Little Engines of Proof

N. Shankar, L. de Moura, H. Ruess, A. Tiwari
shankar@csl.sri.com
URL: http://www.csl.sri.com/~shankar/LEP.html

Computer Science Laboratory
SRI International
Menlo Park, CA

Recall

We discussed procedures for testing satisfiability of linear arithmetic equalities and inequalities over rationals

Signature: $\mathbb{Q}, +, -, <$

Now we move on to nonlinear expressions

Signature: $0, 1, +, -, *$

Today: Interpreted over algebraically closed fields

Tomorrow: Interpreted over real closed fields

Why?

Algebraically closed fields have several nice computational properties, as well as, beautiful connections to geometry.

- Algebraic geometry
- Gröbner basis
- Elimination ideal computation
- Zeroes of a system of polynomial equations

The theory of reals is used across many application domains.

- Real algebraic geometry
- Areas: Dynamical systems, engineering, control, geometry, motion planning

Overview of Decision Problems

In theory T:

Word Problem (WP): $\models_T s = t$, for two terms s and t

Uniform Word Problem (UWP): $\models_T \bigwedge_i s_i = t_i \Rightarrow s = t$

Clausal Validity Problem (CVP): $\models_T \bigvee_i l_i$, where l_i are literals from T

Satisfiability of quantifier-free formuls (QFF): $\models_T \exists \vec{x}.\phi(\vec{x})$, where ϕ is a QFF

Satisfiability of QFF reduces to the CVP

Satisfiability of the full first-order (FO) theory: $\models_T \phi$, where ϕ is a FO formula

WP, UWP, and CVP are special instances of satisfiability in the full FO theory

Overview of Some Methods

In theory T:

Word Problem (WP): Canonizer

Uniform Word Problem (UWP): Solvers/ Solution sets / Completion of ground equations in T

Clausal Validity Problem (CVP): For convex theories, this reduces to UWP

Satisfiability of quantifier-free formuls (QFF): Convert to DNF and use algorithm for CVP

Satisfiability of the full first-order (FO) theory: Quantifier Elimination

Quantifier Elimination in FO theories

A sentence in first-order logic can be arbitrarily quantified.

Some theories admit quantifier elimination: a quantified formula can be shown to be equivalent to a quantifier-free formula.

Example. In $\Re$, $\exists x.(x * y > 0) \;\Leftrightarrow\; y \neq 0$

If T admits quantifier elimination and ground atomic formulas can be evaluated in T, then the full FO theory of T is decidable.

Ex: Prove the above claim.

Algebraically-Closed Fields

Signature: $\Sigma_F = \langle 0, 1, +, -, * \rangle$

1. $\langle F, 0, 1, +, -, * \rangle$ is a field
2. every polynomial in $F[x]$ has a root in F

The set of complex numbers form an ACF.

Before diving into ACFs, we first consider a special case: the UWP for commutative semigroups

Commutative Semigroup

$\Sigma \;=\; \{f, 1\}$

$T \;:\;$ Axioms of equality + ACU axioms for f.

- ACU: Also assume unit element 1
- Example UWP in ACU: $x^2 y = 1 \;\wedge\; x y^2 = y \;\Rightarrow\; x = 1$
- Treat f as variable arity, equivalent AC axioms:

$$\begin{array}{rcll} f(\ldots, f(\ldots), \ldots) & = & f(\ldots, \ldots, \ldots) & (F) \\ f(\ldots, u, v, \ldots) & = & f(\ldots, v, u, \ldots) & (P) \end{array}$$

- Idea: Flatten all equations and do completion modulo P

UWP for Commutative Semigroups

State: Γ, set of equations

Form of equations: $f(\ldots) = f(\ldots)$; $f(\ldots) = c$; $c = d$

Eg: $x^2y = 1, xy^2 = y$ (really, $f(x, x, y) = 1, f(x, y, y) = y$)

$\succ$: (total degree) lexicographic ordering on power-products

$$\text{Orient} \quad \frac{\Gamma, s = t}{\Gamma, s \to t} \quad \text{if } s \succ t$$

$$\text{Superpose} \quad \frac{\Gamma, f(X) \to s, f(Y) \to t}{\Gamma', f(s, Z) = f(t, Z')} \quad \begin{array}{l}\text{for least } Z, Z' \text{ s.t. } f(X, Z) = f(Y, Z') \\ \text{modulo } FP\text{, collapse inapplicable}\end{array}$$

