FILOMAT (Niš) 9:3 (1995), 733–742
Algebra, Logic & Discrete Mathematics
Niš, April 14–16, 1995.

AUTOMATIC THEOREM PROVING IN FIELD THEORY USING QUANTIFIER ELIMINATION

Aleksandar Jovanović and Žarko Mijajlović

ABSTRACT. In this paper we describe a new method of elimination of quantifiers for the theories of algebraically closed fields and theory of ordered real closed fields which may be used for the theorem provers for these theories. The method is based on the properties of resultants of polynomials.

1. Introduction

One could say that mathematics was introduced in logic by Tarski and Gödel while for Abraham Robinson and A. Malcev could be said that they introduced logic in mathematics. Namely, today probably most important applications of logic in other parts of mathematics (nonstandard analysis and model-theoretic algebra) originate in work of A. Robinson. First contributions of this kind in algebra were given by A. Malcev in 1936. The Robinson's solution of Seventeenth Hilbert problem by methods of mathematical logic, more precisely methods of model theory, represents an important contribution to the model-theoretic algebra. The solution is based on the method of elimination of quantifiers and notion of model completeness, the model-theoretic version of the elimination of quantifiers. Beside, this notion can be understood as a transfer principle, which is of significant importance for the applications in algebra.

Definition 1. A theory T in the first order predicate calculus admits elimination of quantifiers if for every formula φ or T there is a formula ψ in the language of T, without quantifiers such that: $T \vdash \varphi \Leftrightarrow \psi$.

Let us remind that the following theorem is basic for the model theoretic solution of the seventeenth Hilbert's problem.

We wish to thank to Professor Albert Dragalin for useful comments and remarks.

Theorem 1. (A. Tarski, 1948) *Theory of ordered real closed fields admits elimination of quantifiers.*

Theories which admit the elimination of quantifiers have this interesting property:

Every theory which admits eliminations of quantifiers is model complete.

In order to explain this notion, suppose that T is any first order theory in the language L. Let $\mathbf{A}$ and $\mathbf{B}$ be any models (i.e. operational-relational structures) of L. Model $\mathbf{A}$ is an elementary submodel of model $\mathbf{B}$, or $\mathbf{B}$ is an elementary extension of $\mathbf{A}$ if the following conditions are satisfied.

1. $\mathbf{A}$ is a submodel of $\mathbf{B}$.
2. For every formula $\varphi(\bar{x})$ of L and every $\bar{a} \in A$,

$$\mathbf{A} \models \varphi(\bar{a}) \qquad \text{if and only if} \qquad \mathbf{B} \models \varphi(\bar{a}).$$

The fact that $\mathbf{A}$ is an elementary submodel of $\mathbf{B}$ we denote by $\mathbf{A} \prec \mathbf{B}$.

Definition 2. Theory T is model complete iff for any two models $\mathbf{A}$ and $\mathbf{B}$ of theory T if $\mathbf{A}$ is a submodel of $\mathbf{B}$ then $\mathbf{A}$ is an elementary submodel of $\mathbf{B}$.

2. Quantifier elimination for the theory of algebraically closed fields

The axioms of the theory of algebraically closed fields are the axioms for fields and the following set of formulas, expressing that every polynomial of degree ≥ 1 has a root. Let T be the field theory and T^* the theory of algebraically closed fields. For example, the fields of complex numbers and algebraic numbers are models of the theory T^*.

Examples of quantifier elimination for theory T^* are known for long time in classical algebra. One of the best known, which will be used here is the Resultant Theorem.

Definition 3. Let $a(x) = \sum_{i \leq m} a_i x^i$, $b(x) = \sum_{j \leq n} x^j$ be complex polynomials. The resultant of polynomials a and b is the determinant

$$\mathrm{Res}(a,b) = \begin{vmatrix} a_0 & a_1 & \dots & a_m & 0 & \dots & 0 \\ 0 & a_0 & a_1 & \dots & a_m & \dots & 0 \\ & & & \vdots & & & \\ 0 & & \dots & a_0 & a_1 & \dots & a_m \\ b_0 & b_1 & \dots & b_n & 0 & \dots & 0 \\ 0 & b_0 & b_1 & \dots & b_n & \dots & 0 \\ & & & \vdots & & & \\ 0 & & \dots & b_0 & b_1 & \dots & b_n \end{vmatrix}$$

Hence, $\mathrm{Res}(a,b)$ is the $m+n$-degree determinant, where m and n are the degrees of polynomials a and b respectively. The main property of resultant is given in the following theorem.

