04.Concolic execution

Unknown macro: 'html'

List

Concolic testing

- **Concrete Execution Symbolic Execution .(Concrete + Symbolic = Concolic)**
  - Symbolic execution (Concrete value) .
    - Symbolic execution (constraint logic programming) (automated theorem prover) constraint solver .
  - .
  - Concolic SMT(Satisfiability modulo theories) Solver Z3, STP, Z3str2, Boolector, .

Example

- **Concolic execution .**
- 3 .
- x, y , .
  - y =
  - x =
- Solver .

Find path and concrete value

		Solved
• z 1000	((* 2) 1000)	: 500
• z 1000 y z	((* 2) = 1000 , (* 2))	: 500, : 1000
• z 1000 y z	((* 2) = 1000, > (* 2))	: 500, : 1000

ConcolicTest.c

```
#include <stdio.h>

void main(){
    int x,y,z;

    scanf("%d",&x);
    scanf("%d",&y);

    z = x * 2;

    if(z == 1000){
        if(y > z){
            printf("Nice!\n");
        }else{
            printf("Wrong!\n");
        }
    }
}
```

Algorithm

- **Concolic .**
    1. symbolic execution .
        a. .
    2. .
    3. Concolic .
    4. Symbolic .
    5. Solver Symbolic
        a. .

Limitations

- .
    - .
- .
    -
    -
    -
- .

Tools

- **Tool Concolic execution .**
    - Angr
    - Triton
    - Ponce
    - .

Related info

- https://en.wikipedia.org/wiki/Concolic_testing
- http://shell-storm.org/talks/SSTIC2015_English_slide_detailed_version_Triton_Concolic_Execution_FrameWork_FSaudel_JSalwan.pdf

Unknown macro: 'html'