Example.

$$\cfrac{\cfrac{x^2y = 1,\ xy^2 = y}{x^2y \to 1,\ xy^2 \to y}}{x^2y \to 1,\ xy^2 \to y, y = xy}$$

UWP for Commutative Semigroup (Contd)

$$\text{Collapse} \quad \frac{\Gamma, f(X, Z) \to t, f(X) \to s}{\Gamma, f(s, Z) = t, f(X) \to s}$$

$$\text{Delete} \quad \frac{\Gamma, s = s}{\Gamma}$$

Example.

$$\begin{array}{c}
x^2y \to 1,\ xy^2 \to y,\ y = xy \\ \hline
x^2y \to 1,\ xy^2 \to y,\ xy \to y \\ \hline
xy = 1,\ y^2 = y,\ xy \to y \\ \hline
xy \to 1,\ y^2 \to y,\ xy \to y \\ \hline
y = 1,\ y^2 \to y,\ xy \to y \\ \hline
y \to 1,\ y^2 \to y,\ xy \to y \\ \hline
y \to 1,\ 1 = y,\ x = y \\ \hline
y \to 1,\ x \to y
\end{array}$$

UWP for Commutative Semigroup

- Note we can decide if $x = 1$ is implied by the original equations
- Termination: Guaranteed by Collapse via Dickson's lemma.

  If $s_1, s_2, \ldots$ is an infinite sequence of power products, then there exists i, j s.t. s_i divides s_j.
- Soundness and Completeness: If R is a result obtained by starting with E, then $T \vdash E \Rightarrow s = t$ iff $s \to_R^* \circ \leftarrow_R^* t$ for all s, t

  Equal terms (modulo E) have identical canonical forms (w.r.t R)

Combining Several AC and UIF symbols

Ground AC-theories:

$$\begin{array}{rcl}
\Sigma & = & \Sigma_F \cup \Sigma_{AC} \\
T & = & \text{Axioms of equality} + \text{AC axioms for each } f \in \Sigma_{AC}.
\end{array}$$

Using the Nelson-Oppen combination result:

- Use Extension inference rule to purify equations
- Use abstract congruence closure on $\Sigma - \Sigma_{AC}$
- Use completion modulo AC on each $\{f\}$, $f \in \Sigma_{AC}$
- Combine by sharing equations between constants

Time Complexity: $O(n^2 * (T_{AC}(n) + n \log(n)))$.

Similarly, ACU-symbols can be added.

Back to Algebraically Closed Fields

$\Sigma \;=\; \{\mathbb{Q}, +, -, *\}$

$T \;:\;$ Axioms for field + algebraic closure

- System of nonlinear equations: $E \equiv \{xy = x, x^2 = x + 1\}$
- We want to "solve" them simultaneously
- Commutative semigroups: had no $+$
- Generalize: Transform E to R (Gröbner basis)

Computing Gröbner Basis

State: Γ, set of equations

Form of equations: $p = 0$, p a polynomial in $\mathbb{Q}[x_1, \ldots, x_n]$

Eg: $xy - x = 0, x^2 - x - 1 = 0$

$\succ$: lex ordering on power-products, extended to polynomials

Orient	$\dfrac{\Gamma, cX + p = 0}{\Gamma, cX \to -p}$	if $X \succ p_0$
Superpose	$\dfrac{\Gamma, cX \to p, dY \to q}{\Gamma', d * p * Z = c * q * Z'}$	for least Z, Z' s.t. $X * Z = Y * Z'$, collapse not applicable

Example.

$$\cfrac{\cfrac{xy - x = 0,\; x^2 - x - 1 = 0}{xy \to x,\; x^2 \to x + 1}}{xy \to x,\; x^2 \to x + 1,\; x * x = y * (x + 1)}$$

Computing Gröbner Basis: More Rules

Collapse	$\dfrac{\Gamma, cXZ \to p, dX \to q}{\Gamma, d * p = c * Z * q, dX \to q}$
Delete	$\dfrac{\Gamma, s = s}{\Gamma}$

Example.

