Quantifier Elimination - Algorithms and Applications

Miloš Milošević, Dragan Doder, Mirna Udovičić, Filip Marić

GIS (Group for Intelligent Systems), Faculty of Mathematics, University of Belgrade, www.gisss.com, *email*: info@gisss.com

Abstract: In this paper we will explain some basic notions related to quantifier elimination in the first order theories. We will give algorithms for quantifier elimination in theories of dense linear orders and algebraically closed fields. At the end, we will see some applications of quantifier elimination in ACF. This article is the part of our long-range research, in GIS, on quantifier elimination.

1 Introduction

First we list basic definitions and well-known theorems, which are of importance for quantifier elimination; the sketches of the proofs are included if they are illustrative and important for the comprehension of considered problems.

The language $\mathcal{L}$ is recursive if the set of codes for symbols from $\mathcal{L}$ is recursive. The first order theory T is recursive if the set of codes for axioms for T is recursive. An $\mathcal{L}$–theory T is complete if for every sentence ϕ in language $\mathcal{L}$ the following holds:

$$T \vdash \phi \quad \text{or} \quad T \vdash \neg\phi \ .$$

For each theory T arises question of its decidability, i.e. existence of algorithm which for given $\phi \in \mathcal{S}ent_{\mathcal{L}}$ gives an answer whether $T \vdash \phi$ or $T \nvdash \phi$. In the case of a recursive complete theory in a recursive language, the answer is affirmative.

Definition 1: *A theory T of language $\mathcal{L}$ admits quantifier elimination if for every $\phi(\overline{v}) \in \mathcal{F}or_{\mathcal{L}}$ there is a quantifier free formula $\psi(\overline{v})$ such that*

$$T \vdash \forall \overline{v}(\phi(\overline{v}) \leftrightarrow \psi(\overline{v}))$$

Every formula is equivalent to its prenex normal form

$$Q_1 x_1 \ldots Q_n x_n \varphi(x_1, \ldots, x_n, y_1, \ldots, y_m)$$

where $Q_i \in \{\forall, \exists\}$ and φ is a formula without quantifiers in DNF; formula of the form $\forall x \varphi$ is equivalent to $\neg\exists x \neg\varphi$; $\exists x(\varphi \vee \psi) \leftrightarrow \exists x \varphi \vee \exists x \psi$ is a valid formula. Using previous three facts we see that an $\mathcal{L}$–theory T admits quantifier elimination if and only if for every $\mathcal{L}$–formula of the form $\exists x \varphi(\overline{y}, x)$, where φ is a conjunction of atomic formulas and negations of atomic formulas, exists T-equivalent quantifier free formula $\psi(\overline{y})$.

Specification : general algorithm for quantifier elimination in theory T
Input : formula φ in language $\mathcal{L}$ of T
Output : quantifier free formula ψ which is $T-$equivalent to φ
convert φ to prenex normal form $Q_1x_1 \dots Q_nx_n\chi(x_1, \dots, x_n, y_1, \dots, y_m)$
$i := n$
while $i > 0$ do
    if Q_i is $\forall$ replace $Q_ix_i\chi_i$ with $\neg\exists x_i\neg\chi_i$
    transform the matrix of the formula to DNF
    let the existential quantifier pass through disjunction
    eliminate existential quantifier using the specific algorithm for theory T
    $i := i - 1$
end
end

There are several tests for checking whether the given theory has quantifier elimination or not. Using appropriate tests we can prove that theories DLO and ACF [1] have quantifier elimination. Also, making a back-and-forth construction we show that DLO is $\aleph_0$-categorical [2]; ACF$_p$ is κ-categorical for every $\kappa > \aleph_1$, because algebraically closed field of transcendence degree κ has $\kappa + \aleph_0$ elements and two algebraically closed fields are isomorphic if and only if they have the same characteristic and transcendence degree over the basic field $\mathbb{Z}_p$ or $\mathbb{Q}$. Theories DLO and ACF$_p$ don't have finite models and are κ-categorical for some infinite κ, so Vaught's test implies their completeness; now we can conclude that these theories are decidable as recursive complete theories in recursive languages.

