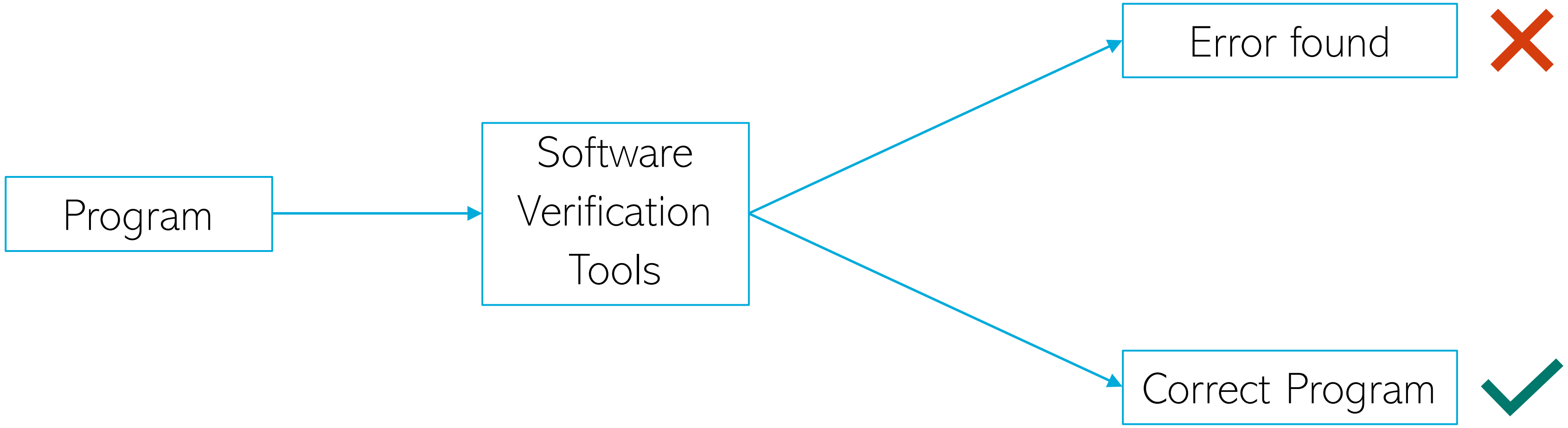
Carl von Ossietzky
Universität
Oldenburg

Online Performance Prediction of Software Verification: Heuristics vs Machine Learning

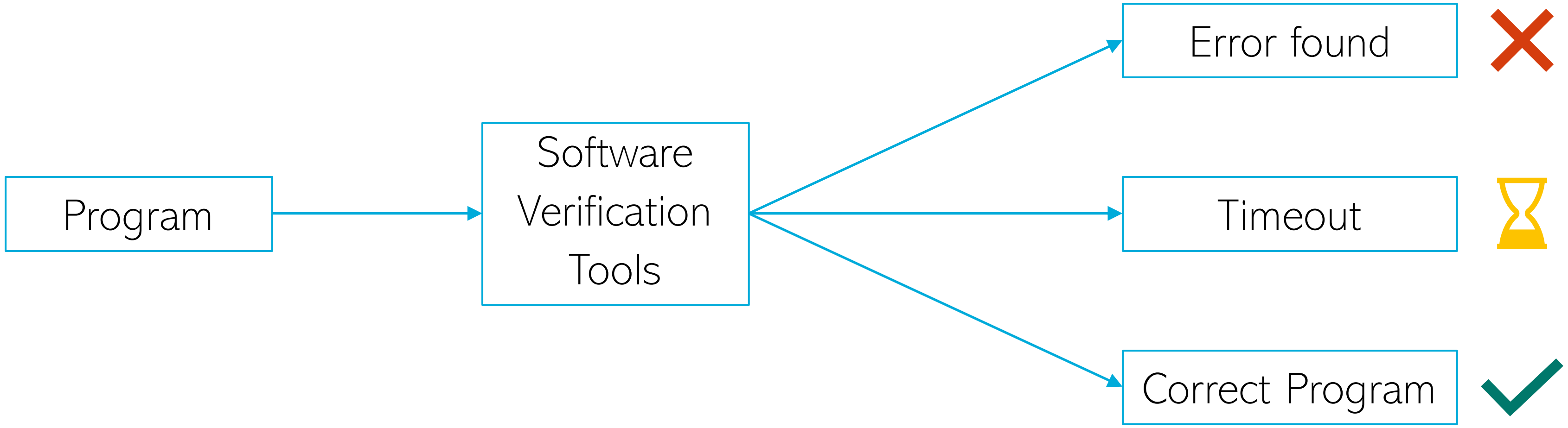
Master Thesis & Student Assistant‘s Work

