Predicate Generation for Learning-Based Quantifier-Free Loop Invariant Inference†

Yungbum Jung,[1] Wonchan Lee,[1] Bow-Yaw Wang,[2] and Kwangkeun Yi[1]

[1] Seoul National University [2] Academia Sinica and Inria

1. Problem : Generate ***enough*** predicates for invariants $\{\delta\}$ `while` ρ `do` S `end` $\{\epsilon\}$

Invariants must satisfy the following conditions:

(A) $\delta \Rightarrow I$ (B) $I \wedge \rho \Rightarrow Pre(I, S)$ (C) $I \wedge \neg\rho \Rightarrow \epsilon$

precondition δ

$n \geq 0 \wedge x = n \wedge y = n$

loop guard ρ

```
while x > 0 do
  { x := x - 1;
    y := y - 1;
end
```

postcondition ϵ

$x + y = 0$

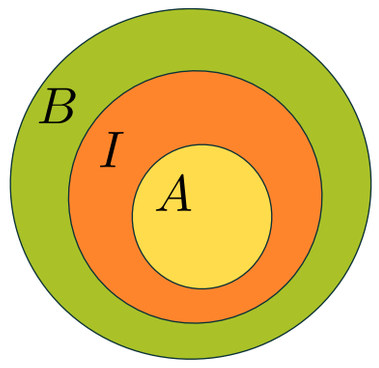
Atomic predicates from annotated loop:

$n \geq 0, x = n, y = n,$
$x > 0, x + y = 0$

Invariant : $x \geq 0 \wedge x = y$

2. Idea : Use Craig's interpolation theorem

We can always find an interpolation I from $A \Rightarrow B$:



(A) $A \Rightarrow I$

(B) $I \Rightarrow B$

(C) $Var(I) \subset Var(A) \cup Var(B)$

Generating new predicates:

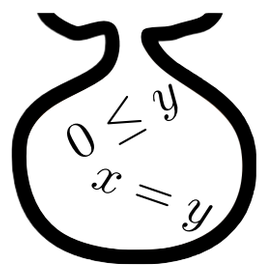
$n \geq 0 \wedge x = n \wedge y = n$

$\Downarrow$

Interpolant $x = y \wedge 0 \leq y$ → New predicates

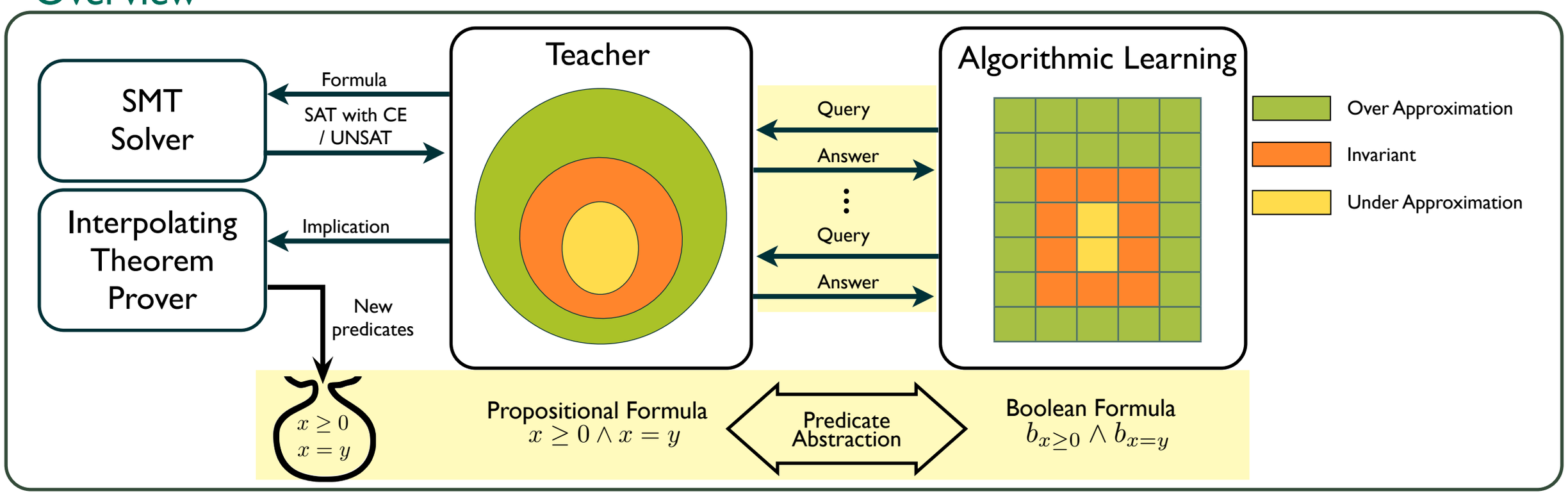
$\Downarrow$

$x > 0 \vee x + y = 0$



3. Solution: Implementing a Teacher both to Answer Queries and Generate Predicates

Overview



From incorrect conjectures

Equivalence query asks whether a conjecture θ is equivalent to an invariant

1. Interpolating over-approximation

$\theta \wedge \rho \Rightarrow Pre(\bar{I}, S)$

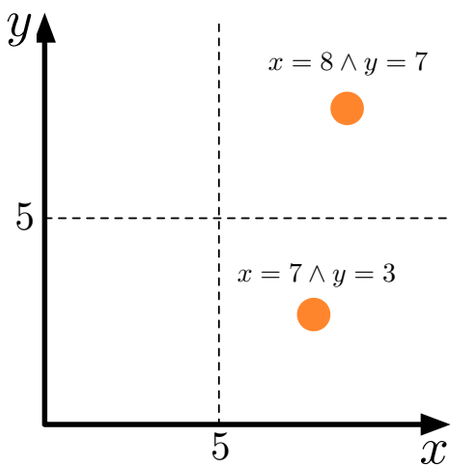
2. Interpolating under-approximation

$\underline{I} \wedge \rho \Rightarrow Pre(\theta, S)$

} monotonicity of $Pre(\cdot, S)$

From conflicting abstract counterexamples

Two distinct valuation can have the same abstract valuation because of the coarse abstraction



$I = x \geq 5 \wedge y \geq 5$

$(x = 7 \wedge y = 3) \Rightarrow \neg(x = 8 \wedge y = 7)$

$y \geq 3$

$x \geq 5$

4. Experimental Result

case	SIZE	PREVIOUS (VMCAI'10)					CURRENT					BLAST	
		P	MEM	EQ	RE	T	P	MEM	EQ	RE	T	P	T
ide-ide-tape	16	6	13	7	1	0.05	4	6	5	1	0.05	21	2.38
ide-wait-ireason	9	5	790	445	33	1.51	5	122	91	7	1.09	9	0.33
parser	37	17	4,223	616	13	13.45	9	86	32	1	0.46	8	1.23
riva	82	20	59	11	2	0.51	7	14	5	1	0.37	12	2.67
tar	7	6	∞	∞	∞	∞	2	2	5	1	0.02	10	0.37
usb-message	18	10	21	7	1	0.10	3	7	6	1	0.04	4	0.32
vpr	8	5	16	9	2	0.05	1	1	3	1	0.01	4	0.23

5. Conclusion

* Novel approach to invariants generation.
* Fully automated with new predicate generation technique.
* We are currently working on its extension supporting quantified invariants.

ROSAEC center
Research On Software Analysis for Error-free Computing
소프트웨어 무결점 연구센터 NRF ERC

Programming Research Laboratory
http://ropas.snu.ac.kr

† This work is to be presented at TACAS'11

SEOUL NATIONAL UNIVERSITY
INRIA