

On Locally Minimal Nullstellensatz Proofs

Leonardo de Moura
Microsoft Research
One Microsoft Way
Redmond, WA 98052, USA
leonardo@microsoft.com

Grant Olney Passmore
LFCS, University of Edinburgh
10 Crichton Street
Edinburgh EH8 9AB, Scotland, UK
g.passmore@ed.ac.uk

ABSTRACT

Hilbert’s weak Nullstellensatz guarantees the existence of algebraic proof objects certifying the unsatisfiability of systems of polynomial equations not satisfiable over any algebraically closed field. Such proof objects take the form of ideal membership identities and can be found algorithmically using Gröbner bases and cofactor-based linear algebra techniques. However, these proof objects may contain redundant information: a proper subset of the equational assumptions used in these proofs may be sufficient to derive the unsatisfiability of the original polynomial system. For using Nullstellensatz techniques in SMT-based decision methods, a *minimal* proof object is often desired. With this in mind, we introduce a notion of *locally* minimal Nullstellensatz proofs and give ideal-theoretic algorithms for their construction.

Categories and Subject Descriptors

I.2.3 [Deduction]: Automated Reasoning

Keywords

Gröbner bases, non-linear arithmetic, satisfiability modulo theories, decision procedures, SMT, formal proofs, computer algebra, automated reasoning

1. INTRODUCTION

Modern Satisfiability Modulo Theories (SMT) solvers have application in the verification of software and hardware artifacts and are seeing increasing use in areas as diverse as planning and formalised mathematics. At a high-level, an SMT solver consists of an orchestrated combination of a DPLL based SAT solver and a number of satellite “theory” solvers (*T*-solvers) which implement decision methods for decidable elementary theories such as linear integer and real arithmetic, bit-vector arithmetic, and the theory of uninterpreted functions with equality. The effectiveness of an SMT decision loop depends crucially upon the ability of its

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

SMT ’09 August 2-3, 2009, Montreal, CA

Copyright 2009 ACM 978-1-60558-484-3 ...\$10.00.

T-solvers to identify “small” inconsistent components of formulas [3, 6]. Thus when one develops a new *T*-solver, the investigation of techniques for finding such “small” inconsistent subformulas is an important concern.

Many verification problems, such as those arising from hybrid systems, embedded and physical systems, and numerical algorithms, require deciding the satisfiability of non-linear arithmetical formulas over the real numbers. By Tarski [11], it is well known that the full elementary theory of polynomial real arithmetic is decidable, but classical (quantifier elimination) approaches to this problem are prohibitively expensive for formulas found in real applications. Recently, a number of new (semi-) decision procedures for the quantifier-free fragment of this theory have been proposed [12, 9, 8]. All of them use a Gröbner bases procedure as a subroutine.

The work described in this paper can be seen as a contribution to the development of effective *T*-solvers for non-linear polynomial arithmetic over both the real and complex numbers. In particular, we consider the problem of finding “small” proof objects certifying the unsatisfiability of systems of polynomial equations over any algebraically closed field. We consider this problem within the context of Gröbner basis calculations.

We start by defining algebraic notions of proof minimality and redundancy, and two proof minimization transformations: *cofactor-subsumption* and *basis-subsumption*. Then, we describe a simple algorithm for extracting proof objects from a Gröbner bases procedure. Our algorithm is optimal for the linear case, that is, it produces only non-redundant proof objects. Finally, we show that a restricted form of cofactor subsumption can be efficiently implemented and used to reduce the amount of redundancy in our proof objects.

2. BACKGROUND

Given $\{p_1, \dots, p_k\}$, a finite subset of $\mathbb{Q}[\vec{x}]$, the polynomial ideal $\mathcal{I}(\{p_1, \dots, p_k\})$ is the set of polynomials

$$\left\{ \sum_{i=1}^k p_i q_i \mid q_i \in \mathbb{Q}[\vec{x}] \right\}.$$

Hilbert’s weak Nullstellensatz states that any set of polynomial equations $\{p_1 \simeq 0, \dots, p_k \simeq 0\}$ is unsatisfiable over \mathbb{C}^n iff $\mathcal{I}(p_1, \dots, p_k) = \mathbb{Q}[\vec{x}]$. Therefore, if $\varphi = \bigwedge_{i=1}^k p_i \simeq 0$, then $\langle \mathbb{C}, +, -, *, 0, 1 \rangle \models \neg \exists \vec{x} (\varphi(\vec{x}))$ iff $\exists q_1, \dots, q_k \in \mathbb{Q}[\vec{x}]$ s.t. $\sum_{i=1}^k p_i q_i = 1$. An element $x_1^{i_1} \dots x_n^{i_n}$ in $\mathbb{Q}[x_1, \dots, x_n]$ is called a *power-product* (or *term*), and an element $c x_1^{i_1} \dots x_n^{i_n}$ with $c \in \mathbb{Q}$ and $x_1^{i_1} \dots x_n^{i_n}$ a power-product is called a *monomial*. We say a monomial is *monic* if $c = 1$. (This terminol-

ogy is not universally agreed upon.) We use \mathbb{M} to denote the set of all power-products in $\mathbb{Q}[x_1, \dots, x_n]$. From hereafter, we use p, q and r to denote polynomials, m to denote power-products and monic monomials, c to denote coefficients, and cm to denote monomials. We say a power-product $x_1^{i_1} \dots x_n^{i_n}$ contains x_k if $i_k > 0$. Given two power-products $m_1 = x_1^{i_1} \dots x_n^{i_n}$ and $m_2 = x_1^{j_1} \dots x_n^{j_n}$, $m_1 m_2$ denotes the power-product $x_1^{i_1+j_1} \dots x_n^{i_n+j_n}$, if $i_k \geq j_k$ for $k \in \{1, \dots, n\}$, then $\frac{m_1}{m_2}$ denotes the power-product $x_1^{i_1-j_1} \dots x_n^{i_n-j_n}$, and the *least common multiple* $\text{lcm}(m_1, m_2)$ of m_1 and m_2 is the power product $x_1^{\max(i_1, j_1)} \dots x_n^{\max(i_n, j_n)}$. We say a polynomial p contains the power-product m if p contains the monomial cm for some coefficient $c \neq 0$. Given a polynomial $p = c_1 m_1 + \dots + c_n m_n$ and a monomial cm , we use cmp to denote the polynomial $(c_1 c)m_1 m + \dots + (c_n c)m_n m$. Similarly, given a polynomial $p = c_1 m_1 + \dots + c_n m_n$ and a polynomial q , we use pq to denote the polynomial $c_1 m_1 q + \dots + c_n m_n q$. In the work that follows, all polynomials are assumed to be in a sum-of-monomials normal form (e.g., a polynomial will never contain two distinct monomials formed from the same power-product).

Given two monic monomials p_1 and p_2 of the form $\frac{m_1}{q_1}$ and $\frac{m_2}{q_2}$, let $\tau_{1,2}$ be the $\text{lcm}(m_1, m_2)$, then we use $\text{spol}(p_1, p_2)$ to denote the polynomial $(\frac{\tau_{1,2}}{m_1})q_1 - (\frac{\tau_{1,2}}{m_2})q_2$. Given a set of polynomials S , it is easy to see that if $\{p_1, p_2\} \subseteq \mathcal{I}(S)$, then $\text{spol}(p_1, p_2) \in \mathcal{I}(S)$.

