raSAT - report

February 7, 2015

1 Old status

In the experiments, we allow 2^{10} test cases, only one variable is decomposed. Two experiments:

1.1 No sbox

We continue decompose intervals even when their length is very small.

Result(see "1.1.xls" file): 50 problems in Zankl, round-off error is more likely to exist.

1.2 SAT directed, sbox=0.1

After one interval is decomposed, we use IA to evaluate the two new intervals. We choose the interval which makes the TEST-UNSAT API have a longer SAT.

Result ("1.2.xls" file): 42 problems in Zankl.

2 Current status

2.1 Unbalanced decomposition using sensitivity

Example: Suppose we have the constraint:

$f = -x_{15} * x_8 + x_{15} * x_2 - x_{10} * x_{16} > 0$.

With $x_2 \in [9.9, 10], x_8 \in [0, 0.1], x_{10} \in [0, 0.1], x_{15} \in [0, 10], x_{16} \in [0, 10]$, the result of AF2 for f is: $0.25\epsilon_2 - 0.25\epsilon_8 - 0.25\epsilon_{10} + 49.5\epsilon_{15} - 0.25\epsilon_{16} +$

$0.75\epsilon_{+-} + 49.25$. The estimated bound for f is thus $[-2, 100.5]$. We will chose $x_{15} \in [0, 10]$ for decomposition based on sensitivity. In addition, the coefficient of ϵ_{15} is positive (49.5), we can conclude that if ϵ_{15} increase, the value of f will likely increase. Because $x_{15} = 5 + 5\epsilon_{15}$, ϵ_{15} increases when x_{15} increases. As the consequence, if x_{15} increases, f will likely increases. Besides, because the constraint is $f > 0$, we expect the intervals that make the value of f as high as possible. So we will decompose $x_{15} \in [0, 10]$ into $x_{15} \in [0, 9.9] \vee x_{15} \in [9.9, 10]$, for example; and we will force $x_{15} \in [9.9, 10]$ to be selected next by MiniSAT. That means the next considered intervals are $x_2 \in [9.9, 10], x_8 \in [0, 0.1], x_{10} \in [0, 0.1], x_{15} \in [9.9, 10], x_{16} \in [0, 10]$. The estimated bounds for f is $[96.01, 100.5]$.

This is a comparison between the proposed unbalanced decomposition and balanced decomposition. Suppose the constraints is still the same $f = -x_{15} * x_8 + x_{15} * x_2 - x_{10} * x_{16} > 0$. The intervals for variables are all $[0, 10]$, that means $x_2 \in [0, 10], x_8 \in [0, 10], x_{10} \in [0, 10], x_{15} \in [0, 10], x_{16} \in [0, 10]$. We will compare methods in terms of the number of steps they need to find IA-VALID intervals of $f > 0$.

Step	Balanced Decomposition	Unbalanced Decompostion
1	[-200, 150]	[-200, 150]
2	[-175, 150]	[-150.5, 150]
3	[-125, 125]	[-51.5, 100.5]
4	[-100, 125]	[-2. 100.5]
5	[-75, 125]	[96.01 100.5] - IA-VALID
6	[-56.25, 125]	
7	[-37.5, 125]	
8	[-18.75, 125]	
9	[6.25, 112.5] - IA-VALID	

2.2 Test cases based on Sensitivity

The signs of the coefficients of noise errors can also guide the testing phase. Let's consider the above example. The constraint is $f = -x_{15} * x_8 + x_{15} * x_2 - x_{10} * x_{16} > 0$. With $x_2 \in [9.9, 10], x_8 \in [0, 0.1], x_{10} \in [0, 0.1], x_{15} \in [0, 10], x_{16} \in [0, 10]$, the result of AF2 for f is: $0.25\epsilon_2 - 0.25\epsilon_8 - 0.25\epsilon_{10} + 49.5\epsilon_{15} - 0.25\epsilon_{16} + 0.75\epsilon_{+-} + 49.25$. The coefficient of ϵ_2 is positive (0.25), then we expect the test case of x_2 is as high as possible in order to satisfy $f > 0$. We will thus take the upper bound value of x_2, i.e. 10. Similarly, we take the test cases for other variables: $x_8 = 0, x_{10} = 0, x_{15} = 10, x_{16} = 0$. With these test cases, we will have $f = 100 > 0$.

2.3 Experiments

In the experiments, we set $sbox = 0.1$. Unbalanced decomposition uses sbox, for example $x_{15} \in [0, 10]$ into $x_{15} \in [0, 10 - sbox] \vee x_{15} \in [10 - sbox, 10]$. Time out is 500s. There are 4 experiments which are different in the way of generating test cases. All the experiments use the unbalanced decomposition as described in 2.1.

2.3.1 All test cases are random

The number of test cases is 2^{10}. All the value of variables are randomly generated. Result ("2.3.1.xls" file): 44 problems solved

2.3.2 1 test case based on sensitivity

The number of test cases is only 1. Each variable is assigned one value based on its sensitivity (section 2.2). Result ("2.3.2.xls" file): 48 problems solved.

2.3.3 At least each variable has one random value

The number of test cases is 2^{10}.

1. First 10 variables: Each variable will have:
   - 1 random value, and
   - another value based on sensitivity (section 2.2).
2. Other variables: Each variable has one random value as test case.

Result ("2.3.3.xls" file): 47 problems solved.

2.3.4 First 10 variables has one random value

The number of test cases is 2^{10}.

1. First 10 variables: Each variable will have:
   - 1 random value, and

- another value based on sensitivity (section 2.2).

2. Other variables: Each variable has one value based on sensitivity (section 2.2).

Result ("2.3.4.xls" file): 53 problems solved.