By the following theorem we can prove the existence of algorithms for quantifier elimination in DLO and ACF$_p$:

Theorem 1: Suppose that T is a decidable theory which admits quantifier elimination. Then there is an algorithm which for given formula ϕ finds $T-$equivalent formula ψ without quantifiers.

Proof. Let ϕ has n free variables and let $(\psi_i)_{i\in\mathbb{N}}$ is an effective enumeration of all quantifier free formulas in language $\mathcal{L}$ with n free variables. Since T is decidable, there is an algorithm which decides whether $T \vdash \phi \leftrightarrow \psi_1$ or $T \nvdash \phi \leftrightarrow \psi_1$. If not $T \vdash \phi \leftrightarrow \psi_1$, we go forth on ψ_2 etc. The described procedure will halt because T has quantifier elimination. □

In next two sections we will give concrete algorithms for these two theories.

[1] See sections 2 and 3 for details about DLO and ACF

[2] Theory T is κ-categorical for an infinite cardinal κ if any two models of T of cardinality κ are isomorphic

2 An algorithm for quantifier elimination in DLO

The language of the theory of dense linear orders contains just one binary relation symbol $<$. The axioms are:

$$\begin{array}{l} \forall x \neg (x < x) \\ \forall x \forall y \forall z ((x < y \land y < z) \rightarrow x < z) \\ \forall x \forall y (x < y \lor x = y \lor y < x) \\ \forall x \forall y (x < y \rightarrow \exists z (x < z < y)) \\ \forall x \exists y \exists z (y < x < z) \end{array}$$

The first three axioms are axioms for linear orders. As we have seen, it is sufficient to eliminate the quantifiers in the formula of the form $\exists x \varphi$, where φ is a conjunction of atomic formulas and negations of atomic formulas. In this specific theory we can replace $\neg x < y$ with $y < x \lor y = x$, and $\neg x = y$ with $x < y \lor y < x$; with obtained formula we proceed as described in introduction. Now, we give an algorithm for quantifier elimination in this theory:

Specification : algorithm $eqDLO(\psi, n)$ for elimination of quantifiers in DLO
Input : formula ψ which is of the form $\exists x(a_1 \land \ldots \land a_n)$, where a_i are atomic formulas and n is the lenght of conjuction
Output : formula φ without quantifiers equivalent to ψ

if $n = 1$ and $\psi \equiv \exists x(y < z)$
 { if $y = x$ and $z = x$ $\{\varphi :=\ false;$ break; }
   if $y \neq x$ and $z \neq x$ $\{\varphi := y < z;$ break; }
   if ($y = x$ and $z \neq x$) or ($y \neq x$ and $z = x$) $\{\varphi := true;$ break; }
 }
if $n = 1$ and $\psi \equiv \exists x(y = z)$
 { if $y \neq x$ and $z \neq x$ $\{\varphi := y = z;$ break; }
   $\varphi := true;$ break;
 }
if for some i $a_i \equiv y < z$ ($y, z \neq x$)
 $\{\psi_1 := \exists x(a_1 \land \ldots \land a_{i-1} \land a_{i+1} \land \ldots \land a_n);$
   $\varphi_1 := eqDLO(\psi_1, n-1);$
   $\varphi := a_i \land \varphi_1;$
 }
if for some i $a_i \equiv y = z$ ($y, z \neq x$)
 $\{\psi_1 := \exists x(a_1 \land \ldots \land a_{i-1} \land a_{i+1} \land \ldots \land a_n);$
   $\varphi_1 := eqDLO(\psi_1, n-1);$
   $\varphi := a_i \land \varphi_1;$
 }
if for some i $a_i \equiv x < x$ $\varphi := false;$
if for some i $a_i \equiv x = x$
 $\{\psi_1 := \exists x(a_1 \land \ldots \land a_{i-1} \land a_{i+1} \land \ldots \land a_n);$

