Content

- Introduction

- Types of software errors

- Five examples

- What can we do ?

> “There are two ways to write error-free programs; only the third one works.”
>
> *(Alan J. Perlis)*

Introduction

- Software failures cause (dangerous) malfunctions of devices and services

- Mars Polar Lander (1999) never landed like this

Introduction

- Software failures cause wrong scientific conclusions

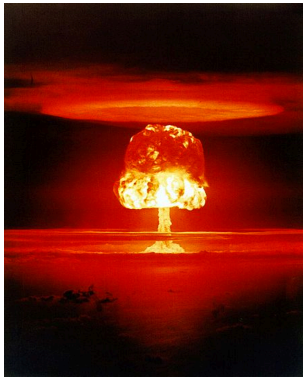
“”””

As a result, codes may be riddled with tiny errors that do not cause the program to break down, but may drastically change the scientific results that it spits out. One such error tripped up a structural-biology group led by Geoffrey Chang of the Scripps Research Institute in La Jolla, California. In 2006, the team realized that a computer program supplied by another lab had flipped a minus sign, which in turn reversed two columns of input data, causing protein crystal structures that the group had derived to be inverted. Chang says that the other lab provided the code with the best intentions, and "you just trust the code to do the right job". His group was forced to retract five papers published in *Science*, the*Journal of Molecular Biology* and *Proceedings of the National Academy of Sciences*, and now triple checks everything, he says.
“””

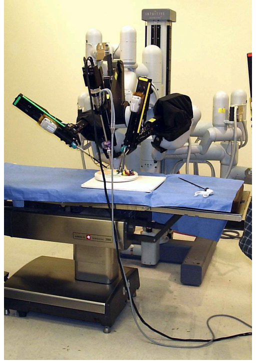
Nature **467**, 775-777 (2010) | doi:10.1038/467775a

Introduction

- Software spreads into almost everything



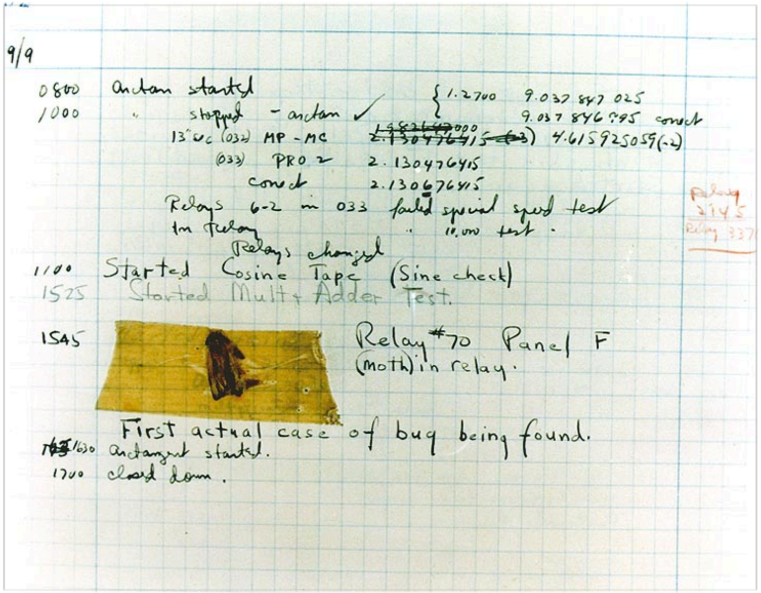
-



- …………

Types of software errors - the bug

Logbuch-Seite des Mark II Aiken Relay Calculator (Harvard) mit dem ersten *bug* (1947) - not so soft



9/9

0800 arctan started

1000 " stopped - arctan ✓ {1.2700 9.037 847 025
9.037 846 995 correct

13" uc (032) MP - MC ~~1.982147000~~ ~~2.130476415~~ (-3)) 4.615925059(-2)

(033) PRO 2 2.130476415

correct 2.130676415

Relays 6-2 in 033 failed special speed test
In relay " 10,000 test.