Nicola Anna Thoben

Motivation

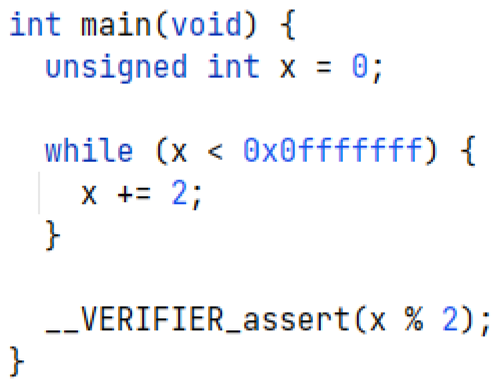

Program
Software Verification Tools
Error found
✗
Correct Program
✓

Motivation


Program
Software Verification Tools
Error found
✗
Timeout
⌛
Correct Program
✓

Example

loop-acceleration/simple_1-1.c

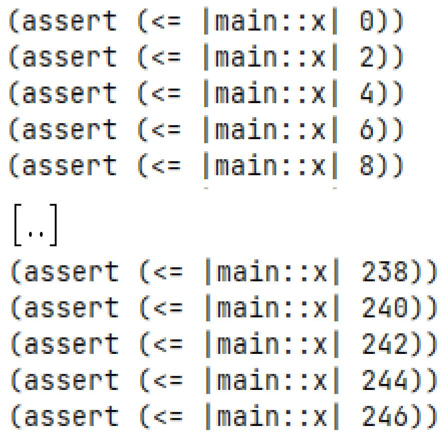


```c
int main(void) {
  unsigned int x = 0;

  while (x < 0x0fffffff) {
    x += 2;
  }

  __VERIFIER_assert(x % 2);
}
```

