An Algebraic Approach for the Unsatisfiability of Nonlinear Constraints[⋆]

Ashish Tiwari

SRI International,
333 Ravenswood Ave,
Menlo Park, CA, U.S.A
tiwari@csl.sri.com

Abstract. We describe a simple algebraic semi-decision procedure for detecting unsatisfiability of a (quantifier-free) conjunction of nonlinear equalities and inequalities. The procedure consists of Gröbner basis computation plus extension rules that introduce new definitions, and hence it can be described as a critical-pair completion-based logical procedure. This procedure is shown to be sound and refutationally complete. When projected onto the linear case, our procedure reduces to the Simplex method for solving linear constraints. If only finitely many new definitions are introduced, then the procedure is also terminating. Such terminating, but potentially incomplete, procedures are used in "incompleteness-tolerant" applications.

1 Introduction

The ability to solve nonlinear constraints is central to the task of developing and automating analysis technology for several classes of systems. Nonlinear constraints arise in robotics, control theory, hybrid system models of physical and embedded control systems and biological systems, and in solving games [8, 15, 17]. Fortunately, the full first-order theory of the reals is known to be decidable [22]. Unfortunately, it has a double exponential lower-bound and most of the decision procedures for this theory are complex, nonlogical, and involve considerable splitting (causing blowups) [7, 24, 18, 5]. Available implementations of the decision procedure [13, 12] can only solve very small-sized examples.

We are particularly interested in the verification of hybrid systems. Our methodology for verification is based on abstraction and model-checking [23]. Automation of this technique requires sound and fast implementations of a procedure for testing unsatisfiability of (a conjunction of) nonlinear constraints. The same is also needed in the lazy approach of extending constraint solvers to handle boolean combination of constraints. Tools such as ICS [9], CVC [21], and MathSat [1], which are used in bounded model-checking of discrete systems,

[⋆] Research supported in part by the National Science Foundation under grants CCR-0311348 and ITR-CCR-0326540.

also implement some form of incomplete nonlinear constraint solving. Fast and sound, but potentially incomplete, implementations that can solve large problem instances are useful in several "incompleteness-tolerant" applications such as the process of creating abstractions, where incompleteness only causes creation of a coarser abstraction.

This paper considers the problem of developing fast reasoners for (quantifier-free conjunction of) nonlinear constraints over the theory of reals. Our goal was to develop a method that efficiently detected the "easy" unsatisfiable instances. For instance, we do not want to compute a full cylindrical algebraic decomposition of the n-dimensional space based on the polynomial p to decide if $p > 0 \wedge p < 0$ is satisfiable. Our goal was to give a logical procedure that can be described using simple inference rules. Moreover, the procedure should be simple and easy to implement and incremental, that is, new constraints can be added without redoing everything.

In this paper, we describe a critical-pair completion approach to nonlinear constraint solving. The main ingredient is the Gröbner basis computation method. Apart from it, we only need some *extension* rules that introduce new definitions. Surprisingly, this is all that is needed for obtaining a sound and refutationally complete procedure for testing unsatisfiability of nonlinear constraints–a consequence of the Positivstellensatz theorem from real algebraic geometry.

Our approach is based on eliminating inequality constraints by introducing slack variables and then constructing a Gröbner basis of the polynomials in the equality constraints. For example, suppose we want to prove unsatisfiability of $\{u_1 + u_2 - 1 \approx 0, -u_2 + 2 \approx 0, u_1 \geq 0\}$. If we construct a (fully reduced) Gröbner basis of the polynomials that appear in the two equations, we get $\{u_1 + 1, -u_2 + 2\}$. The first polynomial, $u_1 + 1$, is a *witness* for unsatisfiability of the original constraints, since $u_1 \geq 0$ implies that $u_1 + 1$ should be strictly greater-than 0, but the equational constraints require that $u_1 + 1 \approx 0$. Unfortunately, it is not the case that whenever the original constraints are unsatisfiable, the corresponding Gröbner basis will necessarily contain such a witness. For example, if we change the constraints slightly to $\{u_1 + u_2 - 1 \approx 0, u_2 u_3 - u_2 + 2 \approx 0, u_1 \geq 0, u_2 \geq 0, u_3 \geq 0\}$, then the Gröbner basis computation does not yield anything new and we fail to detect the witness. The witness here is $u_2 u_3 + u_1 + 1$, which is obtained by adding the two equations. The reason why the witness is not explicitly present in the Gröbner basis is that it is not "small-enough" in the lexicographic ordering chosen to construct the Gröbner basis.

The basic idea in our paper is that new definitions that introduce new constants allow greater flexibility in choosing orderings. For example, we can make the witness polynomial $u_2 u_3 + u_1 + 1$ smaller by introducing a definition $u_2 u_3 \approx u_4$ and giving u_4 the lowest precedence. As a result, we now compute the Gröbner basis for $\{u_1 + u_2 - 1, u_2 u_3 - u_2 + 2, u_2 u_3 - u_4\}$, and we get $\{u_1 + u_4 + 1, u_2 - u_4 - 2, u_2 u_3 - u_4\}$. The first polynomial in this set, $u_1 + u_4 + 1$, is a witness for unsatisfiability of the original set of constraints.

In the linear case, our method would introduce definitions of the form $u_1 \approx u_2$, making the new variable u_2 smaller than all other variables. This has the effect of lowering the precedence of the old variable u_1. This is similar to the Simplex method, where the pivot steps transform a Gröbner basis with respect to a given precedence $\succ_1$ to a Gröbner basis with respect to a different precedence $\succ_2$, doing this until a witness to unsatisfiability is detected, or we have (implicitly) exhausted all possibilities.

The inference rules are nonterminating because of the possibility of introducing infinitely many new definitions. Our procedure can be made terminating by limiting the introduction of new definitions. We could still guarantee completeness if there were known degree bounds for Positivstellensatz, whence we could introduce enough new definitions to cover all polynomials upto the given degree bound. Obtaining such degree bounds is an active area of research [19].

The presentation of the procedure in this paper is incremental. We first present a simple and incomplete procedure in Section 3. Thereafter, we describe the version of Positivstellensatz we use in this paper in Section 4. Using this result, in Section 5 we develop a sound procedure that is refutationally complete relative to an oracle (that provides the new definitions). Finally, we present the complete set of inference rules in Section 6 and show how the job of the oracle can be performed using static analysis of the polynomials.

2 Term Rewriting and Polynomials

Let $\{x_1, \ldots, x_n\}$ be a set of indeterminates, often denoted using vector notation as $\boldsymbol{x}$. The set of power-products over $\boldsymbol{x}$ is the free commutative monoid $[\boldsymbol{x}]$ generated by $\boldsymbol{x}$. Elements of $[\boldsymbol{x}]$, such as $x_1 x_2^2 x_3$, are denoted by μ with possible subscripts. The polynomial ring over the field of rational numbers $\mathbb{Q}$ is the $\mathbb{Q}$ vector space generated by $[\boldsymbol{x}]$, denoted by $\mathbb{Q}[\boldsymbol{x}]$. Elements from $\mathbb{Q}[\boldsymbol{x}]$ are denoted by p, q with possible subscripts. Atomic formulas are given as $p \approx 0$, $p \geq 0$, and $p > 0$. Since we deal with quantifier-free conjunctions of atomic formulas, the indeterminates $\boldsymbol{x}$ are logically constants, but we call them variables. Positive variables are denoted by v and nonnegative by u, w. Elements from $\mathbb{Q}$ will be denoted by c, and hence a polynomial p can be written as $c_0\mu_0 + c_1\mu_1 + \ldots + c_k\mu_k$.