Relays changed

Relay 2145
Relay 3370

1100 Started Cosine Tape (Sine check)

1525 Started Mult + Adder Test.

1545 Relay #70 Panel F
(moth) in relay.

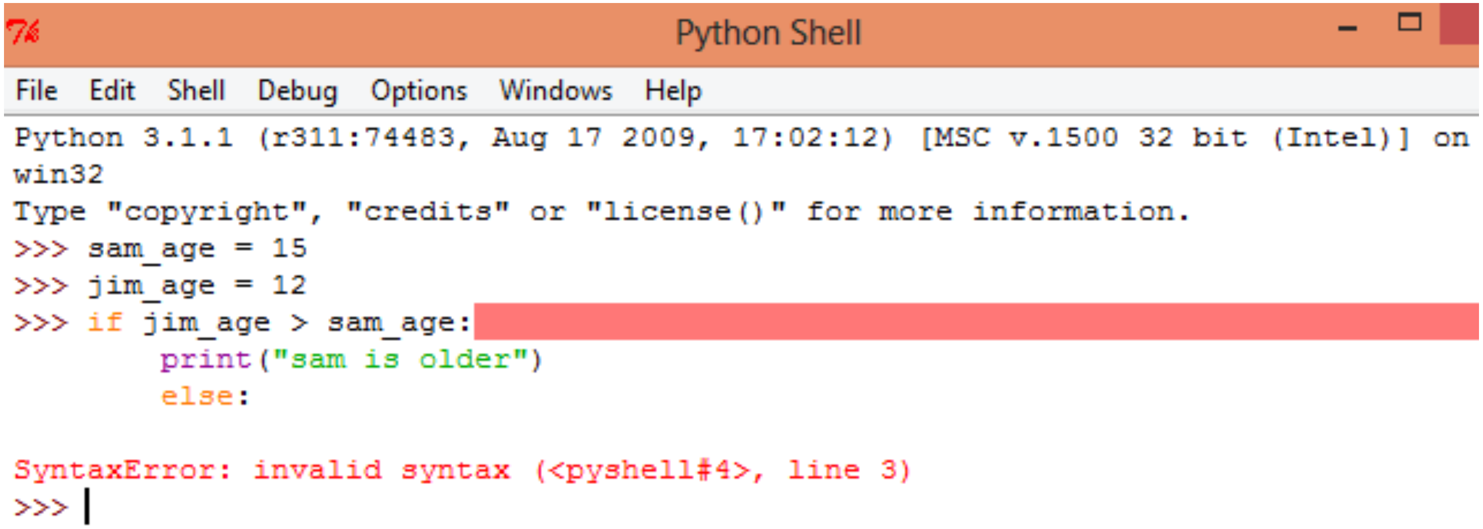
First actual case of bug being found.

~~143~~ 1630 arctangent started.

1700 closed down.

Mark II, general view of calculator frontpiece, 1948.

Syntax error



```
Python 3.1.1 (r311:74483, Aug 17 2009, 17:02:12) [MSC v.1500 32 bit (Intel)] on
win32
Type "copyright", "credits" or "license()" for more information.
>>> sam_age = 15
>>> jim_age = 12
>>> if jim_age > sam_age:
        print("sam is older")
        else:

SyntaxError: invalid syntax (<pyshell#4>, line 3)
>>> 
```

Normally catched by compiler or interpreter

Semantic error

```
x, y = alist[1:2]
```

`when what you actually needed was alist[1:3]`

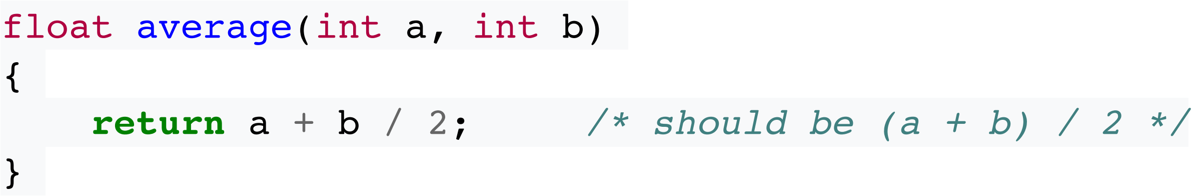
`or`

```
x = math.tan(1.25)
```

`you actually wanted math.atan(1.25)`

Using the wrong word. Not caught by compiler or interpreter.

