SMT-RAT: An SMT-Compliant Nonlinear Real Arithmetic Toolbox
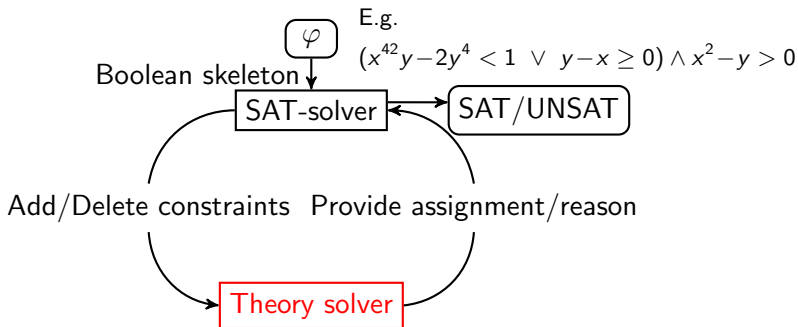
Florian Corzilius, Ulrich Loup, Sebastian Junges, and Erika Ábrahám

RWTH AACHEN UNIVERSITY
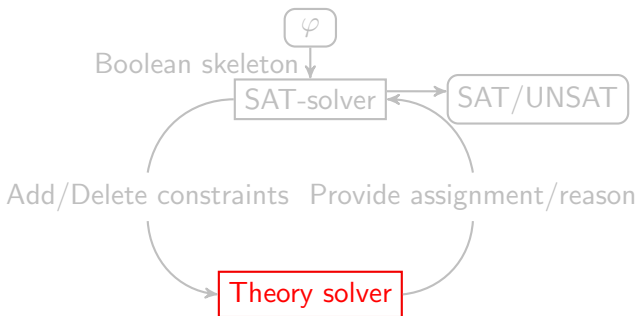
Germany

SAT 2012

Satisfiability-modulo-theories (SMT) compliant solving

E.g.
$(x^{42}y - 2y^4 < 1 \ \lor \ y - x \geq 0) \land x^2 - y > 0$

Solves conjunctions of nonlinear real arithmetic (NRA) constraints
- ▶ incrementally,
- ▶ supporting backtracking,
- ▶ generating minimal reasons.

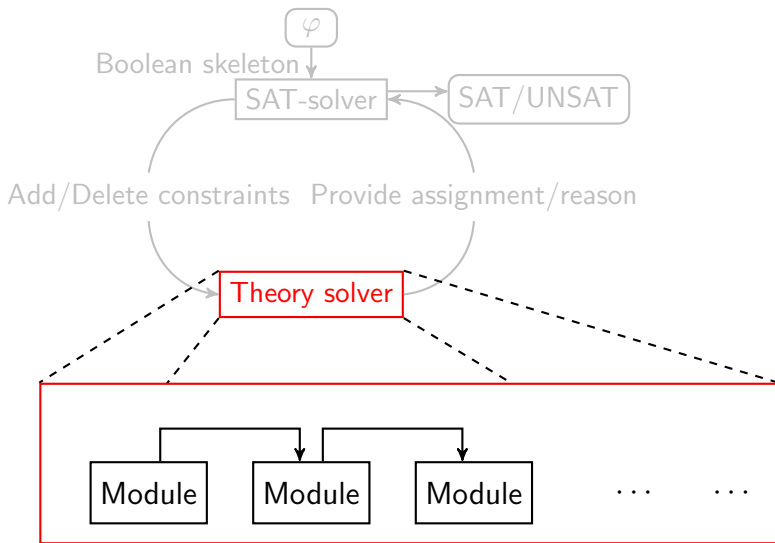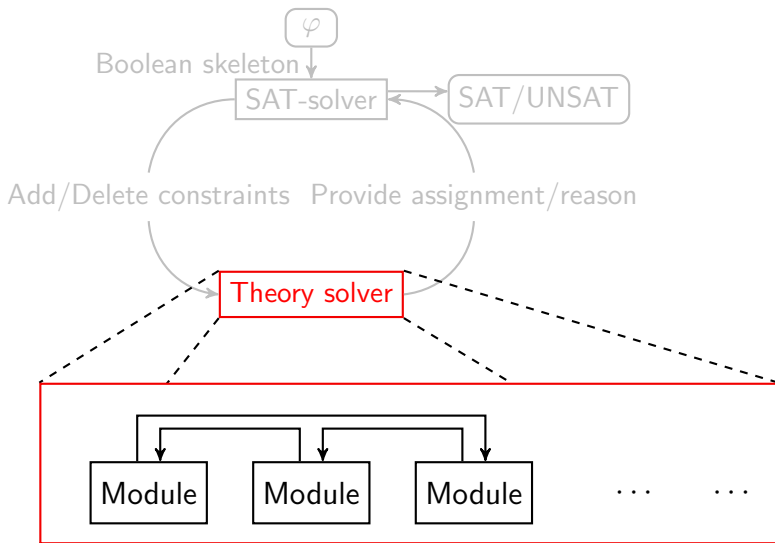# SMT-RAT theory solver