Orderings on polynomials. Let $\langle \boldsymbol{c_1}, \boldsymbol{c_2}, \ldots, \boldsymbol{c_m} \rangle$ be a sequence of m nonnegative vectors in ${\mathbb{Q}^+}^n$ such that $m \geq n$ and $\{\boldsymbol{c_1}, \boldsymbol{c_2}, \ldots, \boldsymbol{c_m}\}$ spans the n-dimensional vector space $\mathbb{Q}^n$. We define an ordering on power-products as follows: $x_1^{d_1} \ldots x_n^{d_n} \succ x_1^{d'_1} \ldots x_n^{d'_n}$ if there is a k such that $1 \leq k \leq m$ and (a) $\boldsymbol{c_k} \cdot \boldsymbol{d} > \boldsymbol{c_k} \cdot \boldsymbol{d'}$, and (b) $\boldsymbol{c_i} \cdot \boldsymbol{d} = \boldsymbol{c_i} \cdot \boldsymbol{d'}$ for all $i < k$. If $\boldsymbol{e_i}$ is a unit vector in i-th direction (that is, only the i-th component is nonzero), then choosing $\langle \boldsymbol{e_1}, \boldsymbol{e_2}, \ldots, \boldsymbol{e_n} \rangle$ results in the pure lexicographic ordering. Note that if $\boldsymbol{e_0}$ contains all 1's, then choosing $\langle \boldsymbol{e_0}, \boldsymbol{e_1}, \boldsymbol{e_2}, \ldots, \boldsymbol{e_n} \rangle$ results in *total-degree* lexicographic ordering. For other choices of $\boldsymbol{c_i}$'s, we can get certain "combinations" of these two orderings.

The ordering $\succ$ on power-products can be extended to monomials by just ignoring the coefficient (if it is nonzero). The ordering on monomials can be extended to polynomials by using the multiset extension of $\succ$ (and viewing a polynomial as a multiset of monomials) [10].

Term rewriting systems. Term rewriting systems are sets containing directed equations, $l \to r$, where the orientation is usually chosen so that $l \succ r$ for some reduction ordering on the set of terms. If R is a rewrite system, the binary relation on terms $\to_R$ is defined as the closure of R under contexts and substitution. We use the usual notation for symmetric ($\leftrightarrow$) and transitive ($\to^*$) closures.

A rewrite system R is said to be *convergent* if the relation $\to_R$ is well-founded and the relation $\to^*_R$ is confluent, that is, $\leftrightarrow^*_R \subseteq \to^*_R \circ \leftarrow^*_R$. A rewrite system R is *fully reduced* if for every rule $l \to r \in R$, the term r is not reducible by R and the term l is not reducible by $R - \{l \to r\}$.

A (finite) fully reduced convergent R has several nice properties. It can be used to decide the relation $\leftrightarrow^*_R$. In fact, if $s \leftrightarrow^*_R t$ and $s \succeq t$, then we actually have $s \to^*_{R|_{\not\succ s}} \circ \leftarrow^*_{R|_{\not\succ s}} t$, where $R|_{\not\succ s}$ contains only those rules in R that contain terms no bigger than s. Furthermore, if r is a $\succ$-minimal term in the R-equivalence class $[[r]]_R$ and l is $\succ$-minimal in $[[r]]_R - \{r\}$, then $l \to_R r$. In other words, the fully reduced convergent R will either contain the rule $l \to r$ explicitly, or some other rule that can be used to rewrite l to r in one step.

Polynomials as rewrite rules. A polynomial expression can be normalized into a sum of monomials form $c_0\mu_0 + \cdots + c_k\mu_k$—intuitively using the distributivity rules and formally using a convergent rewrite system for the theory of polynomial rings [2, 3]. We work modulo this theory of polynomial rings in this paper. As a result, we assume that all terms are automatically converted into sum of monomial form. If we assume that $\mu_0 \succ \mu_i$ for all $1 \leq i \leq k$, then the polynomial equation $c_0\mu_0 + \cdots + c_k\mu_k \approx 0$ can be oriented into a rewrite rule $c_0\mu_0 \to -c_1\mu_1 + \cdots + -c_k\mu_k$. This is a ground rewrite rule (that is, it contains no variables), but we use its AC-extension, $c_0\mu_0\nu \to -c_1\mu_1\nu + \cdots + -c_k\mu_k\nu$, for purposes of rewriting polynomials. Here ν is an extension variable (that can be instantiated by monomials). For example, $-u_2 + 2 \approx 0$ can be used as $u_2 \to 2$ to rewrite $u_1u_2 + u_1$ to $2u_1 + u_1$, which normalizes to $3u_1$. This is denoted by $u_1u_2 + u_1 \to_{u_1 \to 2} 3u_1$. Thus, the rewrite relation $\to_P$ induced by P is defined modulo the theory of the coefficient domain $\mathbb{Q}$ and polynomial ring axioms.

Given a set P, the Gröbner basis for P can now be constructed using standard critical-pair completion [3]. A Gröbner basis is a convergent rewrite system and we can even make it fully reduced. We will denote by $GB_\succ(P)$ the fully reduced Gröbner basis for P computed using the ordering $\succ$.

Given a set $P \subset \mathbb{Q}[\boldsymbol{x}]$, the ideal generated by P (in $\mathbb{Q}[\boldsymbol{x}]$) is defined by

$$\mathit{Ideal}(P) = \{q : q = \Sigma_i\ q_i p_i,\ p_i \in P,\ q_i \in \mathbb{Q}[\boldsymbol{x}]\} = \{q : q \leftrightarrow^*_P 0\}$$

Thus, an ideal of P is the equivalence class of 0, when P is viewed as a set of equations, in the theory of polynomial rings [3]. Elimination ideal consists of the projection of the ideal onto polynomials over a subset of variables (that is, it eliminates the other variables). If P is a set of polynomials in $\mathbb{Q}[\boldsymbol{x}, \boldsymbol{u}]$, then we can eliminate the $\boldsymbol{x}$ variables and define $\mathit{Elim}(P, \boldsymbol{x}) = \mathit{Ideal}(P) \cap \mathbb{Q}[\boldsymbol{u}]$.