Logical error



```
float average(int a, int b)
{
    return a + b / 2;      /* should be (a + b) / 2 */
}
```

Valid program, behaves fine, but produces wrong results.
Not caught by compiler or interpreter.

Categorised by time

Compile time errors

- Not so dangerous, however, may be annoying to fix.

Runtime errors

- Dangerous

And many others …

- Arithmetic
- Memory treatment
- Deadlocks
- Race conditions
- Interfacing
- Team working
- …

EXAMPLE

Therac-25

1. From 1985 to 1987 a computer controlled radiation therapy machine massively overdosed about six people. Some died.

2. Software controlled interlock failed due to a race condition (high dose was possible without appropriate shielding)

https://de.wikipedia.org/wiki/Therac-25

1991 Sinking of Norwegian Sleipner

1. 1991-08-23 The oil and gas platform Sleipner sinks

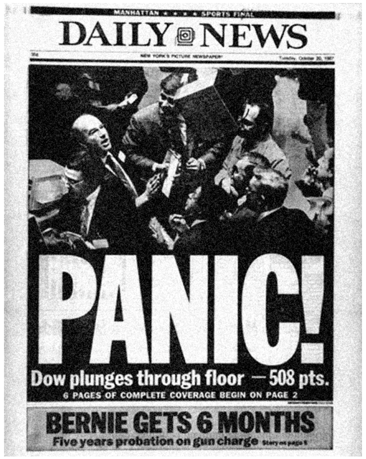
2. Economic loss about 700 MUSD

The post accident investigation traced the error to inaccurate finite element approximation of the linear elastic model of the tricell (using the popular finite element program NASTRAN). The shear stresses were underestimated by 47%, leading to insufficient design. In particular, certain concrete walls were not thick enough. More careful finite element analysis, made after the accident, predicted that failure would occur with this design at a depth of 62m, which matches well with the actual occurrence at 65m.

http://www-users.math.umn.edu/~arnold/disasters/sleipner.html

1987 Black Monday/Tuesday

- Monday 1987-10-19 a world wide stock market crash
- Usual blame is program trading (this is not really a software failure)
- Economic loss (probably most virtual) about 500 BUSD in one day



MANHATTAN ★ ★ ★ ★ SPORTS FINAL

DAILY NEWS

NEW YORK'S PICTURE NEWSPAPER

Tuesday, October 20, 1987

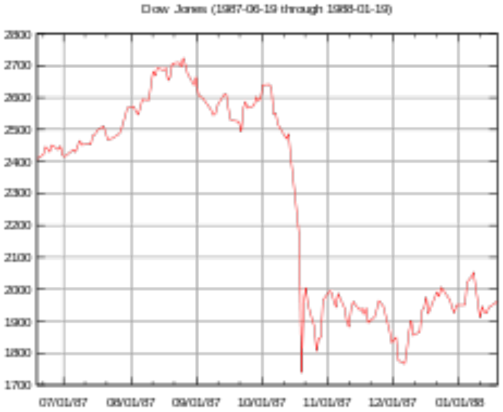
PANIC!

Dow plunges through floor — 508 pts.