Theorem 2. *The complex polynomials a and b have a common root in the field of complex numbers $\mathbf{C}$ iff* $\mathrm{Res}(a,b)=0$.

In other words, if a and b are polynomials of degrees m and n respectively, then

$$(\exists x)(a(x)=0\wedge b(x)=0)\Leftrightarrow \mathrm{Res}(a,b)=0 \tag{1}$$

The resultant of two polynomials in any field can be defined in the same way, thus within the theory T.

Let $a(x)=y_m+y_{m-1}x+\ldots+y_0x^m$, $b(x)=z_n+z_{n-1}x+\ldots+z_0x^n$ be polynomials, where $y_0,\ldots,y_m,z_0,\ldots,z_n$ are variables. Define polynomials $a_0(x)=a(x)$, $a_1(x)=y_m+\ldots y_1x^{m-1}$, $a_m(x)=y_m$ and similarly polynomials $b_i(x)$. Then, by Theorem 2, we have

$$\begin{aligned}&(\exists x)(a(x)=0\wedge b(x)=0)\Leftrightarrow\\ &\bigvee_{\substack{i<m\\ j<n}}\Big(\deg(a_i)=m-i\wedge\deg(b_j)=n-j\wedge\mathrm{Res}(a_i,b_j)=0\Big)\ \vee\\ &\bigwedge_{i,j}(y_i=0\wedge z_j=0)\Leftrightarrow\\ &\bigvee_{\substack{i<m\\ j<n}}\Big(y_0=0\wedge\ldots\wedge y_{i-1}=0\wedge y_i\neq 0\wedge z_0=0\wedge\ldots\wedge z_{j-1}=0\wedge\\ &\qquad z_j\neq 0\wedge\mathrm{Res}(a_i,b_j)=0\Big)\vee\bigwedge_{i,j}(y_i=0\wedge z_j=0).\end{aligned} \tag{2}$$

Consider other two simple quantifier elimination cases. Since every algebraically closed field is infinite (roots of the polynomial $(x-x_0)(x-x_1)\ldots(x-x_n)+1$ are different from $x_0,\ldots,x_n$), for the polynomial $a(x)=\sum_i y_ix^i$ we have

$$(\exists x)(a(x)\neq 0)\Leftrightarrow y_0\neq 0\vee\ldots\vee y_m\neq 0. \tag{3}$$

Now, let us show that quantifier elimination for the formula

$$(\exists x)(a(x)=0\wedge b(x)\neq 0). \tag{4}$$

is reduced to the case (2). First note that $b(x)\neq 0\Leftrightarrow(\exists y)(yb(x)-1=0)$ and that y is a factor of every member of the polynomial $yb(x)-1$, except

in the free member. If we select the variable y so it is not a variable of the formula $a(x) = 0 \wedge b(x) \neq 0$, then

$$(\exists x)(a(x) = 0 \wedge b(x) \neq 0) \Leftrightarrow (\exists y)(\exists x)(a(x) = 0 \wedge yb(x) - 1 = 0).$$

By (2), formula $(\exists x)(a(x) = 0 \wedge yb(x) - 1 = 0)$ is equivalent to the disjunction $\varphi_1 \vee \ldots \vee \varphi_k$, which is quantifier free, and each of the formulas φ_j, $j < k$ is of the form

$$y_0 = 0 \wedge \ldots \wedge y_{i-1} = 0 \wedge y_i \neq 0 \wedge y_i \neq 0 \wedge z_0 y = 0 \wedge \ldots \wedge z_{j-1} y = 0 \wedge$$
$$z_j y \neq 0 \wedge \mathrm{Res}(a_i, b'_j) = 0.$$

for a polynomial b'_j. Since $\exists x \vee_i \varphi_i \Leftrightarrow \vee_i \exists x \varphi$ is a valid formula, it is sufficient to eliminate quantifiers of the formula $\exists y \varphi_i$. Now, observe that the following sentences are true in the field theory:

1° $\exists y(y = 0 \wedge \psi(y)) \Leftrightarrow \psi(0)$,
2° $\exists y(y = 0 \wedge \psi) \Leftrightarrow \psi$, if y does not occur in ψ,
3° $zy \neq 0 \Leftrightarrow z \neq 0 \wedge y \neq 0$,
4° $\exists y(zy = 0 \wedge \psi) \Leftrightarrow (z = 0 \wedge \exists y \psi) \vee \exists y(y = 0 \wedge \psi)$, if z is a variable different from y.

