

How to fix bugs automatically?

Martin Monperrus
University of Lille & Inria
Lille, France

October 2014



“Le Merveilleux”, specialty of Lille



1. Confectionner des meringues plates et rondes avec de la meringue française.



2. Montez une chantilly bien serrée avec le sucre glace.



3. Mélanger la Chantilly avec le mascarpone.



4. Ajouter ensuite le pralin ou la pâte de pistache à la crème et la mettre au frais pour la raffermir un peu.



5. Lorsque la crème (ici crème nature) est prête, masquer le premier disque de meringue avec la crème à l'aide d'une spatule.



6. Placer le deuxième disque de meringue sur la crème en appuyant légèrement.



7. Poser un peu de crème au sommet du deuxième disque de la même façon que pour le premier.



8. Masquer les bords et égaliser la forme.



9. Poser sur les copeaux de chocolat.



10. Bien répartir les copeaux à la surface.



11. Parsemer de copeaux de chocolat brisés sur toute la surface et conservez au frais si vous ne les consommez pas tout de suite.



12. La mousse chocolat noir peut remplacer la crème chantilly mascarpone.

How to fix bugs automatically?

- Choose a class of bugs
- Identify a good bug oracle
- Set up repair operators
- Add a dose of CPU usage
- Serve it

Martin Monperrus' recipe, version of Oct 14 2014

See also A Critical Review of "Automatic Patch Generation Learned from Human-Written Patches": Essay on the Problem Statement and the Evaluation of Automatic Software Repair (Martin Monperrus), In Proceedings of the International Conference on Software Engineering, 2014.

Choose a class of bugs



≠



Buffer overflow?

Unhandled exceptions?

Infinite loops?

Crash?

Memory leak?

API Misusage?

Buggy conditions?

In my group: buggy ifs, missing precondition, infinite loops, unhandled exceptions

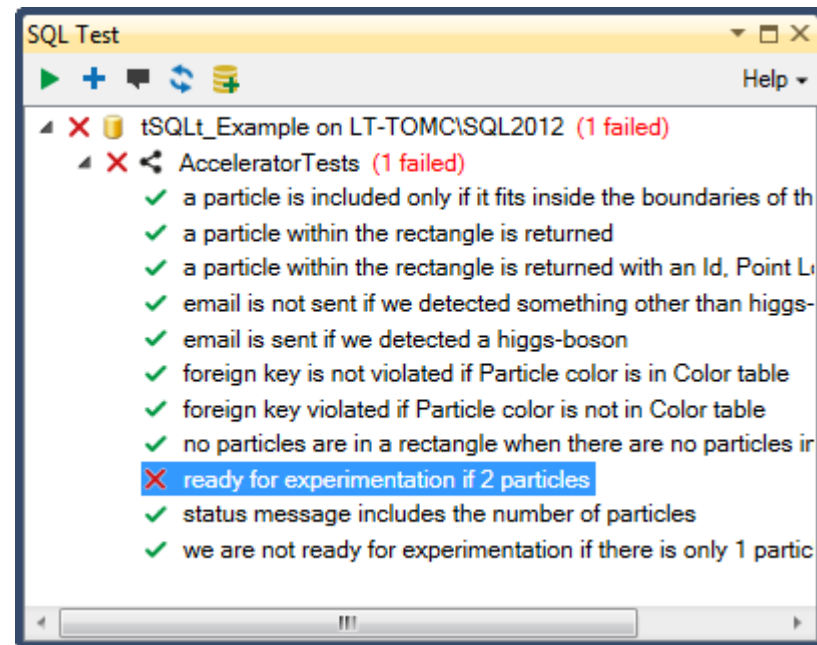
Identify a good bug oracle

A bug oracle tells you “YES there is a bug”,
“No, it is fixed”

Examples:

Crashing input: `$ pgm --input foo`

Failing test case:



Identify a good bug oracle

Core repair algorithm:

```
While "YES there is a bug"  
{  
    Try something else  
}
```

