MANCHESTER 1824

The University of Manchester

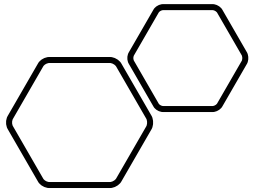
FuSeBMC - AI

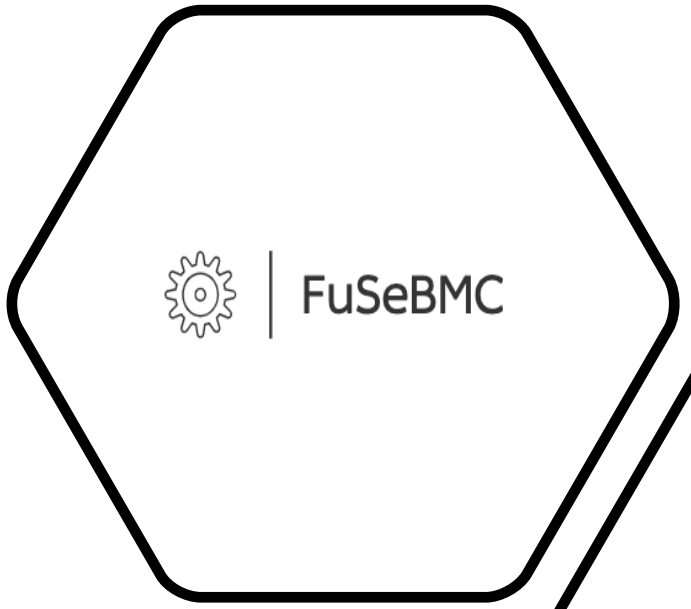
FuSeBMC AI: Acceleration of Hybrid Approach through Machine Learning

Presenter: Rafael Menezes

Author: Kaled Alshmrany

Co-Authors: Mohannad Aldughaim, Chenfeng Wei, Tom Sweet, Richard Allmendinger & Lucas C. Cordeiro





The Outline

- FuSeBMC-AI Team
- Motivation
- FuSeBMC-AI framework
- Setting Features
- Training Set Labeling
- Machine Learning Models
- Competition Results
- Software Project

FuSeBMC Team

Dr. Kaled Alshmrany

FuSeBMC

Dr. Lucas Cordeiro

SCorCH

SCorCH team

ESBMC

ESBMC team

Institute of Public Administration

Motivation

- Software testing is essential for catching critical bugs, ensuring software quality.
- Machine Learning significantly advances software testing, especially as software grows more complex:
  - ❑ Exp: For predicting optimal software testing tool configurations (Parameters/Flags).

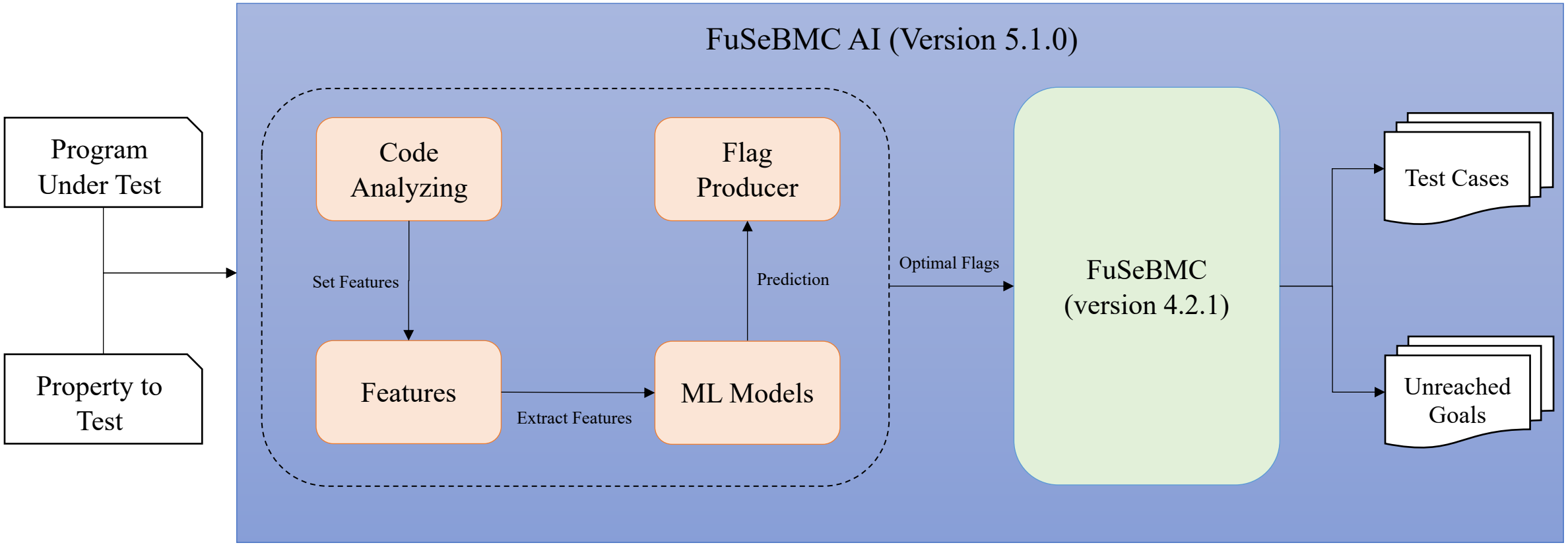
❖ However, different combinations of the (Parameters/Flags) have different overall performance.