An order relation \prec on the set \mathbb{M} is *admissible* if $m_1 \prec m_2$ implies that $m_1 m \prec m_2 m$, for all m_1, m_2 and m in \mathbb{M} . A *monomial order* is a total order on \mathbb{M} which is admissible and a well ordering. Given two polynomials p_1 and p_2 , we say $p_1 \prec p_2$ if there is a monomial cm contained in p_2 s.t. (i) m is not contained in p_1 , and (ii) for all m' contained in p_1 , if $m \prec m'$, then m' is contained in p_2 .

The *lexicographical order* \prec_{lex} is defined as $x_1^{i_1} \dots x_n^{i_n} \prec_{lex} x_1^{j_1} \dots x_n^{j_n}$ if $i_1 = j_1, \dots, i_k = j_k, i_{k+1} < j_{k+1}$ for some k . The *degree reverse lexicographical order* \prec_{dlex} is defined as $m_1 = x_1^{i_1} \dots x_n^{i_n} \prec_{dlex} x_1^{j_1} \dots x_n^{j_n} = m_2$ if $\text{deg}(m_1) < \text{deg}(m_2)$ or if $\text{deg}(m_1) = \text{deg}(m_2)$ and $i_n = j_n, \dots, i_k = j_k, i_{k-1} > j_{k-1}$ for some k . The relations \prec_{lex} and \prec_{dlex} are monomial orders.

2.1 Abstract Gröbner Bases

2.1.1 Motivation

The construction of Gröbner bases for polynomial ideals is one of the central methods in algorithmic algebra. Given a Gröbner basis for an ideal in a polynomial ring over a field, one can use simple algebraic machinery to compute much useful information about both the ideal and the complex variety of points upon which all members of the ideal vanish. Of special interest to us is the way in which Gröbner bases can be used to construct Nullstellensatz proofs establishing the unsatisfiability of systems of polynomial equations over the complexes. Indeed, much of the work that follows is centered around how ideal membership proofs (of which Nullstellensatz refutations are a special case) can be suitably minimised and used effectively in the context of efficient T -solvers.

There are a number of methods for constructing Gröbner bases, such as Buchberger's algorithm [2] and Faugère's F4 and F5 [4][5]. However, these algorithms are in many ways not amenable to the needs of SMT solvers. Thus, for

Input: $\langle F = \{p_1, \dots, p_k\} \subset \mathbb{Q}[\vec{x}], \prec \rangle$
Output: G s.t. G is a GBasis of F w.r.t. \prec
 $G := F; S := \{\langle p_i, p_j \rangle \mid 1 \leq i < j \leq k\}$
while $S \neq \emptyset$ **do**
 Let $\langle p_i, p_j \rangle \in S$
 For some q s.t. S -polynomial(p_i, p_j) \xrightarrow{G} q
 if $q \neq 0$ **then**
 $S := S \cup \{\langle p, q \rangle \mid p \in G\}$
 $G := G \cup \{q\}$
 end if
 $S := S \setminus \{\langle p_i, p_j \rangle\}$
end while

Figure 1: Buchberger's Algorithm

the construction of efficient T -solvers which utilise Gröbner basis reasoning, it is sensible to explore alternative basis construction methods. The development of novel Gröbner basis construction algorithms tailored to the needs of SMT solvers is very much an open problem.

For this reason, we would like to abstract away from the specific basis construction algorithm used, and present our proof minimisation machinery in terms of "arbitrary" correct Gröbner bases procedures. To do so, we will briefly present the framework of Abstract Gröbner Bases and build our subsequent work upon it. Abstract Gröbner Bases is a general theory of Gröbner basis procedures introduced by the authors in [7] and motivated precisely by the need for specialised Gröbner bases procedures tailored to the requirements of SMT solvers. Much more detail on the theory can be found in the above reference.

2.1.2 Overview

Given a monomial order \prec , the key idea in Buchberger's algorithm (and in fact all Gröbner basis procedures) is to use a polynomial $cm + q$, where $q \prec m$, as a rewrite rule $cm \rightarrow -q$. For clarity, we will write polynomials used as rewrite rules in a form in which the head monomial has been underlined. For instance, when using $\underline{cm} + q$ as a rewrite rule we will mean $cm \rightarrow -q$. We say a polynomial used as a rewrite rule $\underline{cm} + q$ is *monic* if $c = 1$. To simplify the presentation that follows, we will assume all polynomials used as rewrite rules are monic. The monic polynomial $p = \underline{m} + q$ induces a *reduction relation* \mapsto_p on polynomials. It is defined as $q_1 + c_1 m_1 m \mapsto_p q_1 - c_1 m_1 q$ for arbitrary polynomials q_1 and monomials $c_1 m_1$. Given a set of monic polynomials $G = \{p_1, \dots, p_k\}$, the reduction relation induced by G is defined as: $\mapsto_G = \bigcup_{i=1}^k \mapsto_{p_i}$.

DEFINITION 1 (GRÖBNER BASES). A finite set of monic polynomials G is a Gröbner basis of the ideal $\mathcal{I}(F)$ iff $\mathcal{I}(G) = \mathcal{I}(F)$ and \mapsto_G is confluent.

The inference rules in Figure 2 work on pairs of sets of polynomials (S, G) . In all rules, the coefficients c and c_1 are assumed to be non-zero. We use $(S_1, G_1) \vdash (S_2, G_2)$ to indicate that (S_1, G_1) can be transformed to (S_2, G_2) by applying one of the inference rules in Figure 2. The proofs of all theorems in this section are included in [7].

EXAMPLE 1. Let F be the set of polynomials:

$$\{x^2 y - 1, x y^2 - y\}.$$

Orient	$\frac{S \cup \{\underline{cm} + q\}, G}{S, G \cup \{\underline{m} + (\frac{1}{c})q\}}$
Superpose	$\frac{S, G \cup \{p_1, p_2\}}{S \cup \{\text{spol}(p_1, p_2)\}, G \cup \{p_1, p_2\}}$
Delete	$\frac{S \cup \{0\}, G}{S, G}$
Simplify-S	$\frac{S \cup \{c_1 m_1 m_2 + q_1\}, G \cup \{\underline{m}_2 + q_2\}}{S \cup \{q_1 - c_1 m_1 q_2\}, G \cup \{\underline{m}_2 + q_2\}}$
Simplify-H	$\frac{S, G \cup \{\underline{m}_1 \underline{m}_2 + q_1, \underline{m}_2 + q_2\}}{S \cup \{q_1 - m_1 q_2\}, G \cup \{\underline{m}_2 + q_2\}} \text{ if } m_1 \neq 1$
Simplify-T	$\frac{S, G \cup \{\underline{m} + c_1 m_1 m_2 + q_1, \underline{m}_2 + q_2\}}{S, G \cup \{\underline{m} - c_1 m_1 q_2 + q_1, \underline{m}_2 + q_2\}}$

Figure 2: Inference rules.

Then, using the inference rules in Figure 2, we can generate the run in Figure 3. A reduced Gröbner basis for F is contained in the final state $(\emptyset, \{y - 1, x - 1\})$.