6 PAGES OF COMPLETE COVERAGE BEGIN ON PAGE 2

BERNIE GETS 6 MONTHS

Five years probation on gun charge



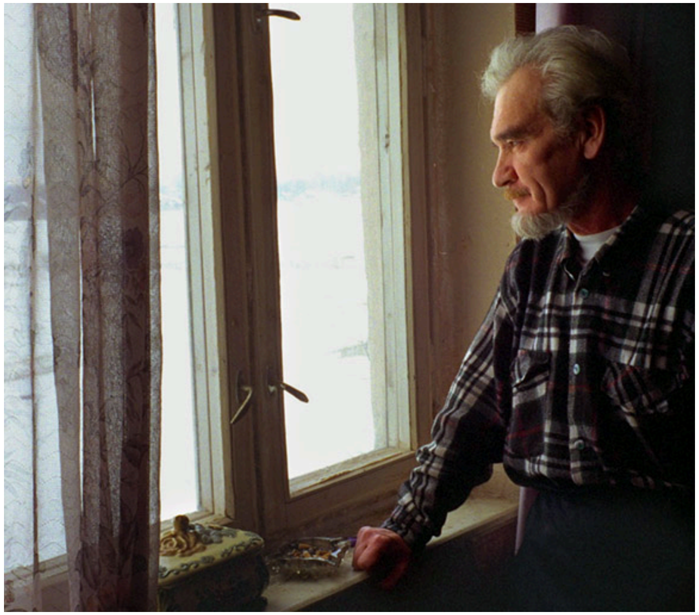
1996 Ariane 5 Explosion

- June 4, 1996, unmanned rocket launched by ESA explodes
- Value about 500 MUSD
- Cause: Integer Overflow (conversion from 64 bit to 16 bit)

https://www.youtube.com/watch?v=kYUrqdUyEpI

1983-09-23 World War III (almost)

- Soviet early warning satellite reports 5 US missiles coming towards Soviet
- S. Petrov reports it as a false alarm (luckily)



- Could have caused massive attack from Soviet
- Was a misinterpretation of reflecting sun light from cloud tops

Stanislav Petrov :”I had a funny feeling in my gut"

What can we do ?

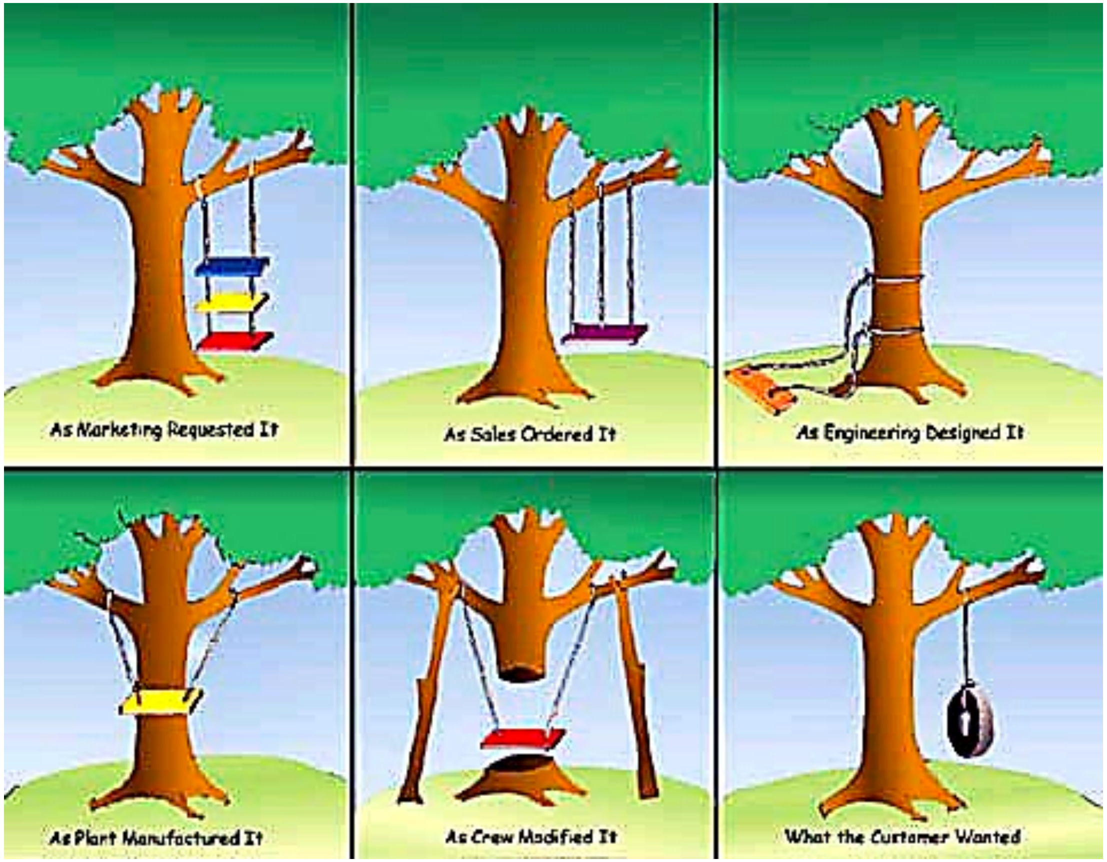
use the Best Practices article as an inspiration