$\varphi := eqDLO(\psi_1, n-1);$
}

if φ is of the form $\exists x(x < y_1 \wedge \ldots \wedge x < y_k \wedge$
$u_1 < x \wedge \ldots \wedge u_l < x \wedge x = v_1 \wedge \ldots \wedge x = v_m)$
{
if $k > 1$
{ $\psi_1 := \exists x(x < y_1 \wedge x < y_3 \wedge \ldots \wedge x = v_m);$
$\psi_2 := \exists x(x < y_2 \wedge x < y_3 \wedge \ldots \wedge x = v_m);$
$\varphi_1 := eqDLO(\psi_1, n-1);$
$\varphi_2 := eqDLO(\psi_2, n-1);$
$\varphi := (y_1 < y_2 \wedge \varphi_1) \vee (\neg(y_1 < y_2) \wedge \varphi_2);$
}
if $l > 1$
{ $\psi_1 := \exists x(x < y_1 \wedge \ldots \wedge u_2 < x \wedge u_3 < x \wedge \ldots \wedge x = v_m);$
$\psi_2 := \exists x(x < y_1 \wedge \ldots \wedge u_1 < x \wedge u_3 < x \wedge \ldots \wedge x = v_m);$

$\varphi_1 := eqDLO(\psi_1, n-1);$
$\varphi_2 := eqDLO(\psi_2, n-1);$
$\varphi := (u_1 < u_2 \wedge \varphi_1) \vee (\neg(u_1 < u_2) \wedge \varphi_2);$
if $m > 1$
{ $\psi_1 := \exists x(x < y_1 \wedge \ldots \wedge x < y_k \wedge u_1 < x \wedge \ldots \wedge u_l < x \wedge x = v_1);$
$\varphi := v_1 = v_2 \wedge \ldots \wedge v_{m-1} = v_m \wedge eqDLO(\psi_1, n-m+1);$
}
if $k = l = m = 1$ $\varphi := u_1 < v_1 \wedge v_1 < y_1;$
if $k = l = 1,\ m = 0$ $\varphi := u_1 < y_1;$
if $l = 0, m = k = 1$ $\varphi := v_1 < y_1;$
if $k = 0, m = l = 1$ $\varphi := u_1 < v_1;$
}
end

3 An algorithm for quantifier elimination in ACF

The language of fields is $\mathcal{L} = \{+, -, \cdot, 0, 1\}$, where $+$ and $\cdot$ are binary function symbols, $-$ is unary function symbol, and 0 and 1 are constant symbols. The axioms for fields are:

$$\begin{array}{l}
\forall x \forall y \forall z\ x + (y + z) = (x + y) + z \\
\forall x\ x + 0 = 0 + x = x \\
\forall x\ x + (-x) = (-x) + x = 0 \\
\forall x \forall y\ x + y = y + x \\
\forall x \forall y \forall z\ x \cdot (y \cdot z) = (x \cdot y) \cdot z \\
\forall x\ x \cdot 1 = 1 \cdot x = x \\
\forall x \forall y\ x \cdot y = y \cdot x \\
\forall x(\ x \neq 0 \rightarrow \exists y\ x \cdot y = 1)
\end{array}$$

$$\forall x \forall y \forall z \; x \cdot (y+z) = (x \cdot y) + (x \cdot z)$$
$$\forall x \forall y \forall z \; (x+y) \cdot z = (x \cdot z) + (y \cdot z)$$

We could axiomatize the class of algebraically closed fields by adding, for each $n \geqslant 1$, the axiom :

$$\forall a_0 \ldots \forall a_n \exists x \; a_n x^n + \ldots + a_0 = 0.$$

As we have noticed in the introduction, in order to obtain the algorithm for quantifier elimination in algebraically closed fields, it is sufficient to know how to eliminate the existential quantifier in the formula of the form

$$\exists x (p_1(x) = 0 \wedge \ldots \wedge p_m(x) = 0 \wedge q_1(x) \neq 0 \wedge \ldots \wedge q_n(x) \neq 0),$$

