Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Computer Algebra and Computer Science

Gereon Kremer[1]

Certain fields within computer science commonly make use of methods from computer algebra. A prominent example for that is satisfiability modulo theories (SMT) solving that extends the traditional question of satisfiability of propositional logic formulas to first-order theories. We consider nonlinear real problems in particular which produces a need for methods to deal with nonlinear real constraints.

This topic is also an important topic in computer algebra, a community that deals with very similar questions but is surprisingly disjoint from the SMT solving community. The disjointness of these groups used to be a significant obstacle for any transfer of knowledge. The SC^2 project tries to resolve this hurdle by forging new collaborations between the communities of satisfiability checking and symbolic computation.

We present SMT solving as an application of methods from computer algebra and motivate functional requirements and use cases for these methods that are uncommon but very important for SMT solving. Though we can modify existing methods to a certain degree, we as computer scientists depend on the computer algebra community to solve some issues. We show several projects that yielded successful adaptations of methods like Gröbner bases[JLCA13], virtual substitution[CA11] or cylindrical algebraic decomposition[KCA16] to our applications.

Finally we give multiple examples of existing implementations of methods from computer algebra – CoCoALib and Maple – that we struggled to integrate in a meaningful way. We provide insights into the actual problems and hope to suggest new directions of research that ease the cooperation between computer science and computer algebra in the future.

Keywords: Computer Algebra, Computer Science, Satisfiability Modulo Theories Solving, Gröbner Bases, Cylindrical Algebraic Decomposition, Virtual Substitution

References

[CA11] Florian Corzilius and Erika Abraham. Virtual Substitution for SMT Solving. In *FCT'11*, volume 6914 of *LNCS*, pages 360–371. Springer, 2011.

[JLCA13] Sebastian Junges, Ulrich Loup, Florian Corzilius, and Erika Abraham. On Gröbner Bases in the Context of Satisfiability-Modulo-Theories Solving over the Real Numbers. In *CAI'13*, volume 8080 of *LNCS*, pages 186–198. Springer, 2013.

[KCA16] Gereon Kremer, Florian Corzilius, and Erika Abraham. A Generalised Branch-and-Bound Approach and its Application in SAT Modulo Nonlinear Integer Arithmetic. In *CASC'16*, volume 9890 of *LNCS*, pages 315–335. Springer, 2016.

[1]Theory of Hybrid Systems
RWTH Aachen University
52056 Aachen Germany
gereon.kremer@cs.rwth-aachen.de