- ❑ loop unwinding bound
- ❑ context switch bound
- ❑ partial order reduction

FuSeBMC- AI

We propose FuSeBMC-AI, a test generation tool grounded in machine learning techniques to improve the hybrid fuzzer to achieve high C programs coverage.

FuSeBMC-AI Framework



Setting Features

We analyze the Program Under Test (PUT) and extract the features that FuSeBMC-AI prioritized, which are based on determining the optimal flags and values that could be supplied to the engines of FuSeBMC-AI:

Program Features	Sub Features
For Loops	For count, For max depth, For depth avg
While Loop	While count, While max depth, While depth avg, While infinite count, While infinite with NonDetCall count
Do Loop	Do Count, Do max depth, Do depth avg, Do infinite count
If – else condition	If count, If max depth, If depth avg, nested If count, Else count, Else depth avg
Non_Det_Call	Non DetCall count, Non DetCall depth avg, has Non DetCall in loop

FuSeBMC-AI exposes a large number of flags that regulate its testing strategy, we list them with their values:

Flags	Values
Strategy	incr, kinduction
Solver	boolector, z3
Encoding	floatbv, fixedbv
KStep	[1,2,3]
ContextBound	[2,4]
Unwind	[10, -1] #-1 default
Fuzz1Enabled	[0,1]
Fuzz1Time	[25,83,188] for 250 seconds (300 - 50) 75% ,33.3% ,10%
Total run	**2*2*2*3*2*2*4 = 384** (for each program)

Training Set Labeling

We use the benchmarks in Test-Comp 2024 as follows:

- Training set comprises 11% (67 benchmarks) of coverage-error categories.
- Training set includes 4% (111 benchmarks) of coverage-branches.
- Run FuSeBMC-AI for 300s with 192 different combinations of flags for coverage-error.
- Run FuSeBMC-AI for 300s with 384 different combinations of flags for coverage-branches.

coverage-error

Parameter	Values
Strategy	incr, kinduction
Solver	boolector, z3
Encoding	floatbv, fixedbv
KStep	[1,2,3]
ContextBound	[2,4]
Fuzz1Enabled	[0,1]
Fuzz1Time	[25,83,188] for 250 seconds (300 - 50) # 10%, 33.3%, 75%
TOTAL	2*2*2*3*2*4=192

coverage-branches

Parameter	Values
Strategy	incr, kinduction
Solver	boolector, z3
Encoding	floatbv, fixedbv
KStep	[1,2,3]
ContextBound	[2,4]
Unwind	[10,-1] #-1 default
Fuzz1Enabled	[0,1]
Fuzz1Time	[25,83,188] for 250 seconds (300 - 50) # 10%, 33.3%, 75%
TOTAL	2*2*2*3*2*2*4=384