The above-mentioned property of fully reduced convergent rewrite systems implies that Gröbner basis can be used to compute elimination ideals. In particular, if $\succ$ is an ordering such that $\mu \succ \nu$ for any $\mu \in [\boldsymbol{x}, \boldsymbol{u}] - [\boldsymbol{u}]$ and $\nu \in [\boldsymbol{u}]$, then $\mathit{Elim}(P, \boldsymbol{x}) = \mathit{Ideal}(GB_{\succ}(P) \cap \mathbb{Q}[\boldsymbol{u}])$. In fact, $GB_{\succ}(P) \cap \mathbb{Q}[\boldsymbol{u}]$ will be a fully reduced Gröbner basis for the elimination ideal $\mathit{Elim}(P, \boldsymbol{x})$. The pure lexicographic ordering with precedence $\boldsymbol{x} \succ \boldsymbol{u}$ satisfies this property. On the other hand, if $\succ$ is a total-degree lexicographic ordering with precedence $\boldsymbol{x} \succ \boldsymbol{u}$, then $\mathit{Ideal}(GB_{\succ}(P) \cap \mathbb{Q}[\boldsymbol{u}])$ will contain all *linear* polynomials over $\boldsymbol{u}$ in $\mathit{Ideal}(P)$.

3 Introducing New and Eliminating Old Variables

Let $E = \{p_i \approx 0 : i \in I_1\}$, $F_1 = \{q_i > 0 : i \in I_2\}$, and $F_2 = \{q_i \geq 0 : i \in I_3\}$, where $p_i, q_i \in \mathbb{Q}[\boldsymbol{x}]$. Here I_1, I_2, I_3 are mutually disjoint, finite sets of indices. As in the Simplex method, we introduce new *slack* variables to convert the inequality constraints into equational constraints. Specifically, we introduce the variables v_i, $i \in I_2$ and w_i, $i \in I_3$ and replace the sets F_1 and F_2 by $E_1 = \{q_i - v_i \approx 0 : i \in I_2\}$ and $E_2 = \{q_i - w_i \approx 0 : i \in I_3\}$.

The set $E \cup E_1 \cup E_2$ of equations now contains polynomials from $\mathbb{Q}[\boldsymbol{x}, \boldsymbol{v}, \boldsymbol{w}]$. We also have the implicit constraints $\boldsymbol{v} > 0$ and $\boldsymbol{w} \geq 0$. It is obvious that the set $E \cup E_1 \cup E_2 \cup \{\boldsymbol{v} > 0,\ \boldsymbol{w} \geq 0\}$ is satisfiable over the reals if and only if the set $E \cup F_1 \cup F_2$ is satisfiable over the reals (all variables are assumed to be existentially quantified).

Example 1. Let $E = \{x_1^3 \approx x_1\}$ and $F = \{x_1 x_2 > 1, -x_2^2 > -1/2\}$. The constraints $E \cup F$ are transformed into the constraints $E' \cup F'$, where $E' = \{x_1^3 - x_1 \approx 0,\ x_1 x_2 - 1 - v_1 \approx 0,\ -x_2^2 + 1/2 - v_2 \approx 0\}$, and $F' = \{v_1 > 0, v_2 > 0\}$.

3.1 Elimination Ideal

Let E denote a set of polynomial equations over $\mathbb{Q}[\boldsymbol{x}, \boldsymbol{v}, \boldsymbol{w}]$. We assume the implicit constraints $\boldsymbol{v} > 0$ and $\boldsymbol{w} \geq 0$. Our goal is to detect unsatisfiability of E. Toward this end, we compute the Gröbner basis for the polynomials in E. Since the witnesses are likely to be in terms of $\boldsymbol{v}, \boldsymbol{w}$, we use an ordering with precedence $\boldsymbol{x} \succ \boldsymbol{v}, \boldsymbol{w}$ (that is, we are eliminating $\boldsymbol{x}$). If we are lucky, the computed Gröbner basis may already contain a witness for unsatisfiability of E.

Example 2. Consider the set $E = \{x_1^3 - x_1 \approx 0,\ x_1 x_2 - 1 - v_1 \approx 0,\ -x_2^2 + 1/2 - v_2 \approx 0\}$ and $F' = \{v_1 > 0, v_2 > 0\}$ from Example 1.

Computing a Gröbner basis for the polynomials in E (using a lexicographic ordering with precedence $x_1 \succ x_2 \succ v_1 \succ v_2$) and then removing all polynomials that contain variables x_1 and x_2, we are left with $\{v_1^3 + 3v_1^2 + 1/2 v_1 v_2 + 5/2 v_1 + 1/2 v_2 + 1/2\}$. This set is a basis for the ideal $\mathit{Elim}(\mathit{Poly}(E), \{x_1, x_2\})$.

The equation $v_1^3 + 3v_1^2 + 1/2 v_1 v_2 + 5/2 v_1 + 1/2 v_2 + 1/2 \approx 0$ is a witness for unsatisfiability: since the constraints $v_1 > 0, v_2 > 0$ imply that $v_1^3 + 3v_1^2 + 1/2 v_1 v_2 + 5/2 v_1 + 1/2 v_2 + 1/2 > 0$ necessarily, whereas Gröbner basis computation shows that it is necessarily zero. We can conclude that the original set of equations and inequalities (from Example 1) is also unsatisfiable.

The method of introducing slack variables and computing Gröbner basis with respect to an ordering that makes the slack variables smallest is not complete.

Example 3. If $E = \{x^2 - 2x + 2 \approx 0\}$, then the procedure described above would not introduce any new "slack" variables. The elimination ideal contains only the 0 polynomial, which results in a set of consistent equations ($0 \approx 0$). However, E is unsatisfiable over the reals.

We wish to make the procedure complete using the positivstellensatz characterization of unsatisfiability over the reals.

4 Positivstellensatz

The following result in real algebraic geometry characterizes the unsatisfiability of a conjunction of nonlinear equations and inequalities. Given a set Q of polynomials, the monoid $[Q]$ generated by Q is the set consisting of all finite products of polynomials in Q, and the cone generated by Q is the smallest set containing $[Q]$ and closed under addition and multiplication by "perfect-square polynomials", that is,

$$\begin{aligned}[Q] &= \{\Pi_{i \in I}\, q_i : q_i \in Q \text{ for all } i \in I\} \\ \mathit{Cone}[Q] &= \{\Sigma_{i \in I}\, p_i^2 q_i : q_i \in [Q], p_i \in \mathbb{Q}[\boldsymbol{x}] \text{ for all } i \in I\}\end{aligned}$$

Note that $1 \in [Q]$ for any set Q and $c^2 \in \mathit{Cone}[\emptyset]$ for all $c \in \mathbb{Q}$.

Theorem 1. *[Positivstellensatz [14, 20, 6]] Let P, Q, and R be sets of polynomials over $\mathbb{Q}[\boldsymbol{x}]$. The constraint*

$$\{p \approx 0 : p \in P\} \cup \{q \geq 0 : q \in Q\} \cup \{r \not\approx 0 : r \in R\}$$

is unsatisfiable (over the reals) iff there exist polynomials p, q, and r such that $p \in \mathit{Ideal}(P)$, $q \in \mathit{Cone}[Q]$, and $r \in [R]$ and $p + q + r^2 = 0$.

The theorem is difficult to use in its above form. However, we can replace the inequality constraints by equality constraints using slack variables and use the following corollary.

Corollary 1. *Let P be a set of polynomials from $\mathbb{Q}[\boldsymbol{x}, \boldsymbol{v}, \boldsymbol{w}]$. The constraint*

$$\{p \approx 0 : p \in P\} \cup \{v > 0 : v \in \boldsymbol{v}\} \cup \{w \geq 0 : w \in \boldsymbol{w}\}$$

is unsatisfiable iff there is a polynomial p' such that $p' \in \mathit{Ideal}(P) \cap \mathit{Cone}[\boldsymbol{v}, \boldsymbol{w}]$ and there is at least one monomial $c\mu$ in p' such that $c > 0$ and $\mu \in [\boldsymbol{v}]$.