Therefore, it will suffice to eliminate existential quantifier of the formula

$$(\exists y)(y \neq 0 \wedge \mathrm{Res}(a_i, b'_j) = 0),$$

i.e. formula of the form $(\exists y)(y \neq 0 \wedge m(y) = 0)$ where $m(y)$ is a polynomial. Let $m(y) = m_0 + m_1 + \ldots + m_k y^k$. Then the following is obvious.

$$(\exists y)(y \neq 0 \wedge m(y) = 0) \Leftrightarrow \bigvee_{i<j} (m_i \neq 0 \wedge m_j \neq 0).$$

Now we consider the general case of quantifier elimination in the theory T^*. Let φ be any formula of the theory T. It is equivalent to a formula

$$(Q_1 x_1) \ldots (Q_n x_n) \psi$$

in the prenex normal form, where x is quantifier free. Using the equivalence

$$(\forall x)\alpha(x) \Leftrightarrow \neg(\exists x)\neg\alpha(x),$$

and the fact that the quantifier elimination for $\neg\varphi$ is done in the same way as for φ, we may assume that Q_n is the existential quantifier.

Further, by the theorem on the disjunctive normal form, there are formulas $\psi_1, \ldots, \psi_k$ such that $\psi \Leftrightarrow \psi_1 \vee \ldots \vee \psi_k$ and each formula ψ_i is a conjunction of formulas of the form $u = 0$, $v \neq 0$, since every algebraic expression of T is equal to a polynomial. Since $v_1 \neq 0 \wedge \ldots v_m \neq 0 \Leftrightarrow v_1 v_2 \ldots v_n \neq 0$ we may suppose that every disjunct ψ_i is of the form

$$a_1 = 0 \wedge \ldots \wedge a_m = 0 \wedge b \neq 0.$$

Using (valid formula) $(\exists x) \bigvee_i \psi_i \Leftrightarrow \bigvee_i (\exists x) \psi_i$ it follows that it is sufficient to eliminate quantifiers for formulas of the form

$$(\exists x)(a_1 = 0 \wedge \ldots \wedge a_m = 0 \wedge b \neq 0). \tag{5}$$

Let us denote by θ the formula (5). Now we describe the recursive procedure of the quantifier elimination for θ. Let $\lambda_i x^{n_i}$ be the highest degree member of the polynomial $a_i(x)$, $i = 1, \ldots, m$, and let $n_0 = m + \sum_i n_i$. We shall determine the formulas θ_1 and θ_2 of the form (5) such that $\theta \Leftrightarrow \theta_1 \vee \theta_2$ and $n_{\theta_1}, n_{\theta_2} < n_\theta$ if $n_\theta > 1$ and $m \geq 2$.

First suppose that $n_1 = 0$. Then

$$\theta \Leftrightarrow a_1 = 0 \wedge (\exists x)(a_2 = 0 \wedge \ldots \wedge a_m = 0 \wedge b \neq 0).$$

So, assume that $n_1 > 0$ and $m > 1$. We can also suppose that $n_2 \leq n_1$. Let $a_1' = \lambda_2 a_1 - \lambda_1 x^{n_1 - n_2} a_2$, $a_2' = a_2 - \lambda_2 x^{n_2}$. Then

$$\begin{aligned} \theta \Leftrightarrow & (\lambda_2 = 0 \wedge (\exists x)(a_1 = 0 \wedge a_2' = 0 \wedge \ldots \wedge a_m = 0 \wedge b \neq 0)) \wedge \\ & (\lambda_2 \neq 0 \wedge (\exists x)(a_1' = 0 \wedge a_2 = 0 \wedge \ldots \wedge a_m = 0 \wedge b \neq 0)). \end{aligned}$$

Now it is clear that for θ_1 we can choose the first disjunct and for θ_2 the second disjunct of the right side of this equivalence. In this way, the recursive procedure of the quantifier elimination is defined which reduces the formula to the cases (2) and (3) whose solutions are described above.

