Uncomputability, Viruses, OOP

Avian Flu Virus

One-Slide Summary

- If a problem is **uncomputable** or **undecideable**, then no deterministic terminating algorithm can exist that correctly solves it.
- The **halting problem** is undecideable.
- Many problems related to **computer security**, such as detecting worms and viruses, are undecideable.
- Undecideability proofs work by **contradiction**.
- **Object-oriented programming** has a lively history.

Outline

- Gödel's Proof
- Unprovability
- Algorithms
- Computability
- The Halting Problem
- OOP History

Informal Proof

```
def: paradox():
      if halts?(paradox):
            loop_forever()
      else:
            return "halt"
```

If paradox halts, the if test is true and it evaluates to loop_forever() - it doesn’t halt!

If paradox doesn’t halt, the if test if false, and it evaluates to ”halt”. It halts!

Proof by Contradiction

Goal: Show A cannot exist.

1. Show *X* is nonsensical.
2. Show that if you have *A* you can make *X*.
3. Therefore, *A* must not exist.

X = paradox
A = halts? algorithm

Evaluates-to-3 Problem

Input: A procedure specification *P*

Output: **True** if evaluating (*P*) would result in 3; **False** otherwise.

```
>>> eval-to-three?(lambda x : (2 + 1))
True
>>> eval-to-three?(lambda x : (2 * 2))
False
```

Is “Evaluates to 3” computable?

Proof by Contradiction

Goal: Show A cannot exist.

1. Show *X* is nonsensical.
2. Show that if you have *A* you can make *X*.
3. Therefore, *A* must not exist.

X = halts? algorithm
A = eval-to-three? algorithm

Undecidability Proof

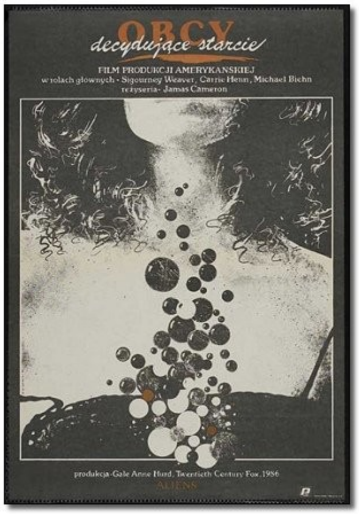
Suppose we could define eval-to-3? that decides it. Then we could define halts?:

```
def halts?(P):
  def widget():
    P()
    return 3
  return eval-to-three?(widget)
```

if True: it evaluates to 3, so we know P() must halt.

if False: the only way it could not evaluate to 3, is if P() doesn't halt. (Note: assumes P() cannot produce an error or raise an exception.)

Hello-World Problem


OBCY
decydujące starcie
FILM PRODUKCJI AMERYKANSKIEJ
w rolach głownych - Sigourney Weaver, Carrie Henn, Michael Biehn
reżyseria- James Cameron
produkcja-Gale Anne Hurd, Twentieth Century Fox 1986
ALIENS

Input: An expression specification *E*

Output: **true** if evaluating *E* would print out "Hello World!"; **false** otherwise.

Is the *Hello-World Problem* computable?

Uncomputability Proof

Suppose we could define prints-hello-world? that solves it. Then we could define halts?:

```
def halts? (P):
  def widget():
    P2 = remove_all_prints(P)
    P2()
    print "Hello World!"
  return prints-hello-world?(widget)
```

Proof by Contradiction

Goal: Show A cannot exist.

1. Show *X* is nonsensical.
2. Show that if you have *A* you can make *X*.
3. Therefore, *A* must not exist.

X = halts? algorithm
A = prints-hello-world? algorithm

From Paul Graham's "Undergraduation":

My friend Robert learned a lot by writing network software when he was an undergrad. One of his projects was to connect Harvard to the Arpanet; it had been one of the original nodes, but by 1984 the connection had died. Not only was this work not for a class, but because he spent all his time on it and neglected his studies, he was kicked out of school for a year. ... When Robert got kicked out of grad school for writing the Internet worm of 1988, I envied him enormously for finding a way out without the stigma of failure. ... It all evened out in the end, and now he's a professor at MIT. But you'll probably be happier if you don't go to that extreme; it caused him a lot of worry at the time.

3 years of probation, 400 hours of community service, $10,000+ fine

Worm Detection Problem

Input: A program *P* and input *I*

Output: **true** if evaluating P(I) would cause a remote computer to be “infected”.

Virus Detection Problem

Input: A program specification *P*

Output: **true** if evaluating P() would cause a file on the host computer to be “infected”.

