Software for a better world

Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

UNIVERSITY OF LONDON

A World Leading SFI Research Centre

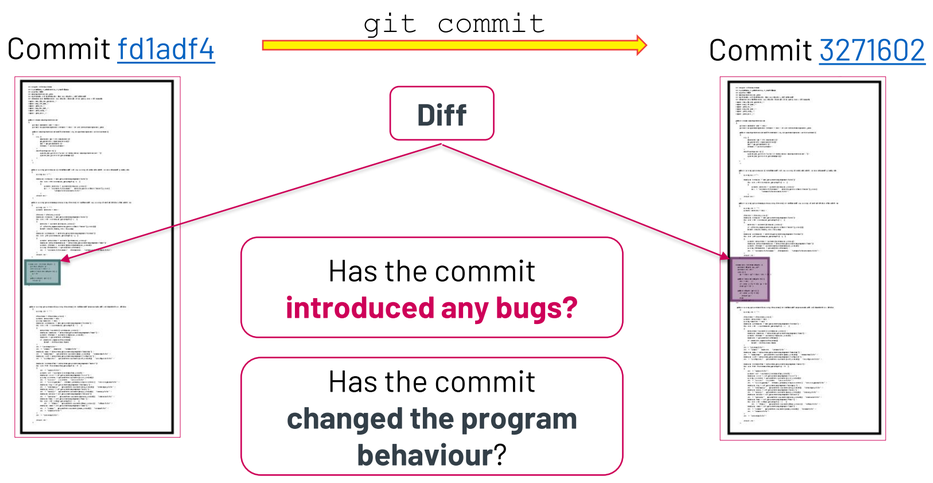
Science Foundation Ireland sfi For what's next

Regression Verification for Modern Programming Languages

Yu Yang Lin Hou, Vasileios Koutavas, Nikos Tzevelekos

1 PROBLEM:

- Global teams making 1000's of commits in large codebases
- Changes may introduce **regression errors**
- **Small changes – big impact**



Current practice: Regression testing

✗ Non-exhaustive analysis
✗ High cost to curate test-suite
  - Coverage? Maintainability?
✗ Many resources to run tests
✗ Feedback delay to developer; Low fix rate
  - Run nightly
✗ Access to entire code

+ peer review, bug-finding tools, etc.

GOOGLE:
- **2 Billion** LOC codebase
- **800K** Builds/day
- **150M** test runs/day
- **9h delay** in test feedback

[Memon et al. ICSE-SEIP'17]

2 OUR APPROACH:

Regression Verification

Prove that Commit 3271602 behaves equivalently to previous Commit fd1adf4

...by proving the changes **Contextually Equivalent***

*in cases of the new commit is **adding good/removing bad behaviour: contextual refinement**

M ≡ N if they are interchangeable in all program contexts C

Proposed Approach: Regression verification

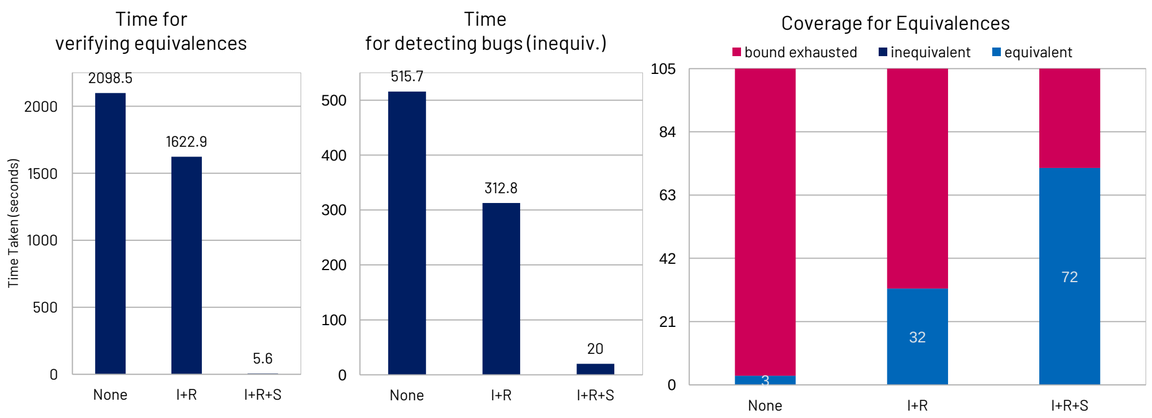
- ✓ **Exhaustive analysis AND use as bug finding tool**
- ✓ Low cost
  - Does not need manual test-suite / formal spec (code is spec)
- ✓ Low resources
  - Does not need full-program test runs / verification
- ✓ Timely Feedback
  - Run at compile time, increasing fix rate
- ✓ No need for full access to code

Lero@TCD is leading research and creating state-of-the-art technology in regression verification

3 RESULTS TO DATE:

Hobbit – (H)igher-(O)rder (Bi)simulation (T)ool
[github.com/LaifsV1/Hobbit]

- **State-of-the-art verification tool** for Contextual Equivalence for programs such as those written in OCaml, Python, Java, Lisp, ...
- **Guaranteed to find all bugs (inequivalences)** that are not due to infinite loops
  - More equivalences verified than ever before
  - Novel techniques speed up verification by 400x.



pcfeq – Equivalence Verification tool for functional (PCFv) programs
[github.com/LaifsV1/pcfeq]

- **a breakthrough model of functional programs considered impossible before**
- **State-of-the-art verification tool** for Contextual Equivalence for programs such as those written in Haskell
- **Distinguished paper @LICS, invited for publication @Journal of ACM**

4 FUTURE DIRECTIONS:

- **More powerful equivalence verification techniques**
- Equivalence verification for **concurrent programming languages**
- Integration in **software development environments**
- Validation in **real-world use cases:**

CISCO ethereum foundation

Funded project for applying the technology on **Blockchain Smart Contracts**

- More potential applications in Security, Privacy, protocol verification, compiler correctness, testing frameworks...

See details in:

Koutavas, V., Lin, YY., Tzevelekos, N. (2022).
From Bounded Checking to Verification of Equivalence via Symbolic Up-to Techniques
In: TACAS 2022 (ETAPS 2022). LNCS, v.13244. Springer.
doi.org/10.1007/978-3-030-99527-0_10
Software tool: github.com/LaifsV1/Hobbit

Koutavas, V., Lin, YY., Tzevelekos, N. (2023).
Fully Abstract Normal Form Bisimulation for Call-by-Value PCF.
In: ACM/IEEE LICS 2023, pp. 1-13.
Distinguished paper, invited for publication in JACM.
doi.org/10.1109/LICS56636.2023.10175778
Software tool: github.com/LaifsV1/pcfeq

HOST INSTITUTION

UNIVERSITY OF LIMERICK
OLLSCOIL LUIMNIGH

PARTNER INSTITUTIONS

Ollscoil na Gaillimhe University of Galway · Maynooth University National University of Ireland Maynooth · Trinity College Dublin Coláiste na Tríonóide, Baile Átha Cliath The University of Dublin · University College Dublin An Coláiste Ollscoile, Baile Átha Cliath · UCC University College Cork, Ireland Coláiste na hOllscoile Corcaigh · MTU Ollscoil Teicneolaíochta na Mumhan Munster Technological University · DCU · SETU South East Technological University · Dundalk Institute of Technology Institiúid Teicneolaíochta Dhún Dealgan · TUS · ATU Atlantic Technological University

FUNDED BY:
Ireland's European Structural and Investment Funds Programmes 2014-2020 Co-funded by the Irish Government and the European Union
European Union European Regional Development Fund
Science Foundation Ireland sfi For what's next