Now, we can derive few corollaries for the theory of algebraically closed fields T^*.

1. Let φ be a sentence of the field theory and let ψ be the quantifier free formula such that $T^* \vdash \varphi \Leftrightarrow \psi$. Then ψ is variable free. Since the language of the field theory is $\{+, \cdot, 0, 1\}$, it is clear that for ψ we can take a Boolean combination of formulas of the form $n = 0$, where $n = 1 + \ldots + 1$ (n times). If $p_1, \ldots, p_k$ are all prime factors of n then $T^* \vdash n = 0 \Leftrightarrow p_1 = 0 \vee \ldots \vee p_k = 0$. Further, for a formula φ of T^* and distinct primes p, q we have:

1° $T^* \vdash p = 0 \Rightarrow q \neq 0$, 2° $T^* \vdash p = 0 \vee q \neq 0 \Leftrightarrow q \neq 0$,

3° $T^* \vdash p = 0 \vee (p \neq 0 \wedge \varphi) \Leftrightarrow p = 0 \vee \varphi$,

4° $p = 0 \wedge q = 0$ is inconsistent with T^*.

Using DNF and the above listed properties, we see that $T^* \vdash \psi \Leftrightarrow \psi'$, where ψ' is true, false, or one of the formulas:

$p_1 = 0 \vee p_2 = 0 \vee \ldots \vee p_k = 0$,

finite disjunction of formulas of the form $q_1 \neq 0 \wedge q_2 = 0 \wedge \ldots q_l = 0$,

where $p_1, p_2, \ldots, p_k, q_1, q_2, \ldots, q_l$ are distinct primes. As for a prime q in any field $\mathbf{F}$ of finite characteristic holds

$$q \neq 0 \Leftrightarrow \bigvee_{p \neq q} p = 0,$$

it follows that all complete extensions of theory T^* are the theories of the form $T_p = T^* \cup \{p = 0\}$, p is prime, (theories of algebraically closed fields of the characteristic p), and $T_0 = T^* \cup \{p_1 \neq 0, p_2 \neq 0, p_3 \neq 0, \ldots\}$, p_i are primes, (the theory of algebraically closed fields of the characteristic 0).

2. We have just described all complete extensions of T^*, and we see that there are countable many of them, and all of them can be listed in an effective and uniform way. Therefore, see e.g. Theorem 2.4.15, p. 57, [Mijajlović 1987], the theory of algebraically closed fields is decidable. Let us remind the reader that the field theory is not decidable.

3. Real closed fields

Artin-Schreier theory of real fields is used for the solution of seventeenth Hilbert's problem in the algebraic way. Beside it has applications in the other parts of mathematics, especially in algebraic geometry, as in Hilbert's the proof of Nullstellensatz, and nonstandard analysis. We note that every model of nonstandard analysis is a real algebraically closed field. On the other side, we used elements of this theory in the development of an algorithm for quantifier elimination for the theory of ordered real closed fields.

Sturm's algorithm

The quantifier elimination for the theory of algebraically closed fields can be done in somewhat another way. Let $\mathbf{F}$ be an algebraically closed field and let f and g be polynomials over $\mathbf{F}$ in the variable x. If f and g have a common root a, then the greatest common divisor of polynomials f and g is of degree ≥ 1 (since $x - a$ divides both f and g). Thus

$$(\exists x)(f(x) = 0 \wedge g(x) = 0) \Leftrightarrow \text{degree GCD}(f, g) \geq 1.$$

