HyDiff: Hybrid Differential Software Analysis

DOI 10.5281/zenodo.3627893

Yannic Noller

Corina S. Pasareanu

Marcel Böhme

Youcheng Sun

Hoang Lam Nguyen

Lars Grunske

HUMBOLDT-UNIVERSITÄT ZU BERLIN

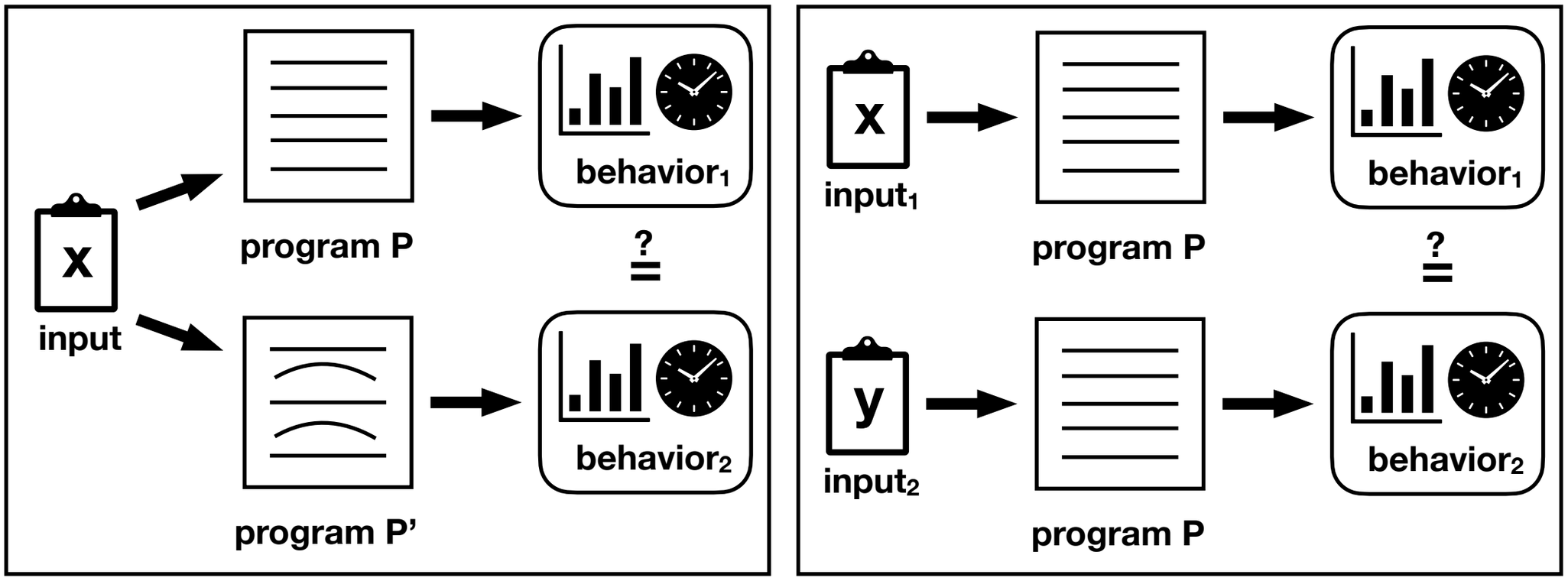
Carnegie Mellon University

NASA Ames Research Center

MONASH University

QUEEN'S UNIVERSITY BELFAST

Differential Analysis



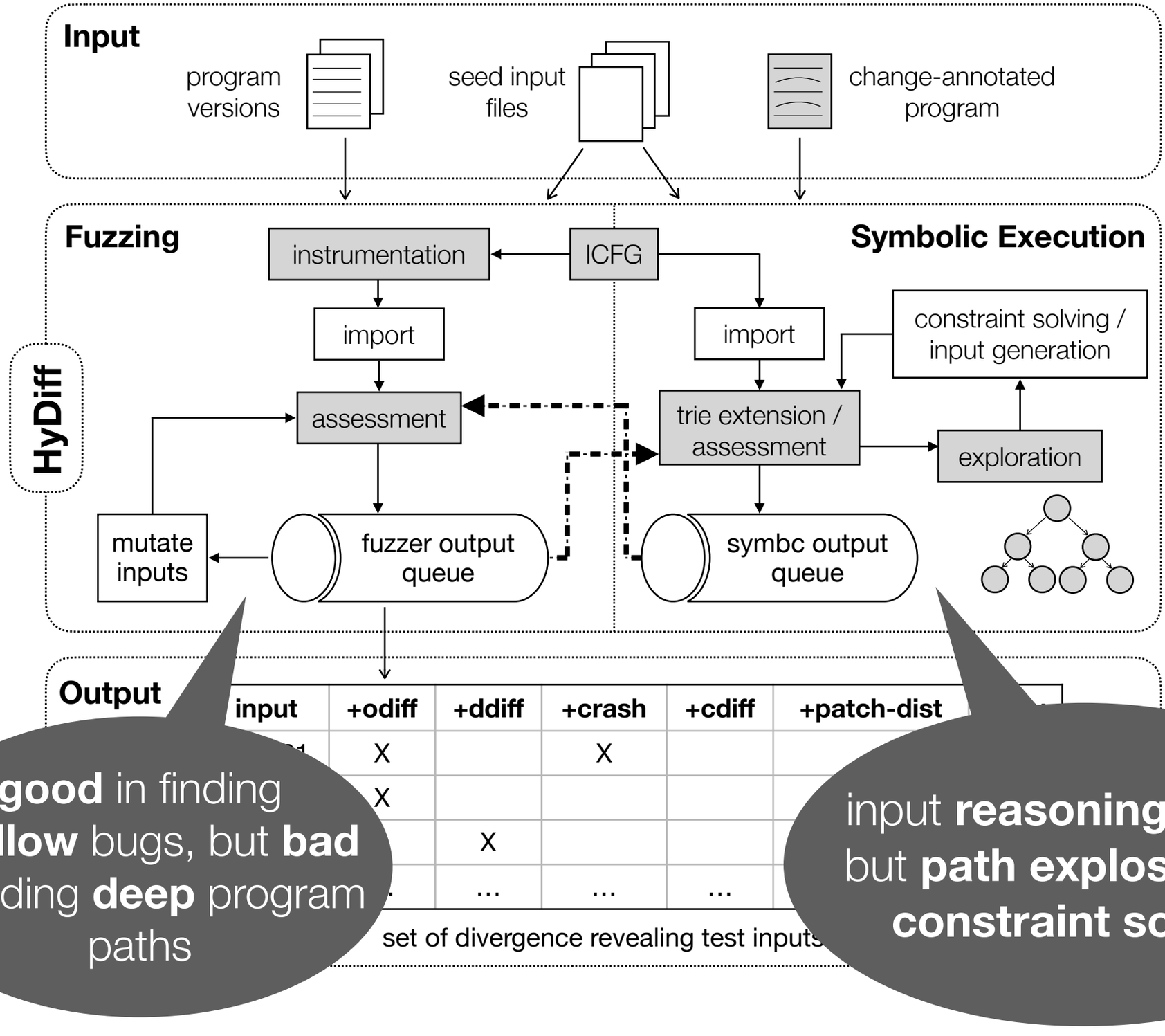
1

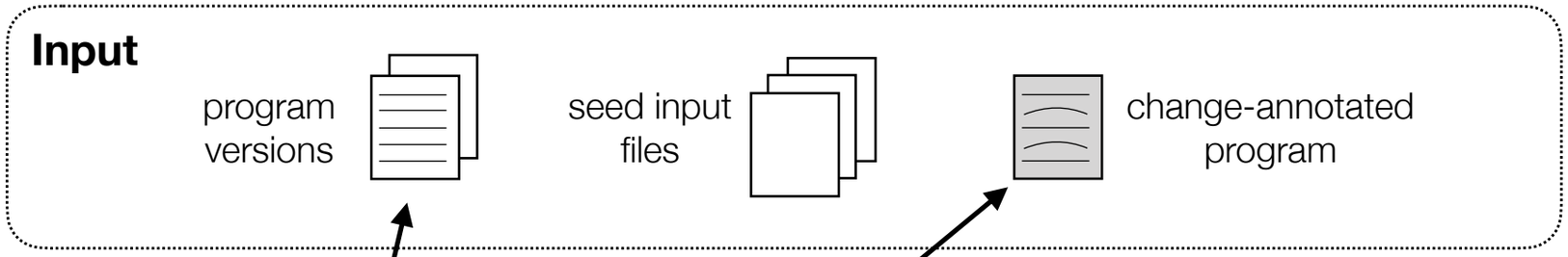
2

Regression Analysis

Side-Channel Analysis

Robustness Analysis of Neural Networks


Input
program versions
seed input files
change-annotated program
Fuzzing
Symbolic Execution
HyDiff
instrumentation
ICFG
import
import
constraint solving / input generation
assessment
trie extension / assessment
exploration
mutate inputs
fuzzer output queue
symbc output queue
Output
input
+odiff
+ddiff
+crash
+cdiff
+patch-dist
X
X
X
X
...
...
...
set of divergence revealing test inputs
good in finding shallow bugs, but bad in finding deep program paths
input reasoning ability, but path explosion and constraint solving



