中国科学院软件研究所学术年会 暨重点实验室科技活动周 2025 第十届

学术论文

A Complete Algorithm for Optimization Modulo Nonlinear Real Arithmetic

贾富琦, 董宇航, 韩瑞, 黄沛, 刘明昊, 马菲菲, 张健

The 39th Annual AAAI Conference on Artificial Intelligence (AAAI 2025), 39(11), 11255-11263.

{jiafq, maff, zj}@ios.ac.cn

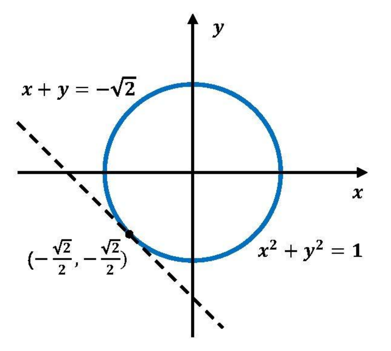
Motivation

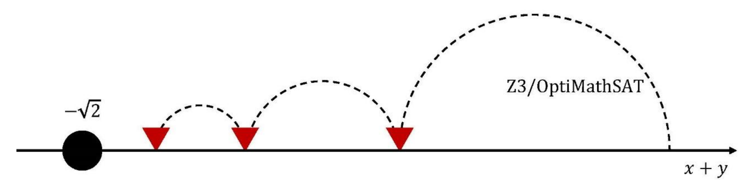
Example

Consider an OMT(NRA) formula,

$\min x+y,\ s.t.\ x^2+y^2=1,$

the objective $x+y$ *has a minimum value of* $-\sqrt{2}$.





Using 2 hours:
- *Z3: timeout;*
- *OptiMathSAT: timeout.*

Contributions

- ***Development of the first complete OMT solver for NRA:*** *Present OCAC and CDCL(OCAC), sound and complete algorithms, along with proofs of correctness and termination.*
- ***Investigation of Variants:*** *Explore two additional solving algorithm variants, using CAD and a first-order formulation.*
- ***Evaluation:*** *Integrated this algorithm into CVC5 and conducted empirical evaluations showing that it outperforms the leading OMT solver, OptiMathSAT.*

Basic Definitions

*Definition 1 (**NRA Formula**):*

$p ::= x \mid c \mid p+p \mid p\cdot p,$ (polynomial)

$\phi ::= b \mid p\geq 0 \mid p=0 \mid \neg\phi \mid \phi\wedge\phi \mid \phi\vee\phi$ (formula)

$x\in\mathbb{R}, c\in\mathbb{Q}, b\in\mathbb{B}$

*Definition 2 (**Cell**):*

Given $P=\{p_1,\cdots,p_m\}\subseteq\mathbb{Q}[x_1,\cdots,x_n]$ *and* $s\in\mathbb{R}^n$, *a cell* $\mathbb{C}(P,s)$ *is a non-empty connected subset of* $\mathbb{R}^n$ *that is sign-invariant for P and contains s. For all* $i\in\{1,\cdots,m\}$,

$\forall s'\in\mathbb{C}(P,s), sign(p_i(s))=sign(p_i(s')).$

*Definition 3 (**Cell Interval**):*

$\mathbb{C}(P,s)_{x_i}$ *is an interval* $\{\mathbb{l},\mathbb{U}\}$ *over* x_i, *i.e.,*

$\forall r\in\mathbb{R}.(\mathbb{l}<r<\mathbb{U}\rightarrow\bar{s}\in\mathbb{C}(P,s)),$

where $\bar{s}:=(s^1,\cdots,s^{i-1},r,s^{i+1},\cdots,s^n)$, *replacing* s_i *with* r.