THEOREM 1. $(S_1, G_1) \vdash (S_2, G_2)$ implies $\mathcal{I}(S_1 \cup G_1) = \mathcal{I}(S_2 \cup G_2)$.

DEFINITION 2 (PROCEDURE). A Gröbner basis procedure \mathfrak{G} is a program that accepts a set of polynomials $S = \{p_1, \dots, p_k\}$, a monomial order \prec , and uses the rules in Figure 2 to generate a (finite or infinite) sequence $(S_1 = S, G_1 = \emptyset) \vdash (S_2, G_2) \vdash (S_3, G_3) \vdash \dots$. This sequence is called a run of \mathfrak{G} .

Given a set of monic polynomials G , the set of S-polynomials $\text{SP}(G)$ is defined as the set $\{\text{spol}(p_1, p_2) \mid p_1, p_2 \in G\}$.

DEFINITION 3 (CORRECT PROCEDURE). A Gröbner basis procedure \mathfrak{G} is said to be correct iff it produces only finite runs $(S_1, G_1 = \emptyset) \vdash \dots \vdash (S_n = \emptyset, G_n)$, and $\text{SP}(G_n) \subseteq (S_1 \cup S_2 \cup \dots \cup S_{n-1})$.

THEOREM 2. Let \mathfrak{G} be a correct Gröbner basis procedure, then for any run $(S_1, G_1 = \emptyset) \vdash \dots \vdash (S_n = \emptyset, G_n)$, G_n is a Gröbner basis for $\mathcal{I}(S_1)$.

DEFINITION 4 (EAGER SIMPLIFICATION). Given a Gröbner basis procedure \mathfrak{G} , we say \mathfrak{G} implements eager simplification iff \mathfrak{G} only applies Orient to $p \in S_i$ when Simplify-S cannot be applied to p .

PROPOSITION 3. Given a Gröbner basis procedure \mathfrak{G} using eager simplification, then for any run $(S_1, G_1) \vdash (S_2, G_2) \vdash \dots$, for all $j \geq 1$, there is no $\underline{m}_1 + q_1$ and $\underline{m}_2 + q_2$ in G_j such that $m_1 = m_2$ and $q_1 \neq q_2$. Moreover, in this case, the condition $m_1 \neq 1$ in the rule Simplify-H is only restricting self simplifications.

$\{x^2y - 1, xy^2 - y\}, \emptyset$
 \vdash Orient: $x^2y - 1$
 $\{xy^2 - y\}, \{x^2y - 1\}$
 \vdash Orient: $xy^2 - y$
 $\emptyset, \{x^2y - 1, xy^2 - y\}$
 \vdash Superpose: $\text{spol}(x^2y - 1, xy^2 - y) = xy - y$
 $\{xy - y\}, \{x^2y - 1, xy^2 - y\}$
 \vdash Orient: $xy - y$
 $\emptyset, \{x^2y - 1, xy^2 - y, xy - y\}$
 \vdash Simplify-H: $xy - y$ over $x^2y - 1$
 $\{xy - 1\}, \{xy^2 - y, xy - y\}$
 \vdash Simplify-S: $xy - y$ over $xy - 1$
 $\{y - 1\}, \{xy^2 - y, xy - y\}$
 \vdash Orient: $y - 1$
 $\emptyset, \{xy^2 - y, xy - y, y - 1\}$
 \vdash Simplify-H: $y - 1$ over $xy^2 - y$
 $\{xy - y\}, \{xy - y, y - 1\}$
 \vdash Simplify-S: $xy - y$ over $xy - y$
 $\{0\}, \{xy - y, y - 1\}$
 \vdash Delete
 $\emptyset, \{xy - y, y - 1\}$
 \vdash Simplify-H: $y - 1$ over $xy - y$
 $\{x - y\}, \{y - 1\}$
 \vdash Simplify-S: $y - 1$ over $x - y$
 $\{x - 1\}, \{y - 1\}$
 \vdash Orient: $x - 1$
 $\emptyset, \{y - 1, x - 1\}$
 \vdash Superpose: $\text{spol}(y - 1, x - 1) = x - y$
 $\{x - y\}, \{y - 1, x - 1\}$
 \vdash Simplify-S: $y - 1$ over $x - y$
 $\{x - 1\}, \{y - 1, x - 1\}$
 \vdash Simplify-S: $x - 1$ over $x - 1$
 $\{0\}, \{y - 1, x - 1\}$
 \vdash Delete:
 $\emptyset, \{y - 1, x - 1\}$

Figure 3: A run for $\{x^2y - 1, xy^2 - y\}$ w.r.t. \prec_{dlex} with $x \prec y$.

Input: $\langle S = \{p_1, \dots, p_k\} \subset \mathbb{Q}[\vec{x}], \prec \rangle$
Output: G s.t. G is a GBasis of S w.r.t. \prec
Apply Orient to every member of S
Apply Superpose between every $p_i, p_j \in G$ ($p_i \neq p_j$)
while $S \neq \emptyset$ **do**
 Choose $\text{spol}(p_i, p_j) \in S$
 Apply Simplify- S to $\text{spol}(p_i, p_j) \in S$ as long as possible
 Call the resulting simplified polynomial (in S) q
 if $q \neq 0$ **then**
 Apply Orient to q
 Apply Superpose to all pairs $\langle p, q \rangle$ ($p \neq q \in G$)
 for which Superpose has not been previously applied
 else
 Apply Delete to q
 end if
end while

Figure 4: Rule-based Simulation of Buchberger’s Algorithm

DEFINITION 5 (FAIRNESS). A Gröbner basis procedure \mathfrak{G} is said to be fair iff for any run $(S_1, G_1) \vdash (S_2, G_2) \vdash \dots$

$$\text{SP}\left(\bigcup_{i \geq 1} \bigcap_{j \geq i} G_j\right) \subseteq \bigcup_{i \geq 1} S_i.$$

THEOREM 4. If a Gröbner basis procedure \mathfrak{G} implements eager simplification, is fair, and Superpose is applied at most once for any pair of polynomials in $\bigcup_{i \geq 1} G_i$, then \mathfrak{G} is correct.

As an exercise in gaining familiarity with the inference rules, we illustrate how they can be used to simulate Buchberger’s algorithm in Figure 4.

3. ALGEBRAIC NOTIONS OF PROOF MINIMALITY

Let $\mathbb{B} = \{p_1, \dots, p_k\}$ be a finite subset of $\mathbb{Q}[\vec{x}]$. As the considered Nullstellensatz proofs take the form of ideal membership certificates, we first build much of the algebraic machinery that follows in terms of *general* ideal membership certificates (e.g., those of the form $p \in \mathcal{I}(\mathbb{B})$ for arbitrary $p \in \mathbb{Q}[\vec{x}]$) and then later specialise the results to the case of Nullstellensatz proofs (e.g., those of the form $1 \in \mathcal{I}(\mathbb{B})$). We use the word “proof” to mean exclusively “Nullstellensatz proof” and “certificate” to mean “arbitrary ideal membership certificate,” the latter of which could be a proof.

3.1 Algebraic Notions of Redundancy

DEFINITION 6 (BASIS REDUNDANCY). We say \mathbb{B} is p -non-redundant iff $p \in \mathcal{I}(\mathbb{B})$ and $\forall B \subset \mathbb{B}$ ($p \notin \mathcal{I}(B)$). Similarly, we say \mathbb{B} is p -redundant iff $p \in \mathcal{I}(\mathbb{B})$ and $\exists B \subset \mathbb{B}$ ($p \in \mathcal{I}(B)$).