Solves conjunctions of nonlinear real arithmetic (NRA) constraints
- incrementally,
- supporting backtracking,
- generating minimal reasons.

SMT-RAT theory solver

SMT-RAT theory solver

SMT-RAT theory solver

Methods available in SMT-RAT modules

Virtual substitution (VS) [W97]

- bounded degree of input polynomials, but efficient in practice
- SMT compliant [ÁCL10, ÁC11]

Methods available in SMT-RAT modules

Virtual substitution (VS) [W97]

- ▶ bounded degree of input polynomials, but efficient in practice
- ▶ SMT compliant [ÁCL10, ÁC11]

Gröbner bases (GB) [DS97]

- ▶ suitable for equations
- ▶ applicable as preprocessor

Methods available in SMT-RAT modules

Virtual substitution (VS) [W97]

- ▶ bounded degree of input polynomials, but efficient in practice
- ▶ SMT compliant [ÁCL10, ÁC11]

Gröbner bases (GB) [DS97]

- ▶ suitable for equations
- ▶ applicable as preprocessor

Cylindrical algebraic decomposition (CAD) [C75]

- ▶ complete for NRA
- ▶ often inefficient for equations, but efficient for inequalities

Demonstration

- Strategy design in SMT-$\mathbf{X}$RAT

- SMT-RAT theory solver embedded into OpenSMT

Demonstration

Demonstration 1

Theory call: $\{\ x^2 + y^2 + z^2 - 2 = 0,$
$(x-1)^2 + y^2 + z^2 - 2 = 0,$
$(x-1)^2 + (y-1)^2 + z^2 - 2 = 0\ \}$

Strategy:

Result: sat

Call trace: $\texttt{Simplifier} \rightarrow \texttt{VS}$

Demonstration 2

Theory call: $\{ \ x^2 + y^2 + z^2 - 2 = 0,$
$(x-1)^2 + y^2 + z^2 - 2 = 0,$
$(x-1)^2 + (y-1)^2 + z^2 - 2 = 0,$
$(x-1)^2 + (y-1)^2 + (z-1)^2 - 2 = 0 \ \}$

Strategy:

Result: unknown

Call trace: Simplifier $\rightarrow$ VS

Demonstration 3

Theory call: $\{ x^2 + y^2 + z^2 - 2 = 0,$
$(x - 1)^2 + y^2 + z^2 - 2 = 0,$
$(x - 1)^2 + (y - 1)^2 + z^2 - 2 = 0,$
$(x - 1)^2 + (y - 1)^2 + (z - 1)^2 - 2 = 0 \}$

Strategy:

Result: unsat

Call trace: $\texttt{Simplifier} \rightarrow \texttt{VS} \rightarrow \texttt{CAD} \rightarrow \texttt{VS} \rightarrow \texttt{CAD} \rightarrow \texttt{VS} \rightarrow \texttt{CAD}$
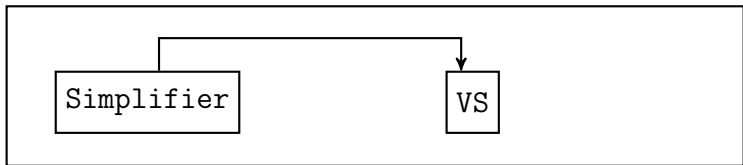
Demonstration 4