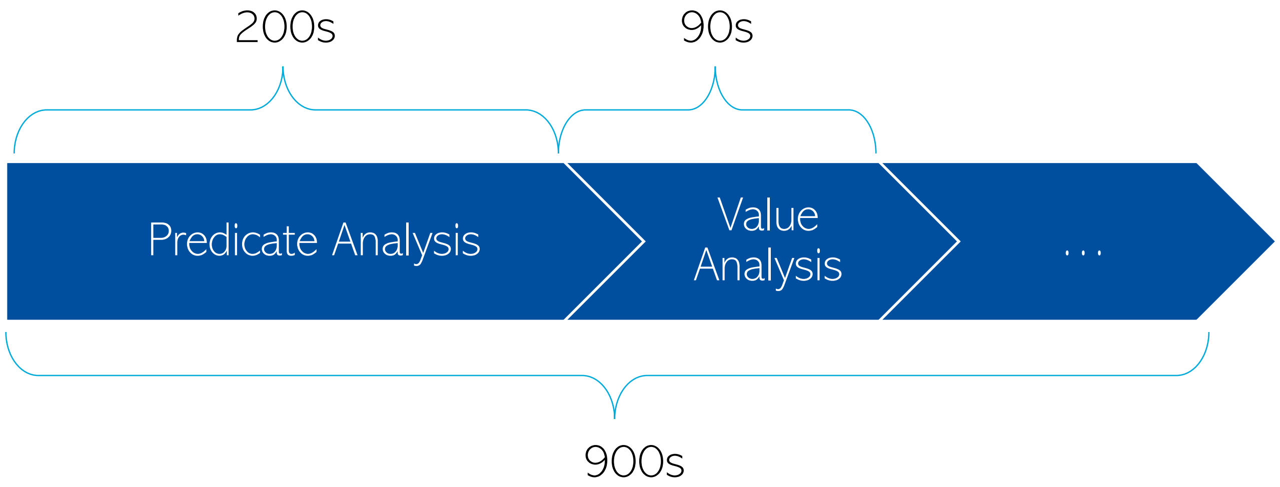
Predicates



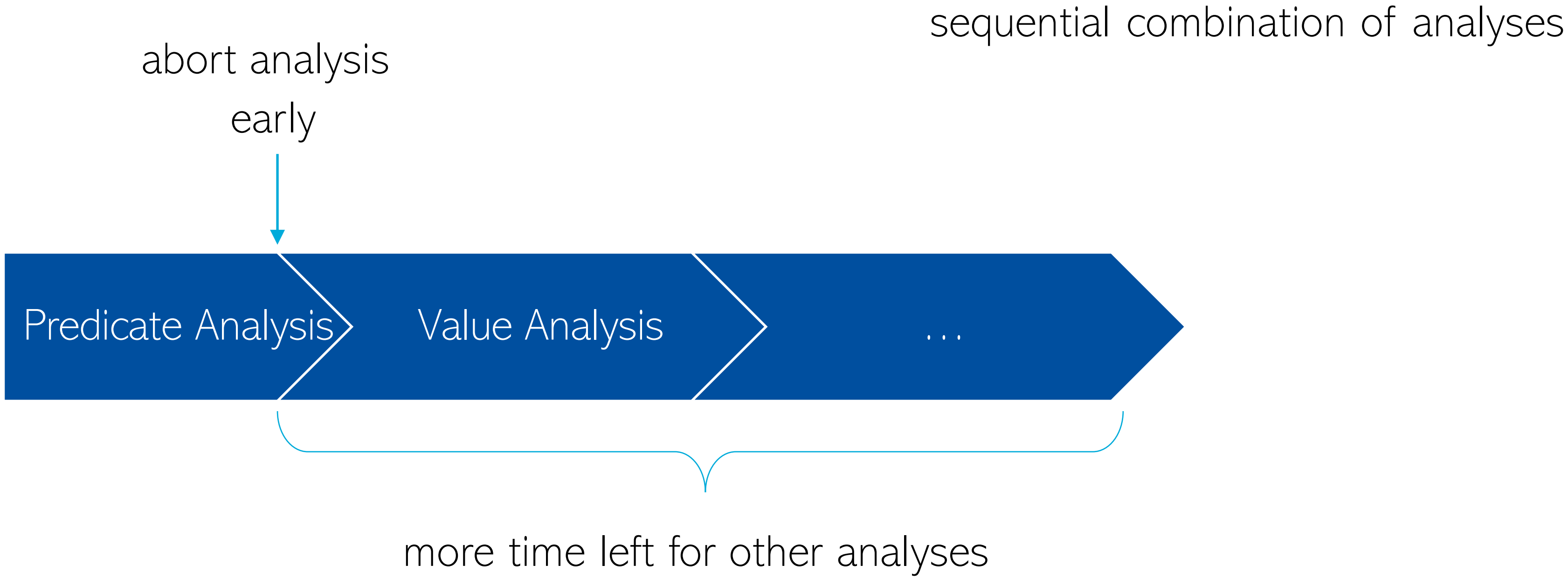
```
(assert (<= |main::x| 0))
(assert (<= |main::x| 2))
(assert (<= |main::x| 4))
(assert (<= |main::x| 6))
(assert (<= |main::x| 8))
[..]
(assert (<= |main::x| 238))
(assert (<= |main::x| 240))
(assert (<= |main::x| 242))
(assert (<= |main::x| 244))
(assert (<= |main::x| 246))
```

Motivation

sequential combination of analyses



Motivation


sequential combination of analyses
abort analysis
early
Predicate Analysis
Value Analysis
. . .
more time left for other analyses

When to abort an analysis?

