Instantiation for Theory Reasoning in Vampire

Giles Reger Martin Riener

Theory Reasoning in saturation provers

Previous approaches to reasoning with theories (such as integer or real arithmetic) in saturation-based theorem provers include:

- Adding axioms (e.g. $x + y = y + x$)
- Evaluating ground expressions
- Using an SMT solver to decide ground sub-problems

Only axioms deal with *quantifiers* but they are explosive in proof search and in many cases are only useful when used to generate consequences of the theory in an undirected way.

Where instantiation helps

Theory axiom reasoning does not find useful instances of clauses which can be very useful. For example, if we can guess the instance $x = 7$ for the clause

$$14x \neq x^2 + 49 \vee p(x)$$

we obtain the simpler instance

$$p(7)$$

The literal $14 \cdot 7 \neq 7 \cdot 7 + 49$ can be deleted because it is inconsistent with integer arithmetic.

Instantiation can be too specific

When we consider the clause

$$x \neq y + 1 \vee p(x, y)$$

we could use the instantiation $x = 1$, $y = 0$ to infer $p(1, 0)$. But using equality resolution to infer

$$p(y + 1, y)$$

covers all instances while still simplifying the clause.

Trivial literals

We do not want to consider literals that only have overly specific instantiations. A simple criterion is triviality.

A literal is trivial if...

- it is of the form $x \neq t$ (x does not occur in t)
- and it is pure
- and in all other literals of the clause, when x appears the clause is either trivial or not pure

Instantiation Rule

$$\frac{P \vee D}{D\theta}$$

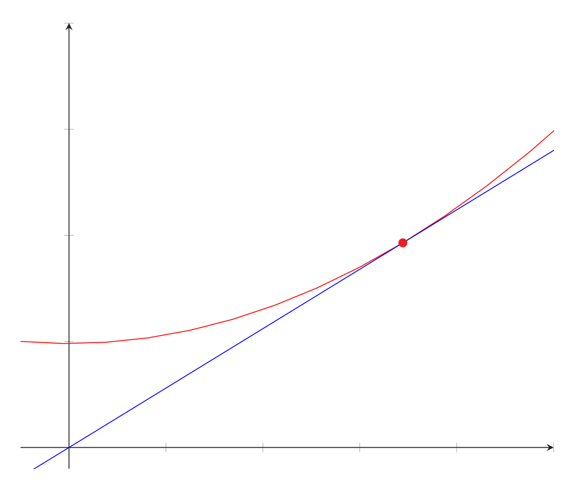
- $P\theta$ unsatisfiable in the background theory
- P does not contain uninterpreted symbols
- P does not contain trivial literals

Using SMT solvers for instantiation

We use an SMT solver to find a θ such that $P\theta$ is unsatisfiable by finding a model of $\neg P$. Note that this only works because P only contains symbols that have a single interpretation in the given theory e.g. arithmetic functions.

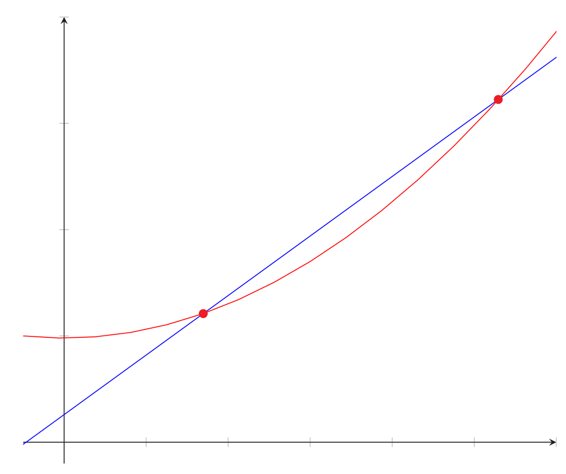
Literals with small sets of solutions

$y = 14x$; $y = x^2 + 49$



$x = 7$

$y = 14x + 13$; $y = x^2 + 49$



$x_1 = 3$, $x_2 = 11$

Abstraction

The problem passed to the SMT solver needs to be pure but most literals are not. Abstraction introduces fresh variables for subterms to separate theory from non-theory literals.

The clause set

$$\{r(14y); r(x^2 + 49) \vee p(x)\}$$

is abstracted to

$$\{u \neq 14y \vee r(u); v \neq x^2 + 49 \vee r(v) \vee p(x)\}$$

Applying abstraction generally interferes with proof search in various ways. Our solution is to extend unification apply abstraction lazily by producing constraints under which theory subterms unify. For example, $r(14y)$ and $r(x^2 + 49) \vee p(x)$ unify to give $14y \neq x^2 + 49 \vee p(x)$.

Vampire

- Automated first-order theorem prover
- Based on superposition
- Supports theories, datatypes, AVATAR
- Available at `https://github.com/vprover/vampire`

Experiments

SMT-LIB

Logic	New solutions	Uniquely solved
ALIA	1	0
LIA	14	0
LRA	4	0
UFDTLIA	5	0
UFLIA	28	14
UFNIA	13	4

TPTP

Category	New solutions	Uniquely solved
ARI	13	0
NUM	1	1
SWW	3	1

References

- Laura Kovács and Andrei Voronkov.
First-order theorem proving and Vampire.
In *CAV 2013*, volume 8044 of *LNCS*, pages 1–35, 2013.
- Giles Reger, Nikolaj Bjørner, Martin Suda, and Andrei Voronkov.
AVATAR modulo theories.
In *GCAI 2016*, volume 41 of *EPiC Series in Computing*, pages 39–52. EasyChair, 2016.
- Giles Reger and Martin Suda.
Set of support for theory reasoning.
In *IWIL Workshop and LPAR Short Presentations*, volume 1 of *Kalpa Publications in Computing*, pages 124–134. EasyChair, 2017.
- Giles Reger, Martin Suda, and Andrei Voronkov.
Unification with abstraction and theory instantiation in saturation-based reasoning.
In *TACAS*, 2018.