where coefficients of p_i and q_j are polynomials from $\mathbb{Z}[y_1, \ldots, y_k]$, $y_i \neq x$. The crucial part is the polynomial pseudo-division algorithm. We pseudo-divide $s(x) = a_n x^n + s_1(x)$ by $p(x) = b_m x^m + p_1(x)$, where $s(x)$, $p(x) \in \mathbb{Z}[y_1, \ldots, y_k, x]$, a_n, $b_m \in \mathbb{Z}[y_1, \ldots, y_k]$, $deg_x s_1(x) < n$ and $deg_x p_1(x) < m$, by finding $k \in \mathbb{N}$ and $q(x), r(x) \in \mathbb{Z}[y_1, \ldots, y_k, x]$ such that

$$b_m^k s(x) = q(x)p(x) + r(x),$$

where $deg_x r(x) < deg_x p(x)$ (deg_x- degree in variable x). We denote by lc_x the leading coefficient in x.

Specification : algorithm $pseudo(s(x), p(x))$ for pseudo $-$ division
Input : $s(x), p(x)$
Output : $k, q(x), r(x)$

begin
$r(x) := s(x)$
$q(x) := 0$
$k := 0$
while $deg_x r(x) \geqslant m$ do
  $q(x) := b_m q(x) + lc_x(r(x)) x^{deg_x r(x) - m}$
  $r(x) := b_m r(x) - lc_x(r(x)) x^{deg_x r(x) - m} p(x)$
  $k := k + 1$
end
$return(k, q(x), r(x))$
end.

This algorithm will terminate, because in each step $deg_x r(x)$ will decrease. We can prove by induction that in l-th step holds

$$b_m^l s(x) = q_l(x)p(x) + r_l(x),$$

so the algorithm really returns pseudo-quotient and pseudo-remainder. We will use next algorithm several times in the main algorithm:

Specification : algorithm $decrease(\psi)$ which for given formula returns equivalent disjunction of the conjunctions, where each conjunction contains only one atomic formula in which x occurs

Input : formula ψ which is the conjunction of atomic formulas

Output φ

begin

write the formula ψ in the form

$p(x) = 0 \wedge p_1(x) = 0 \wedge \ldots \wedge p_n(x) = 0 \wedge c_1 = 0 \wedge \ldots c_m = 0,$

where $1 \leqslant deg_x p \leqslant deg_x p_i,\ deg_x c_j = 0$ and $p(x) = ax^l + q(x),\ deg_x q < deg_x p$

if $n = 0$ then $\varphi := \psi$

else begin

for $i = 1, n\ pseudo(p_i(x), p(x))$

($pseudo$ will return pseudo − remainders r_i)

$\varphi := decrease(a = 0 \wedge q(x) = 0 \wedge p_1(x) = 0 \wedge \ldots \wedge p_n(x) = 0 \wedge c_1 = 0 \wedge \ldots \wedge c_m = 0) \quad \bigvee$

$decrease(a \neq 0 \wedge p(x) = 0 \wedge r_1(x) = 0 \wedge \ldots \wedge r_n(x) = 0 \wedge c_1 = 0 \wedge \ldots c_m = 0)$

end

end

Specification : algorthm $eqACF(\psi)$ for quantifier elimination in ACF

Input : formula ψ which is of the form

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

(atomic formulas which don′t contain x are already outside the scope of the quantifier)

Output : formula φ, without quantifiers, equivalent to ψ

begin

if $m > 1$ replace the conjuction of inequalities with $q_1(x) \ldots q_m(x) \neq 0$

if $n > 1$ replace the conjuction of equalities with

$decrease(p_1(x) = 0 \wedge \ldots \wedge p_n(x) = 0)$, transform the obtained formula to DNF, let the existential quantifier pass through disjunction, and for each disjunct pull out all atomic formulas and the negations of atomic formulas, which don′t contain x, outside the scope of the quantifier, and for each disjunct proceed algorithm

if $\psi \equiv \exists x(a_n x^n + \ldots + a_0 = 0)$ then $\varphi := a_0 = 0 \vee a_1 \neq 0 \vee \ldots \vee a_n \neq 0$

if $\psi \equiv \exists x(a_n x^n + \ldots + a_0 \neq 0)$ then $\varphi := a_0 \neq 0 \vee a_1 \neq 0 \vee \ldots \vee a_n \neq 0$

if $\psi \equiv \exists x(p(x) = 0 \wedge q(x) \neq 0)$ then

begin

write $p(x)$ in the form $ax^n + p_1(x), deg_x p_1(x) < n$

$pseudo(aq(x)^n, p(x))$ ($pseudo$ will return pseudo − remainder r)