Proof. The $\Leftarrow$ direction is obvious. For the $\Rightarrow$ direction, we use the Positivstellensatz to conclude that there exist polynomials p, q, and r such that $p \in \mathit{Ideal}(P)$, $q \in \mathit{Cone}[\boldsymbol{v}, \boldsymbol{w}]$, and $r \in [\boldsymbol{v}]$ and $p + q + r^2 = 0$. Note that $r^2 \in \mathit{Cone}[\boldsymbol{v}, \boldsymbol{w}]$ and hence the polynomial $q + r^2 \in \mathit{Cone}[\boldsymbol{v}, \boldsymbol{w}] \cap \mathit{Ideal}(P)$.

To prove that the polynomial $q + r^2$, equivalently $-p$, is the required p', we need to show that the polynomial $q + r^2$ contains a monomial $c\mu$ such that $c > 0$ and $\mu \in [\boldsymbol{v}]$. (Note that r^2 is such a monomial, but it could get canceled when added to q.) Suppose $p' = q + r^2$ and p' contains no such monomial $c\mu$. But then, if we set all $\boldsymbol{x}, \boldsymbol{w}$ to 0 and all $\boldsymbol{v}$ to 1 (or any positive number), then q will evaluate to something greater-than or equal to 0 (by definition of *Cone*), r^2 will evaluate to something strictly greater-than 0, and hence $q + r^2$ will evaluate to something strictly positive, whereas each monomial in p' will evaluate to either 0 or something negative (since every monomial $c\mu$ in p' has either $c < 0$ or a factor from $\boldsymbol{x}, \boldsymbol{w}$). This contradiction concludes the proof. ■

We have now reduced the problem of testing unsatisfiability of nonlinear constraints to deciding if, given a finite set P of polynomials over $\mathbb{Q}[\boldsymbol{x}, \boldsymbol{v}, \boldsymbol{w}]$, does there exist a polynomial $p \in \mathit{Ideal}(P) \cap \mathit{Cone}[\boldsymbol{v}, \boldsymbol{w}]$ that also contains a monomial $c\mu$ with $c > 0$ and $\mu \in [\boldsymbol{v}]$. The polynomial p is the witness to unsatisfiability. We need to search for the existence of such a p.

5 Searching a Witness, Searching an Ordering

It would be nice if we could establish that if such a witness p (to unsatisfiability) exists, then it would be present in the Gröbner basis of P. Note that this was indeed the case in Example 2. But this may not be true always. Fortunately, the property of fully reduced convergent rewrite systems discussed in Section 2 guarantees that this will be true *if* p were the minimal nonzero polynomial in $\mathit{Ideal}(P)$ with respect to the ordering $\succ$ used to construct the Gröbner basis for P. However, standard restrictions on term-orderings, such as monotonicity ($xy \succ x$), could mean that under no admissible ordering p were minimal.

Example 4. Consider $P = \{v + w_1 - 1, w_1 w_2 - w_1 + 1\}$. Note that we implicitly assume that $v > 0$ and $w_1, w_2 \geq 0$. The set P is a Gröbner basis for the ideal generated by P with respect to the lexicographic ordering with $v \succ w_1 \succ w_2$.

There is a witness polynomial, $v + w_1 w_2$, in $\mathit{Ideal}(P)$, but P itself does not contain any witness polynomial. In fact, none of the fully reduced canonical Gröbner basis computed using *any* lexicographic ordering contains a witness polynomial for this example.

The problem here is that the witness polynomial $v + w_1 w_2 \in \mathit{Ideal}(P)$ is not a minimal nonzero polynomial in $\mathit{Ideal}(P)$ under any ordering. However, if we could have $w_1 \succ w_1 w_2$ (contrary to the requirements of term orderings), then Gröbner basis computation “could” eliminate w_1 by adding the two polynomials in P and obtain the witness.

We know from Corollary 1 that the witness polynomial p is in $\mathit{Ideal}(P) \cap \mathit{Cone}[\boldsymbol{v}, \boldsymbol{w}]$ and hence it is of the form $p_1^2 \nu_1 + p_2^2 \nu_2 + \cdots + p_k^2 \nu_k$ where, for all i, $\nu_i \in [\boldsymbol{v}, \boldsymbol{w}]$ and p_i is an arbitrary polynomial. There are two issues with making this minimal:
(i) The power-products ν_i can not be smaller than the individual variables contained in them. This was illustrated in Example 4.
(ii) The squares p_i^2 can not be smaller than any of the monomials or variables contained in them.

We solve both these problems using the idea of introducing new definitions and new variables. The new variables will be forced to be smaller than the other variables.

Example 5. Consider $P = \{v + w_1 - 1, w_1w_2 - w_1 + 1\}$ from Example 4. If we introduce a new definition $D = \{w_1w_2 \approx w_3\}$, and we choose an ordering in which $v \succ w_1 \succ w_2 \succ w_3$, then $GB_{\succ}(P \cup \{w_1w_3 - w_3\}) = \{v + w_3, w_1 - w_3 - 1, w_2w_3 + w_2 - w_3\}$. The witness $v + w_3$ is present in the above fully reduced Gröbner basis.

Next consider $P = \{w_1^2 - 2w_1w_2 + w_2^2 + 1\}$. There is no polynomial with all coefficients positive in $Ideal(P)$ [11]. But there is a witness containing perfect squares: $(w_1 - w_2)^2 + 1$. If we introduce the definition $D = \{(w_1 - w_2)^2 \approx w_3\}$ and compute the Gröbner basis for $P \cup \{(w_1 - w_2)^2 - w_3\}$, we get $\{w_3 + 1, w_1^2 - 2w_1w_2 + w_2^2 - w_3a\}$. The witness $w_3 + 1$ is present in the above fully reduced Gröbner basis.

5.1 Completeness Relative to an Oracle

If an oracle can identify the monomials $p_i^2\nu_i$ that are present in the witness, then the introduction of definitions and computing Gröbner basis is a sound and complete method for detecting unsatisfiability of nonlinear constraints.

If all coefficients in a polynomial are positive (negative) when it is written in its sum of monomials normal form representation, then we call it a positive (negative) polynomial.

Theorem 2 (Relative Completeness). *Let P be a set of nonlinear equations over $\mathbb{Q}[\boldsymbol{x}, \boldsymbol{v}, \boldsymbol{w}]$. Let $\Sigma_{i=1}^{k} p_i^2\nu_i$ be a witness for unsatisfiability of $\{p \approx 0 : p \in P\} \cup \{v > 0 : v \in \boldsymbol{v}\} \cup \{w \geq 0 : v \in \boldsymbol{w}\}$. Let D be the set of definitions $\{p_i^2\nu_i - w_i' : i = 1, \ldots, k\}$, where w_i' are new constants.*

Then, there exists a precedence $\succ'$ on $\boldsymbol{w'}$ such that $GB_{\succ}(P \cup D)$ will contain a positive or negative polynomial over $[\boldsymbol{w'}]$, where $\succ$ extends $\succ'$ such that the only power-products smaller than any w' are possibly other variables in $\boldsymbol{w'}$.