Morris Internet Worm (1988)

- *P* = fingerd
  - Program used to query user status
  - Worm also attacked other programs
- *I* = “nop^{400} pushl $68732f pushl $6e69622f movl sp,r10 pushl $0 pushl $0 pushl r10 pushl $3 movl sp,ap chmk $3b”

  is-worm?(P(I)) should evaluate to True
- Worm infected several thousand computers (~10% of Internet in 1988)

Liberal Arts Trivia: Greek Mythology

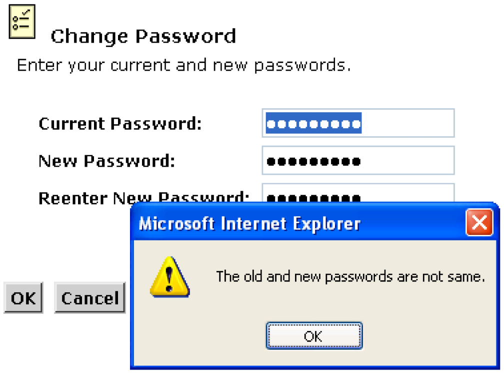
- This multi-headed hound guards the gates of Hades and prevents those who have crossed the river Styx from ever escaping. The task of capturing it alive, without using weapons, was the final labor assigned to Heracles by King Eurystheus.

Liberal Arts Trivia: Music

- This genre of rock music developed in the late 1960s and early 1970s, largely in the UK and USA. With roots in blues-rock and psychedelic rock, it developed a thick, massive sound, characterized by highly amplified distortion, extended guitar solos, emphatic beats, and overall loudness. Lyrics and performance styles are generally associated with masculinity and machismo. Early bands included Led Zeppelin and Black Sabbath.

Computer Security Paradoxes

- Is is-virus? computable?



Change Password

Enter your current and new passwords.

Current Password: ●●●●●●●●●

New Password: ●●●●●●●●●●

Reenter New Password: ●●●●●●●●●●

Microsoft Internet Explorer

The old and new passwords are not same.

Uncomputability Proof

Suppose we could define is-virus? Then:

```
def halts?(P):
  def widget():
    P2 = remove_infects(P)
    P2()
    infect_files()
  return is-virus?(widget)
```

Uncomputability Proof

```
def halts?(P):
  def widget():
    P2 = remove_infects(P)
    P2()
    infect_files()
  return is-virus?(widget)
```

True: Since it *is* a virus, we know infect_files() was evaluated, and *P* must halt.

False: The infect_files() would not evaluate, so *P* must not halt.

Can we make ***remove-infects***?

Yes, just remove all file writes.

"Solving" Undecidable Problems

- No perfect solution exists:
  - **Undecidable** means there is no procedure that:
    1. Always gives the correct answer

    and also 2. Always terminates
- Must give up one of these to "solve" undecidable problems
  - Giving up #2 is not acceptable in most cases
  - Must give up #1
- Or change the problem: e.g., detect file infections during an execution

Conclusion?

- Anti-Virus programs cannot exist!

"The **Art** of Computer Virus Research and Defense"
Peter Szor, Symantec

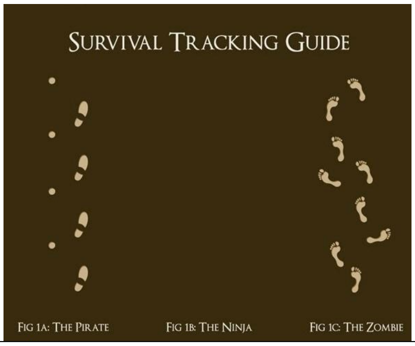
Actual is-virus? Programs

- Give the wrong answer sometimes
  - "**False positive**": say P is a virus when it isn't
  - "**False negative**": say P is safe when it is
- Database of known viruses: if P matches one of these, it is a virus
- Clever virus authors can make viruses that change each time they propagate
  - Emulate program for a limited number of steps; if it doesn't do anything bad, assume it is safe

Proof Recap

- If we had is-virus? we could define halts?
- We know halts? is undecidable
- Hence, we can't have is-virus?
- Thus, we know is-virus? is undecidable