Work in teams

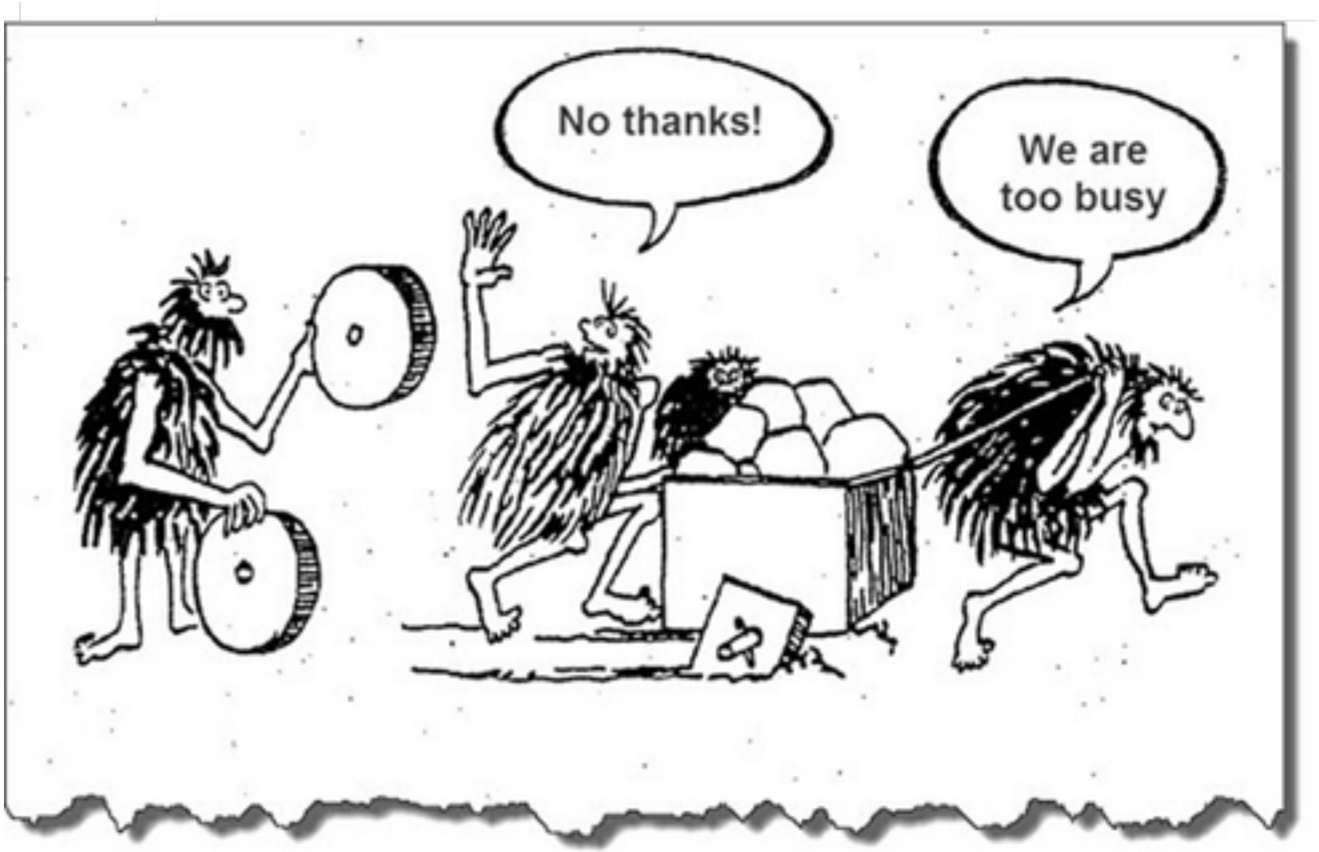
“You can’t have great software without a great team, and most software teams behave like dysfunctional families.”