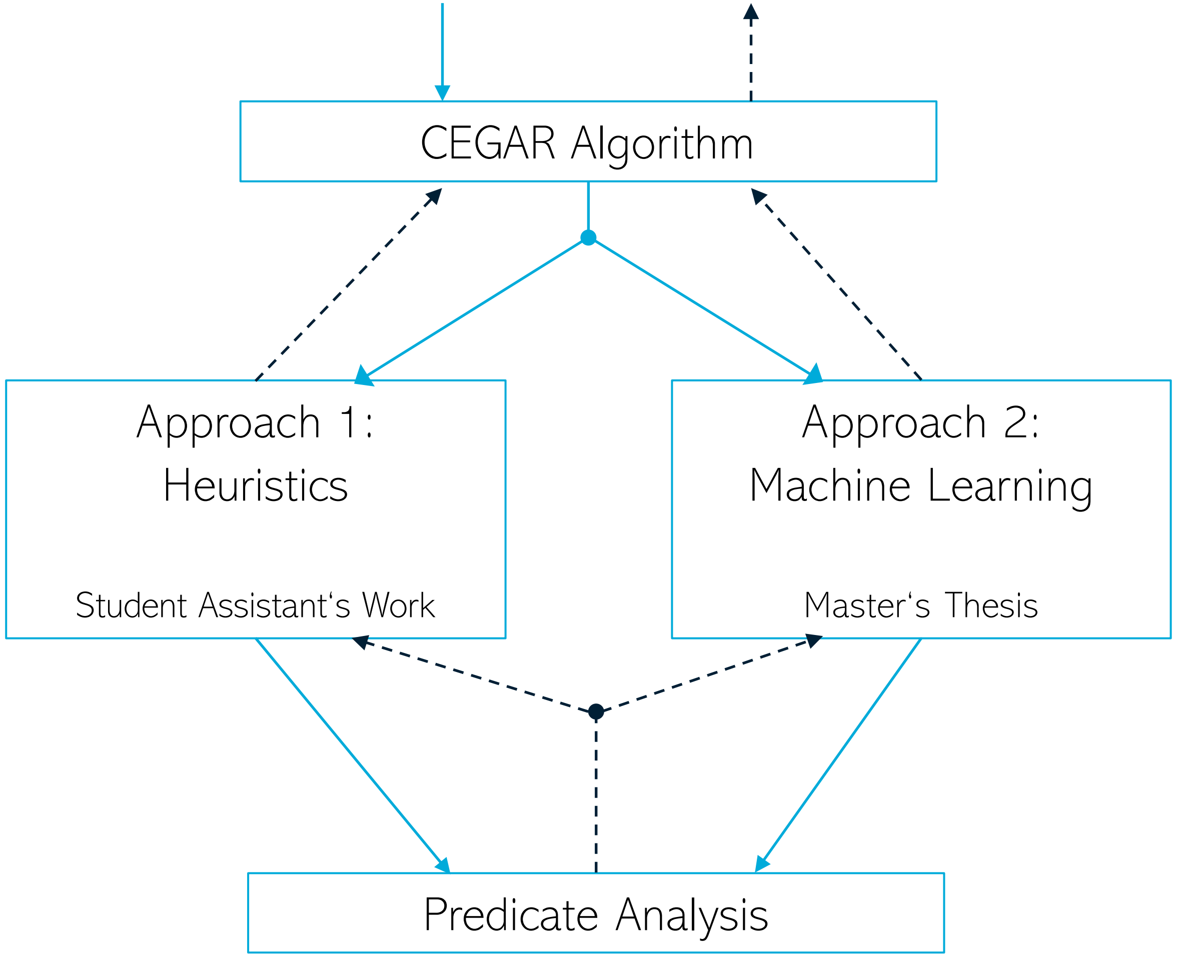
Approach 1:
Heuristics

Student Assistant‘s Work

Approach 2:
Machine Learning

Master‘s Thesis

When to abort an analysis?



