

RAHD: Real Algebra in High Dimensions

A tool for proving high-dimensional non-linear theorems over real closed fields

Grant Olney Passmore and Paul B. Jackson

g.passmore@ed.ac.uk, pbj@inf.ed.ac.uk

Motivation

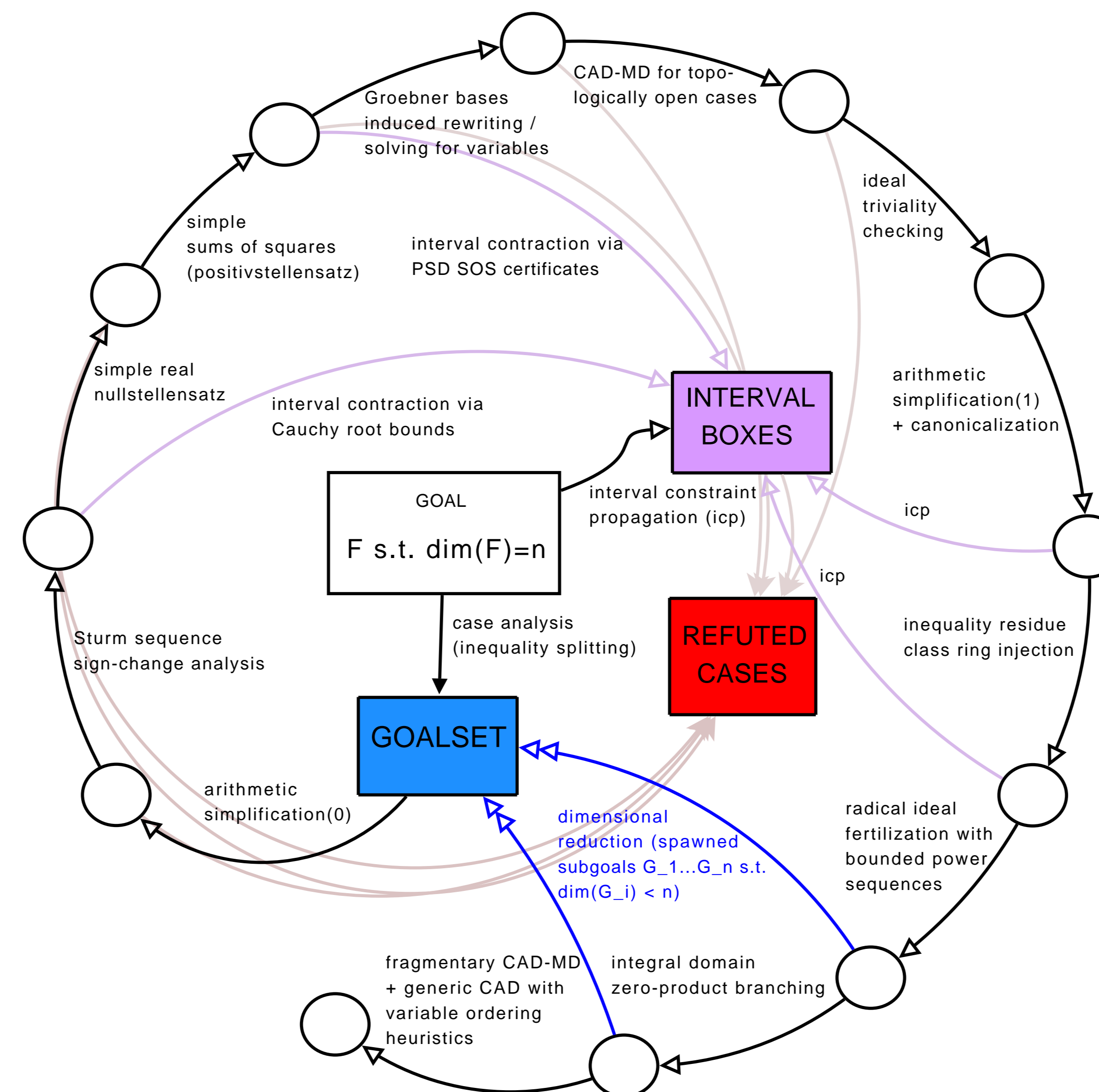
- Methods for deciding non-linear arithmetical conjectures over \mathbb{R} are crucial in the formal verification of many real-world (software, hardware, biological, ...) systems and in formalised mathematics
- While non-linear polynomial arithmetic over \mathbb{R} is *decidable*, it is fundamentally *infeasible*: any *general* decision method for this problem must take time exponential in the *dimension* of the problem
- But, many important real algebraic problems are *high-dimensional*
- For these applications, we need to focus not on the *general* problem, but instead on the development of *feasible, specialized* proof procedures for the types of high-dimensional problems that *arise in practice*

Decision-theoretic “sweet-spots”

