Valigator Examples

Thibaud Hottelier

June 20, 2008

1 Simple Coutner

Program code:

```
assume(x < 10);
while(x < 10) {
    x = x + 1
};
x = x + 1;
assert(x = 11)
```

Valigator output when invoked with "valigator –cvc3 examples/counter":

```
Starting analysis...
Info: Program is linear
Info: 3 proof obligation(s) generated
Running CVC3 for proving...

**************************************************************************
*           Result: YES    (All proof obligations proved!)           *
**************************************************************************
```

The invariant infered by Aligator is

$$(x0 < 10 \Rightarrow x \leq 10) \wedge (x0 \geq 10 \Rightarrow x = x0)$$

2 Adder

Program code:

```
assume(b >= 0);
result = a;
counter = b;
while(counter > 0) {
    counter = counter - 1;
    result = result + 1
};
assert(result = a + b)
```

Valigator output when invoked with "valigator –cvc3 examples/adder":

```
Starting analysis...
Info: Program is linear
Info: 3 proof obligation(s) generated
Running CVC3 for proving...

**************************************************************************
*           Result: YES    (All proof obligations proved!)           *
**************************************************************************
```

The invariant infered by Aligator is

$$counter + result = a + b \wedge (b \leq 0 \Rightarrow counter = b \wedge result = a) \wedge (b > 0 \Rightarrow counter \geq 0)$$

3 Cousot 77

Program code:

```
x = a;
y = b;
while((x > y) | (y > x)) {
    x = x + 1;
    y = y - 1
};
assert(x = y & 2*x = a + b)
```

Valigator output when invoked with "valigator –cvc3 examples/cousot77":

```
Starting analysis...
Info: Program is linear
Info: 3 proof obligation(s) generated
Running CVC3 for proving...

**************************************************************************
*           Result: YES    (All proof obligations proved!)           *
**************************************************************************
```

The invariant infered by Aligator is

$$x + y = a + b \wedge (((a < b \vee a > b \vee (a = x \wedge b = y)) \wedge (x < y \vee x > y \vee \\ (a + b = 2 * x \wedge a + b = 2 * y))) \vee (a = b \wedge a = x \wedge b = y))$$

4 Fibonacci Even

Program code:

```
assume(cnt > 0);
f0 = 0;
f1 = 1;
while(cnt > 0) {
    tmp = f1;
    f1 = f1 + f0;
    f0 = tmp;
```

```
    cnt = cnt - 1
};
assert(!(f0%2 = 0 & f1%2 = 0))
```

Valigator output when invoked with "valigator examples/fiboEven":

```
Starting analysis...
Info: Program is linear
Info: 3 proof obligation(s) generated
Running STP for proving...

********************************************************************
*           Result: YES    (All proof obligations proved!)         *
********************************************************************
```

The invariant infered by Aligator is

$$f0^4 + 2 * f0^3 * f1 + f1^4 = 1 + f0^2 * f1^2 + 2 * f0 * f1^3 \wedge (cnt0 > 0 \Rightarrow cnt \geq 0)$$
$$\wedge (cnt0 \leq 0 \Rightarrow f1 = 1 \wedge f0 = 0 \wedge tmp = tmp0 \wedge cnt = cnt0)$$

5 Commuting branches

Program code:

```
x = 0;
c = 0;
a = 0;
while(x < 10) {
    if (x % 2 = 0) {
        c = c + x
    } else {
        a = a + x
   };
    x = x + 1
};
assume(a >= 0 & a <= 63 & c >= 0 & c <= 63);
assert(a + c = 45)
```

Valigator output when invoked with "valigator examples/commutable":

```
Starting analysis...
Info: Program is linear
Info: 3 proof obligation(s) generated
Running STP for proving...

********************************************************************
*           Result: YES    (All proof obligations proved!)         *
********************************************************************
```

The invariant infered by Aligator is

$$2 * a + 2 * c + x = x^2 \wedge x \leq 10$$

6 10^{th} Fibonacci number

Program code:

```
cnt = 10;
f0 = 0;
f1 = 1;
while(cnt > 0) {
    tmp = f1;
    f1 = f1 + f0;
    f0 = tmp;
    cnt = cnt - 1
};
assert(f1 = 89)
```

Valigator output when invoked with "valigator examples/fibo10":

```
Starting analysis...
Info: Program is linear
Info: 3 proof obligation(s) generated
Running STP for proving...

**************************************************************************
*           Result: NO    (One or more assertion disproved)          *
**************************************************************************
```

The invariant infered by Aligator is

$$f0^4 + 2 * f0^3 * f1 + f1^4 = 1 + f0^2 * f1^2 + 2 * f0 * f1^3 \wedge cnt \geq 0$$

This example fails because the invariant is not strong enough. It does not relate in any way cnt and $f1$ or $f0$. The invariant we would need to infer in order to prove this example is the closed formula of the Fibonacci numbers, which involves exponentials and is therefore completely out of reach.

7 Unsound Invariant

Program code:

```
assume(a >= 0);
x = a;
cnt = 1;
while(cnt > 0) {
    cnt = cnt - 1;
    x = (2*(x/2)) + 1
};
assert(x = a + 2)
```

Valigator output when invoked with "valigator examples/btest":

```
Starting analysis...
Info: Program is linear
```

```
Info: 3 proof obligation(s) generated
Running STP for proving...

*************************************************************************
*     Result: UNKNOWN    (Aligator generated an invalid invariant)   *
*************************************************************************
```

The incorrect invariant infered by Aligator is

$$cnt + x = 1 + a \wedge cnt \geq 0$$