Theory call: $\{\ x^2 + y^2 + z^2 - 2 = 0,$
$(x-1)^2 + y^2 + z^2 - 2 = 0,$
$(x-1)^2 + (y-1)^2 + z^2 - 2 = 0,$
$(x-1)^2 + (y-1)^2 + (z-1)^2 - 2 = 0\ \}$
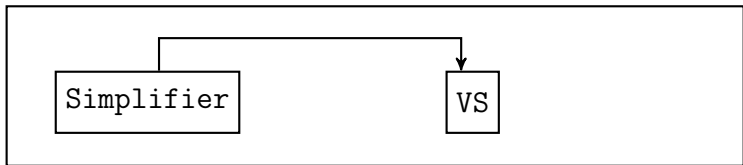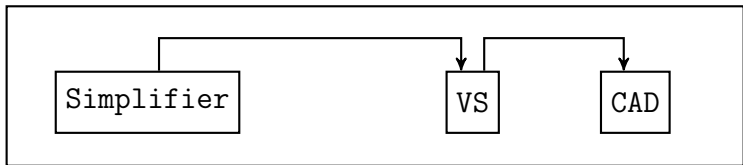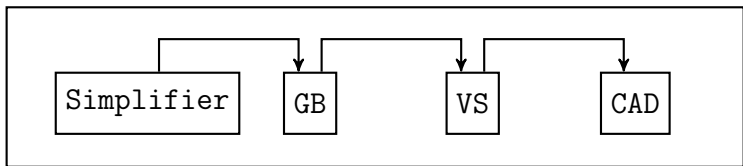
Strategy:

Result: unsat

Call trace: $\text{Simplifier} \rightarrow \text{GB}$

Experimental results

		bouncing ball (**52**)	etcs (**5**)	rectanglar pos. (**22**)	zankl (**166**)
VS	solved	**32**	**1**	**14**	**18**
	acc. time	424.02 s	0.35 s	94.07 s	4.42 s
VS $+$CAD	solved	**43**	**2**	**16**	**22**
	acc. time	4226.24 s	136.15 s	305.54 s	26.30 s
VS $+$GB $+$CAD	solved	**43**	**2**	**16**	**22**
	acc. time	424.63 s	135.05 s	299.54 s	25.81 s
Z3	solved	**0**	**1**	**22**	**62**
	acc. time	0.00 s	0.042 s	27.29 s	1138.96 s
CVC3	solved	**0**	**1**	**0**	**9**
	acc. time	0.00 s	0.11 s	0.00 s	2.86 s

Experimental results

		bouncing ball (**52**)	etcs (**5**)	rectanglar pos. (**22**)	zankl (**166**)
VS	solved	**32**	**1**	**14**	**18**
	acc. time	424.02 s	0.35 s	94.07 s	4.42 s
VS +CAD	solved	**43**	**2**	**16**	**22**
	acc. time	4226.24 s	136.15 s	305.54 s	26.30 s
VS +GB +CAD	solved	**43**	**2**	**16**	**22**
	acc. time	424.63 s	135.05 s	299.54 s	25.81 s
Z3	solved	**0**	**1**	**22**	**62**
	acc. time	0.00 s	0.042 s	27.29 s	1138.96 s
CVC3	solved	**0**	**1**	**0**	**9**
	acc. time	0.00 s	0.11 s	0.00 s	2.86 s

Visit our SMT-RAT on
http://smtrat.sourceforge.net/.

References

📄 G. E. Collins. *Quantifier Elimination for Real Closed Fields by Cylindrical Algebraic Decomposition*. Springer, Automata Theory and Formal Languages, LNCS 33, 134–183, 1975.

📄 A. Dolzmann and T. Sturm. *Simplification of Quantifier-free Formulae over Ordered Fields*. Journal of Symbolic Computation, 1997.

📄 V. Weispfenning. *Quantifier Elimination for Real Algebra – The Quadratic Case and Beyond*. Springer, AAECC, 8 (2), 85–101, 1997.

📄 U. Loup, F. Corzilius and E. Ábrahám. *A Lazy SMT-Solver for a Non-Linear Subset of Real Algebra*. SMT 2010 (peer-reviewed contribution).

📄 F. Corzilius and E. Abraham. *Virtual Substitution for SMT Solving*. Springer, FCT, LNCS 6914, 360 – 371, 2011.