The GCD(f, g) can be found bu use of the Euclid algorithm. For given polynomials f and g the algorithm ends in finally many steps, because its

length depends essentially only on the degrees of f and g. Hence, we can easily see that this algorithm is described with the quantifier free formula, i.e. if

$$
\begin{aligned}
&f = q_1 g + m_2, \quad g = q_2 m_2 + m_3, \quad m_2 = q_3 m_3 + m_4, \ldots, \\
&m_{i-2} = q_{i-1} m_{i-1} + m_i, \quad m_{i-1} = q_i m_i \qquad \text{and} \\
&\deg(f) > \deg(g) > \deg(m_2) > \ldots > \deg(m_i),
\end{aligned} \tag{1}
$$

then

$$(\exists x)(f(x) = 0 \wedge g(x) = 0) \Leftrightarrow f = q_1 g + m_1 \wedge \ldots \wedge m_{i-1} = q_i m_i \wedge z \neq 0,$$

where z is the coefficient of the highest degree of variable x in m_i. Note that the right side of this equivalence is quantifier free. The other details of the proof are the same as in Section 2.

The method of the quantifier elimination for the theory of ordered real closed fields is similar to the previous procedure for algebraically closed fields. In fact, the procedure for the ordered real closed fields can be built on Sturm's algorithm in the way the above described algorithm is using the Euclid algorithm.

Sturm's Theorem. *Let $p(x)$ be a real polynomial and let $p_0, p_1, \ldots, p_r$ be the sequence of real polynomials defined by:*

1. $p_0 = p$.
2. $p_1 = p'$, where p' is the first derivation of p.
3. For all i, $0 < i < r$, there is a polynomial q such that $p_{i-1} = p_i q_i - p_{i+1}$, where $p_{i+1} \neq 0$ and $\deg(p_{i+1}) < \deg(p_i)$. In other words q_i is the quotient, $-p_{i+1}$ is the reminder when p_{i-1} is divide by p_i.
4. $p_{r-1} = p_r q_r$.

Let $d(a)$ be the number of the sign changes in the sequence $p_0(a), \ldots, p_r(a)$ (zeroes are ignored). Let a and b be real numbers which are not roots of p and let $a < b$. Then the number of roots of p (not counting the multiplicity of a root) in the interval $[a, b]$ is equal to $d(a) - d(b)$.

Now we give an illustration of Sturm's theorem application to the quantifier elimination on the example of a formula of the theory of ordered fields. Applying Sturm's theorem we get at once

$$(\exists x)(a < x \wedge x < b \wedge p(x) = 0) \Leftrightarrow d(a) > d(b).$$

Besides, similarly as for the formula (1), using Sturm's theorem, we can find quantifier free formulas ψ such that $d(a) > d(b) \Leftrightarrow \psi$. In this way the quantifier is eliminated from the formula $(\exists x)(a < x < b \wedge p(x) = 0)$.

Further reduction is obtained similarly to the procedure of algebraically closed fields. In this reduction the following equivalence is useful:

$$p_1 = 0 \wedge \ldots \wedge p_n = 0 \Leftrightarrow p_1^2 + \ldots + p_n^2 = 0$$

(note that this formula is not a theorem of the theory of algebraically closed fields).

Also, one can obtain in a similar way the following for the theory T of ordered real closed fields:

1. T is complete,
2. T is decidable.

4. Programming implementation

A group of students under our supervision implemented a prover for the theory of algebraically closed fields in the standard programming language C. The program is based on the procedures described in Section 2. It is running well on personal computers quickly solving problems stated in the language of the field theory. The input formula is proved or refuted by reducing it to a quantifier free formula.

The processing of sentences with more than a few quantifiers would be greatly accelerated with the introduction of fast calculators for long and very long disjunctive normal forms, and fast DNF transformers, which are suitable for parallelisation.

The prover for ordered real closed fields based on Sturm's theorem is being integrated. The plan is to optimize, accelerate and collect these procedures in one Elementary Mathematics problem solver, which might be expanded to other applications as well.

