Algorithms for Software Model Checking: Predicate Abstraction vs. IMPACT

Philipp Wendler

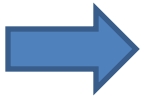
oint work with:
! irk " e#er

Software $erification

C program

```
int main() {
  int x = 10;
  int y = 3;
  int z = x+y;
  assert(z > 0);
```

Specification



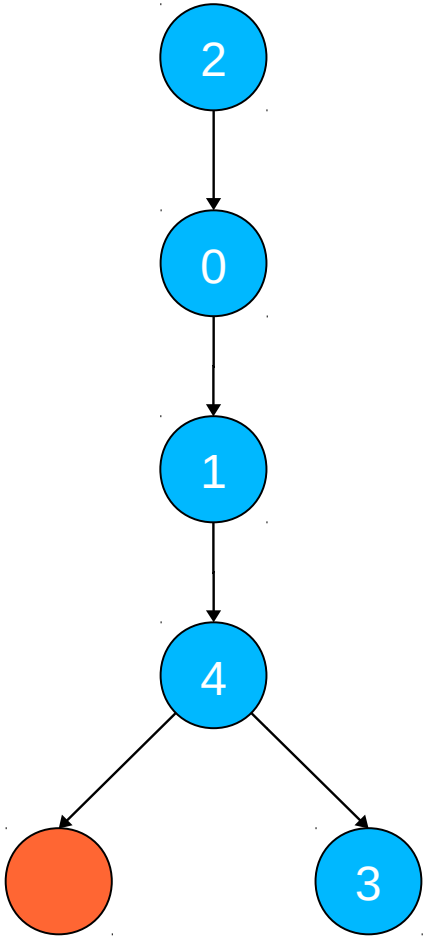
$erification Tool

i.e.% assertions cannot be violated

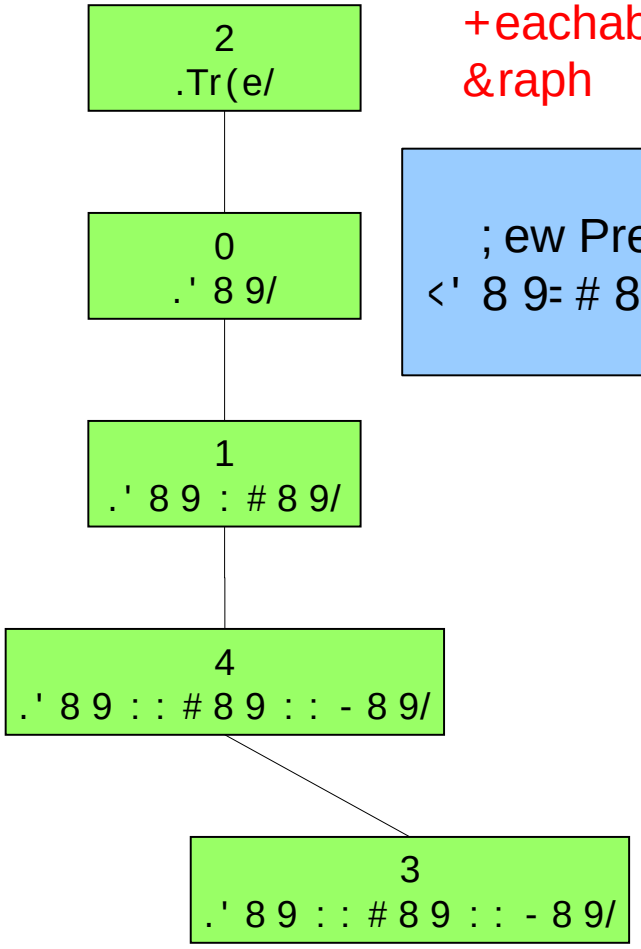
&eneral method:
Create an overappro'imation of the program states

