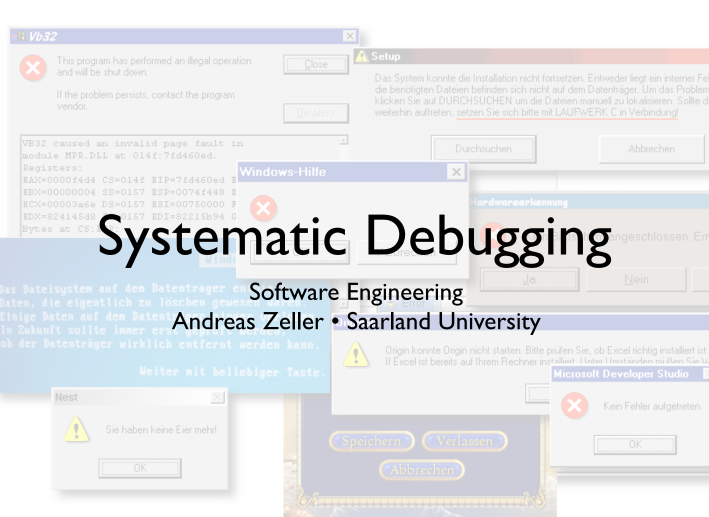


Systematic Debugging

Software Engineering

Andreas Zeller • Saarland University

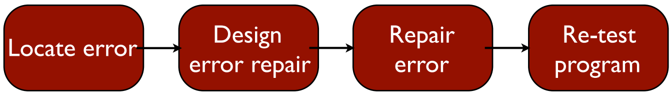
The Problem

Facts on Debugging

- Software bugs cost ~60 bln US$/yr in US
- Improvements could reduce cost by 30%
- Validation (including debugging) can easily take up to 50-75% of the development time
- When debugging, some people are *three times* as efficient than others

How to Debug

(Sommerville 2004)



The Process

T rack the problem
R eproduce
A utomate
F ind Origins
F ocus
I solate
C orrect

T
R
A
F
F
I
C

Tracking Problems

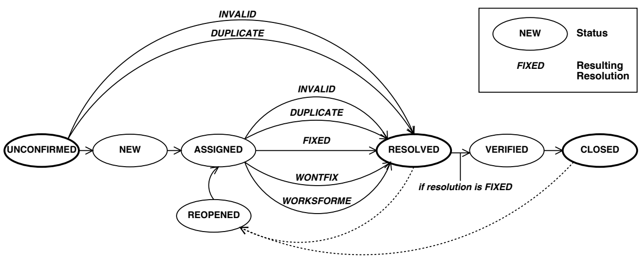
T
R
A
F
F
I
C

Tracking Problems

- Every problem gets entered into a *problem database*
- The *priority* determines which problem is handled next
- The product is ready when all problems are resolved

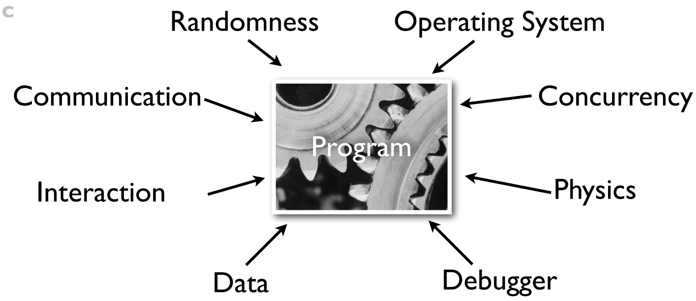
T
R
A
F
F
I
C

Problem Life Cycle



T R A F F I C

Reproduce



T R A F F I C

Automate

```
// Test for host
public void testHost() {
  int noPort = -1;
  assertEquals(askigor_url.getHost(), "www.askigor.org");
  assertEquals(askigor_url.getPort(), noPort);
}

// Test for path
public void testPath() {
  assertEquals(askigor_url.getPath(), "/status.php");
}

// Test for query part
public void testQuery() {
  assertEquals(askigor_url.getQuery(), "id=sample");
}
```

T R A F F I C

Automate

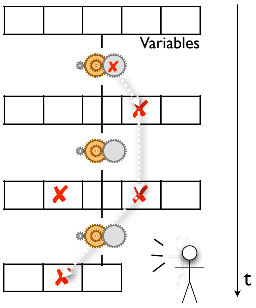
- Every problem should be *reproducible automatically*
- Achieved via appropriate (unit) tests
- After each change, we re-run the tests

T
R
A
F
F
I
C

Finding Origins

1. The programmer creates a *defect* in the code.
2. When executed, the defect creates an *infection*.
3. The infection *propagates*.
4. The infection causes a *failure*.