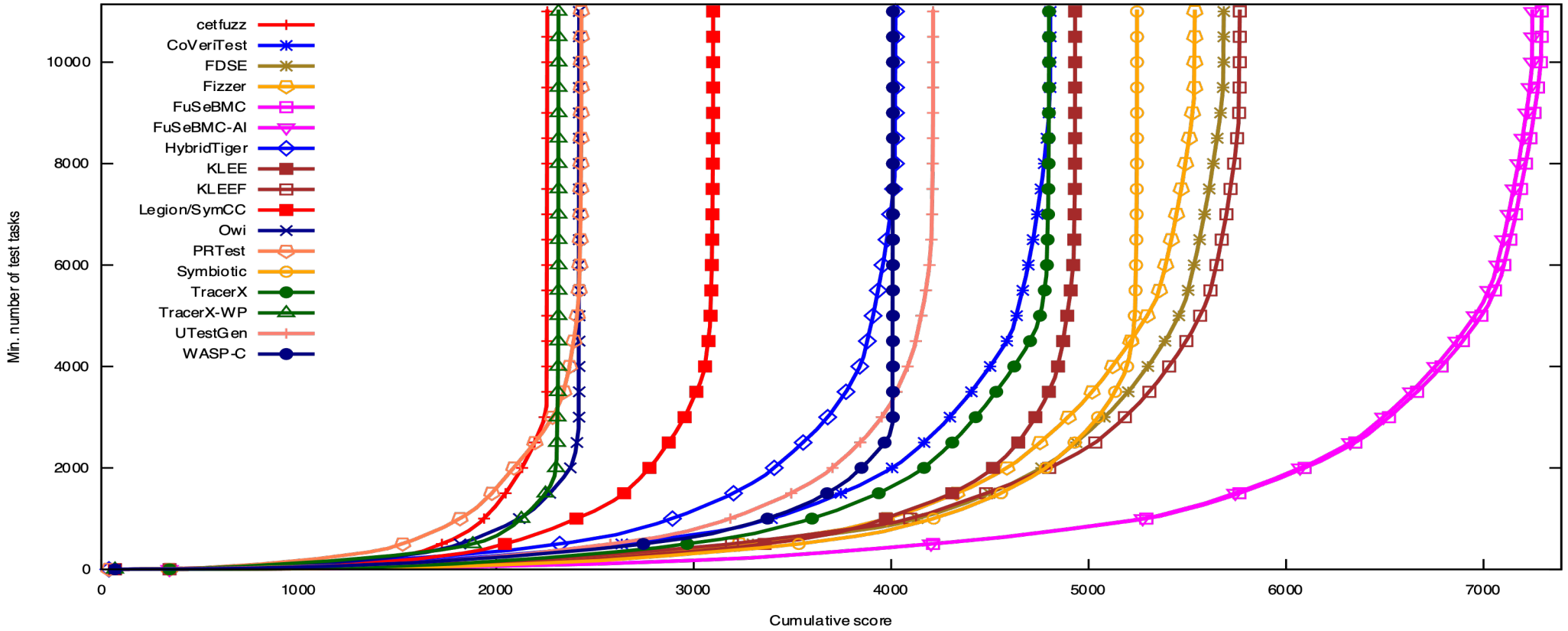
Machine Learning Models

- Machine Learning Models (DTC, SVC, and NNR) learn to predict the 0-5 output class given the features of the program and a given choice of flags.
- We try (192 cover-error & 384 cover-branches) flag combinations and pick the one that yields the lowest output class

Testing Result (Cover-Error)	Class
detect bug & IF restTimeRatio >= 0.8	0
detect bug & ELSE IF restTimeRatio >= 0.6	1
detect bug & ELSE IF restTimeRatio >= 0.4	2
detect bug & ELSE IF restTimeRatio >= 0.2	3
detect bug & ELSE IF restTimeRatio >= 0.0	4
Unknown	5

Coverage Result (Cover-Branches)	Class
score coverage >= 0.85	0
score coverage >= 0.68	1
score coverage >= 0.51	2
score coverage >= 0.34	3
score coverage >= 0.17	4
score coverage >= 0.0	5

Competition on Software Testing 2024: Results of the `Overall` Category



FuSeBMC achieved 3 awards: 2nd place in `Cover-Error`, 2nd place in `Cover-Branches`, and 2nd place in `Overall`