(Jim McCarthy)

Good specifications and planning



Use the right language



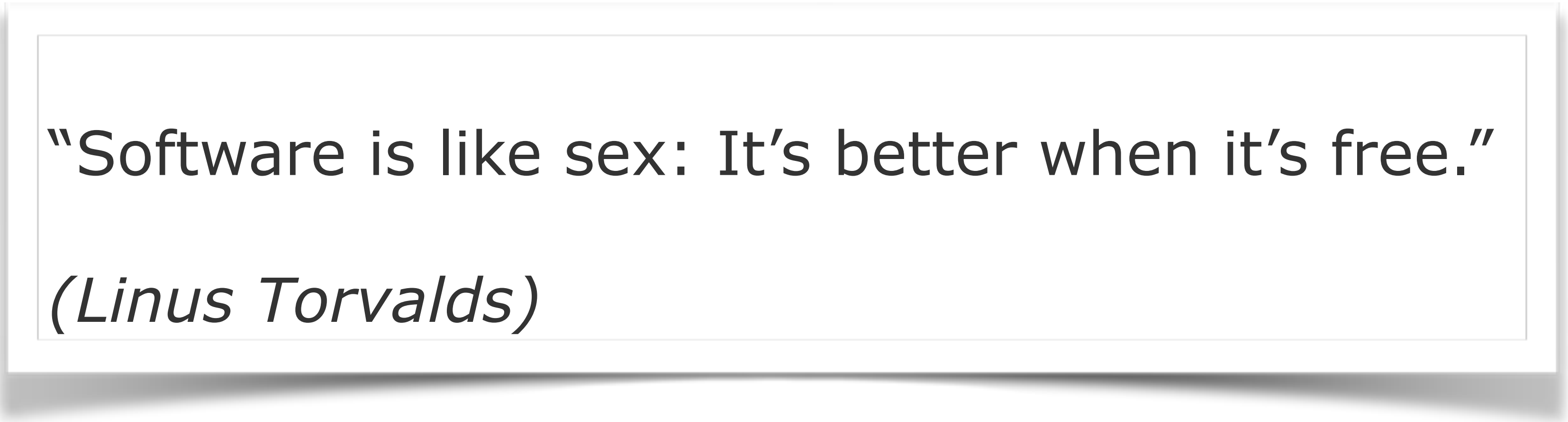
Write for people

- Style (linters etc)
- Modular
- Readable semantics
- Good commenting
- …

> “Always code as if the guy who ends up maintaining your code will be a violent psychopath who knows where you live.”
>
> *(Martin Golding)*

- Work test driven
- Unit testing
- Use VCS
- Agile develop agile (continues integration)
- Code analysis and review (pre-merge)
- Performance monitoring
- …

Do free open source



> “Software is like sex: It’s better when it’s free.”
>
> *(Linus Torvalds)*

b
UNIVERSITÄT
BERN

Thank you for your attention !

scits.unibe.ch
scits@math.unibe.ch