



# VeriAbs

Afzal, Asia, Avriti Chauhan, Bharti Chimdyalwar, Priyanka Darke,  
Advaita Datar, Shrawan Kumar, **Charles Babu M**, Tanha Shah, R Venkatesh

Tata Consultancy Services, **Chennai Mathematical Institute**

March 28, 2019

# Techniques in VeriAbs

- Ideas to prove properties
  - Loop Abstraction to scale Bounded Model Checking (LABMC) [DATE'15, FM'15, ICST'17, LCTES'18]
    - Abstract Acceleration + split case k induction
  - Invariants from program behavior and syntax [Prabhu et al SAS'18]
  - Shrinking and pruning for array loops [Kumar et al TACAS'18]
- Ideas to falsify properties
  - Test generation by fuzzing
  - Bounded model checking

Category	# Programs	Score (# prgs. verified)	Highest score (# prgs. verified)	VeriAbs Position
ReachSafety	3831	4638 (3173)	-	Gold
SoftwareSystems	2809	1061 (1757)	1185 (2202)	Bronze

# Invariant Synthesis using Syntax & Behaviours

```
int x = 0, y = 0;

while (*) {
    x = x + 1;
    y = y + x;
}

assert (y >= 0);
```

$x \geq 0 \ \&\& \ y \geq 0$

```
int n, sum = 0, i = 1;
assume (1 <= n <= 1000);

while (i <= n) {
    sum = sum + i;
    i = i + 1;
}

assert (2*sum = n*(n+1));
```

$2*sum = i*(i-1) \ \&\& \ (i \leq n+1)$

- Data candidates are learned from program behaviors [Prabhu et al SAS'18]
- Guess and check framework
- Highest score in ECA

# Array Pruning

```
1. #define N 100000
2.
3. void computeMin(){
4.     int i, min, a[N]
5.
6.     min = a[0]
7.
8.     for (i = 1; i < N; i++)
9.         if(min > a[i]){
10.            min = a[i]
11.        }
12.
13.    assert (
14.        forall j in [0,N)
15.            a[j] >= min
16.        exists j in [0,N)
17.            a[j] == min
18.    )
19. }
```

- Initialized with non-deterministic values (or initialized programmatically)
- Constant loop bound and increment steps
- Indices must have a constant offset from the counter
- Limited support for multiple and nested loops
- Second in arrays category
- In collaboration with IIT Bombay

Programs	Safe	Unsafe
Total	123	44
Not pruneable	85	34
Pruneable	38	10
By shrinkability [TACAS'18]	65	17
By pruning	22	01
By both	16	09

Thank you