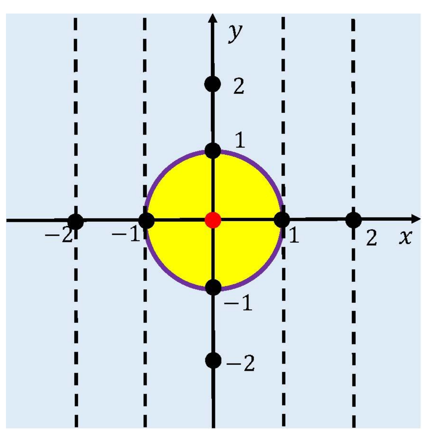
*Definition 4 (**Extended Domain**):*

$\bar{\mathbb{R}}:=\mathbb{R}\cup\{\infty\}\cup\{\epsilon\}$ and $\epsilon\rightarrow 0$.

A Cylindrical Algebraic Decomposition (CAD) is a decomposition algorithm for a set of polynomials in $\mathbb{R}^n, n\in\mathbb{N}$ *space resulting in a finite number of cells.*

Consider $\{x^2+y^2-1\}$ *and* $x<y$ *:*
- *Projects* y *and obtains* $\{x^2-1\}$;
- *Isolates roots, i.e.,* $x=-1$ *and* $x=1$;
- *Divides* $\mathbb{R}$ *to 5 segments;*
- *Samples* $x=\{-2,-1,0,1,2\}$, *resulting in* $\{y^2+3\}$, $\{y^2\}$, *and* $\{y^2-1\}$;
- *Isolates roots for* $\{y^2-1\}$, *i.e.,* $\{-1,1\}$;
- *Divides* $\mathbb{R}$ *to 5 segments;*
- *Repeats and obtains all representatives.*

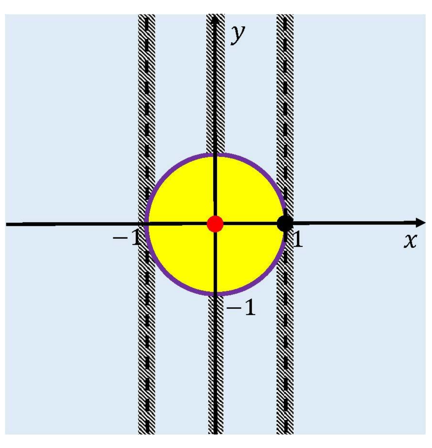
Red point $(0,0)$ *represents the sign-invariant region* $\{x^2+y^2-1<0\}$



The Cylindrical Algebraic Covering Algorithm (CAC) is a variant of CAD, adjusted to the context of SMT.

Consider $x^2+y^2<1$ *and* $x<y$ *:*
- *Assigns* $x=1$ *and obtains* $y^2<0\equiv\bot$;
- *Identifies the characterizing set* $\{x^2-1\}$;
- *Excludes unsatisfiable region* $\{-1,1\}\times\mathbb{R}$;
- *Assigns* $x=0$ *and obtains* $y^2<1$;
- *Excludes* $\{0\}\times(-\infty,-1]\cup[1,+\infty)$;
- *Assigns* $y=0$ *and reports* $\top$.

Finally, it finds a model, i.e., the red point (0, 0).



Generalized Optimization Modulo Theories

*Definition 5 (**GOMT problem**):*

A General Optimization Modulo Theories problem is a tuple $\mathcal{GO}:=(t,\prec,\phi)$, *where,*
- t, *a* Σ*–term of some sort* σ, *is an objective term to optimize;*
- $\prec$ *is a strict partial order definable in* $\mathbb{T}$, *whose defining formula has two free variables, each of sort* σ, *and*
- φ *is a* Σ*-formula.*

Example *is a simple example of* $\mathcal{GO}(x+y,\ <,\ x^2+y^2=1)$.

For any GOMT problem $\mathcal{GO}$ *and* $\mathbb{T}$*-interpretations* $\mathbb{I}$ *and* $\mathbb{I}'$, *we say that:*
- $\mathbb{I}$ *is* $\mathcal{GO}$*–consistent if* $\mathbb{I}\models\phi$;
- $\mathbb{I}$*-dominates,* $\mathbb{I}'$ *denoted by* $\mathbb{I}<_{\mathcal{GO}}\mathbb{I}'$, *if* $\mathbb{I}$ *and* $\mathbb{I}'$ *are* $\mathcal{GO}$*–consistent and* $t^{\mathbb{I}}<t^{\mathbb{I}'}$;
- $\mathbb{I}$ *is a* $\mathcal{GO}$*-solution if* $\mathbb{I}$ *is* $\mathcal{GO}$*-consistent and no* $\mathbb{T}$*-interpretation* $\mathcal{GO}$*-dominates* $\mathbb{I}$.