$$xy \to x,\; x^2 \to x + 1,\; x * x = y * (x + 1)$$
$$\overline{}$$
$$xy \to x,\; x^2 \to x + 1,\; x^2 \to xy + y$$
$$\overline{}$$
$$xy \to x,\; x^2 \to x + 1,\; x + 1 = xy + y$$
$$\overline{}$$
$$xy \to x,\; x^2 \to x + 1,\; xy \to x - y + 1$$
$$\overline{}$$
$$xy \to x,\; x^2 \to x + 1,\; x = x - y + 1$$
$$\overline{}$$
$$xy \to x,\; x^2 \to x + 1,\; y \to 1$$
$$\overline{}$$
$$x = x,\; x^2 \to x + 1,\; y \to 1$$
$$\overline{}$$
$$x^2 \to x + 1,\; y \to 1$$

Gröbner Basis: Correctness

Same as for commutative semigroups

- Termination: Same as before
- Soundness and Completeness: If R is a result obtained by starting with E, then $T \vdash E \Rightarrow s = t$ iff $s \to_R^* \circ \leftarrow_R^* t$ for all s, t; and T is the theory of polynomial rings

  Equal terms (modulo E) have identical canonical forms (w.r.t R)

Example. Note that $y = 1$ modulo $\{xy = x, x^2 = x + 1\}$.

W.r.t $\{x^2 \to x + 1,\; y \to 1\}$, y and 1 have the same canonical form 1.

GB: UWP in the theory of ACFs

GB decides the UWP for the theory T of polynomial rings

But what about UWP for ACFs? In ACFs,

$$\begin{aligned} &\forall x, y.(xy = x \ \wedge \ x^2 = x + 2 \ \Rightarrow \ y = 1) \\ \Leftrightarrow\ &\neg \exists x, y.(xy = x \ \wedge \ x^2 = x + 2 \ \wedge \ y \neq 1) \\ \Leftrightarrow\ &\neg \exists x, y, z.(xy = x \ \wedge \ x^2 = x + 2 \ \wedge \ (y-1)z = 1) \end{aligned}$$

Thus, GB can be used to decide the UWP for ACFs.

GB: Eliminating Variables

We can infer all equational consequences of an existentially quantified conjunction of equations

Notice that

$$\exists x.(xy = x \ \wedge \ x^2 = x + 2) \ \Rightarrow \ y = 1$$

Elimination Ideal. If $\succ$ is lex and $x_n \succ x_{n-1} \succ \cdots \succ x_1$,

$$GB(E|_{\mathbb{Q}[x_1,\ldots,x_i]}) \ \equiv \ GB(E) \cap \mathbb{Q}[x_1, \ldots, x_i]$$

The elimination ideal is a logical consequence of the existential formula

But not logically equivalent to it

GB: Eliminating Variable II

In the more general case,

$$\exists x.(p_1 = 0 \ \wedge \ \ldots \ \wedge \ p_n = 0 \ \wedge \ q_1 \neq 0 \ \wedge \ \ldots \ \wedge \ q_m \neq 0)$$

Over ACFs, this is equivalent to

$$\exists x, z_1, \ldots, z_m.(p_1 = 0 \wedge \ldots \wedge p_n = 0 \wedge q_1 z_1 = 1 \wedge \ldots \wedge q_m z_m = 1)$$

And using the Elimination Ideal Theorem, we can eliminate $x, z_1, \ldots, z_m$ simultaneously

Hence, we can compute equational consequences of any conjunction.

Algebraic Geometry I

There is a correspondence between algebra and geometry

Algebra		Geometry
Polynomial p	:	$Zeroes(p)$
Set S of polynomials	:	$Zeroes(S) = V(S)$
Ideal I gen by S	:	Variety $V(I) = Zeroes(S)$
$I = (1)$ (alt. $I \neq (1)$)	:	$V(I) = \emptyset$ (alt. $V(I) \neq \emptyset$)
$f \in I$	:	$V(I) \subseteq Zeroes(f)$
Elimination ideal	:	projection
$Id(I_1 \cup I_2)$	:	$V(I_1) \cap V(I_2)$
$I_1 \cap I_2$	:	$V(I_1) \cup V(I_2)$

This correspondence is valid only when the geometry is interpreted over polynomial rings

