# 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

#### 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

1

#### 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

#### **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  $\phi$  is a QFF

Satisfiability of QFF reduces to the CVP

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

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

3

## **Overview of Some Methods**

In theory T:

Word Problem (WP): Canonizer

Uniform Word Problem (UWP): Solvers/ Solution sets / Completion of ground equations in  ${\cal T}$ 

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

#### 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

5

#### 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.

#### Commutative Semigroup

- $\Sigma = \{f, \mathbf{1}\}$
- T : Axioms of equality + ACU axioms for f.
- ACU: Also assume unit element 1
- Example UWP in ACU:  $x^2y = 1 \land xy^2 = y \Rightarrow x = 1$
- Treat *f* as variable arity, equivalent AC axioms:

$$f(\dots, f(\dots), \dots) = f(\dots, \dots, \dots)$$
 (F)  
$$f(\dots, u, v, \dots) = f(\dots, v, u, \dots)$$
 (P)

• Idea: Flatten all equations and do completion modulo P

7

## **UWP** for Commutative Semigroups

State:  $\Gamma$ , set of equations

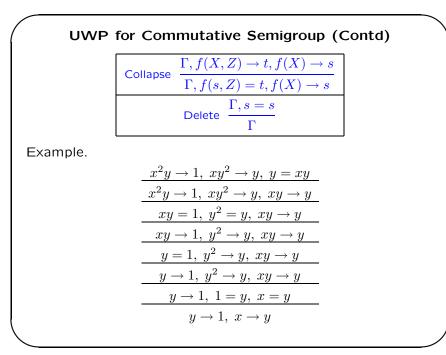
Form of equations:  $f(\ldots) = f(\ldots)$ ;  $f(\ldots) = c$ ; c = d

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

$\label{eq:orient_constraint} \begin{array}{c} \Gamma,s=t\\ \Gamma,s\rightarrow t \end{array} \text{ if } s\succ t \end{array}$	
$\label{eq:superpose} \begin{array}{ c c } \hline \mbox{Superpose} & \frac{\Gamma, f(X) \rightarrow s, f(Y) \rightarrow t}{\Gamma', f(s,Z) = f(t,Z')} for least $Z,Z'$ s.t. $f(X,Z) = f(X,Z) = $	
Example.	
$x^2y = 1, \ xy^2 = y$	
$x^2y \to 1, \ xy^2 \to y$	
$x^2y \to 1, \ xy^2 \to y, y = xy$	

9



## 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  $s \rightarrow_R^* \circ \leftarrow_R^* t$  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:

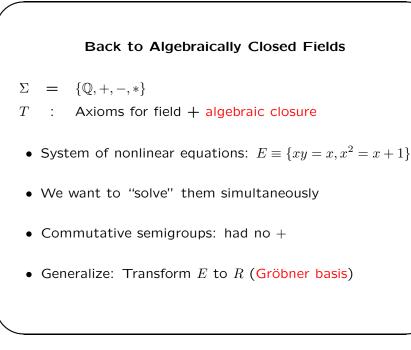
$$\Sigma = \Sigma_F \cup \Sigma_{AC}$$

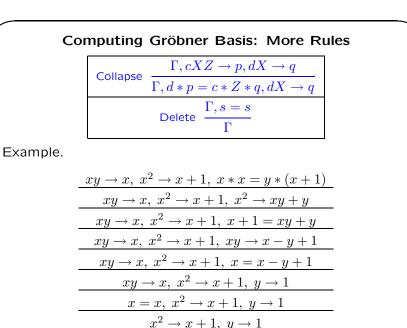
T = Axioms of equality + AC axioms for each  $f \in \Sigma_{AC}$ . Using the Nelson-Oppen combination result:

- 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.





13

# Computing Gröbner Basis State: $\Gamma$ , 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

 $\begin{array}{c} \label{eq:constraint} \hline & \Gamma, cX + p = 0 \\ \hline & \Gamma, cX \to -p \end{array} \text{ if } X \succ p_0 \\ \\ \text{Superpose } & \frac{\Gamma, cX \to p, dY \to q}{\Gamma', d * p * Z = c * q * Z'} \text{ for least } Z, Z' \text{ s.t. } X * Z = Y * Z', \end{array}$ 

Example.

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

**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  $s \rightarrow_R^* \circ \leftarrow_R^* t$ 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  $\{x^2 \rightarrow x + 1, y \rightarrow 1\}$ , 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,

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

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

#### **GB:** Eliminating Variable II

In the more general case,

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

Over ACFs, this is equivalent to

$$\exists x, z_1, \dots, z_m (p_1 = 0 \land \dots \land p_n = 0 \land q_1 z_1 = 1 \land \dots \land q_m z_m = 1)$$

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.

17

#### **GB:** Eliminating Variables

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

Notice that

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

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

# 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 ${\cal S}$	:	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. $V(I) \neq \emptyset$ )
$f^{m k} \in I$	:	$V(I)\subseteq Zeroes(f)$ (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

# 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 $\{1 \to 0\}$

21

#### 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 (CVP over ACFs)  $\forall x.x^2 = 1 \Rightarrow (x = 1 \lor x = -1)$  is true over ACFs This can be deduced by checking the unsatisfiability of  $x^2 = 1 \land (x - 1)y = 1 \land (x + 1)z = 1$ Ex. Show that a GB for these three equations is  $\{1 \rightarrow 0\}$ . 23

# Examples (FO theory over ACFs)

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

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

Ex. Verify that you obtain

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

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

# 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  $l_i \rightarrow r_i$  is different from  $l_j \rightarrow r_j$  or  $l'_i \rightarrow r'_i$  is different from  $l'_j \rightarrow r'_j$
- W.I.o.g assume j > i and  $l_i \rightarrow r_i$  is different from  $l_j \rightarrow r_j$
- Side condition of *j*-th superposition is violated: if  $l_i \rightarrow r_i$  is not present, then the rule that "collapsed" it (recursively) will also collapse  $l_i \rightarrow r_j$

25

## A Note on Termination

We have tried hard to ensure that inference rules terminate But we have missed certain nontermination behaviors

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

Assume side condition that prevents application of the same inference again