

Lab: Z3 Theorem Prover

(Week 5)

Yulei Sui

School of Computer Science and Engineering

University of New South Wales, Australia

Quiz-2 + Lab-Exercise-2 + Assignment-2

- A set of quizzes on WebCMS (5 points)
 - Logical formula and predicate logic
 - Z3's knowledge and translation rules
- Lab-Exercise-2 (5 points)
 - **Goal:** Manually translate code into z3 formulas/constraints and verify the assertions embedded in the code.
 - **Specification:**<https://github.com/SVF-tools/Software-Security-Analysis/wiki/Lab-Exercise-2>
 - **SVF Z3 APIs:** <https://github.com/SVF-tools/Software-Security-Analysis/wiki/SVF-Z3-API>
- Assignment-2 (25 points)
 - **Goal:** automatically perform assertion-based verification for code using static symbolic execution.
 - **Specification:**<https://github.com/SVF-tools/Software-Security-Analysis/wiki/Assignment-2>

Intraprocedural Example

```
1 void main() {  
2   int *p;  
5   int q;  
7   int *r;  
9   int x;  
10  p = malloc(...);  
13  q = 5;  
15  *p = q;  
17  x = *p;  
19  assert(x == 10);  
20 }
```

Source code

```
1 expr p = getZ3Expr("p");  
2 expr q = getZ3Expr("q");  
3 expr r = getZ3Expr("r");  
4 expr x = getZ3Expr("x");  
5 printExprValues();
```

Translation code using Z3Mgr

-----Var and Value-----

nothing printed because
expressions have no value

Output on terminal

Intraprocedural Example

```
1 void main() {  
3   int *p;;  
5   int q;;  
7   int *r;;  
9   int x;;  
10  p = malloc(...);  
12  q = 5;;  
15  *p = q;  
17  x = *p;  
19  assert(x == 10);  
20 }
```

Source code

```
1 expr p = getZ3Expr("p");  
2 expr q = getZ3Expr("q");  
3 expr r = getZ3Expr("r");  
4 expr x = getZ3Expr("x");  
5 expr malloc1 = getMemObjAddress("malloc1");  
6 addToSolver(p == malloc1);  
7 printExprValues();
```

Translation code using Z3Mgr

```
-----Var and Value-----  
Var5 (malloc1)   Value: 0x7f000005  
Var1 (p)         Value: 0x7f000005  
-----
```

0x7f000005 (or 2130706437 in decimal)

represents the virtual memory
address of this object

Each SVF object starts with 0x7f + its ID.

Output on terminal

Intraprocedural Example

```
1 void main() {  
3   int *p;;  
5   int q;;  
7   int *r;;  
9   int x;;  
11  p = malloc(...);  
12  q = 5;;  
15  *p = q;;  
17  x = *p;;  
18  assert(x == 10);;  
20 }
```

Source code

```
1 expr p = getZ3Expr("p");  
2 expr q = getZ3Expr("q");  
3 expr r = getZ3Expr("r");  
4 expr x = getZ3Expr("x");  
5 expr malloc1 = getMemObjAddress("malloc1");  
6 addToSolver(p == malloc1);  
7 addToSolver(q == getZ3Expr(5));  
8 storeValue(p, q);  
9 addToSolver(x == loadValue(p));  
10 printExprValues();
```

Translation code using Z3Mgr

```
-----Var and Value-----  
Var5 (malloc1)   Value: 0x7f000005  
Var1 (p)         Value: 0x7f000005  
Var2 (q)         Value: 5  
Var4 (x)         Value: 5  
-----
```

store value of q to address 0x7f000005

load the value from 0x7f000005 to x

Output on terminal

Intraprocedural Example

```
1 void main() {  
3   int *p;;  
5   int q;;  
7   int *r;;  
9   int x;;  
11  p = malloc(...);  
13  q = 5;;  
15  *p = q;;  
17  x = *p;;  
18  assert(x == 10);  
20 }
```

Source code

```
1 expr p = getZ3Expr("p");  
2 expr q = getZ3Expr("q");  
3 expr r = getZ3Expr("r");  
4 expr x = getZ3Expr("x");  
5 expr malloc1 = getMemObjAddress("malloc1");  
6 addToSolver(p == malloc1);  
7 addToSolver(q == getZ3Expr(5));  
8 storeValue(p, q);  
9 addToSolver(x == loadValue(p));  
10 printExprValues();  
11 addToSolver(x == getZ3Expr(10));  
12 std::cout<< solver.check() << std::endl;
```

Translation code using Z3Mgr

```
-----Var and Value-----  
Var5 (malloc1)   Value: 0x7f000005  
Var1 (p)         Value: 0x7f000005  
Var2 (q)         Value: 5  
Var4 (x)         Value: 5  
unsat  
Assertion failed: (false &&  
"The assertion is unsatisfiable");  
-----
```

Contradictory Z3 constraints!