*Definition 6 (**GOMT over NRA**):*

A $\mathcal{GO}_{\mathcal{NRA}}$ *is a tuple* $\mathcal{GO}_{\mathcal{NRA}}:=(t,<,\phi)$, *where,*
- t *is the polynomial objective term to optimize;*
- $<$ *is a strict partial order definable in NRA, whose formula defines over* $\bar{\mathbb{R}}\times\bar{\mathbb{R}}$,
- ϕ *is an SMT(NRA) formula.*

Optimization Cylindrical Algebraic Covering

Algorithm 1 OCAC

Input: $\psi\wedge t=x_t$: The *OMT branch formula*, with n variables.
Output: g, v, l: A flag that $\psi\wedge t=x_t$ is satisfiable; The optimum value; The cutting lemma.

```
1: I := ∅, g := ⊥, v := None
2: while ⋃_{I∈I} I ≠ ℝ do
3:     s_t := Sample_Objective_Value(I)
4:     (T, O) := Solve_Internal(ψ ∧ t = x_t ∧ x_t = s_t)
5:     if T = ⊤ then
6:         g := ⊤, v := Analyze_Cell(O)
7:         O := O ∪ [s_t, +∞)
8:     end if
9:     I := I ∪ {O}
10: end while
11: return (g, v, Lemma(v))
```

*Definition 7 (**GOMT in OCAC**):*

A $\mathcal{GO}_{\mathcal{OCAC}}$ *is a tuple* $\mathcal{GO}_{\mathcal{OCAC}}:=(x_t,\prec_{Cell},\psi)$, *where,*
- x_t, *a variable with* $x_t=t$, *is the objective variable where t is the polynomial objective term to optimize;*
- $\prec_{Cell}$ *is a strict partial order definable in NRA, whose formula defines over* $\mathbb{R}\times\mathbb{R}$, *and* $x_t^1\prec_{Cell}x_t^{1'}$ *is equivalent to:* $\mathbb{l}(\mathbb{C}(\mathbb{P}(\psi),\mathbb{1}_{\mathbb{R}})_{x_t})<\mathbb{l}(\mathbb{C}(\mathbb{P}(\psi),\mathbb{1}'_{\mathbb{R}})_{x_t})$,
- ψ *is a conjunction of polynomial atoms.*

Correctness and Termination

*Theorem (**Correctness of CAC**):*

Let ψ *be a conjunction of polynomial atoms with* $x_1,\cdots,x_n$, $S=\{s'_1,\cdots,s'_m\}\subseteq\mathbb{R}$, $P^1,\cdots,P^m\subseteq\mathbb{Q}[x_1,\cdots,x_i]$ *and* $s\in\mathbb{R}^{i-1}$ *for* $1<i\leq n$. *If* $\{s\}\times\mathbb{R}\subseteq\bigcup_{j=1}^{m}\mathbb{C}(P_j,(s,s'_j))$ *and for* $1\leq j\leq m$, $\mathbb{C}(P_j,(s,s'_j))$ *is unsatisfiable for* ψ, *then* $\mathbb{C}(proj_{cov},(P^1,\cdots,P^m,s,S),s)$ *is unsatisfiable for* ψ.