DEFINITION 7 (MEMBERSHIP SET). We define

$$\text{Mem}(p, p_1, \dots, p_k) \subseteq \mathbb{Q}[\vec{x}]^k$$

to be the collection of (flat) ideal membership certificates showing $p \in \mathcal{I}(p_1, \dots, p_k)$ as follows:

$$\text{Mem}(p, p_1, \dots, p_k) = \left\{ \langle q_1, \dots, q_k \rangle \mid \sum_{i=1}^k p_i q_i = p \right\}.$$

When no confusion can arise, we will write $\text{Mem}(p, \mathbb{B})$ in place of $\text{Mem}(p, p_1, \dots, p_k)$. Given $\alpha \in \text{Mem}(p, \mathbb{B})$, coordinate $\alpha(i)$ is known as the i th cofactor (of p w.r.t. \mathbb{B}) in α .

DEFINITION 8 (PROOF SET). We define $\text{Pr}(p_1, \dots, p_k)$ to be the collection of (flat) Nullstellensatz proofs of the complex unsatisfiability of $\{p_1 \simeq 0, \dots, p_k \simeq 0\}$ ¹ over \mathbb{C}^n . That is, $\text{Pr}(p_1, \dots, p_k) = \text{Mem}(1, p_1, \dots, p_k)$. When no confusion can arise, we will write $\text{Pr}(\mathbb{B})$ in place of $\text{Pr}(p_1, \dots, p_k)$.

It is natural to identify the collection of hypotheses used in a certificate $\alpha \in \text{Mem}(p, \mathbb{B})$ with those members of \mathbb{B} whose corresponding cofactors in α are non-zero.

DEFINITION 9 (BASIS OF HYPOTHESES). Given an ideal membership certificate $\alpha \in \text{Mem}(p, \mathbb{B})$, we define $\text{Hyp}(\mathbb{B}, \alpha)$ to be the collection of \mathbb{B} -hypotheses used in α as follows:

$$\text{Hyp}(\mathbb{B}, \alpha) = \{p_i \in \mathbb{B} \mid \alpha(i) \neq 0 \mid 1 \leq i \leq k\}.$$

DEFINITION 10 (NON-REDUNDANT CERTIFICATES). We say a membership certificate $\alpha \in \text{Mem}(p, \mathbb{B})$ is non-redundant iff the collection of \mathbb{B} -hypotheses used in α , $\text{Hyp}(\mathbb{B}, \alpha)$, is p -non-redundant.

Observe that $\alpha \in \text{Mem}(p, \mathbb{B})$ (resp. $\alpha \in \text{Pr}(\mathbb{B})$) is non-redundant iff $\neg \exists \alpha' \in \text{Mem}(p, \mathbb{B})$ (resp. $\alpha' \in \text{Pr}(\mathbb{B})$) s.t. $\text{Hyp}(\mathbb{B}, \alpha') \subset \text{Hyp}(\mathbb{B}, \alpha)$. Thus if $\alpha \in \text{Pr}(\mathbb{B})$ is a non-redundant proof, then no strict subset of the hypotheses used in the proof is sufficient to show the unsatisfiability of the system \mathbb{B} over \mathbb{C}^n . However, this is an essentially local notion, dependent on the context of the current proof. In particular, the non-redundancy of a proof α does not in general mean that there is no smaller subset $B \subset \mathbb{B}$ s.t. $|B| < |\text{Hyp}(\mathbb{B}, \alpha)|$ that is itself unsatisfiable over \mathbb{C}^n . This can be seen with the following simple example.

EXAMPLE 2. Let the system Γ of polynomial equations be defined as follows:

$$\Gamma = \{x^2 y^2 - 1 \simeq 0, x^2 y \simeq 0, xy \simeq 0, x + 1 \simeq 0, y + 1 \simeq 0\}.$$

Let $B = \{x^2 y^2 - 1, x^2 y, xy, x + 1, y + 1\}$ be the basis of polynomials corresponding to Γ . Observe that $\text{Pr}(B) \neq \emptyset$. Among others, it contains the following two proofs:

$$\alpha = \langle -1, y, 0, 0, 0 \rangle \text{ for } 1 = (-1)(x^2 y^2 - 1) + y(x^2 y), \text{ and}$$

$$\beta = \langle 0, 0, 1, -y, 1 \rangle \text{ for } 1 = xy - y(x + 1) + y + 1.$$

Then, we have, $\text{Hyp}(B, \alpha) = \{x^2 y^2 - 1, x^2 y\}$, $\text{Hyp}(B, \beta) = \{xy, x + 1, y + 1\}$. Observe that both $\text{Hyp}(B, \alpha)$ and $\text{Hyp}(B, \beta)$ are non-redundant and $|\text{Hyp}(B, \alpha)| < |\text{Hyp}(B, \beta)|$.

Thus, non-redundancy of a proof does not mean it is a proof that uses the *globally* least number of hypotheses, but rather that it is in some sense *locally* minimal: If one begins with a non-redundant proof and drops any used hypothesis, then no proof of unsatisfiability for the resulting system will exist. This is made precise with the following lemma.

LEMMA 1. Let $\alpha \in \text{Pr}(\mathbb{B})$ be a non-redundant proof. Then, every $B \subset \text{Hyp}(\mathbb{B}, \alpha)$ is satisfiable over \mathbb{C}^n .

¹The interested reader may note the connection between $\text{Pr}(p_1, \dots, p_k)$ and the first syzygy module of $\langle p_1, \dots, p_k \rangle$. In particular, $\text{Syz}(p_1, \dots, p_k) = \text{Mem}(0, p_1, \dots, p_k)$ while $\text{Pr}(p_1, \dots, p_k) = \text{Mem}(1, p_1, \dots, p_k)$.

PROOF. By definition, α is non-redundant iff $\text{Hyp}(\mathbb{B}, \alpha)$ is non-redundant. Thus, we have $\forall B \subset \text{Hyp}(\mathbb{B}, \alpha)$ ($\mathcal{I}(B) \neq \mathbb{Q}[\bar{x}]$). But, by Hilbert's weak Nullstellensatz, any $B \subseteq \mathbb{Q}[\bar{x}]$ is unsatisfiable over \mathbb{C}^n iff $\mathcal{I}(B) = \mathbb{Q}[\bar{x}]$. Hence every $B \subset \text{Hyp}(\mathbb{B}, \alpha)$ is satisfiable over \mathbb{C}^n . \square

We now wish to address the following fundamental problem: Given a certificate $\alpha \in \text{Mem}(p, \mathbb{B})$, can α be feasibly transformed into a non-redundant certificate? With feasibility in mind, we look only for transformations which arise by a combination of (i) dropping used hypotheses and (ii) modifying non-zero cofactors. In particular, all transformations $\alpha \mapsto \alpha'$ are s.t. $\text{Hyp}(\mathbb{B}, \alpha') \subset \text{Hyp}(\mathbb{B}, \alpha)$. In devising such techniques, one needs to refer to individual hypotheses contributing to the redundancy.