CEGAR Algorithm

Approach 1:
Heuristics

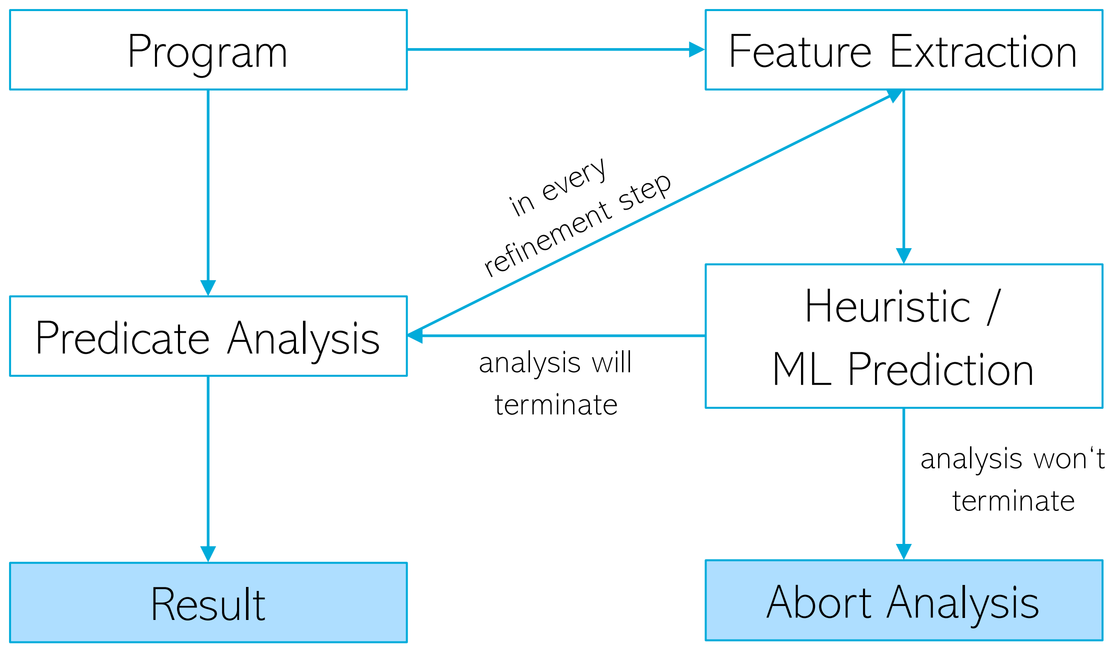
Student Assistant's Work

Approach 2:
Machine Learning

Master's Thesis

Predicate Analysis

System Design



Approach 1: Heuristics

Approach 1:
Heuristics

Student Assistant's Work

Approach 2:
Machine Learning

Master's Thesis

Carl von Ossietzky Universität Oldenburg

Approach 1: Heuristics

Heuristic 1

|ARG States| > |CFA Nodes| * factor

Heuristic 2

|ARG node a| > factor

factor = min(max loop iterations, [100, 20])

Approach 1: Results

Technique	Abort on Timeout	Abort on Success	Timeout	Success
Heuristic 1	91	44	1937	2961
Heuristic 2	469	596	1559	2409