Algebraic Geometry II

Correspondence between algebra and geometry over ACFs

Algebra	:	Geometry
(Polynomial p	:	$Zeroes(p)$)
Radical Ideal $\sqrt{I}$	:	Variety $V(I) = Zeroes(I)$
$I = (1)$ (alt. $I \neq (1)$)	:	$V(I) = \emptyset$ (alt. $V(I) \neq \emptyset$)
$f^k \in I$	:	$V(I) \subseteq Zeroes(f)$ (Hilbert Nullstellensatz)
$\sqrt{Id(\sqrt{I_1} \cup \sqrt{I_2})}$	:	$V(I_1) \cap V(I_2)$
$\sqrt{I_1} \cap \sqrt{I_2}$	:	$V(I_1) \cup V(I_2)$

This correspondence is valid when the geometry is interpreted over ACF

Summary

- Gröbner basis is a canonical representation of a set of nonlinear equations
- They decide the UWP for polynomial rings, and not for the reals. They can be used to decide UWP for ACFs using the negation trick.
- They have several nice properties, such as elimination ideal computation
- All interesting behavior of GB computation is reflected in the case of commutative semigroups (case of binomial ideals)

Examples (UWP over rings and ACFs)

$\forall x. x^2 = 0 \Rightarrow x = 0$ is true over ACFs, but not over rings

A GB for $\{x^2 = 0\}$ is $R_1 \equiv \{x^2 \to 0\}$

x and 0 have different normal forms w.r.t R_1

Hence, the given formula is not true over rings

A GB for $\{x^2 = 0, xy = 1\}$ is $R_2 \equiv \{1 \to 0\}$

Hence, the above formula is true over ACFs

Ex. Prove: $\exists k. p^k \in Id(S)$ iff $GB(S \cup \{pz = 1\})$ is $\{1 \to 0\}$

Examples (CVP over ACFs)

$\forall x. x^2 = 1 \Rightarrow (x = 1 \ \vee \ x = -1)$ is true over ACFs

This can be deduced by checking the unsatisfiability of

$$x^2 = 1 \ \wedge \ (x-1)y = 1 \ \wedge \ (x+1)z = 1$$

Ex. Show that a GB for these three equations is $\{1 \to 0\}$.

Examples (FO theory over ACFs)

For what "values" of c is it the case that
$\exists x. x^2 + c = 0 \wedge x^3 = x$

Construct a GB for $x^2 + c = 0,\ x^3 = x$ using lex ordering with precedence $x \succ c$

Ex. Verify that you obtain

$$\{x^2 \to -c,\ cx \to -x,\ c^2 \to -c\}$$

Conclude that $\exists x. x^2 + c = 0 \wedge x^3 = x$ implies

$$c^2 = -c$$

over both rings and ACFs.

Over ACFs, this means that c is either 0 or -1.

Ex. Verify the last claim using GB computation.

A Note on Termination

We have tried hard to ensure that inference rules terminate

But we have missed certain nontermination behaviors

$$\begin{array}{c}\{xy^2 \to y^3,\ x^2y \to xy^2\} \\ \hline \{xy^2 \to y^3,\ x^2y \to xy^2,\ x^2y^2 = xy^3\} \\ \hline \{xy^2 \to y^3,\ x^2y \to xy^2,\ x^2y^2 \to xy^3\} \\ \hline \{xy^2 \to y^3,\ x^2y \to xy^2,\ xy^3 = xy^3\} \\ \hline \{xy^2 \to y^3,\ x^2y \to xy^2\} \\ \hline \vdots \end{array}$$

Assume side condition that prevents application of the same inference again

Termination of GB computation

Assume this extra side condition

- Any infinite derivation will have infinite Superposition steps
- Let $\{l_i \to r_i, l'_i \to r'_i\}$ be the rules involved in i-th superposition
- By Dickson's lemma*, $\exists i, j.\ l_i | l_j$ and $l'_i | l'_j$
- By new assumption, either $l_i \to r_i$ is different from $l_j \to r_j$ or $l'_i \to r'_i$ is different from $l'_j \to r'_j$
- W.l.o.g assume $j > i$ and $l_i \to r_i$ is different from $l_j \to r_j$
- Side condition of j-th superposition is violated: if $l_i \to r_i$ is not present, then the rule that "collapsed" it (recursively) will also collapse $l_j \to r_j$