DEFINITION 11. Given a certificate $\alpha \in \text{Mem}(p, \mathbb{B})$ and a j s.t. $1 \leq j \leq k$, we say α is j -redundant iff $\alpha(j) \neq 0$ and $\text{Mem}(p, \text{Hyp}(\mathbb{B}, \alpha) \setminus \{p_j\}) \neq \emptyset$.

3.2 Redundancy in the Linear Case

Before discussing the elimination of redundancy in the general non-linear setting, it is instructive to examine the linear case. If \mathbb{B} is a system of linear polynomials, then the calculation of a Gröbner basis for \mathbb{B} degenerates into Gaussian elimination. By adopting the strategy of *eager simplification*, one can guarantee that for every proof $\alpha \in \text{Mem}(p, \mathbb{B})$, α is not j -redundant.

THEOREM 5. If \mathcal{G} is a fair Gröbner basis procedure implementing eager simplification, $p \in \mathcal{I}(\mathbb{B})$, p and \mathbb{B} are linear, then for all $\alpha \in \text{Mem}(p, \mathbb{B})$, α is non-redundant.

PROOF. Assume $\alpha \in \text{Mem}(p, \mathbb{B})$ is redundant. Then, there must exist some strict subset $B \subset \mathbb{B}$ s.t. $p \in \mathcal{I}(B)$. Moreover, we have two corresponding certificates $\alpha, \alpha' \in \text{Mem}(p, \mathbb{B})$ s.t. $\text{Hyp}(\mathbb{B}, \alpha') \subset \text{Hyp}(\mathbb{B}, \alpha)$. In particular, $\alpha(i) = 0 \implies \alpha'(i) = 0$. Let $X = \{j_1, \dots, j_m\}$ be the collection of indices s.t. $(\alpha'(j_i) - \alpha(j_i)) \neq 0$. That is, X is the collection of indices for which α and α' differ. Note that X cannot be empty, as $\text{Hyp}(\mathbb{B}, \alpha') \subset \text{Hyp}(\mathbb{B}, \alpha)$. Now, \mathcal{G} must have processed the members of \mathbb{B} in some order. WLOG, assume that p_{j_i} was processed before $p_{j_{i+1}}$ when $j_i, j_{i+1} \in X$. Then, we have:

$$p = \sum_{i=1}^k \alpha(i)p_i = \sum_{i=1}^k \alpha'(i)p_i.$$

Therefore,

$$0 = \sum_{i=1}^k (\alpha(i) - \alpha'(i))p_i = \sum_{i=j_1}^{j_m} (\alpha(i) - \alpha'(i))p_i$$

and so,

$$(\alpha'(j_m) - \alpha(j_m))p_{j_m} = \sum_{i=j_1}^{j_{m-1}} (\alpha(i) - \alpha'(i))p_i,$$

and so

$$p_{j_m} = \sum_{i=j_1}^{j_{m-1}} \frac{\alpha(i) - \alpha'(i)}{\alpha'(j_m) - \alpha(j_m)} p_i.$$

Hence $p_{j_m} \in \mathcal{I}(p_1, \dots, p_{j_{m-1}})$. Thus, eager simplification would have reduced $\alpha(j_m)$ to 0, so $\alpha(j_m) = 0$. But recall that $\alpha(i) = 0$ implies $\alpha'(i) = 0$. Hence $\alpha'(j_m) = 0$. But then $j_m \notin X$. Contradiction. \square

Thus the simple process of excluding all p_i s.t. $\alpha(i) = 0$ from contributing to a certificate, as is done by the use of $\text{Hyp}(\mathbb{B}, \alpha)$ in our definition of redundancy, is sufficient to eliminate all redundant linear certificates when an eagerly simplifying Gröbner basis procedure is used. If eager simplification is not used, however, this property may fail to hold.

EXAMPLE 3. Let Γ be a set of polynomial equations be defined as follows:

$$\Gamma = \left\{ \begin{array}{l} x_1 - x_2 \simeq 0, \quad x_2 - x_3 \simeq 0, \quad x_3 - x_4 \simeq 0, \\ x_2 + x_3 - 2x_4 \simeq 0, \quad x_1 + x_2 + x_3 - 3x_4 + 1 \simeq 0 \end{array} \right\}$$

Let $B = \{x_1 - x_2, x_2 - x_3, x_3 - x_4, x_2 + x_3 - 2x_4, x_1 + x_2 + x_3 - 3x_4 + 1\}$ be the basis of polynomials corresponding to Γ . Observe that $\text{Pr}(B) \neq \emptyset$. Among others, it contains the following two proofs:

$$\alpha = \langle -1, -1, -1, -1, 1 \rangle, \text{ and} \\ \beta = \langle -1, -2, -3, 0, 1 \rangle.$$

The certificate α is redundant because $\text{Hyp}(B, \beta) \subset \text{Hyp}(B, \alpha)$. The following run shows how certificate α can be produced by a Gröbner Basis procedure which does not use eager simplification.

B, \emptyset

\vdash Orient: $x_1 - x_2$

$\{x_2 - x_3, x_3 - x_4, x_2 + x_3 - 2x_4, x_1 + x_2 + x_3 - 3x_4 + 1\},$
 $\{x_1 - x_2\}$

\vdash Orient: $x_2 - x_3$

$\{x_3 - x_4, x_2 + x_3 - 2x_4, x_1 + x_2 + x_3 - 3x_4 + 1\},$
 $\{x_1 - x_2, x_2 - x_3\}$

\vdash Orient: $x_3 - x_4$

$\{x_2 + x_3 - 2x_4, x_1 + x_2 + x_3 - 3x_4 + 1\},$

$\{x_1 - x_2, x_2 - x_3, x_3 - x_4\}$

\vdash Orient: $x_2 + x_3 - 2x_4$

$\{x_1 + x_2 + x_3 - 3x_4 + 1\},$

$\{x_1 - x_2, x_2 - x_3, x_3 - x_4, x_2 + x_3 - 2x_4\}$

\vdash Simplify-S: $x_2 + x_3 - 2x_4$ over $x_1 + x_2 + x_3 - 3x_4 + 1$

$\{x_1 - x_4 + 1\}, \{x_1 - x_2, x_2 - x_3, x_3 - x_4, x_2 + x_3 - 2x_4\}$

\vdash Simplify-S: $x_1 - x_2$ over $x_1 - x_4 + 1$

$\{x_2 - x_4 + 1\}, \{x_1 - x_2, x_2 - x_3, x_3 - x_4, x_2 + x_3 - 2x_4\}$

\vdash Simplify-S: $x_2 - x_3$ over $x_2 - x_4 + 1$

$\{x_3 - x_4 + 1\}, \{x_1 - x_2, x_2 - x_3, x_3 - x_4, x_2 + x_3 - 2x_4\}$

\vdash Simplify-S: $x_3 - x_4$ over $x_3 - x_4 + 1$

$\{1\}, \{x_1 - x_2, x_2 - x_3, x_3 - x_4, x_2 + x_3 - 2x_4\}$

3.3 Redundancy in the General Case

We now return to proof redundancy in the context of the general non-linear case. The following concepts form the basis for our proof minimization transformations.