Proof. By Corollary 1, the polynomial $\Sigma_{i=1}^{k} p_i^2\nu_i$ is in the ideal generated by P. Therefore, the linear polynomial $w_1' + \cdots + w_k'$ is in the ideal generated by $P \cup D$. Since the ordering $\succ$ guarantees that linear polynomials over $\boldsymbol{w'}$ are smaller than other polynomials, it follows that the polynomial $w_1' + \cdots + w_k'$ is in the ideal generated by $GB' = GB \cap \mathbb{Q}[\boldsymbol{w'}]$ (property of fully reduced convergent systems). If this polynomial is in GB', we are done.

If not, let $p' = c_1w_1' + \cdots + c_kw_k'$ be the minimal size (that is, with least cardinality of $\{i : c_i \neq 0\}$) linear positive polynomial in the ideal generated by GB'. We claim that p' will be in GB' if we choose $\succ$ so that each constant in $\{w_i' : c_i \neq 0\}$ has lower precedence than other variables. Suppose p' is not in GB'. Then p' is reducible by some polynomial q' in GB'. The polynomial $q' = d_1w_1' + \cdots + d_kw_k'$ is necessarily linear. Wlog assume that $c_1 > 0$ and $d_1 > 0$. (i) If there is a j s.t. $d_j \neq 0$, but $c_j = 0$, then w_j' is greater than all constants in p', and hence q' can not reduce p'. (ii) Consider $p' - c_j q'/d_j$, where $j = min\{c_l/d_l : d_l > 0, l = 1, \ldots, k\}$. Note that if q' is positive/negative, then we are done. Hence, we assume that q' is not positive, and consequently j is well-defined. Now, clearly $p' - c_j q'/d_j$ is positive, and smaller than p' in size, a contradiction. This completes the proof. ■

As we have seen in Section 2, there are several orderings $\succ$ that can extend $\succ'$ in the required way. One example is the total degree lexicographic ordering with precedence $\boldsymbol{x} \succ \boldsymbol{v} \succ \boldsymbol{w} \succ \boldsymbol{w'}$.

6 The Inference Rules

Following the presentation of Gröbner basis computation as a critical-pair completion procedure [2, 3], we present the inference rules that describe a procedure for testing unsatisfiability of nonlinear constraints. It consists of rules that compute Gröbner basis and rules that insert new definitions, which are required for identifying witnesses.

The inference rules operate on states. A state (V, P) consists of a set P of polynomials and a set V of variables occurring in P. We also implicitly maintain subsets $V_{>0}$ and $V_{\geq 0}$ of V. The initial state is $(\{\boldsymbol{x}, \boldsymbol{v}, \boldsymbol{w}\}, P)$, where P is the set of polynomials obtained by adding slack variables to the original nonlinear constraints as described in Section 3 before and $V_{>0} = \{\boldsymbol{v}\}$ and $V_{\geq 0} = \{\boldsymbol{v}, \boldsymbol{w}\}$.

We use an ordering $\succ$ on polynomials. As we observed in Section 3, it is a good heuristic to use a precedence $\boldsymbol{x} \succ \boldsymbol{v}, \boldsymbol{w}$; more generally, $V - V_{\geq 0} \succ V_{\geq 0}$. We also assume that the ordering guarantees that *only linear polynomials are smaller than a linear polynomial*, cf. Theorem 2. When we write a polynomial as $c_0\mu_0 + p$, then we implicitly mean that μ_0 is the largest power-product, that is, $\mu_0 \succ p$ and $c_0 \neq 0$. As we add new definitions, such as $p - w'$, where $w' \in V^{new}$ is a new variables, we need to extend the ordering. We can choose any extension that guarantees that $p \succ w'$. Note that the new variable w' can be added to either $V - V_{\geq 0}$ or $V_{\geq 0}$. In most cases, we can extend the ordering without violating the invariant that $V - V_{\geq 0} \succ V_{\geq 0}$.

The inference rules are presented in Table 1. The inference rules *Simplify*, *Deduce*, and *Delete* are used for constructing a Gröbner basis of the polynomials in the set P. Note that the rules for normalizing an arbitrary polynomial expression into a sum of monomial form (with the largest monomial moved to the left and its coefficient normalized to 1) are left implicit in the presentation here; they have been formalized in previous presentations of Gröbner basis algorithm as completion [2, 3]. The collapse rule is subsumed by the *Simplify* rule.

The novelty in the inference rules in Table 1 comes from the rules that add new definitions. We use the largest monomials in P to determine the terms to be named by new variables. The notation $|\mu|$ denotes the total degree of the power-product μ. The notation $[V]^{0,1}$ denotes power-products in which every variable in V occurs with degree at most one.

The *Extend1* rule introduces a new nonnegative variable w' as a name for leading power-product μ_0 that is known to be nonnegative, that is, $\mu_0 \in [V_{\geq 0}]$.

Simplify:	$\dfrac{(V, P \cup \{c_0\mu_0 + p, q\})}{(V, P \cup \{c_0\mu_0 + p, q'\})}$	if $q \rightarrow_{c_0\mu_0 \rightarrow -p} q'$
Deduce:	$\dfrac{(V, P' = P \cup \{c_0\mu_0 + p, d_0\nu_0 + q\})}{(V, P' \cup \{c_0\mu' q - d_0\nu' p\})}$	if $\mu_0\mu' = \nu_0\nu' = lcm(\mu_0, \nu_0) \neq \mu_0\nu_0$
Delete:	$\dfrac{(V, P \cup \{0\})}{(V, P)}$	
Extend1:	$\dfrac{(V, P' = P \cup \{\mu_0 + p\})}{(V \cup \{w'\}, P' \cup \{\mu_0 - w'\})}$	if $\mu_0 \in [V_{\geq 0}]$, $w' \in V_{\geq 0}^{new}$
Extend2:	$\dfrac{(V, P)}{(V \cup \{x'\}, P \cup \{\nu_0 + \alpha\nu_1 - x'\})}$	if $\langle \nu_0, \nu_1 \rangle$ occurs in P, $x' \in V^{new}$
Extend3:	$\dfrac{(V, P' = P \cup \{\mu_0 + p\})}{(V \cup \{x'\}, P' \cup \{\nu_0 - x'\})}$	if $\nu_0^2\nu_0' = \mu_0\mu_0'$, $\nu_0' \in [V_{\geq 0}]^{0,1}$, $x' \in V^{new}$, $\lvert\nu_0\rvert > 1$
Detect:	$\dfrac{(V, P' = P \cup \{c_0\mu_0 + p\})}{(V, P \cup \{c_0\mu_0, p\})}$	if $c_0\mu_0 + p$ is a positive/negative polynomial over $[V_{\geq 0}]$
Witness:	$\dfrac{(V, P \cup \{c\mu\})}{\perp}$	if $\mu \in [V_{>0}]$, $c \neq 0$

