UC Berkeley EECS
Teaching Professor
Dan Garcia

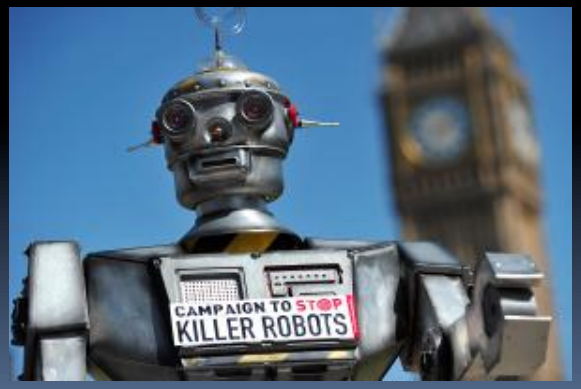
The Beauty and Joy of Computing

bjc

Lecture #23
Future of Computing

NSA Building Quantum Co

"The United Nations' Convention on Certain Conventional Weapons this week heard from technical and legal experts on the subject of killer robots, or 'lethal autonomous weapons systems.' There's a growing consensus that it's unacceptable for robots to kill without human control."



www.newscientist.com/article/dn27339-can-we-stop-killer-robots-un-meets-to-debate-possible-treaty.html

(Cal) Admin Notes

- Schedule (see website)

(Cal) Lecture Overview

- Where will today's computers go?
- Quantum Computing
- Biological Computing & Interfaces

Where will today's computers go?

Computer Technology … Growth!

- Processor
  - Speed 2x / 2 years (since '71)
  - 100X performance last decade
  - When you graduate: 4 GHz, 32 Cores
- Memory (DRAM)
  - Capacity: 2x / 2 years (since '96)
  - 64x size last decade.
  - When you graduate: 128 GibiBytes
- Disk
  - Capacity: 2x / 1 year (since '97)
  - 250X size last decade.
  - When you graduate: 16 TeraBytes

Kilo (10^3) & Kibi (2^{10})

↓

Mega (10^6) & Mebi (2^{20})

↓

Giga (10^9) & Gibi (2^{30})

↓

Tera (10^{12}) & Tebi (2^{40})

↓

Peta (10^{15}) & Pebi (2^{50})

↓

Exa (10^{18}) & Exbi (2^{60})

↓

Zetta (10^{21}) & Zebi (2^{70})

↓

Yotta (10^{24}) & Yobi (2^{80})

Kilo, Mega, Giga, Tera, Peta, Exa, Zetta, Yotta

- Kid meets giant Texas people exercising zen-like yoga. – Rolf O
- Kind men give ten percent extra, zestfully, youthfully. – Hava E
- Kissing Mentors Gives Testy Persistent Extremists Zealous Youthfulness. – Gary M
- Kindness means giving, teaching, permeating excess zeal yourself. – Hava E
- Killing messengers gives terrible people exactly zero, yo
- Kindergarten means giving teachers perfect examples (of) zeal (&) youth
- Kissing mediocre giraffes teaches people (to) expect zero (from) you
- Kinky Mean Girls Teach Penis-Extending Zen Yoga
- Kissing Mel Gibson, Teddy Pendergrass exclaimed: "Zesty, yo!" – Dan G
- Kissing me gives ten percent extra zeal & youth! – Dan G (borrowing parts)

(Cal) Peer Instruction

What was recently proposed to go after Yotta? (i.e., 10^{27})

a) Lotta
b) Lotsa
c) Wholelotta
d) Hella
e) Zillion

Both Google's and WolframAlpha's calculator can understand and use "Hella" in their calculations!