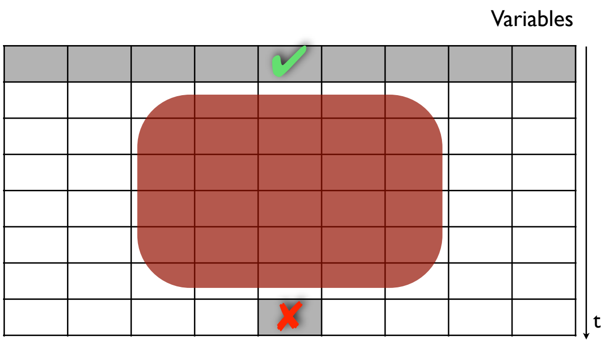
This infection chain must be traced back – and broken.



Not every defect creates an infection – not every infection results in a failure

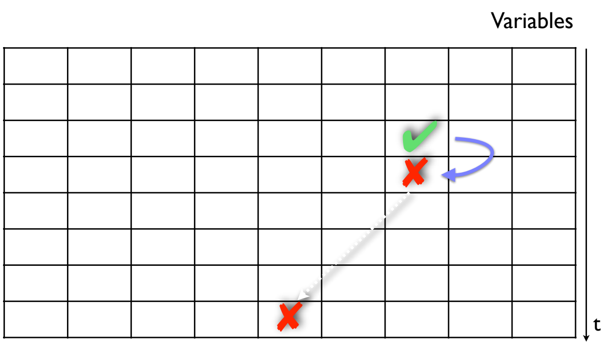
T
R
A
F
F
I
C

Finding Origins



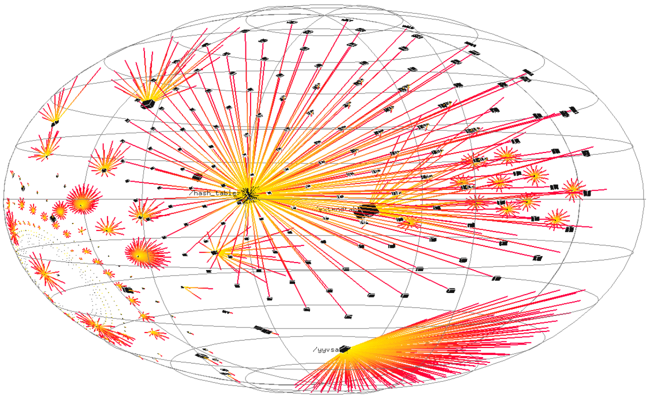
T
R
A
F
F
I
C

The Defect



T
R
A
F
F
I
C

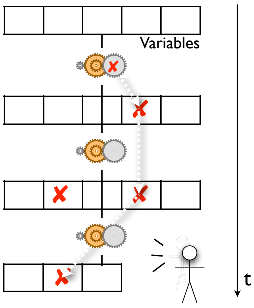
A Program State

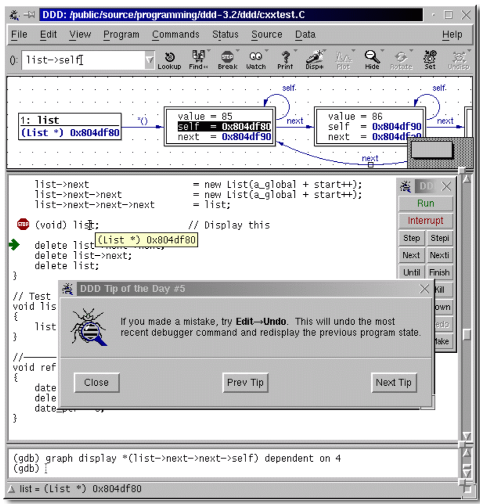


T
R
A
F
F
I
C

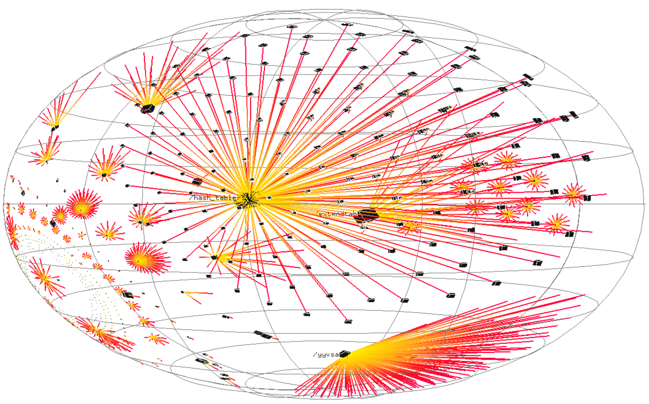
Finding Origins

1. We start with a *known infection* (say, at the failure)
2. We search the infection in the *previous state*

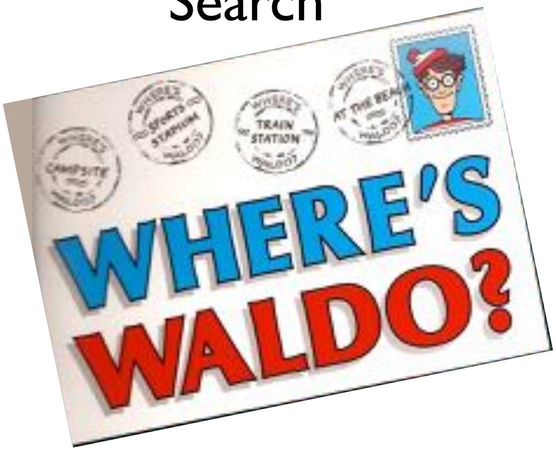




A Program State



Search



Focus

During our search for infection, we focus upon locations that

- *are possibly wrong*
  (e.g., because they were buggy before)
- *are explicitly wrong*
  (e.g., because they violate an *assertion*)

Assertions are the best way to find infections!

T R A F F I C

Finding Infections

```
class Time {
public:
    int hour();     // 0..23
    int minutes();  // 0..59
    int seconds();  // 0..60 (incl. leap seconds)

    void set_hour(int h);
    …
}
```

Every time between 00:00:00 and 23:59:60 is valid

T R A F F I C

Finding Origins

```
bool Time::sane()
{