History of Object-Oriented Programming

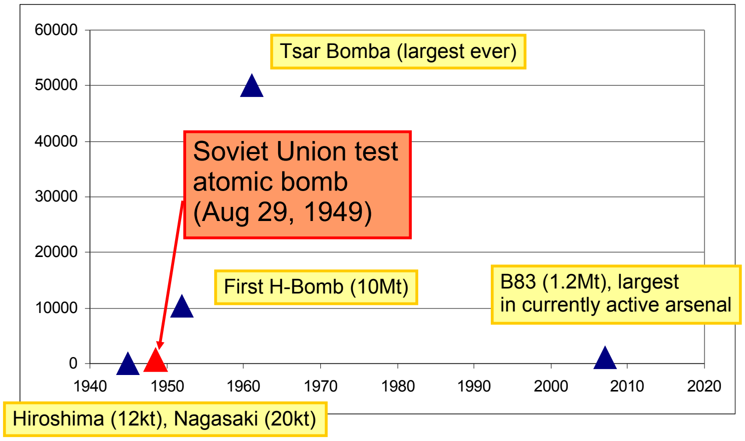


Pre-History: MIT’s Project Whirlwind (1947-1960s)

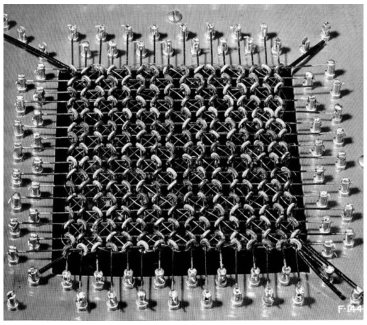
Jay Forrester

Why Whirlwind?

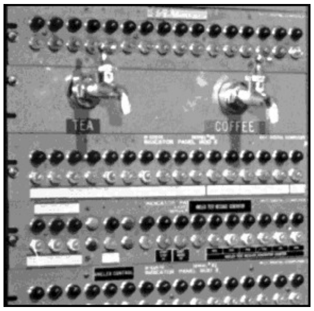
From an earlier class ...



Whirlwind Innovations



Magnetic Core Memory
(first version used vacuum tubes)



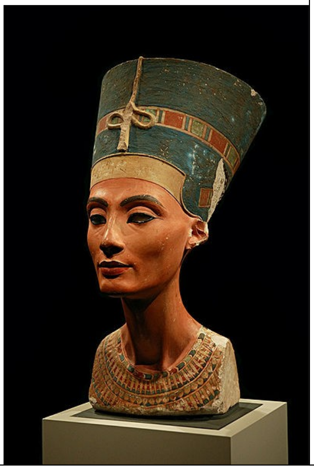
... the first computer that operated in real time, used video displays for output, and the first that was not simply an electronic replacement of older mechanical systems. Its development led directly to the United States Air Force's Semi Automatic Ground Environment (SAGE) system, and indirectly to almost all business computers and minicomputers in the 1960s.

Liberal Arts Trivia: Spanish Culture

- This region, loosely located between France and Spain, features a strong separatist movement. It is currently the wealthiest region in Spain, with gross domestic product per capita being 40% higher than that of the European Union and 33.8% higher than Spain's average in 2008. The Euskadi Ta Askatasuna or ETA is an armed “terrorist” or “separatist” organization associated with this region.

Liberal Arts Trivia: Art History

- *This* is a cosmetic that is applied on the eyelids and under the eyebrows. It is commonly used to make the wearer's eyes stand out or look more attractive. It is demonstrated in Egyptian burials dating to 10,000 BCE. The word "cosmetae" was first used to describe Roman slaves whose duty was to bathe men and women in perfume.



Liberal Arts Trivia: Grammar

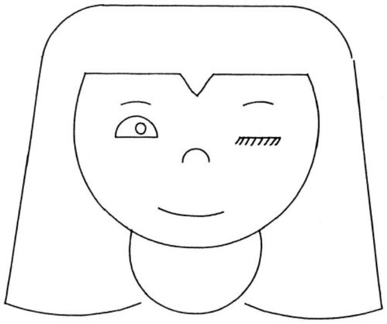
- This linguistic verb mood is typically used in dependent clauses to express a wish, emotion, possibility, judgment, opinion, necessity, or action that has not yet occurred. It often follows a conjunction. Typical examples include “Long live the Queen!” and “It is necessary that he speak.” and “You would know if we were lying.”

Sketchpad

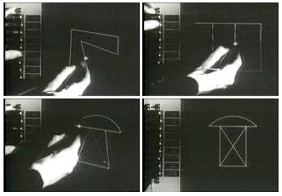
- Ivan Sutherland, 1963 (PhD thesis supervised by Claude Shannon)
- Interactive drawing program
- Light pen
- Turing Award 1988

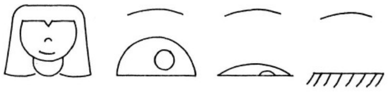
http://www.cl.cam.ac.uk/TechReports/UCAM-CL-TR-574.pdf

Components in Sketchpad



Actual Sketchpad:





Objects in Sketchpad

In the process of making the Sketchpad system operate, a few very general functions were developed which make no reference at all to the specific types of entities on which they operate. These general functions give the Sketchpad system the ability to operate on a wide range of problems. The motivation for making the functions as general as possible came from the desire to get as much result as possible from the programming effort involved. For example, the general function for expanding instances makes it possible for Sketchpad to handle *any* fixed geometry subpicture. The rewards that come from implementing general functions are so great that the author has become reluctant to write any programs for specific jobs.