$x \equiv 5$ contradicts $x \equiv 10$

Output on terminal

Intraprocedural Example

```
1 void main() {  
3   int *p;;  
5   int q;;  
7   int *r;;  
9   int x;;  
11  p = malloc(...);  
13  q = 5;;  
15  *p = q;;  
17  x = *p;;  
18  assert(x == 10);  
20 }
```

Source code

```
1 expr p = getZ3Expr("p");  
2 expr q = getZ3Expr("q");  
3 expr r = getZ3Expr("r");  
4 expr x = getZ3Expr("x");  
5 expr malloc1 = getMemObjAddress("malloc1");  
6 addToSolver(p == malloc1);  
7 addToSolver(q == getZ3Expr(5));  
8 storeValue(p, q);  
9 addToSolver(x == loadValue(p));  
10 printExprValues();  
11 std::cout<< getEvalExpr(x == getZ3Expr(10))  
12 << std::endl;
```

Translation code using Z3Mgr

```
-----Var and Value-----  
Var5 (malloc1)   Value: 0x7f000005  
Var1 (p)         Value: 0x7f000005  
Var2 (q)         Value: 5  
Var4 (x)         Value: 5  
false
```

There is no model available (unsat)
when evaluating `x == getZ3Expr(10)`

Output on terminal

Interprocedural Example (Call and Return)

```
1 int bar(int a)(){  
3   int r = a;;  
5   return r;;  
6 }  
7 void main() {  
9   int p, q;;  
10  p = bar(2);;  
12  q = bar(3);;  
15  assert(p == 2);;  
16 }
```

Source code

```
1 expr p = getZ3Expr("p");  
2 expr q = getZ3Expr("q");  
3 solver.push();  
4 expr a = getZ3Expr("a");  
5 addToSolver(a == getZ3Expr(2));  
6 solver.check();  
7 expr r = getEvalExpr(a);  
8 printExprValues();  
9 solver.pop();  
10 addToSolver(p == r);
```

Handle first callsite p=bar(2)

Translation code using Z3Mgr

```
-----Var and Value-----  
Var2 (a)           Value: 2  
-----
```

- (1) push the z3 constraints when calling bar and pop when returning from bar
- (2) Expression r is the return value evaluated from a after returning from callee bar

Output on terminal

Interprocedural Example (Call and Return)

```
1 int bar(int a)(){  
3   int r = a;;  
5   return r;;  
6 }  
7 void main() {  
9   int p, q;;  
10  p = bar(2);;  
12  q = bar(3);;  
15  assert(p == 2);;  
16 }
```

Source code

```
1 expr p = getZ3Expr("p");  
2 expr q = getZ3Expr("q");  
3 solver.push();  
4 expr a = getZ3Expr("a");  
5 addToSolver(a == getZ3Expr(2));  
6 solver.check();  
7 expr r = getEvalExpr(a);  
8 solver.pop();  
9 addToSolver(p == r);  
10 printExprValues();
```

Handle first callsite p=bar(2)

Translation code using Z3Mgr

```
-----Var and Value-----  
Var1 (p)           Value: 2  
-----
```

Now we only have p's value and
a is not in the current stack since
constraint a == getZ3Expr(2)
has been popped

Output on terminal

Interprocedural Example (Call and Return)

```
1 int bar(int a)(){  
3   int r = a;  
5   return r;;  
6 }  
7 void main() {  
9   int p, q;  
11  p = bar(2);;  
12  q = bar(3);;  
15  assert(p == 2);;  
16 }
```

```
1 expr p = getZ3Expr("p");  
2 expr q = getZ3Expr("q");  
3 solver.push();  
4 expr a = getZ3Expr("a");  
5 addToSolver(a == getZ3Expr(2));  
6 expr r = getEvalExpr(a);  
7 solver.pop();  
8 addToSolver(p == r);  
9 solver.push();  
10 addToSolver(a == getZ3Expr(3));  
11 r = getEvalExpr(a);  
12 solver.pop();  
13 addToSolver(q == r);  
14 printExprValues();
```

Handle second callsite q=bar(3)

```
-----Var and Value-----  
Var1 (p)      Value: 2  
Var2 (q)      Value: 3  
-----
```

We have two expressions and their values
in main's scope

Source code

Translation code using Z3Mgr

Output on terminal

Bad Interprocedural Example Without push/pop

```
1 int bar(int a)(){  
3   int r = a;;  
5   return r;;  
6 }  
7 void main() {  
9   int p, q;;  
11  p = bar(2);;  
13  q = bar(3);;  
15  assert(p == 2);;  
16 }
```

Source code

```
1 expr p = getZ3Expr("p");  
2 expr q = getZ3Expr("q");  
3 expr a = getZ3Expr("a");  
4 addToSolver(a == getZ3Expr(2));  
5 expr r = getEvalExpr(a);  
6 addToSolver(p == r);  
7 addToSolver(a == getZ3Expr(3));  
8 r = getEvalExpr(a);  
9 addToSolver(q == r);  
10 printExprValues();
```