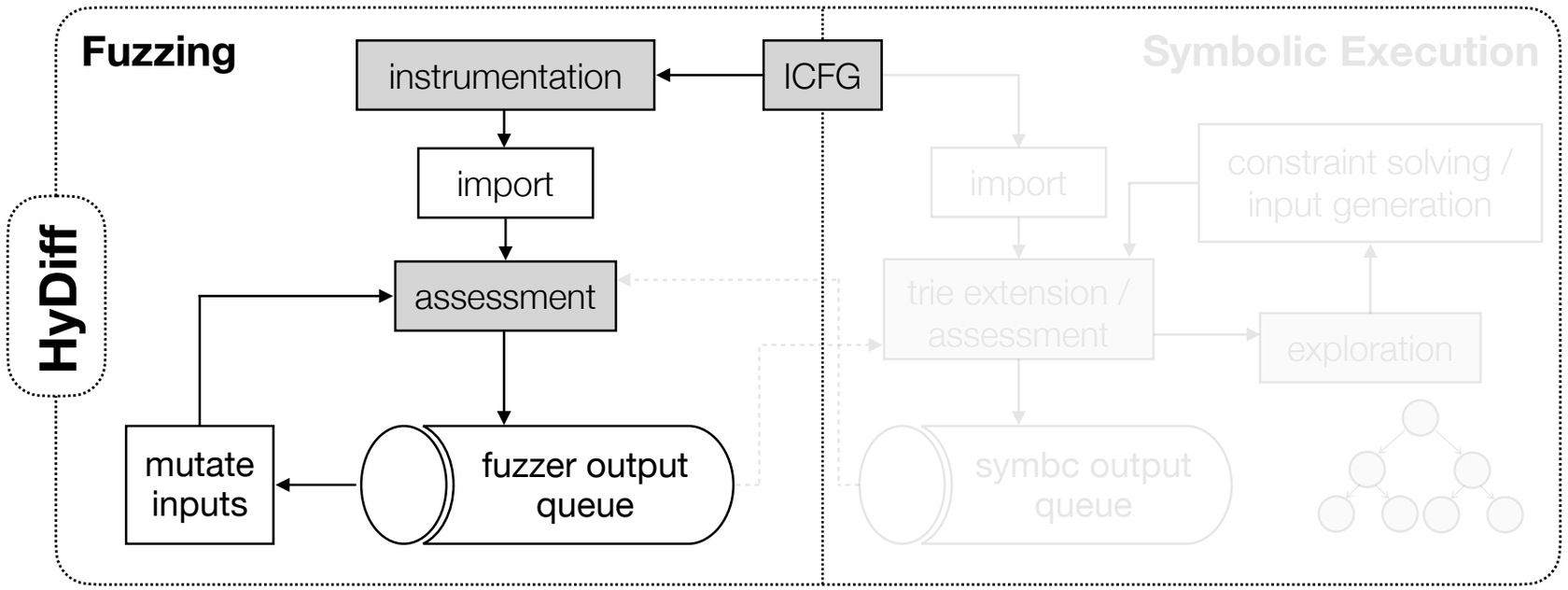
HyDiff's Input

- seed inputs
- **program** under test
- **two different** change types
  - (1) **inside** the **program code**
  - (2) **in** the **input**

```
input := change(input₁, input₂)
```