Each of the general functions implemented in the Sketchpad system abstracts, in some sense, some common property of pictures independent of the specific subject matter of the pictures themselves.

Ivan Sutherland, *Sketchpad: a Man-Machine Graphical Communication System*, 1963 (major influence on Alan Kay developing OOP in 1970s)

Simula

- Considered the first “object-oriented” programming language
- Language designed for *simula*tion by Kristen Nygaard and Ole-Johan Dahl (Norway, 1962)
- Had special syntax for defining classes that package state and procedures together

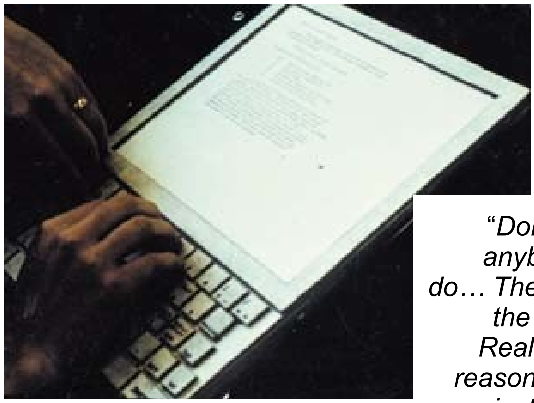
Counter in Simula

```
class counter;
   integer count;
   begin
     procedure reset(); count := 0; end;
     procedure next();
          count := count + 1; end;
     integer procedure current();
         current := count; end;
   end
```

XEROX Palo Alto Research Center (PARC)

1970s:

- Bitmapped display
- Graphical User Interface
  - Steve Jobs paid $1M to visit PARC (bought their stock), and returned to make Apple Lisa/Mac
- Ethernet
- First personal computer (Alto)
- PostScript Laser Printers
- **Object-Oriented Programming**



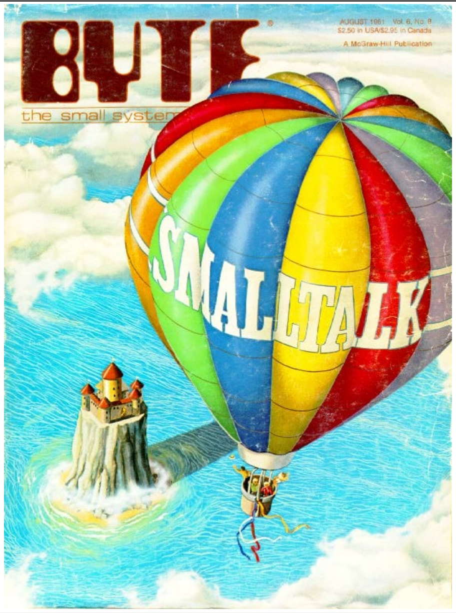
Dynabook, 1972

(Just a model)

> *"Don't worry about what anybody else is going to do… The best way to predict the future is to invent it. Really smart people with reasonable funding can do just about anything that doesn't violate too many of Newton's Laws!"*
> *— Alan Kay, 1971*

Dynabook 1972

- Tablet computer
- Intended as tool for learning
- Kay wanted children to program it also
- Hallway argument, Kay claims you could define "the most powerful language in the world in a page of code"
- Proof: Smalltalk
  - Scheme is as powerful, but takes two pages
  - Before the end of CS 1120, we will see an equally powerful language that fits in ¼ page


BYTE
the small systems journal
AUGUST 1981 Vol. 6, No. 8
$2.50 in USA/$2.95 in Canada
A McGraw-Hill Publication
SMALLTALK

BYTE Magazine, August 1981

Smalltalk

- Everything is an *object*
- Objects communicate by sending and receiving *messages*
- Objects have their own state (which may contain other objects)
- How do you do 3 + 4?

send the object **3** the message **"+ 4"**

Counter in Smalltalk

```
class name counter
  instance variable names count
  new count <- 0
  next count <- count + 1
  current ^ count
```

[redacted] [redacted] omg can it get anymore hotter. This day just confirmed that HELL has came. I wounder if I can used that excuse not to go to work tomorrow???hmmm :)

about an hour ago via Windows Phone · Comment · Like

[redacted] likes this.