Identify a good bug oracle

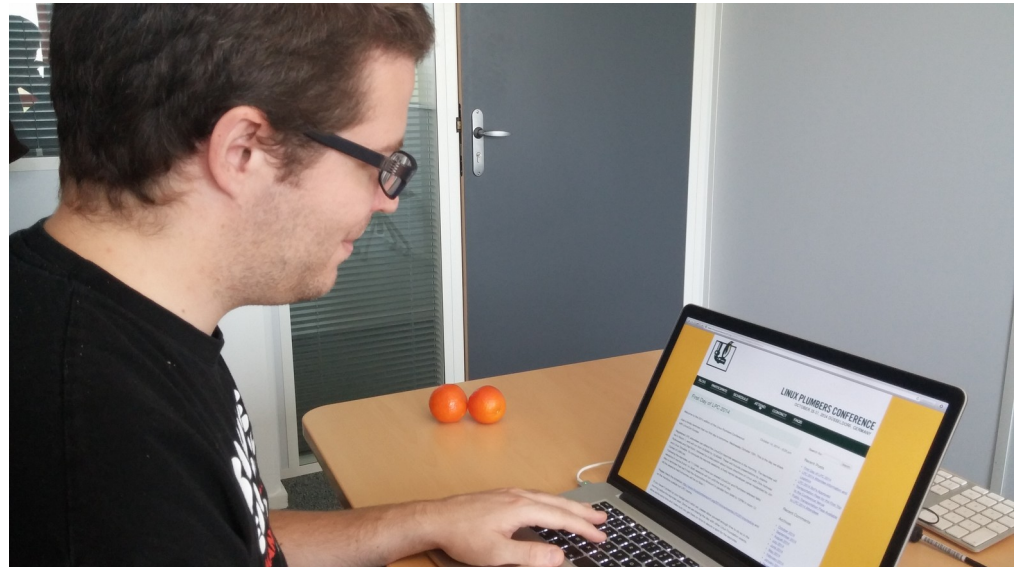
A good bug oracle is:

- Automated
- Does not take too long

Other examples of oracle:



Lawall et al., "WYSIWIB: A declarative approach to finding API protocols and bugs in Linux code.", 2009



Carzaniga, Antonio, et al. "Automatic workarounds for web applications.", 2010

Set up repair operators

A repair operator is a generic modification on source code

Examples:

- add a precondition

+ if (age >= 18)

 serve_adult_content()

Set up repair operators

Most repair operators have holes

If (___HOLE___)

There are different techniques to fill the holes:

- Pick some code elsewhere [1]
- Synthesize it using constraint solving [2]

[1] Martinez et al., "Do the Fix Ingredients Already Exist? An Empirical Inquiry into the Redundancy Assumptions of Program Repair Approaches", ICSE 2014

[2] Nguyen, Hoang Duong Thien, et al. "SemFix: Program repair via semantic analysis." Proceedings of the 2013 International Conference on Software Engineering. IEEE Press, 2013.

Set up repair operators

Some repair operators are surgical, other are very violent

“In some cases one needs a regression oracle”

```
For some time {
  While “YES there is a bug” {
    Try something else
  }
  Is there a regression?
}
```

Add a dose of CPU usage

- “An average repair run took 356.5 seconds” [1]
- “Repairing system.Windows.forms (.NET) takes 62 minutes” [2]

What about the unrepaired bugs?

[1] Le Goues et al., “GenProg A generic method for automatic software repair, In TSE, 2012”

[2] Logozzo et al. “Modular and Verified Automatic Program Repair”, In OOPSLA, 2012

Serve it

Repairs can be served at runtime or as a recommendation to the developer

```
From: Léonce the Repair Bot <repairbot@inria.fr>  
To: LKML  
Subject: Patch for bug #1234
```

Dear maintainer,

I found a patch for bug #1234
In streaming.c

```
+ if (age >= 18)  
    serve_adult_content()
```

You can pull it at `git://univ-lille1.fr/soft.git`

Léonce, your repair bot

Does it really work?

- It is only the beginning
- ~ 100 real bugs have been fixed automatically
- Some research prototypes

“My dream is a fully generated patch accepted by human developers (without knowing it has been created by a robot)”

How to fix bugs automatically?

- Choose a class of bugs
- Identify a good bug oracle
- Set up repair operators
- Add a dose of CPU usage
- Serve it



Specialties of Lille :-)

With an amazing team of cookers (no order): Matias Martinez, Benoit Cornu, Vincenzo Musco, Jifeng Xuan, Sebastian Marcote, Favio DeMarco, and others