    return (0 <= hour() && hour() <= 23) &&
           (0 <= minutes() && minutes() <= 59) &&
           (0 <= seconds() && seconds() <= 60);
}

void Time::set_hour(int h)
{
    assert (sane());  // Precondition
    …
    assert (sane());  // Postcondition
}
```

T R A F F I C

Finding Origins

```
bool Time::sane()
{
    return (0 <= hour() && hour() <= 23) &&
           (0 <= minutes() && minutes() <= 59) &&
           (0 <= seconds() && seconds() <= 60);
}
```

sane() is the *invariant* of a Time object:

- valid *before* every public method
- valid *after* every public method

T R A F F I C

Finding Origins

- Precondition fails = Infection *before* method
- Postcondition fails = Infection *after* method
- All assertions pass = no infection

```
void Time::set_hour(int h)
{
    assert (sane());  // Precondition
    …
    assert (sane());  // Postcondition
}
```

T R A F F I C

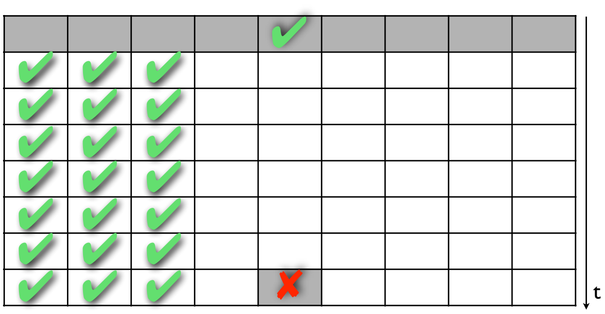
Complex Invariants

```
class RedBlackTree {
  …
  boolean sane() {
      assert (rootHasNoParent());
      assert (rootIsBlack());
      assert (redNodesHaveOnlyBlackChildren());
      assert (equalNumberOfBlackNodesOnSubtrees());
      assert (treeIsAcyclic());
      assert (parentsAreConsistent());

      return true;
  }
}
```