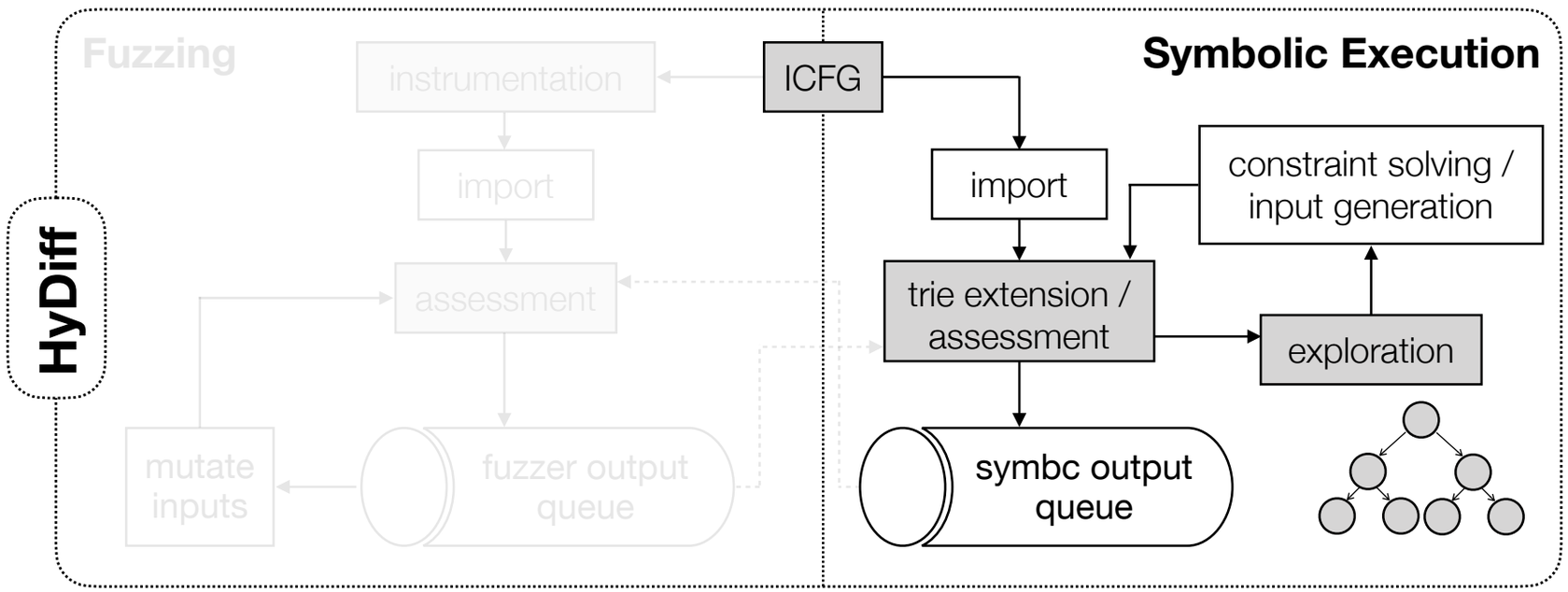
change-annotations by Palikareva et al. [2]

Change Type	Example
Update assignment	`x = x + change(E1, E2);`
Update condition	`if(change(E1, E2)) ...`
Add extra assignment	`x = change(x, E);`
Remove assignment	`x = change(E, x);`
Add conditional	`if(change(false, C)) ...`
Remove conditional	`if(change(C, false)) ...`
Remove code	`if(change(true, false)) ...`
Add code	`if(change(false, true)) ...`



Differential Greybox Fuzzing (DF)

- built upon AFL [1] (genetic algorithm)
- mutant selection driven by differential heuristics:
  - output difference
  - decision history difference
  - cost difference
  - patch distance
- additionally guided by branch coverage



Differential Symbolic Execution (DSE)

- built upon Symbolic PathFinder (SPF) [3]
- central data structure: trie
- node selection driven by differential heuristics:
  - decision history difference
  - cost difference
  - patch distance
- additionally guided by branch coverage

Output

input	+odiff	+ddiff	+crash	+cdiff	+patch-dist	+cov
id:0001	X		X			X
id:0002	X					X
id:0003		X			X	
…	…	…	…	…	…	…

set of divergence revealing test inputs

HyDiff's Output

- set of generated inputs
- classified by divergence
  - output difference (+odiff)
  - control-flow (+ddiff)
  - crashing behavior (+crash)
  - execution cost (+cdiff)
- additionally
  - patch distance (+patch-dist)
  - branch coverage (+cov)

Experiments

Regression Analysis

- HyDiff classifies all subjects correctly
- significantly more output and decision differences