*Theorem (**Termination of OCAC**):*

Given an OMT branch formula $\psi\wedge t=x_t$, *OCAC terminates.*

*Theorem (**Satisfiable Interval**):*

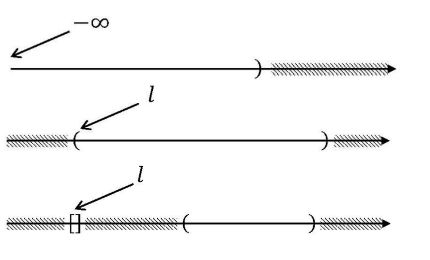
Given an OMT branch formula $\psi\wedge t=x_t$, *P denotes the set of polynomials in* $\psi\wedge t=x_t$. *If* $\psi\wedge t=x_t$ *is satisfiable, that is, there exists a complete assignment* $s=(s_t,s_1,\cdots,s_n)$ *that satisfies* $\psi\wedge t=x_t$, *then* $\forall\gamma_o\in\mathbb{C}(proj^n_{dec}(P),s)_{x_t}$, $\psi\wedge t=\gamma_o$ *is satisfiable.*

*Theorem (**Correctness of OCAC**):*

Given an OMT branch formula $\psi\wedge t=x_t$, *if* $\psi\wedge t=x_t$ *is unsatisfiable, OCAC returns UNSAT; otherwise, OCAC can find the optimum.*

Corollary

Given a conjunction of polynomial atoms ψ, *let* I_o *of* x_t *represent the leftmost satisfiable interval for minimization, which can be characterized by three cases:*
- $I_o=(-\infty,u)$ *implies* $\min(x_t)=-\infty$;
- $I_o=(l,u)$ *implies* $\min(x_t)=l+\varepsilon$;
- $I_o=[l,l]$ *implies* $\min(x_t)=l$.



*Theorem (**Termination and Correctness**):*

For a given instance $\mathcal{GO}_{\mathcal{NRA}}:=(t,<,\phi)$, *the CDCL(OCAC) algorithm is guaranteed to terminate and produce correct results.*

Experiments

- ***CAD-Based Variant.*** *Using CAD to precompute the candidate intervals and select representatives from the leftmost interval until finding the optimal.*
- ***First-Order Formulation.*** *Converting the optimization problem into the first-order formula and solving it.*
- ***OptiMathSAT.*** *The leading OMT solver using linear or binary search.*

- *Benchmarks:*
  - *Generated from QF_NRA benchmarks of SMT-LIB.*
  - *For satisfiable instances:*
    - *Randomly select from declared variables;*
    - *Add minimization objectives:* x, $x+y$, x^2+y^2, xy, *or* $xy+z$;
    - *Randomly select 10000 instances.*
  - *For unsatisfiable instances, use original benchmarks, a total of 5532 instances.*
- *Timeout: 1200 s.*
- *For FOL baseline: select the best results from CVC5, dReal, yicesQS, and Z3.*

	#(RAN)	#(RAN +ϵ)	#(ℚ)	#(ℚ + ϵ)	#(∞)	#SAT	#UNSAT
CDCL(CAD)	246	551	802	2990	1129	5718	4568
FOL	304	610	**1101**	3545	1165	6725	4392
OptiMathSAT(Bin)	0	0	943	1870	353	3166	**5040**
OptiMathSAT(Lin)	0	0	928	1819	336	3083	**5040**
CDCL(OCAC) (Ours)	**369**	**981**	1084	**4248**	**1250**	**7932**	5019

Table 1: Performance on the number of solved instances, including 10000 satisfiable and 5532 unsatisfiable ones.

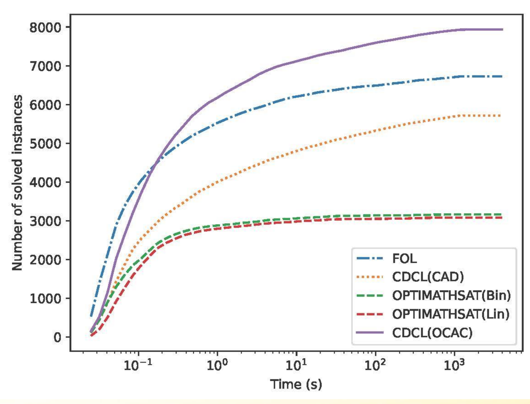


Figure 1: Performance on satisfiable instances over time.