Let us mention just one possible application, namely we can apply the method of elimination of quantifiers in mathematical programming. Programming problem with algebraic constraints in several variables $x_1, \ldots, x_n$

$$f \longrightarrow \min, \quad p_1 = 0, \ldots, p_k = 0, \quad q_1 > 0, \ldots, q_m > 0$$

where $f, p_1, \ldots, p_k, q_1, \ldots, q_m$ are polynomials in variables $x_1, \ldots, x_m$ with rational coefficients, is easily stated in the theory of ordered fields as follows:

$$\begin{aligned}
&\exists x_1 \ldots x_n (y = f(x_1, \ldots, x_n) \wedge \\
&p_1(x_1, \ldots, x_n) = 0 \wedge \ldots \wedge p_k(x_1, \ldots, x_n) = 0 \wedge \\
&q_1(x_1, \ldots, x_n) > 0 \wedge \ldots \wedge q_m(x_1, \ldots, x_n) > 0) \wedge \\
&\forall x_1 \ldots x_n (p_1(x_1, \ldots, x_n) = 0 \wedge \ldots \wedge p_k(x_1, \ldots, x_n) = 0 \wedge \\
&q_1(x_1, \ldots, x_n) > 0 \wedge \ldots \wedge q_m(x_1, \ldots, x_n) > 0 \Rightarrow \\
&y \leq f(x_1, \ldots, x_n))).
\end{aligned}$$

Eliminating quantifiers from the above formula, we obtain a formula $\psi(y)$ of the theory of ordered fields in the single variable y. This formula is a finite disjunction of the formulas of the form $y > r$, $y < r$, $y = r$, where r is a rational number. Obviously this is a solution of the above stated mathematical programming problem. Observe that we, in fact, proved that problem of finding of solutions of mathematical programming problems with polynomial constraints is decidable.

5. Bibliographical and other remarks

First and most important step in the solution of the seventeenth Hilbert's problem was given in [Artin 1927]. Artin-Schreir theory of formally real fields is presented in detail in [Lang 1965]. The proof of Hilbert's basis theorem can be found in [Artin 1955]. Solution of Hilbert's seventeenth problem with described methods of mathematical logic is given in [Robinson 1955]. Elimination of quantifiers in the theory of algebraically closed fields and in the theory of ordered real closed fields with some detailed analysis evolving from these procedures, could be found in [Kreisel, Krivine 1971]. Here presented procedure of elimination of quantifiers differs from the last source, e.g. where we use the resultant of polynomials, in [Kreisel, Krivine 1971] one lemma which relates to divisibility of polynomials is used.

The proof of the theorem on resultant of polynomials could be found in any book on higher algebra, for example in [Kurepa 1965].

Complete solution of Hilbert's seventeenth problem based on Logic can be found in [Cherlin 1976] as well.

Problem of quantifier elimination can be treated in model theory in other way, too. In the other approach the diagrams of models, saturated models and elementary embedding have special importance. This approach is more complex but results are deeper, see ([Sacks 1972]).

References

[1] E. Artin, *Über die Zerlegung definiter Funktionen in Quadrate*, Abhandlungen aus dem mathematischen Seminar der Universitat Hamburg **5** (1927), 100-115.

[2] E. Artin, *Elements of Algebraic Geometry*, Courant Institute of Mathematical Scienes, New York University, New York, 1955..

[3] C.C. Chang, H.J. Keisler, *Model Theory*, North-Holland, Amsterdam, 1973.

[4] G. Cherlin, *Model-Theoretoc Algebra: Selected Topics, Lecture Notes in Mathematics 521*, Springer, Berlin, 1976.

[5] G. Kreisel, J.L. Krivine, *Elements of Mathematical Logic : Model Theory*, North-Holland, Amstedam, 1971.

[6] Đ. Kurepa, *Viša algebra I*, Školska knjiga, Zagreb, 1965.

[7] S. Lang, *Algebra*, Addison-Wesley, Reading Mass., 1965.

[8] Ž. Mijajlović, Z. Marković, K. Došen, *Hilbertovi problemi i logika*, Zavod za udžbenike i nastavna sredstv, Beograd, 1986..

[9] Ž. Mijajlović, *An Introduction to Model Theory*, Univ. of Novi Sad, Institute of Mathematics, Novi Sad, 1987.
[10] A. Robinson, *On ordered fields and definite functions*, Mathematishe Annalen **130** (1955), 257-277..
[11] G. Sacks, *Saturated Model Theory*, Benjamin, Reading Mass., 1972.
[12] J.R. Shoenfield, *Mathematical Logic*, Addison-Wesley, Reading Mass, 1967.

Matematički fakultet, Studentski trg 11, 11000 Beograd, Yugoslavia