DEFINITION 12. Given a certificate $\alpha \in \text{Mem}(p, \mathbb{B})$ and a j s.t. $1 \leq j \leq k$. Let H_j be the set $\text{Hyp}(\mathbb{B}, \alpha) \setminus \{p_j\}$. We say α is

- j -cofactor-subsumed $\iff \alpha(j) \in \mathcal{I}(B)$ s.t. $B \subseteq H_j$,
- j -basis-subsumed $\iff p_j \in \mathcal{I}(B)$ s.t. $B \subseteq H_j$,
- j - \star -subsumed $\iff \alpha(j)p_j \in \mathcal{I}(B)$ s.t. $B \subseteq H_j$.

We use $\mathbf{1}_j$ to denote $\langle q_1, \dots, q_k \rangle \in \mathbb{Q}[\bar{x}]^k$, where $q_j = 1$, and $q_i = 0$ for all $j \neq i$. Let α and β be in $\mathbb{Q}[\bar{x}]^k$, and

p in $\mathbb{Q}[\bar{x}]$. Then $\alpha + \beta$ denotes $\langle \alpha(1) + \beta(1), \dots, \alpha(k) + \beta(k) \rangle$, and $p\alpha$ denotes $\langle p\alpha(1), \dots, p\alpha(k) \rangle$. First, we focus on cofactor-subsumption. Note that j -cofactor-subsumption is an algebraic generalisation – using the intuition that ideals are an algebraic generalisation of zeroness – of the fact that if a cofactor coordinate $\alpha(j)$ of a certificate is explicitly 0, then its corresponding hypothesis p_j does not contribute to the certificate in an essential way. Let $\alpha \in Mem(p, \mathbb{B})$ and $\beta \in Mem(\alpha(j), \mathbb{B})$ with $Hyp(\mathbb{B}, \beta) \subseteq Hyp(\mathbb{B}, \alpha) \setminus \{p_j\}$. Then, we define the *certificate transformer* $\prod_{j,\beta}(\alpha)$ for j -cofactor-subsumption (w.r.t. $\mathbb{B} = \{p_1, \dots, p_k\}$) as $\alpha + (-\alpha(j))\mathbf{1}_j + p_j\beta$.

THEOREM 6. *Let $\alpha \in Mem(p, \mathbb{B})$ be a j -cofactor-subsumed certificate with $Hyp(\mathbb{B}, \alpha) = B$, and $\beta \in Mem(\alpha(j), \mathbb{B})$ with $Hyp(\mathbb{B}, \beta) \subseteq B \setminus \{p_j\}$. Then, $\prod_{j,\beta}(\alpha) \in Mem(p, \mathbb{B})$, and $Hyp(\mathbb{B}, \prod_{j,\beta}(\alpha)) \subseteq B \setminus \{p_j\}$.*

The proof of Theorem 6 is verified by the following identity.

PROOF.

$$\begin{aligned}
p &= \sum_{i=1}^k \alpha(i)p_i = \left(\sum_{i=1}^{j-1} \alpha(i)p_i \right) + \alpha(j)p_j + \left(\sum_{i=j+1}^k \alpha(i)p_i \right) \\
&= \left(\sum_{i=1}^{j-1} \alpha(i)p_i \right) + p_j \left(\left(\sum_{i=1}^{j-1} \beta(i)p_i \right) + \left(\sum_{i=j+1}^k \beta(i)p_i \right) \right) \\
&\quad + \left(\sum_{i=j+1}^k \alpha(i)p_i \right) \\
&= \left(\sum_{i=1}^{j-1} \alpha(i)p_i \right) + \left(\sum_{i=1}^{j-1} p_j\beta(i)p_i \right) + \left(\sum_{i=j+1}^k p_j\beta(i)p_i \right) \\
&\quad + \left(\sum_{i=j+1}^k \alpha(i)p_i \right) \\
&= \left(\sum_{i=1}^{j-1} \alpha(i)p_i + p_j\beta(i)p_i \right) + \left(\sum_{i=j+1}^k \alpha(i)p_i + p_j\beta(i)p_i \right) \\
&= \left(\sum_{i=1}^{j-1} (\alpha(i) + p_j\beta(i))p_i \right) + \left(\sum_{i=j+1}^k (\alpha(i) + p_j\beta(i))p_i \right) \\
&= \sum_{i=1}^k \left(\prod_j(\alpha)(i) \right) p_i
\end{aligned}$$

$$\text{where } \left[\prod_j(\alpha)(i) = \left(\prod_{j,\beta}(\alpha) \right)(i) \right]. \quad \square$$

Similarly, we define the *certificate transformer* $\prod_{j,\beta}(\alpha)$ for j -basis-subsumption (w.r.t. $\mathbb{B} = \{p_1, \dots, p_k\}$) as $\alpha + (-\alpha(j))\mathbf{1}_j + \alpha(j)\beta$. The correctness of this transformer is verified by an algebraic computation analogous to the proof of Theorem 6. Note that, in this case, $\beta \in Mem(p_j, \mathbb{B})$. Finally, j - \star -subsumption is actually not needed. This is because $\mathbb{Q}[\bar{x}]$ is an integral domain, and thus a given certificate $\alpha \in Mem(p, \mathbb{B})$ is j - \star -subsumed iff it is either j -cofactor-subsumed or j -basis-subsumed.

Orient

$$\frac{S \cup \{(cm + q, \alpha)\}, G}{S, G \cup \{(\underline{m} + (\frac{1}{c})q, (\frac{1}{c})\alpha)\}}$$

Superpose

$$\frac{S, G \cup \{(\overbrace{m_1 + q_1}^{p_1}, \alpha_1), (\overbrace{m_2 + q_2}^{p_2}, \alpha_2)\}}{S \cup \{(\text{spol}(p_1, p_2), m_2\alpha_1 - m_1\alpha_2)\}, G \cup \{(p_1, \alpha_1), (p_2, \alpha_2)\}}$$

Delete

$$\frac{S \cup \{(0, \alpha)\}, G}{S, G}$$

Simplify-S

$$\frac{S \cup \{(c_1m_1m_2 + q_1, \alpha_1)\}, G \cup \{(m_2 + q_2, \alpha_2)\}}{S \cup \{(q_1 - c_1m_1q_2, \alpha_1 - c_1m_1\alpha_2)\}, G \cup \{(\underline{m}_2 + q_2, \alpha_2)\}}$$

Simplify-H

$$\frac{S, G \cup \{(m_1m_2 + q_1, \alpha_1), (m_2 + q_2, \alpha_2)\}}{S \cup \{(q_1 - m_1q_2, \alpha_1 - m_1\alpha_2)\}, G \cup \{(m_2 + q_2, \alpha_2)\}}$$

if $m_1 \neq 1$

Simplify-T

$$\frac{S, G \cup \{(\underline{m} + c_1m_1m_2 + q_1, \alpha_1), (m_2 + q_2, \alpha_2)\}}{S, G \cup \{(\underline{m} - c_1m_1q_2 + q_1, \alpha_1 - c_1m_1\alpha_2), (m_2 + q_2, \alpha_2)\}}$$

Figure 5: Lifted inference rules.

4. ALGORITHMICS AND SMT

We now address the problem of how to build certificates in Gröbner basis procedures based on the inference rules in Figure 2. A *certified polynomial* (w.r.t. \mathbb{B}) is a pair (p, α) s.t. $\alpha \in Mem(p, \mathbb{B})$. The basic idea is lift the rules in Figure 2 to certified polynomials. Figure 5 contains the lifted rules.

