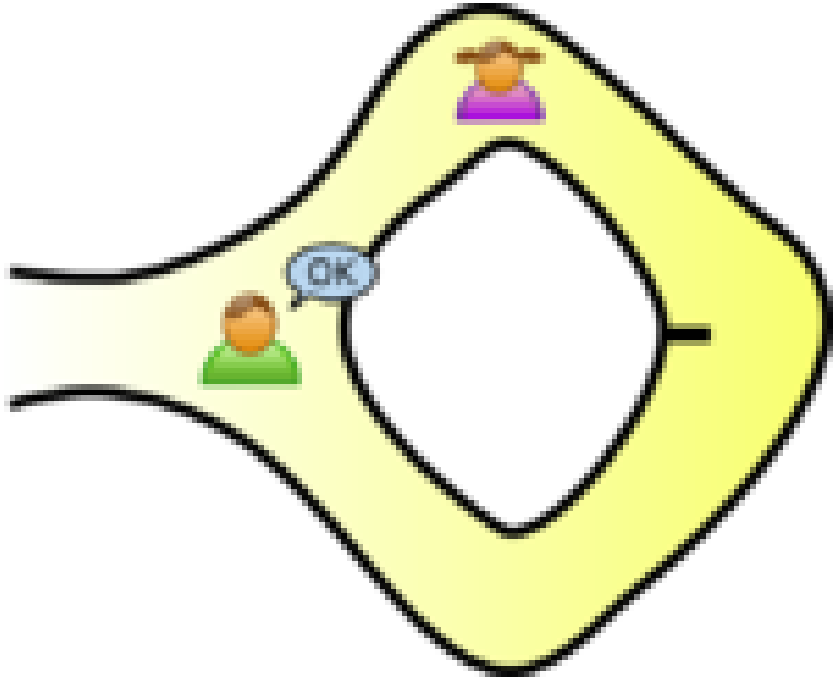
Zero Knowledge Proof

Second, Victor randomly calls out a path for Peggy to take back to the mouth of the cave.



Cryptography

Third, Peggy takes the indicated path proving she may have opened the door.



With a 50% probability, Peggy has returned by using the password. Victor can repeat the test as long as it takes to convince himself that Peggy indeed knows the password. Each test decreases the chance the Peggy got lucky by standing on the side of the door which Victor will pick.