Heuristic 1

|ARG States| > |CFA Nodes| * factor

Heuristic 2

|ARG node a| > factor

Approach 2: Machine Learning

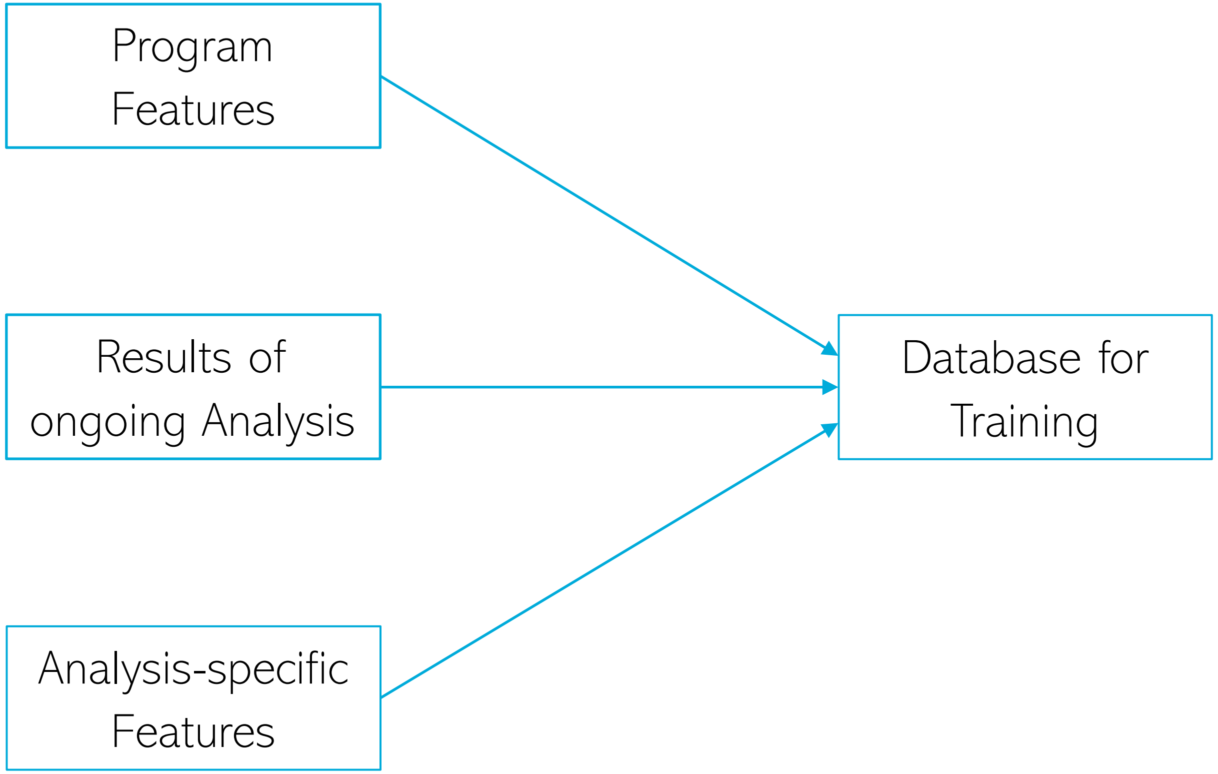
Approach 1:
Heuristics

Student Assistant's Work

Approach 2:
Machine Learning

Master's Thesis

Approach 2: Features



Approach 2: Features

Program Features

Results of ongoing Analysis

Analysis-specific Features

- Number of (nested) loops
- Number of endless loops
- Loop iterations
- Number of CFA nodes

Approach 2: Features

Program Features

Results of ongoing Analysis

Analysis-specific Features

- Refinement step
- Time in seconds
- Number of ARG states in total
- Number of new ARG states since last refinement step
- Occurrence of abstraction locations on path to ARG state
- Most frequent location in ARG

Approach 2: Features

Program Features

Results of ongoing Analysis

Analysis-specific Features

- Atoms in abstraction formula with specific operators: == / < / >
- Number of variables in abstraction formulas of states
- Highest number of boolean operations in abstraction formulas of states

Approach 2: Preprocessing

- Undersampling (Random Undersampler)
- Normalization (MinMaxScaler)
- Hyperparameter Tuning (GridSearchCV)
- Feature Selection (SelectKBest)

Approach 2: Best Result So Far

Technique	F1-Score	Precision	Recall
Random Forests	0.899	0.905	0.893

$$\text{Precision} = \frac{TP}{TP+FP}$$

$$\text{Recall} = \frac{TP}{TP+FN}$$

$$\text{F1-Score} = 2 * \frac{Precision * Recall}{Precision+Recall}$$

Approach 2: To Do

□ Other ML Techniques

□ More features (e.g. count predicates with increasing values ($x < 2$, $x < 3, \dots$))

□ Optional: Regression Model

□ Insert model into CPAChecker to predict analysis outcome

□ Online evaluation

Carl von Ossietzky Universität Oldenburg

Comparison: Heuristic and Machine Learning

Technique	Abort on Timeout	Abort on Success	Timeout	Success
ML: Random Forests	2018	239	10	2766
Heuristic 2	469	596	1559	2409