DEFINITION 13 (CERTIFIED PROCEDURE). *A certified Gröbner basis procedure \mathfrak{G} is a program that accepts a set of polynomials $\{p_1, \dots, p_k\}$, a monomial order \prec , and uses the lifted versions of the rules in Figure 2 to generate a (finite or infinite) sequence $(S_1 = \{(p_1, \mathbf{1}_1), \dots, (p_k, \mathbf{1}_k)\}, G_1 = \emptyset) \vdash (S_2, G_2) \vdash (S_3, G_3) \vdash \dots$*

Note that if $(1, \alpha) \in S_i$ for some i , then α is a proof for the unsatisfiability of $\{p_1 \simeq 0, \dots, p_k \simeq 0\}$ over \mathbb{C}^n .

In the linear case, *zero variables* are used to represent certified polynomials using a single polynomial [1, 10]. The idea is to represent the certified polynomial (p, α) as $p - \alpha(1)z_1 - \dots - \alpha(k)z_k$, where z_i 's are new fresh variables. The new polynomial is still linear because $\alpha(i)$ is always a constant for the linear case. An approach based on zero variables is attractive because a regular procedure can be easily used to obtain certificates. The main idea is to make the zero variables z_i smaller than the variables $\{x_1, \dots, x_n\}$. This approach cannot be directly applied to the non linear case, because it would require us to make any monomial containing a zero variable z_i smaller than a monomial not containing any zero variable. There is no monomial order with such property, because it violates admissibility. For example, it would require $z_2x_1 \prec x_1$.

Orient	$S \cup \{\underline{cm} + q, \varphi\}, G$
	$S, G \cup \{\underline{m} + (\frac{1}{c})q, D(\varphi)\}$
Superpose	$S, G \cup \{(p_1, \varphi_1), (p_2, \varphi_2)\}$
	$S \cup \{\text{spol}(p_1, p_2), S(\varphi_1, \varphi_2)\}, G \cup \{(p_1, \varphi_1), (p_2, \varphi_2)\}$
Delete	$S \cup \{(0, \varphi)\}, G$
	S, G
Simplify-S	$S \cup \{(c_1 m_1 m_2 + q_1, \varphi_1)\}, G \cup \{(\underline{m}_2 + q_2, \varphi_2)\}$
	$S \cup \{(q_1 - c_1 m_1 q_2, R(\varphi_1, \varphi_2, m_1 m_2))\}, G \cup \{(\underline{m}_2 + q_2, \varphi_2)\}$
Simplify-H	$S, G \cup \{(m_1 m_2 + q_1, \varphi_1), (m_2 + q_2, \varphi_2)\}$
	$S \cup \{(q_1 - m_1 q_2, R(\varphi_1, \varphi_2, m_1 m_2))\}, G \cup \{(\underline{m}_2 + q_2, \varphi_2)\}$ if $m_1 \neq 1$
Simplify-T	$S, G \cup \{(\underline{m} + c_1 m_1 m_2 + q_1, \varphi_1), (\underline{m}_2 + q_2, \varphi_2)\}$
	$S, G \cup \{(\underline{m} - c_1 m_1 q_2 + q_1, R(\varphi_1, \varphi_2, m_1 m_2)), (\underline{m}_2 + q_2, \varphi_2)\}$

Figure 6: Lifted inference rules with structured certificates.

4.1 Structured Certificates

The overhead in a certified Gröbner basis procedure is substantial, since the certificates α can grow in size very quickly. Moreover, it is wasteful to compute a certificate for a polynomial that is deleted using the Delete rule. We address this issue using *structured certificates*. Structured certificates are represented using the constructors A (assumption), S (superpose), R (simplify), D (divide).

DEFINITION 14 (STRUCTURED CERTIFICATES). *The set of polynomial structured certificates, \mathcal{C} , is defined as the least set s.t.*

Assert: $p \in \mathbb{Q}[\vec{x}] \implies A(p) \in \mathcal{C}$,

Superpose: $\varphi_1, \varphi_2 \in \mathcal{C} \implies S(\varphi_1, \varphi_2) \in \mathcal{C}$,

Simplify: $\varphi_1, \varphi_2 \in \mathcal{C} \wedge m \in \mathbb{M} \implies R(\varphi_1, \varphi_2, m) \in \mathcal{C}$,

Divide: $\varphi \in \mathcal{C} \implies D(\varphi) \in \mathcal{C}$.

Figure 6 contains the lifted rules using structured certificates. The initial state (S_1, G_1) for a procedure using structured certificates is:

$$(\{(p_1, A(p_1)), \dots, (p_k, A(p_k))\}, \emptyset).$$

The set of hypothesis $\text{hyp}(\varphi)$ of a structured certificate φ

is defined as:

$$\begin{aligned} \text{hyp}(A(p)) &= p, \\ \text{hyp}(S(\varphi_1, \varphi_2)) &= \text{hyp}(\varphi_1) \cup \text{hyp}(\varphi_2), \\ \text{hyp}(R(\varphi_1, \varphi_2, m)) &= \text{hyp}(\varphi_1) \cup \text{hyp}(\varphi_2), \\ \text{hyp}(D(\varphi)) &= \text{hyp}(\varphi). \end{aligned}$$

DEFINITION 15 (POLYNOMIAL OF A CERTIFICATE). *Given a structured certificate $\varphi \in \mathcal{C}$, the polynomial of φ , $\text{pol}(\varphi)$, is defined as follows:*

1. $\text{pol}(A(p)) = p$,
2. $\text{pol}(S(\varphi_1, \varphi_2)) = \text{spol}(\text{pol}(\varphi_1), \text{pol}(\varphi_2))$
3. $\text{pol}(R(\varphi_1, \varphi_2, m)) = \begin{cases} q_1 - c_1 m_1 q_2 & \text{if } \text{pol}(\varphi_1) \text{ contains } m \\ \text{where} & \\ \text{pol}(\varphi_1) = c_1 m_1 m_2 + q_1, & \\ m = m_1 m_2, & \\ \text{pol}(\varphi_2) = \underline{m}_2 + q_2 & \\ \text{pol}(\varphi_1) \text{ otherwise.} & \end{cases}$
4. $\text{pol}(D(\varphi)) = m + (\frac{1}{c})q$, if $\text{pol}(\varphi) = \underline{cm} + q$

DEFINITION 16 (FLAT CERTIFICATES). *Given a structured certificate $\varphi \in \mathcal{C}$, where $\text{hyp}(\varphi) \subseteq \mathbb{B} = \{p_1, \dots, p_k\}$, the flat certificate with respect to \mathbb{B} , $\text{flat}(\varphi)$, is defined as follows:*

1. $\text{flat}(A(p_i)) = \mathbf{1}_i$,
2. $\text{flat}(S(\varphi_1, \varphi_2)) = m_2(\text{flat}(\varphi_1)) - m_1(\text{flat}(\varphi_2))$,
where $\text{pol}(\varphi_1) = \underline{m}_1 + q_1$, and $\text{pol}(\varphi_2) = \underline{m}_2 + q_2$.