Translation code using Z3Mgr

```
-----Var and Value-----  
Assertion failed: (res!=z3::unsat &&  
"unsatisfied constraints! Check your  
contradictory constraints added to  
the solver")  
-----
```

both `a == getZ3Expr(2)` and
`a == getZ3Expr(3)` are added
into the solver in the same scope

Output on terminal

Bad Interprocedural Example Without Evaluating Return

```
1 int bar(int a)(){  
3   int r = a;;  
5   return r;;  
6 }  
7 void main() {  
9   int p, q;;  
11  p = bar(2);;  
13  q = bar(3);;  
15  assert(p == 2);;  
16 }
```

```
1  expr p = getZ3Expr("p");  
2  expr q = getZ3Expr("q");  
3  expr r = getZ3Expr("r");  
4  expr a = getZ3Expr("a");  
5  solver.push();  
6  addToSolver(a == getZ3Expr(2));  
7  addToSolver(r == a); // invalid after pop  
8  solver.pop();  
9  addToSolver(p == r);  
10 printExprValues();  
11 solver.push();  
12 addToSolver(a == getZ3Expr(3));  
13 addToSolver(r == a); // invalid after pop  
14 solver.pop();  
15 addToSolver(q == r);  
16 printExprValues();
```

```
-----Var and Value-----  
Var1 (p)      Value: random  
Var2 (q)      Value: random  
Var3 (r)      Value: random  
-----
```

the values of p,q,r are
the same random number

Source code

Translation code using Z3Mgr

Output on terminal

Array and Struct Example

```
1 void main() {  
3   int * a;;  
5   int * x;;  
7   int y;;  
9   a = malloc(...);;  
11  x = &a[2];;  
13  *x = 3;;  
15  y = *x;;  
17  assert(y == 3);  
18 }
```

Source code

```
1 expr a = getZ3Expr("a");  
2 expr x = getZ3Expr("x");  
3 expr y = getZ3Expr("y");  
4 addToSolver(a == getMemObjAddress("malloc"));  
5 addToSolver(x == getGepObjAddress(a,2));  
6 storeValue(x, getZ3Expr(3));  
7 addToSolver(y == loadValue(x));  
8 printExprValues();
```

Translation code using Z3Mgr

```
-----Var and Value-----  
Var1 (a)           Value: 0x7f000004  
Var4 (malloc)      Value: 0x7f000004  
Var2 (x)           Value: 0x7f000003  
Var3 (y)           Value: 0x7f000003  
-----
```

getGepObjAddress returns the field
address of the aggregate object *a*
The virtual address also in the form of
0x7f... + VarID

Output on terminal

Array and Struct Example

```
1 void main() {  
3   int * a;;  
5   int * x;;  
7   int y;  
9   a = malloc(...);;  
11  x = &a[2];;  
13  *x = 3;;  
15  y = *x;;  
17  assert(y == 3);  
18 }
```

Source code

```
1 expr a = getZ3Expr("a");  
2 expr x = getZ3Expr("x");  
3 expr y = getZ3Expr("y");  
4 addToSolver(a == getMemObjAddress("malloc"));  
5 addToSolver(x == getGepObjAddress(a,2));  
6 storeValue(x, getZ3Expr(3));  
7 addToSolver(y == loadValue(x));  
8 printExprValues();  
9 std::cout<< getEvalExpr(y)<<std::endl;
```

Translation code using Z3Mgr

```
-----Var and Value-----  
Var1 (a)           Value: 0x7f000004  
Var4 (malloc)      Value: 0x7f000004  
Var2 (x)           Value: 0x7f000003  
Var3 (y)           Value: 0x7f000003  
-----  
3
```

getEvalExpr retrieve the value
from the expression

Output on terminal

Branch Example

```
1 main(int argv)
{
3   int y = 2;;
5   if(argv > 2)
7       y = argv;;
9   assert(y >= 2);;
10 }

1 expr argv = getZ3Expr("argv");
2 expr y = getZ3Expr("y");
3 addToSolver(y == getZ3Expr(2));
4 bool cond=(getEvalExpr(argv>getZ3Expr(2))).is_true();
5 if(cond){ // add branch condition into solver
6     addToSolver(argv > getZ3Expr(2));
7     addToSolver(y == argv);
8 }else{ // add negation of branch condition into solver
9     addToSolver(argv <= getZ3Expr(2));
10 }
11 printExprValues();
12 std::cout<<getEvalExpr(y >= getZ3Expr(2))<<"\n";
```

```
-----Var and Value-----
Var1 (argv)      Value: 0
Var2 (y)         Value: 2
-----
true
```

Source code

Translation code using Z3Mgr

Output on terminal