T R A F F I C

Assertions



T
R
A
F
F
I
C

Focusing

- All possible influences must be checked
- Focusing on most likely candidates
- Assertions help in finding infections fast

T
R
A
F
F
I
C

Isolation

- Failure causes should be *narrowed down systematically*
- Use *observation* and *experiments*

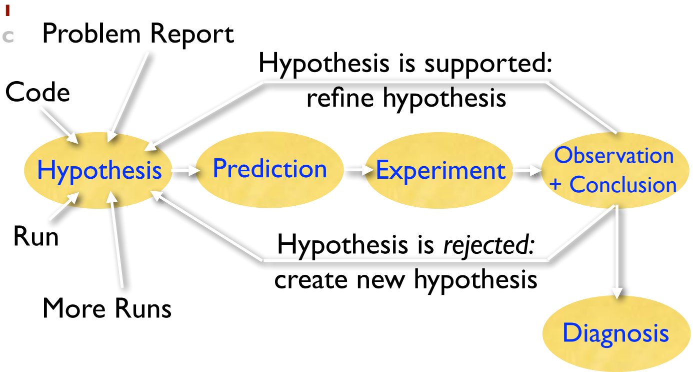
T
R
A
F
F
I
C

Scientific Method

1. Observe some aspect of the universe.
2. Invent a *hypothesis* that is consistent with the observation.
3. Use the hypothesis to make *predictions*.
4. Tests the predictions by experiments or observations and modify the hypothesis.
5. Repeat 3 and 4 to refine the hypothesis.

TRAFFIC

Scientific Method



TRAFFIC

TRAFFIC

Explicit Hypotheses

Hypothesis	*The exec… causes a[0] = 0*
Prediction	*At L… should hold.*
Experiment	*… Line 37.*
Observat…	*… olds as predicted.*
Conclusion	*… hesis is confirmed.*

Keeping everything in memory is like playing mastermind blind!

Explicit Hypotheses

Isolate

- We repeat the search for infection origins until we found the defect
- We proceed *systematically* along the scientific method
- *Explicit steps* guide the search – and make it repeatable at any time

Study in Summer –
Call for Volunteers

Correction

Before correcting the defect, we must check whether the defect

- actually is an *error* and
- *causes* the failure

Only when we understood both, can we correct the defect

T R A F F I C

The Devil's Guide to Debugging

Find the defect by guessing:

- Scatter debugging statements everywhere
- Try changing code until something works
- Don't back up old versions of the code
- Don't bother understanding what the program should do

T R A F F I C

The Devil's Guide to Debugging

Don't waste time understanding the problem.

- Most problems are trivial, anyway.

T R A F F I C

The Devil's Guide to Debugging

Use the most obvious fix.

- Just fix what you see:

```
x = compute(y)
// compute(17) is wrong - fix it
if (y == 17)
    x = 25.15
```

Why bother going into compute()?