[redacted] [redacted] Oh my. I think that one statement just demonstrated every single abuse of English grammar and spelling possible.

58 minutes ago · Like

Counter in Python

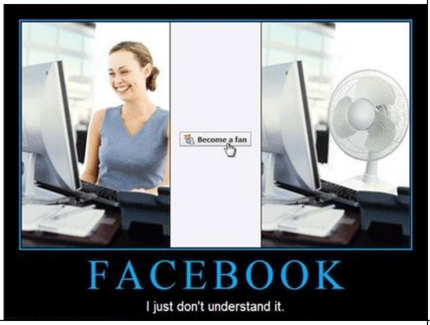
```
class counter:
  def __init__(self): self._count = 0
  def reset(self): self._count = 0
  def next(self): self._count = self._count + 1
  def current(self): return self._count
```

counter() creates a new counter using the __init__ method
count is the instance variable (is just a naming convention)

Pencil and Paper Time

- Write a **Python** class **FriendList** that supports the following operations:
  - Initially, the list is empty.
  - .add(*string*) adds a new friend of the given name, but does nothing if you're already friends
  - .unfriend(*string*) removes the friend of the given name
  - .listing() prints each friend in the friend list on its own line

```
>>> a = ["carrie", "samantha", "charlotte" ]
>>> a
['carrie', 'samantha', 'charlotte']
>>> a = a + ["miranda"]
>>> a
['carrie', 'samantha', 'charlotte', 'miranda']
>>> a.remove("samantha")
>>> a
['carrie', 'charlotte', 'miranda']
>>> "carrie" in a
True
```



FriendList

```
class FriendList:
  def __init__(self):
    self.friends = [ ]
  def add(self,friend):
    if not friend in self.friends:
      self.friends = self.friends + [friend]
  def unfriend(self,loser):
    if loser in self.friends:
      self.friends.remove(loser)
  def listing(self):
    for buddy in self.friends:
      print buddy
```

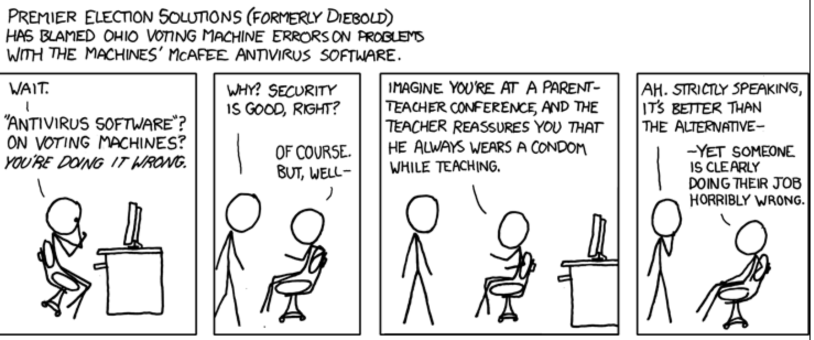
Who was the first object-oriented programmer?

By the word operation, we mean any process which alters the mutual relation of two or more things, be this relation of what kind it may. This is the most general definition, and would include all subjects in the universe. Again, it might act upon other things besides number, were objects found whose mutual fundamental relations could be expressed by those of the abstract science of operations, and which should be also susceptible of adaptations to the action of the operating notation and mechanism of the engine... Supposing, for instance, that the fundamental relations of pitched sounds in the science of harmony and of musical composition were susceptible of such expression and adaptations, the engine might compose elaborate and scientific pieces of music of any degree of complexity or extent.

Ada, Countess of Lovelace, around 1843

Homework

- Re-Read Chapter 11


PREMIER ELECTION SOLUTIONS (FORMERLY DIEBOLD) HAS BLAMED OHIO VOTING MACHINE ERRORS ON PROBLEMS WITH THE MACHINES' MCAFEE ANTIVIRUS SOFTWARE.
WAIT.
"ANTIVIRUS SOFTWARE"? ON VOTING MACHINES? YOU'RE DOING IT WRONG.
WHY? SECURITY IS GOOD, RIGHT?
OF COURSE. BUT, WELL–
IMAGINE YOU'RE AT A PARENT-TEACHER CONFERENCE, AND THE TEACHER REASSURES YOU THAT HE ALWAYS WEARS A CONDOM WHILE TEACHING.
AH. STRICTLY SPEAKING, IT'S BETTER THAN THE ALTERNATIVE–
–YET SOMEONE IS CLEARLY DOING THEIR JOB HORRIBLY WRONG.