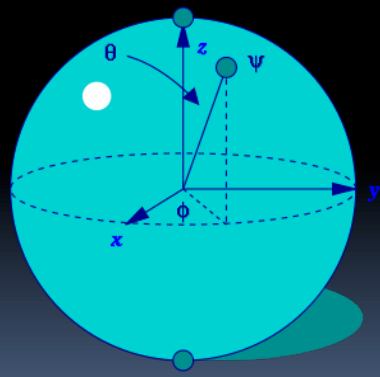
www.makehellaofficial.blogspot.com

Quantum Computing

Quantum Computing (1/3)

- Proposed computing device using quantum mechanics
  - This field in its infancy…
- Normally: bits, which are either 0 or 1
- Quantum: qubits, either 0, 1 or "quantum superposition" of these
  - This is the key idea

- If you have 2 bits, they're in exactly one of these:
  - 00, 01, 10 or 11
- If you have 2 qubits, they're in ALL these states with varying probabilities



A Bloch sphere is the geometric representation of 1 qubit

en.wikipedia.org/wiki/Quantum_computer

Quantum Computing (2/3)

- Imagine a problem with these four properties:
  - The only way to solve it is to guess answers repeatedly and check them,
  - There are *n* possible answers to check,
  - Every possible answer takes the same amount of time to check, and
  - There are no clues about which answers might be better: generating possibilities randomly is just as good as checking them in some special order.
- …like trying to crack a password from an encrypted file
- A normal computer
  - would take (in the worst case) n steps
- A quantum computer
  - can solve the problem in steps proportional to $\sqrt{n}$
- Why does this matter?

Quantum Computing (3/3)

- Say the password is exactly 72 bits (0/1)
- That's 2^{72} possibilities
- Let's say our Mac lab attacked the problem
  - 30 machines/lab * 8 cores/machine * 3 GHz (say 3 billion checks per second/core)

  = 720,000,000,000 checks/sec/lab

  = 720 Gchecks/sec/lab

- **Regular computers**
  - 2^{72} checks needed / 720 Gchecks/sec/lab

  ≈ 6.6 billion sec/lab

  ≈ 208 years/lab
- **72-qubit quantum computers in time∝to $\sqrt{2^{72}} = 2^{36}$**
  - 2^{36} checks needed / 720 Gchecks/sec/lab

  ≈ 0.1 sec/lab

www.washingtonpost.com/world/national-security/nsa-seeks-to-build-quantum-computer-that-could-crack-most-types-of-encryption/2014/01/02/8fff297e-7195-11e3-8def-a33011492df2_story.html

NSA seeks to build Quantum computer

- **Washington Post**, 2014-01-03: *"The U.S. National Security Agency (NSA) is trying to develop a quantum computer that could be used to crack almost any type of encryption currently in use, according to documents released by former NSA contractor Edward Snowden."*
- *"Once completed, the computer could be used to crack almost every type of encryption used to protect state secrets and other sensitive information, such as 1,024-bit RSA encryption keys, which would take hundreds of standard computers working together about 2,000 years to crack."*

www.youtube.com/watch?v=T2DXrs0OpHUs

Quantum Computing Explained by Physicists

Biological Computing & Interfaces

en.wikipedia.org/wiki/DNA_computing

DNA Computing

- Proposed computing device using DNA to do the work
  - Take advantage of the different molecules of DNA to try many possibilities at once
  - Ala parallel computing
  - Also in its infancy
- Papers in "Nature"
  - In 2004, researchers claimed they built DNA Computer!
  - In 2013, researchers stored (and retrieved!) data on DNA (All Shakespeare's sonnets and audio clip of "I have a dream")

www.technologyreview.com/article/412185/tr10-biological-machines/

Biological Machines

- Michel Maharbiz and his team at Cal have wired insects (here a giant flower beetle) and can control flight
  - Implated as Pupa
- Vision
  - Imagine devices that can collect, manipulate, store and act on info from environment

(Cal) Peer Instruction

What is the most exciting future for computing?

a) Incremental improvements in computing architectures
b) Quantum computing
c) DNA computing
d) Biological Machines
e) Something completely different

(Cal) Summary

- What a wonderful time we live in; we're far from done
  - What about privacy?
- Find out the problem you want to solve
  - Computing will probably help get you there!
- We probably can't even imagine future software + hardware breakthroughs