T R A F F I **C**

Successful Correction

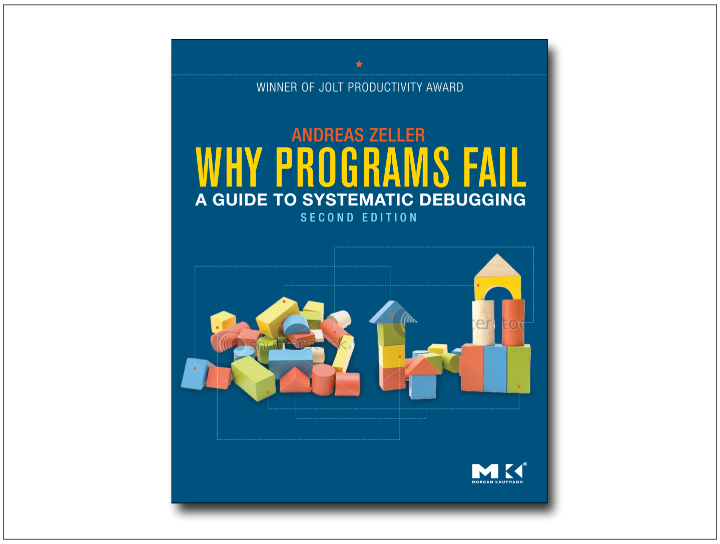
T R A F F I **C**

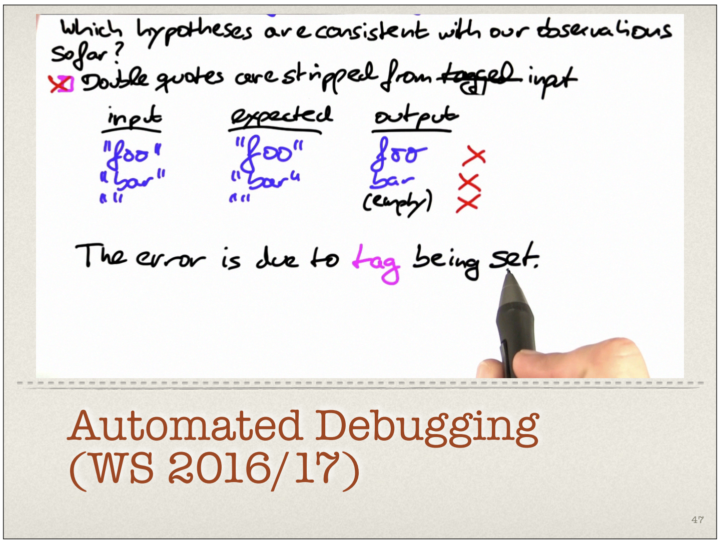
Homework

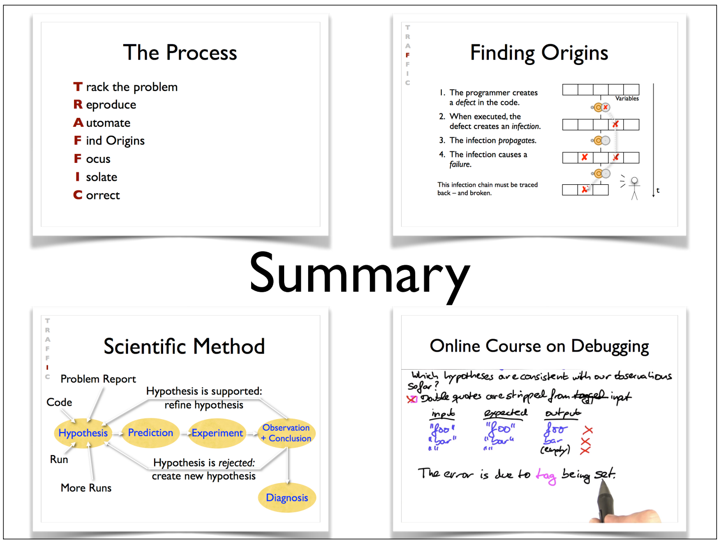
- Does the failure no longer occur?
  (If it does still occur, this should come as a big surprise)
- Did the correction introduce new problems?
- Was the same mistake made elsewhere?
- Did I commit the change to version control and problem tracking?

The Process

T rack the problem
R eproduce
A utomate
F ind Origins
F ocus
I solate
C orrect


WINNER OF JOLT PRODUCTIVITY AWARD
ANDREAS ZELLER
WHY PROGRAMS FAIL
A GUIDE TO SYSTEMATIC DEBUGGING
SECOND EDITION
MK MORGAN KAUFMANN


Which hypotheses are consistent with our observations so far?
Double quotes are stripped from ~~tagged~~ input
input
expected
output
"foo"
"bar"
""
"foo"
"bar"
""
foo
bar
(empty)
The error is due to tag being set.
Automated Debugging
(WS 2016/17)
47


The Process
T rack the problem
R eproduce
A utomate
F ind Origins
F ocus
I solate
C orrect
Finding Origins
1. The programmer creates a defect in the code.
2. When executed, the defect creates an infection.
3. The infection propagates.
4. The infection causes a failure.
This infection chain must be traced back – and broken.
Variables
Summary
Scientific Method
Problem Report
Code
Run
More Runs
Hypothesis
Prediction
Experiment
Observation + Conclusion
Hypothesis is supported: refine hypothesis
Hypothesis is rejected: create new hypothesis
Diagnosis
Online Course on Debugging
The error is due to tag being set.