3. $\text{flat}(R(\varphi_1, \varphi_2, m)) = \begin{cases} \text{flat}(\varphi_1) - c_1 m_1(\text{flat}(\varphi_2)) & \text{if } \text{pol}(\varphi_1) \text{ contains } m, \\ \text{where} & \\ \text{pol}(\varphi_1) = c_1 m_1 m_2 + q_1, & \\ m = m_1 m_2, & \\ \text{pol}(\varphi_2) = \underline{m}_2 + q_2 & \\ \text{flat}(\varphi_1) \text{ otherwise.} & \end{cases}$

4. $\text{flat}(D(\varphi)) = \frac{1}{c}(\text{flat}(\varphi))$, where $\text{pol}(\varphi) = \underline{cm} + q$

THEOREM 7. *Given $\mathbb{B} = \{p_1, \dots, p_k\}$, and a certificate $\varphi \in \mathcal{C}$ where $\text{hyp}(\varphi) \subseteq \mathbb{B}$, then $\text{flat}(\varphi) \in \text{Mem}(\text{pol}(\varphi), \mathbb{B})$.*

4.2 Restricted cofactor-subsumption and basis-subsumption

We use j -subsumption to denote j -cofactor-subsumption and j -basis-subsumption. We now address the following issue: How to apply j -subsumption effectively in practice? In general, it is too expensive to check whether a certificate α can be j -subsumed or not, because it requires us to answer ideal membership subqueries. That is, given a certificate α , to check whether α can be j -subsumed, we need to compute a Gröbner basis for $\text{Hyp}(\mathbb{B}, \alpha) \setminus \{p_j\}$. We overcome this difficulty by approximating the ideal membership subqueries. The idea is to answer these queries using a set of rewrite rules that is not necessarily confluent.

DEFINITION 17 (j - φ -INDEPENDENT POLYNOMIAL). *Given a certificate φ , a certified polynomial (r, φ') is j - φ -independent iff $\text{hyp}(\varphi') \subseteq \text{hyp}(\varphi) \setminus \{p_j\}$.*

Let $(S_1, G_1) \vdash \dots \vdash (S_m, G_m)$ be a run produced by a certified Gröbner basis procedure \mathfrak{G} , (p, φ) be some certified polynomial in $\cup_{i=0}^m (S_i \cup G_i)$, and $\Delta_{j,\varphi}$ be the set of j - φ -independent polynomials in $\cup_{i=0}^m G_i$. Now, suppose we want to check whether $\alpha = \text{flat}(\varphi)$ is j -cofactor-subsumed or not. Then, we can simply check whether $\alpha(j)$ rewrites to 0 using an arbitrary subset of $\Delta_{j,\varphi}$. For example, in our prototype, we do not track all polynomials produced in a run. Thus, whenever a certified polynomial (c, φ) (with $c \neq 0$) is included in S_m , we use just the j - φ -independent polynomials in G_m (instead of $\cup_{i=0}^m G_i$) to check whether $\text{flat}(\varphi)$ can be j -cofactor-subsumed or not.

EXAMPLE 4. Let S be a set of polynomials $\{p_1, p_2, p_3, p_4\}$, where:

$$\begin{aligned} p_1 &= x_1 - x_2, \\ p_2 &= x_1x_3^2 - x_1x_4^2 + 1, \\ p_3 &= x_5x_4 - x_3, \\ p_4 &= x_5x_3 - x_4 \end{aligned}$$

The set $\{p_1 \simeq 0, p_2 \simeq 0, p_3 \simeq 0, p_4 \simeq 0\}$ is unsatisfiable over \mathbb{C}^5 . Let \mathfrak{G} be a correct Gröbner basis procedure that produces the run $(S_1 = S, G_1 = \emptyset) \vdash \dots \vdash (S_m, G_m)$, where S_m contains the certified polynomial $(1, \varphi)$, where:

$$\varphi = \mathbf{R}(S(p_3, p_4), \mathbf{R}(A(p_1), \mathbf{R}(A(p_1), A(p_2), x_3^2, x_4^2), x_2)$$

The flat certificate $\text{flat}(\varphi)$ associated with φ is:

$$\text{flat}(\varphi) = \langle (-x_3^2 + x_4^2), 1, x_2x_3, -x_2x_4 \rangle.$$

Assume also that some G_i in the run contains the certified polynomial $(r, \varphi') = (x_3 - x_4, \mathbf{S}(A(p_3), A(p_4)))$. Note that (r, φ') is 1- φ -independent, and $-x_3^2 + x_4^2 \mapsto_r 0$. Thus, $\text{flat}(\varphi)$ can be 1-cofactor-subsumed.

5. CONCLUSION

The effectiveness of an SMT solver depends crucially upon the ability of its T -solvers to identify “small” inconsistent sets of formulas. Hence, to address this need in the context of T -solvers for nonlinear arithmetic, we defined algebraic notions of proof minimality and redundancy for complex unsatisfiability proofs based upon Hilbert’s weak Nullstellensatz, and introduced two useful certificate transformations aimed at the local minimisation of such proofs: *cofactor-subsumption* and *basis-subsumption*. We also described how ideal membership certificates can be extracted in the framework of Abstract Gröbner Bases.

6. ACKNOWLEDGEMENTS

The authors are very grateful to a number of anonymous referees for their helpful comments and suggestions, and to Bruno Dutertre who kindly corrected an error present in a previous version of our paper.

7. REFERENCES

- [1] G. B. Alan and A. Borning. The cassowary linear arithmetic constraint solving algorithm. *ACM Transactions on Computer Human Interaction*, 1998.
- [2] B. Buchberger. Ein algorithmus zum auffinden der basiselemente des restklassenringes nach einem nulldimensionalen polynomideal. Technical report, Mathematical Institute, University of Innsbruck, Austria, 1965.

- [3] L. de Moura, H. Rueß, and N. Shankar. Justifying equality. In *PDPAR’04*, 2004.
- [4] Jean Charles Faugère. A new efficient algorithm for computing gröbner bases (f4). *Journal of Pure and Applied Algebra*, 1999.
- [5] Jean Charles Faugère. A new efficient algorithm for computing gröbner bases without reduction to zero (f5). In *ISSAC ’02: Proceedings of the 2002 international symposium on Symbolic and algebraic computation*, pages 75–83, New York, NY, USA, 2002. ACM.
- [6] R. Nieuwenhuis and A. Oliveras. Fast Congruence Closure and Extensions. *Inf. Comput.*, 2005(4), 2007.
- [7] G. O. Passmore and L. de Moura. Superfluous S-polynomials in Strategy-Independent Gröbner Bases. In *SYNASC’09*, 2009.
- [8] G. O. Passmore and P. B. Jackson. Combined decision techniques for the existential theory of the reals. In *Calulemus’09*, 2009.
- [9] A. Platzer, J. Quesel, and P. Rümmer. Real world verification. In *CADE-22*, 2009.
- [10] H. Rueß and N. Shankar. Solving linear arithmetic constraints. Technical Report SRI-CSL-04-01, SRI International, 2004.
- [11] A. Tarski. A decision method for elementary algebra and geometry. Technical report, 2nd edn. University of California Press, Berkeley, 1951.
- [12] A. Tiwari. An algebraic approach for the unsatisfiability of nonlinear constraints. In *CSL’05*, volume 3634 of *LNCS*, 2005.