Side-Channel Analysis

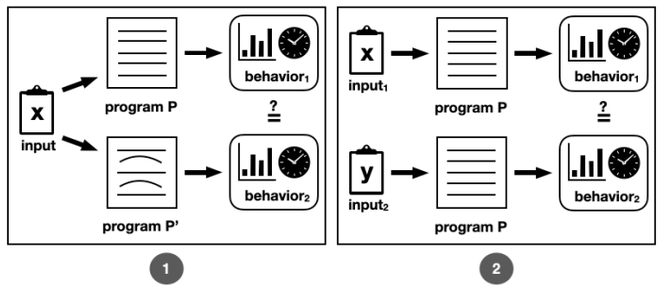
- HyDiff shows good trade-off between DSE and DF
- no significant amplification of the exploration

Robustness Analysis of Neural Networks

- stress test for HyDiff
- HyDiff significantly more output differences

HyDiff: Hybrid Differential Software Analysis

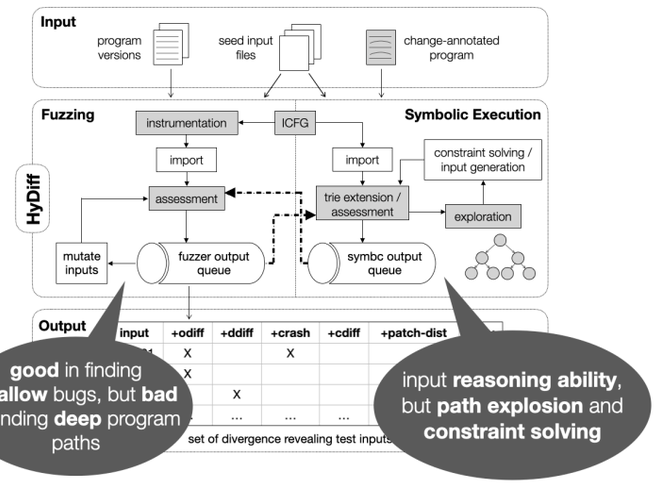
Differential Analysis

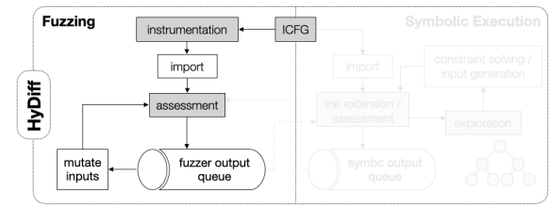


Regression Analysis

Side-Channel Analysis

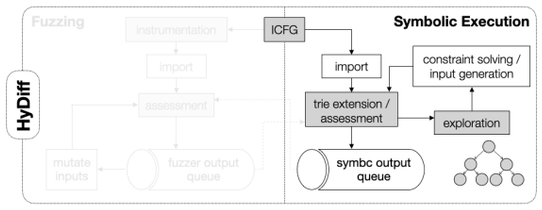
Robustness Analysis of Neural Networks





Differential Greybox Fuzzing (DF)

- built upon AFL [1] (genetic algorithm)
- mutant selection driven by differential heuristics:
  - output difference
  - decision history difference
  - cost difference
  - patch distance
- additionally guided by branch coverage



Differential Symbolic Execution (DSE)

- built upon Symbolic PathFinder (SPF) [3]
- central data structure: trie
- node selection driven by differential heuristics:
  - decision history difference
  - cost difference
  - patch distance
- additionally guided by branch coverage

Experiments

Regression Analysis
- HyDiff identifies all output differences
- significantly more output and decision differences

Side-Channel Analysis
- HyDiff shows good trade-off between DSE and DF
- no significant amplification of the exploration

Robustness Analysis of Neural Networks
- stress test for HyDiff
- HyDiff significantly more output differences

DOI 10.5281/zenodo.3627893

GitHub
`yannicnoller/hydiff`

References

[1] Website. American Fuzzy Lop (AFL). http://lcamtuf.coredump.cx/afl/.

[2] Hristina Palikareva, Tomasz Kuchta, and Cristian Cadar. 2016. *Shadow of a Doubt: Testing for Divergences between Software Versions*. In 2016 IEEE/ACM 38th International Conference on Software Engineering (ICSE). 1181–1192. https: //doi.org/10.1145/2884781.2884845

[3] Corina S. Păsăreanu, Willem Visser, David Bushnell, Jaco Geldenhuys, Peter Mehlitz, and Neha Rungta. 2013. *Symbolic PathFinder: integrating symbolic execution with model checking for Java bytecode analysis.* Automated Software Engineering 20, 3 (2013), 391–425. https://doi.org/10.1007/s10515-013-0122-2