Predicate Abstraction

Control5 6low A(tomaton



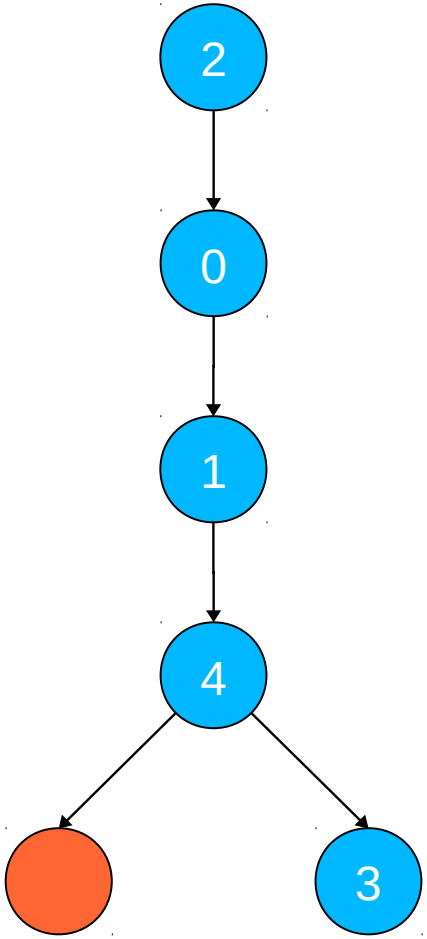
Abstract
+eachabilit#
&raph



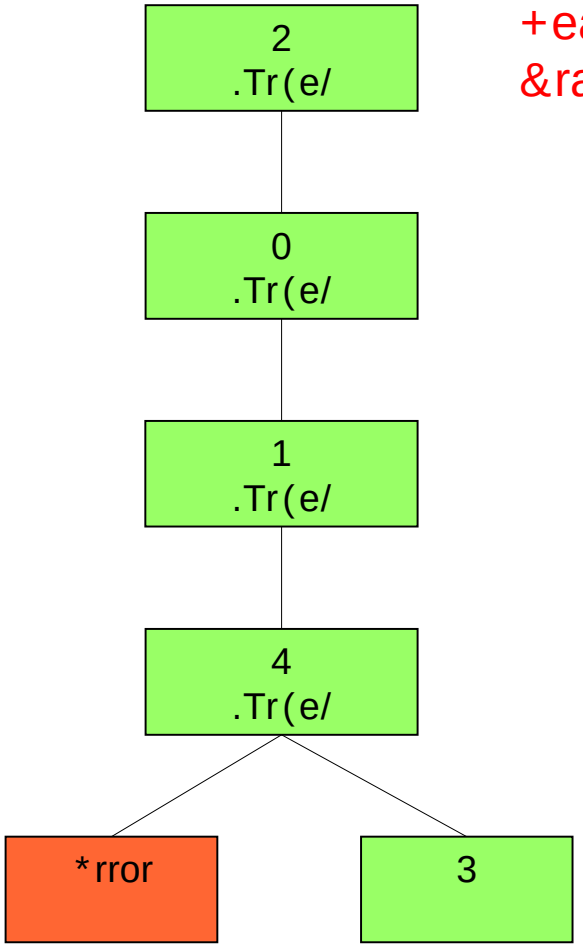
; ew Precision:
<' 8 9= # 8 9= - 8 9>

Impact

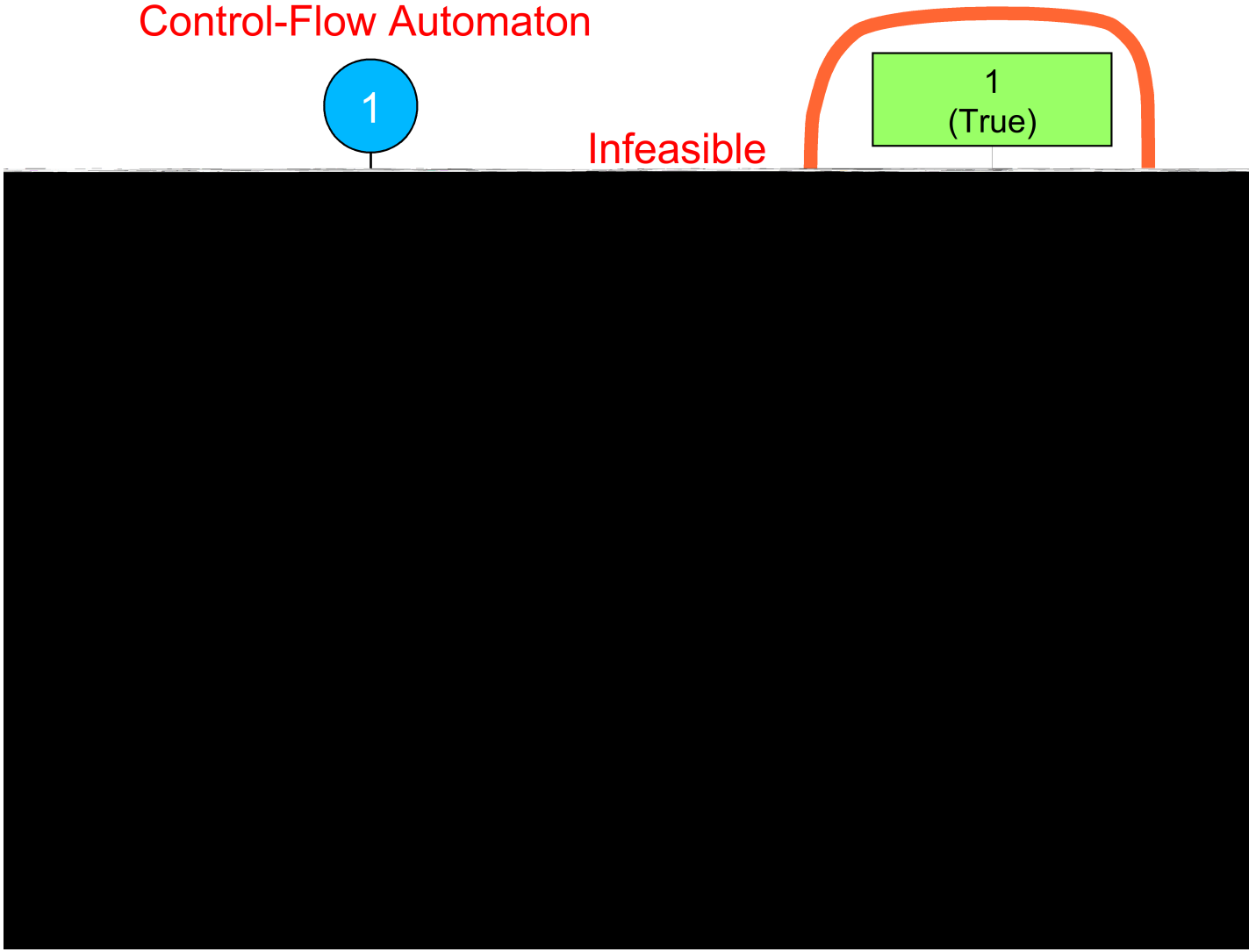
Control5 6low A(tomaton



Abstract
+eachabilit#
&raph



Impact



Comp(ted
Interpolants

Tr(e

' 8 9

' 8 9 : :
8 9

- 8 9

6alse