Table 1. Inference rules for detecting unsatisfiability of nonlinear constraints

The *Extend2* rule introduces a new name for $\nu_0 + \alpha\nu_1$, in the hope that some polynomial of the form $(\nu_0 + \alpha\nu_1 + p)^2$ appears in the unsatisfiability witness. We say that a power-product ν *occurs directly in* P if there is polynomial in P which contains a monomial with power-product ν. We generalize this notion and say that a power-product ν *occurs in* P with factor $\nu_0' \in [V_{\geq 0}]^{0,1}$ if there exists $\mu_0 \in [V]$ such that $\mu_0 | \nu\nu_0'$ and μ_0 occurs directly in P. (As a heuristic rule, we prefer cases when $\mu_0 = \nu\nu_0'$.) Finally, we say that a pair of power-products $\langle \nu_0, \nu_1 \rangle$ *occurs in* P if (i) $\nu_0\nu_1$ occurs in P with factor ν_0', and (ii) either $\nu_0^2\nu_0'$ occurs in P with factor 1 or $\nu_0^3\nu_0'/w$ occurs in P with factor 1 for some $w \in V_{\geq 0}$, and (iii) either $\nu_1^2\nu_0'$ occurs in P with factor 1 or $\nu_1^3\nu_0'/w$ occurs in P with factor 1 for some $w \in V_{\geq 0}$.

In the *Extend2* rule, the symbol α denotes a (real) rigid variable that needs to be instantiated by a constant in $\mathbb{Q}$. We use symbolic α here and continue application of the inference rules by working over the field $\mathbb{Q}(\alpha)$ (instead of just $\mathbb{Q}$). As soon as we obtain a nontrivial expression in $\mathbb{Q}(\alpha)$, we instantiate α by the zero of that expression. The *Extend3* rule says that we need not bother about finding ν_1 (and α) if total degree of ν_0 is greater-than one.

We have not shown that the new variables introduced in *Extend* rules are pushed appropriately into the sets $V_{\geq 0}$ or $V_{>0}$.

Example 6. Consider the set $P = \{v + w_1 - 1, w_1 w_2 - w_1 + 1\}$ from Example 4. Assuming $v > 0, w_1 \geq 0, w_2 \geq 0$, one possible derivation to $\perp$ is shown below.

To illustrate the other extension rules, we also show the derivation with a new set $P = \{x_1^2 - 2x_2 + 3, x_1x_2 - x_2^2\}$ below.

i	Polynomials P_i	Transition Rule
0	$\{v + w_1 - 1, w_1w_2 - w_1 + 1\}$	
1	$\{v + w_1 - 1, w_1w_2 - w_1 + 1, w_1w_2 - w'\}$	**Extend1**
2	$\{v + w_1 - 1, -w_1 + w' + 1, w_1w_2 - w'\}$	**Simplify**
3	$\{v + w', -w_1 + w' + 1, w_1w_2 - w'\}$	**Simplify**
4	$\{v, w', -w_1 + w' + 1, w_1w_2 - w'\}$	**Detect**
5	$\bot$	**Witness**

i	Polynomials P_i	Rule
0	$P = P_0 = \{x_1^2 - 2x_2 + 3, x_1x_2 - x_2^2\}$	
1	$P_0 \cup \{x_1 + \alpha x_2 - y_1\}$	**Extend2**
2	$\{x_2^2 - 2\alpha x_2y_1 + y_1^2 - 2x_2 + 3, -(\alpha + 1)x_2^2 + y_1x_2, x_1 + \alpha x_2 - y_1\}$	**Simplify**
3	$\{x_2^2 + 2x_2y_1 + y_1^2 - 2x_2 + 3, y_1x_2, x_1 - x_2 - y_1\}$	$\alpha \mapsto \mathbf{-1}$
4	$\{x_2^2 + y_1^2 - 2x_2 + 3, y_1x_2, x_1 - x_2 - y_1\}$	**Simplify**
5	$P_4 \cup \{x_2 + \beta - y_2\}$	**Extend2**
6	$\{y_1^2 + y_2^2 - (2\beta + 2)y_2 + (\beta^2 + 2\beta + 3), y_1y_2 - \beta y_1, \ldots\}$	**Simplify**
7	$\{y_1^2 + y_2^2 + 2, y_1y_2 + y_1, \ldots\}$	$\beta \mapsto \mathbf{-1}$
8	$\{y_1^2, y_2^2, 2, y_1y_2 + y_1, \ldots\}$	**Detect**
9	$\bot$	**Witness**

Lemma 1. *Suppose $(V, P) \vdash (V', P')$ is a one-step application of the inference rules. Then, P is satisfiable over the reals iff P' is satisfiable over the reals.*

Theorem 3 (Refutational completeness). *Suppose P_0 is unsatisfiable and $(V_0, P_0) \vdash^* (V, P)$ is a derivation such that $P \neq \bot$. Then, there exists a derivation from (V, P) to $\bot$.*

Proof. By Lemma 1 we conclude that P is unsatisfiable. Therefore, by Corollary 1 we know that there exist several witness polynomials $wp = \Sigma_i p_i^2 \nu_i \in Ideal(P) \cap Cone[V_{\geq 0}]$ for unsatisfiability of P. Assume that $p_0 \succeq p_1 \succeq p_2 \succeq \cdots$; and whenever $p_i \not\succ p_{i+1}$ then $\nu_i \succeq \nu_{i+1}$. Let μ be the leading power-product (LPP) of the largest polynomial in P that divides the leading power-product of $p_0^2\nu_0$. If no such μ exists, then μ is set to 1. Now, we say that the witness polynomials wp (and the corresponding μ) is *bigger than* wp' (and the corresponding μ') if either the multiset $\{|p_0|, |p_1|, \ldots\}$ of the sizes of the p_i's is greater-than the multiset of the sizes $\{|p'_0|, |p'_1|, \ldots\}$; or these are equal and the size of μ' is greater-than the size of μ. (Note here that the size of a polynomial is just the multiset of the sizes of its monomials and the size of a monomial is the total-degree of its power-product.) This ordering on witnesses is clearly well-founded and hence a minimal is well-defined. Let $wp = \Sigma_i p_i^2 \nu'_i$ be such a minimal witness.

Note that none of the inference steps can increase the size of the minimal witness. We will show below that either we can always reduce the size of the minimal witness by applying an appropriate inference rule, or reach $\bot$.

Since we have the inference rules for constructing a Gröbner basis, we can assume that the polynomials in P form a Gröbner basis. Hence, there exists a polynomial $\mu_0 - p \in P$ such that $\mu_0 | LPP(p_0^2 \nu_0')$. If $\nu_0 = LPP(p_0)$, then we should have $\mu_0 | \nu_0^2 \nu_0'$, or equivalently, $\mu_0 \mu_0' = \nu_0^2 \nu_0'$ for some μ_0'.

Case 1. $|\nu_0| > 1$. In this case, the *Extend3* rule is applicable. Using this rule, we can introduce a variable equivalent to ν_0. In the minimal witness, if we replace ν_0 by this variable, then we get a smaller witness.