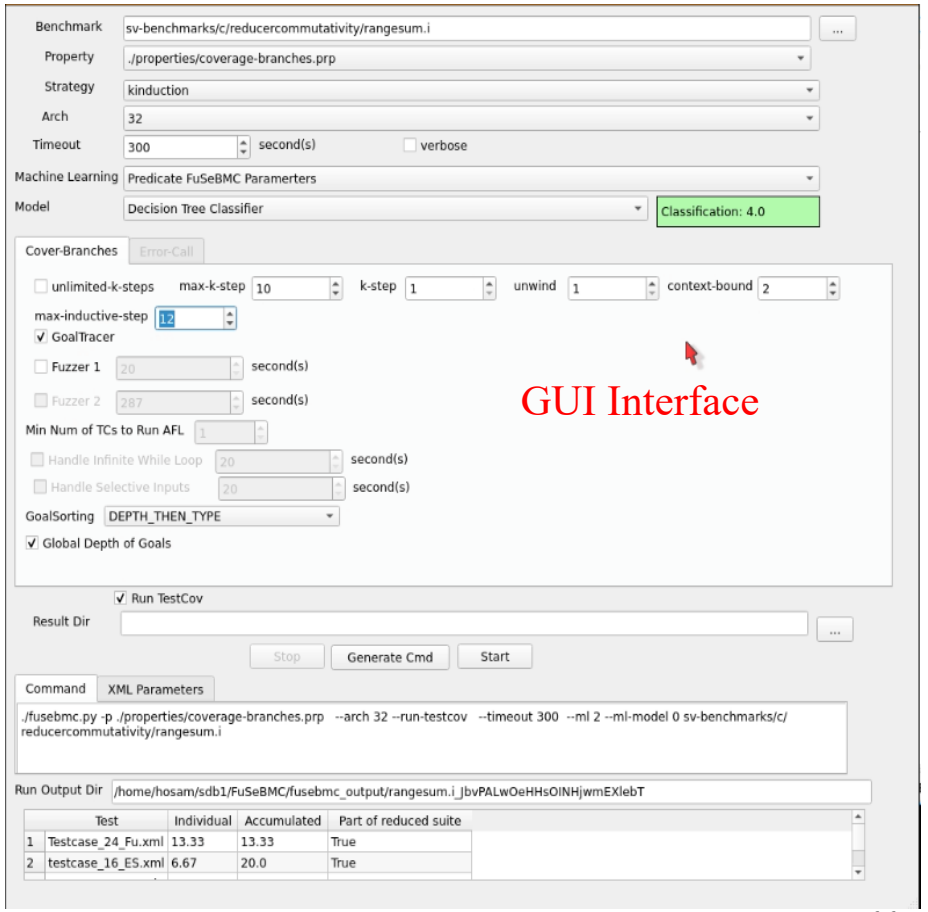
https://test-comp.sosy-lab.org/2024/

Alshmrany, K., Aldughaim, M., Chenfeng Wei., Tom Sweet., Richard Allmendinger., Cordeiro, L.: FuSeBMC AI: Acceleration of Hybrid Approach through Machine Learning - arXiv 2024

Software Project

FuSeBMC-AI is implemented using C++, and it is publicly available under the terms of the MIT License at GitHub. The repository includes the latest version of FuSeBMC AI (version 5.1.0). FuSeBMC AI dependencies and instructions for building from source code are all listed in the README.md file.

```
['-p', './properties/unreach-call.prp', '--arch', '64', '--timeout', '300', '--ml', '2', '--ml-m
BitCounterPointer.c']
finish
<outputdir>/home/hosam/sdb1/FuSeBMC/fusebmc_output/4BitCounterPointer.c_FfcEUPIyJVJznnKzkWdFMFGj
time_out_s 297

Command:
 /home/hosam/sdb1/FuSeBMC/FuSeBMC_instrument/FuSeBMC_instrument --input /home/hosam/sdb1/FuSeBMC
inter.c --output /dev/null --export-line-number-for-NonDetCalls --info-file /home/hosam/sdb1/FuS
VJznnKzkWdFMFGjO/info.xml --extract-features --compiler-args -I/home/hosam/sdb1/FuSeBMC/sv-bench
No changes can be made.
The input file will be copied to the output file.

We have: 0 Goals.
Starting NonDetVisitor ....

NonDetVisitor is Done!....
info File: /home/hosam/sdb1/FuSeBMC/fusebmc_output/4BitCounterPointer.c_FfcEUPIyJVJznnKzkWdFMFGj

FuSeBMC_instrument finished !!!

/home/hosam/.local/lib/python3.10/site-packages/sklearn/base.py:439: UserWarning: X does not hav
was fitted with feature names
  warnings.warn(

<mlparams><prop>1</prop><strategy>0</strategy><isClassification>1</isClassification><bestScoreCl
P>50</MAX_K_STEP><contextBound>2</contextBound><maxInductiveStep>3</maxInductiveStep><UNWIND>1</
lparams>
========== FEATURE BEGIN ==========
FuseBMC_forCount: 0
FuseBMC_forMaxDepth: 0
FuseBMC_forDepthAvg: 0.0
FuseBMC_whileCount: 1
FuseBMC_whileMaxDepth: 1
FuseBMC_whileDepthAvg: 1.0
FuseBMC_whileInfiniteCount: 0
FuseBMC_whileInfiniteWithNonDetCallCount: 0
FuseBMC_doCount: 0
FuseBMC_doMaxDepth: 0
FuseBMC_doDepthAvg: 0.0
FuseBMC_doInfiniteCount: 0
FuseBMC_ifCount: 3
```



GUI Interface

Want to Try it?

Find out more about FuSeBMC-AI at :
https://github.com/kaled-alshmrany/FuSeBMC/tree/FuSeBMC-AI

FuSeBMC - AI

arXiv 2024 paper: "FuSeBMC AI: Acceleration of Hybrid Approach through Machine Learning (Competition Contribution)"

kaa14ed@gmail.com