- Over the years, a number of (mathematically very different) general decision methods for this problem have been developed
- While all such methods are hampered by the complexity-theoretic issues mentioned previously, most have “sweet-spots,” e.g. types of problems for which they perform much better than they do in general
- For instance, though Collins’ Cylindrical Algebraic Decomposition (CAD) method is *doubly-exponential* in the dimension of the formula being analysed, McCallum has shown that it can be made much more efficient if the set of satisfying real vectors of the formula in question is an *open set* in the Euclidean topology on \mathbb{R}^n
- A guiding strategy underlying the development of RAHD is to study known decision methods, work to isolate their “sweet-spots,” and develop heuristic methods in RAHD that exploit their combination

RAHD

RAHD combines modern techniques in computational commutative algebra, semialgebraic geometry, and restricted variants of classical real quantifier elimination algorithms, including: Sturm sequence calculations, ideal triviality checking, Gröbner basis reductions for canonically injecting terms in inequalities into the quotient ring induced by the equalities in the problem, light-weight Real Nullstellensatz and Positivstellensatz Sums of Squares methods, interval arithmetic and constraint propagation, a hierarchy of nested arithmetical simplifiers, a Gröbner basis induced form of directed rewriting and completion for solving for variables, a number of novel dimensional-reduction techniques, a case-splitting and case-analysis procedure, and a variant of Cylindrical Algebraic Decomposition for topologically open constraints (CAD-MD) into a tightly-integrated heuristic proof procedure designed to reduce high-dimensional real algebraic conjectures into equisatisfiable sequences of simpler, lower-dimensional conjectures that can themselves be solved with a combination of light-weight heuristic reasoning and available decision methods operating within their respective “sweet-spots.”



Using RAHD

RAHD is written in Allegro Common Lisp, and can be used in two ways: (i) As “push-button” automatic proof procedure, and (ii) as an interactive, tactic-style proof-assistant. Both the “push-button” proof procedure (called the “RAHD waterfall” due to the influence of the “Boyer-Moore waterfall” on our design; see diagram above) and the interactive mode produce “proof objects” at a level of detail that should be amenable to independent verification.

Examples

RAHD is currently able to solve a number of problems that were to our knowledge previously unsolvable by automatic means. The following are two examples which neither a state-of-the-art CAD procedure (QEPCAD-B), nor a modern semidefinite programming based Sums of Squares Positivstellensatz method (REAL_SOS in HOL-Light) can prove on our available machines, while RAHD (using its “waterfall” procedure) can prove them on our desktop machine in approximately 8 and 9 seconds (real time), respectively:



- A medium-degree problem in 4-dimensions:

$$\begin{aligned} & \forall a \forall b \forall c \forall d \\ & ((0 \leq a) \wedge (a \leq 1) \wedge (0 \leq b) \wedge (b \leq 1) \wedge \\ & (0 \leq c) \wedge (c \leq 1) \wedge (0 \leq d) \wedge (d \leq 1)) \\ & \Rightarrow \\ & (((1 - a^2b^2)(1 - cd)(ad - bc)(ad - bc) + \\ & (2ab)(cd - ab)(1 - ab)(c - d)(c - d) + \\ & (a^2b^2 - c^2d^2)(1 - cd)(a - b)(a - b)) \geq 0) \end{aligned}$$

To prove the above problem, RAHD (in around 3 seconds) uses Sturm chain analysis and an SOS Positivstellensatz method to reduce the truth of the problem to that of 22 topologically open conjectures (1 in 3 dimensions, the rest in 2). These low-dimensional open problems are then all proved by QEPCAD-B’s implementation of the CAD-MD algorithm in a total of about 5 seconds.

- A low-degree problem in 11-dimensions:

$$\begin{aligned} & \forall a \forall b \forall c \forall d \forall e \forall f \forall g \\ & \forall h \forall i \forall j \forall k \\ & ((12bce - 3e^2f \geq hk + 11) \wedge (45hk(d + 1) = g) \wedge \\ & (g > e + f + 82) \wedge (j < -1) \wedge (h \geq k) \wedge \\ & (k \geq 1) \wedge (a^2 = 0) \wedge (ij = a)) \\ & \Rightarrow \\ & ((h^3k^2 < i) \vee (h^3k^2 > i)) \end{aligned}$$

To prove the above problem, RAHD (in around 8 seconds) uses a method for approximate computations in the quotient ring induced by the radical of the ideal generated by equations in the problem, together with a dimensional reduction technique, to reduce the problem to two conjectures that are each proved by CAD in a total of about 1 second.

Future

- Driven by problems gathered from those with real algebraic decision need, develop RAHD into a tool that can solve the types of high-dimensional real algebraic problems researchers encounter in practice
- Further integrate RAHD into SRI FV tool-chain (PVS complete with Sam Owre; HybridSAL, Yices2 ongoing) and apply to difficult problems
- Use RAHD to contribute to FLYSPECK project and develop a method for the verification of RAHD’s proof objects within HOL-Light

Acknowledgements

Thank you to John Rushby, N. Shankar, Sam Owre, Ashish Tiwari, and Bruno Dutertre of SRI International, John Harrison of Intel, and Matt Kaufmann, J Strother Moore, and Bob Boyer of UT Austin.