Case 2. $|\nu_0| = 0$. In this case, $\mu_0 | \nu_0'$ and hence $\mu_0 \in [V_{\geq 0}]$. Hence the *Extend1* rule is applicable. If $|\mu_0| > 1$, we can again get a smaller witness as in Case 1. If $|\mu_0| = 1$, then the rule $\mu_0 - p$ is necessarily linear (because the ordering guarantees that only linear polynomials are smaller than linear polynomials). Also, each p_i is a constant. Let $c_i = p_i^2$. Consider two cases now.
Case 2.1. There is a rewrite step using a nonlinear polynomial in the derivation $\Sigma_i c_i \nu_i' \rightarrow_P^* 0$. Wlog assume ν_0' is rewritten to $c'' \nu_0'' + \ldots$ by linear rules, and ν_0'' is reducible by a nonlinear rule. Using *Extend1* rules, we make ν'' bigger than ν_0'. As a result, in the new system, the nonlinear rule directly reduces the witness. Hence, the size of the witness remains unchanged, but the the size of the corresponding μ_0 increases (see the example following the proof).
Case 2.2. There is a no rewrite step using a nonlinear polynomial in the derivation $\Sigma_i c_i \nu_i' \rightarrow_P^* 0$. In this case, the linear polynomials in P are unsatisfiable. Therefore, there exists a smallest linear witness $\Sigma_i c_i w_i$ s.t. $c_i > 0$ and $w_i \in V_{\geq 0}$ (and there is some j s.t. $w_j \in V_{>0}$). Again, using the *Extend1* rule, we can make the variables w_i appearing in this witness smaller. As a result, the polynomial $\Sigma_i c_i w_i$ will appear in the set P and we would detect inconsistency (as in the proof of Theorem 2).

Case 3. $|\nu_0| = 1$. Our assumption on the ordering guarantees that all p_i's in the witness $wp = \Sigma_{i \geq 0} p_i^2 \nu_i'$, where $\nu_i' \in [V_{\geq 0}]^{0,1}$ are linear polynomials. Suppose $p_i = c_{i0} w_{i0} + \cdots + c_{il} w_{il}$. In the monomial expansion of $p_i^2 \nu_i'$, we distinguish between the *cross-product terms*, which are of the form $2 c_{ij} d_{ik} w_{ij} w_{ik} \nu_i'$ (for $j \neq k$), and the *square terms*, which are of the form $c_{ij}^2 w_{ij}^2 \nu_i'$. We wish to identify w_{ij} and w_{ik} and apply the *Extend2* rule. The problem is that the cross-product terms can cancel out in the summation $\Sigma_{i \geq 0} p_i^2 \nu_i'$ and hence the witness wp may not contain any monomial whose power-product is, for instance, $w_{ij} w_{ik} \nu_i'$ (and hence the polynomials in P also may not contain this power-product).

Case 3.1. There is no monomial in wp whose power-product comes from a cross-product term. In this case the polynomial wp is itself of the form $\Sigma_i q_i^2 \nu_i'$, where q_i's are all monomials now. We conclude that the original p_i's are necessarily monomials: if not, then the new witness would be a smaller witness. If $|q_0^2 \nu_0'| > 1$, we can use *Extend1* on the leading monomial $q_0^2 \nu_0'$ and reduce the size of the witness. If $|q_0^2 \nu_0'| = 1$, the witness polynomial wp is linear. We make the variables that occur in wp minimal using *Extend1*. This will cause the witness polynomial to appear explicitly in P, whence we can use detect and witness to reach the $\bot$ state.

Case 3.2. There is a monomial in wp whose power-product comes from a cross-product term. Let the power-product be $w_{ij} w_{ik} \nu_i'$. If both $w_{ij}^2 \nu_i'$ and $w_{ik}^2 \nu_i'$ are also present in wp, then they also necessarily occur in P, and hence, the *Extend2* rule would be applicable and it would introduce the polynomial $(w_{ij} +$

$\alpha w_{ik}) - w'$ for some new variable w'. If α is appropriately instantiated, this reduces the witness size.

Suppose $w_{ij}^2 \nu_i'$ is not present in *wp*. This implies that it was canceled in the summation. It can only be canceled by a cross-product term. That cross-product term can only come from something of the form $(\cdots + w_{ij} + w + \cdots)^2 w_{ij}(\nu_i'/w)$ (ignoring coefficients). But this implies that there will be a square term of the form $w_{ij}^3(\nu_i'/w)$. This term can not be canceled by any other cross-product term. Hence we can detect w_{ij} by searching for the occurrence of either $w_{ij}^2 \nu_i'$ or $w_{ij}^3(\nu_i'/w)$. In the latter case, note that $w, w_{ij} \in V_{\geq 0}$. This completes the proof. ■

To illustrate the second case of the above proof, consider $P = \{v - v_1 + v_2, v_1 w - v_2 w + 1\}$. The witness for unsatisfiability is $vw + 1$. We notice that $vw + 1 \rightarrow v_1 w - v_2 w + 1 \rightarrow 0$ by P. Here the nonlinear polynomial in P is used after reducing the witness using the linear rules. Hence, we apply *Extend1* to make v smaller than v_1 by adding $v - v'$. After closing under the Gröbner basis rules, the result is $P = \{v_1 - v_2 - v', v'w + 1\}$ and the new witness is $v'w + 1$. Now, $\mu_0 = v'w$, which divides the leading power-product $v'w$ of the witness. The size of μ_0 that reduces $LPP(wp)$ has increased from 1 to 2.

6.1 Other Remarks and Future Work

The *Extend* rules can potentially introduce infinitely many new definitions in a derivation, thus leading to nontermination. Specifically, there are infinitely many choices in the application of the *Extend3* rule. If effective degree bounds on the witness polynomial (obtained using the Positivstellensatz) are known, then the application of the *Extend* rules (*Extend3* in particular) can be restricted to enforce termination, resulting in a decision procedure. The problem of obtaining effective degree bounds for the Positivstellensatz is still open [19]. We conjecture that the *Extend3* inference rule can be restricted to use only the minimal instance of ν_0 (that is, only the most-general unifier of $\nu_0^2 \nu_0' = \mu_0 \mu_0'$) and that this could be used to obtain a terminating set of inference rules that are also complete. This could provide an alternate approach to obtaining degree bounds for the Positivstellensatz.

The process of searching for the witnesses can be understood in the context of the Gröbner basis P as follows. The monomials in a polynomial can be colored by *pos* and *unknown* based on whether we know if they are necessarily nonnegative or not. For example, in $x^2 - 2x + 2$, the monomials x^2 and 1 are *pos*, while $-2x$ is *unknown*. The goal is to construct a polynomial in the ideal of P in which the *unknown* monomials have been eliminated. There are two ways to eliminate the *unknown* monomials. First, they can be captured as a cross-product term in a perfect-square polynomial. For example, $(x-1)^2$ captures $-2x$. The inference rule *Extend2* aims to achieve this. Second, the monomials can be canceled when constructing a polynomial in the ideal of P. For example, consider the polynomials $v^2 - w_1 w_2 + 1$ and $w_1 w_2 + w_3 - 1$. The monomial $-w_1 w_2$ can be canceled by adding the two polynomials. This is reflected in the "critical-pair" overlap between $-w_1 w_2$ and $w_1 w_2$. However, since $-w_1 w_2$ is not the largest monomial in the first polynomial, Gröbner basis computation will not perform this operation.

The *Extend1* rule aims to make the leading monomials smaller, so that the inner monomials such as $-w_1 w_2$ are exposed for critical-pair computation. This is clearly a generalization of the pivoting step in Simplex. The colored monomials can also be used to restrict the choices in the application of the *Extend* rules.

The value of the proposed approach for unsatisfiability testing of nonlinear constraints arises from the fact that it successfully solves the "easy" instances cheaply. A lot of the easy unsatisfiable instances are detected just by adding slack variables and then projecting the polynomial ideal onto the slack variables. This was illustrated in Example 2. In most of the other instances, we noticed that we need to apply the *Extend* rules at most one or two times to detect inconsistency. We also remark here that several other decision procedures for nonlinear constraints tend to do expensive computations on relatively simple instances. For example, if we have two constraints, $p > 0$ and $p < 0$ over $\mathbb{Q}[x_1, \ldots, x_n]$, then a naive procedure based on cylindrical algebraic decomposition, for instance, would attempt to create a decomposition of $\mathbb{R}^n$ based on the polynomial p. For sufficiently large p, this process could fail (run out of memory or time). It is easy to see that our procedure will generate the unsatisfiability witness $v_1 + v_2$, where v_1 and v_2 are the two slack variables, in just one inference step.

We believe that fast implementations for unsatisfiability testing of nonlinear constraints can be obtained by implementing (an extension or variant of) the inference rules presented here. One missing aspect is detecting satisfiable instances quickly. However, simple ideas to detect satisfiable instances can be integrated. In particular, we can use the fact that *every odd degree polynomial has a zero* to eliminate an old variable when we introduce a new variable. This can be done if the new variable names an odd-degree polynomial over the old variable.

Example 7. Consider $P = \{x^2 + 2x - 1\}$. We introduce a new variable y for $x + 1$ to get $P_1 = \{y^2 - 2, x + 1 - y\}$. Now, we can eliminate x from this set and just have $P_2 = \{y^2 - 2\}$. The reason is that if P_2 is satisfiable, then we are guaranteed that there will exist an assignment for x (since $x + 1 - y$ has an odd-degree in x). Since P_2 can be detected to be satisfiable, we can conclude that P is satisfiable.

7 Conclusion

We have presented an algebraic semi-decision procedure, based on Gröbner basis computation and extension rules, for detecting unsatisfiability of nonlinear constraints. The procedure is given as a set of inference rules that are sound and refutationally complete. Our approach has the potential of resulting in fast solvers for testing unsatisfiability of nonlinear constraints. This is especially significant in the context of satisfiability testing tools [21, 9, 1] that are being increasingly used for program analysis. There is also much recent progress in computational aspects of real algebraic geometry and computational tools for building a sums-of-squares representation using semi-definite programming [16, 15, 4], which indicates that our work will be actively refined and developed further in the future. We are presently exploring the effectiveness of the new procedure for improving the implementation of the abstraction algorithm for hybrid systems [23].

References

[1] G. Audemard, P. Bertoli, A. Cimatti, A. Kornilowicz, and R. Sebastiani. A SAT based approach for solving formulas over boolean and linear mathematical propositions. In *CADE*, volume 2392 of *LNCS*, pages 195–210. Springer, 2002.

[2] L. Bachmair and H. Ganzinger. Buchberger's algorithm: A constraint-based completion procedure. In *CCL*, volume 845 of *LNCS*. Springer, 1994.

[3] L. Bachmair and A. Tiwari. D-bases for polynomial ideals over commutative noetherian rings. In *RTA*, volume 1103 of *LNCS*, pages 113–127. Springer, 1997.

[4] S. Basu and L. Gonzalez-Vega, editors. *Algorithmic and Quantitative Real Algebraic Geometry*, volume 60 of *DIMACS Series in DMTCS*, 2003.

[5] S. Basu, R. Pollack, and M.-F. Roy. On the combinatorial and algebraic complexity of quantifier elimination. *J. of the ACM*, 43(6):1002–1045, 1996.

[6] J. Bochnak, M. Coste, and M.-F. Roy. *Real Algebraic Geometry*. Springer, 1998.

[7] G. E. Collins. Quantifier elimination for the elementary theory of real closed fields by cylindrical algebraic decomposition. In *Proc. 2nd GI Conf. Automata Theory and Formal Languages*, volume 33 of *LNCS*, pages 134–183. Springer, 1975.

[8] R. S. Datta. Using computer algebra to compute Nash equilibria. In *Intl. Symp. on Symbolic and Algebraic Computation, ISSAC 2003*, pages 74–79, 2003.

[9] L. de Moura, S. Owre, H. Rueß, J. Rushby, and N. Shankar. The ICS decision procedures for embedded deduction. In *IJCAR*, volume 3097 of *LNAI*. Springer, 2004.

[10] N. Dershowitz and Z. Manna. Proving termination with multiset orderings. *Communications of the ACM*, 22(8):465–476, 1979.

[11] M. Einsiedler and H. Tuncel. When does a polynomial ideal contain a positive polynomial? *J. Pure Appl. Algebra*, 164(1-2):149–152, 2001.

[12] J. Harrison. *Theorem proving with the real numbers*. Springer-Verlag, 1998.

[13] H. Hong. Quantifier elimination in elementary algebra and geometry by partial cylindrical algebraic decomposition version 13, 1995. `http://www.gwdg.de/~cais/systeme/saclib,www.eecis.udel.edu/~saclib/`.

[14] J. L. Krivine. Anneaux preordonnes. *J. Anal. Math.*, 12:307–326, 1964.

[15] P. A. Parrilo. SOS methods for semi-algebraic games and optimization. In *HSCC 2005*, volume 3414 of *LNCS*, page 54. Springer, 2005.

[16] S. Prajna, A. Papachristodoulou, and P. A. Parrilo. SOSTOOLS: Sum of Square Optimization Toolbox, 2002. `http://www.cds.caltech.edu/sostools`.

[17] S. Ratschan. Applications of quantified constraint solving over the reals: Bibliography, 2004. `http://http://www.mpi-sb.mpg.de/~ratschan/appqcs.html`.

[18] J. Renegar. On the computational complexity and geometry of the first order theory of the reals. *J. of Symbolic Computation*, 13(3):255–352, 1992.

[19] M.-F. Roy. Degree bounds for Stengle's Positivstellensatz, 2003. Network workshop on real algebra. `http://ihp-raag.org/index.php`.

[20] G. Stengle. A Nullstellensatz and a Positivstellensatz in semialgebraic geometry. *Math. Ann.*, 207:87–97, 1974.

[21] A. Stump, C. W. Barrett, and D. L. Dill. CVC: A cooperating validity checker. In *CAV*, volume 2404 of *LNCS*, pages 500–504. Springer, 2002.

[22] A. Tarski. *A Decision Method for Elementary Algebra and Geometry*. University of California Press, 1948. Second edition.

[23] A. Tiwari and G. Khanna. Series of abstractions for hybrid automata. In *HSCC*, volume 2289 of *LNCS*, pages 465–478. Springer, 2002.

[24] V. Weispfenning. The complexity of linear problems in fields. *J. of Symbolic Computation*, 5, 1988.