$\varphi := (a \neq 0 \wedge eqACF(\exists x(r(x) \neq 0))) \ \bigvee$

$(a = 0 \wedge eqACF(\exists x(p_1(x) = 0 \wedge q(x) \neq 0)))$

end

4 Applications of quantifier elimination in ACF

In this section we give elegant proofs for some well-known theorems from algebraic geometry. All these proofs are based on the fact that ACF has quantifier elimination.

Theorem 2(weak Nullstellensatz) Let K be an algebraically closed field and $f_1(\overline{X}), \ldots, f_n(\overline{X}) \in K[\overline{X}]$. Then the system of polynomial equations $f_1(\overline{X}) = 0, \ldots, f_n(\overline{X}) = 0$ has a solution in K if and only if $1 \notin < f_1(\overline{X}), \ldots, f_n(\overline{X}) >$, where $< f_1(\overline{X}), \ldots, f_n(\overline{X}) >$ is the ideal in $K[\overline{X}]$ generated by $f_1(\overline{X}), \ldots, f_n(\overline{X})$.

Proof. Let $1 \notin < f_1(\overline{X}), \ldots, f_n(\overline{X}) >$; then the ideal $< f_1(\overline{X}), \ldots, f_n(\overline{X}) >$ is a proper ideal and it is contained in some prime ideal P. We denote by L the algebraic closure of the fraction field of $K[\overline{X}]/P$. $(X_1 + P, \ldots, X_n + P)$ is the solution of the system $f_1(\overline{X}) = 0, \ldots, f_n(\overline{X}) = 0$ in algebraically closed field L; thus

$$L \models \exists \overline{x}\ (f_1(\overline{x}) = 0 \wedge \ldots \wedge f_n(\overline{x}) = 0).$$

The formula $\exists \overline{x}\ (f_1(\overline{x}) = 0 \wedge \ldots \wedge f_n(\overline{x}) = 0)$ is equivalent to some quantifier free formula φ, with parameters from K, because theory ACF admits quantifier elimination. By the construction, K is substructure of L, which means that for every quantifier free formula ψ and for every $\overline{a} \in K$ holds:

$$K \models \psi(\overline{a}) \text{ if and only if } L \models \psi(\overline{a}).$$

We have the following equivalences:

$$L \models \exists \overline{x}\ (f_1(\overline{x}) = 0 \wedge \ldots \wedge f_n(\overline{x}) = 0) \ \Leftrightarrow\ L \models \varphi \ \Leftrightarrow$$

$$K \models \varphi \ \Leftrightarrow\ K \models \exists \overline{x}\ (f_1(\overline{x}) = 0 \wedge \ldots \wedge f_n(\overline{x}) = 0).$$

The given system has a solution in L, so, by the upper equivalence, it must have a solution in K. The rest of the proof is obvious. □

Let $K \models$ ACF and $A \subseteq K^n$. We call A constructible, if it is definable by a formula φ, which is finite boolean combination of atomic formulas, i.e. $A = \{\overline{a} \in K^n |\ K \models \varphi(\overline{a})\}$.

Theorem 3(Chevalley's Theorem) The image of a constructible set under a polynomial map is constructible.

Proof. Suppose that $A = \{\overline{x} \in K^m \mid K \models \varphi(\overline{x}, \overline{a})\}$ is a constructible set and that $f : K^m \to K^n$ is a polynomial map. $B = f[A] = \{\overline{y} \in K^n \mid K \models \exists x(\varphi(\overline{x}, \overline{a}) \wedge f(\overline{x}) = \overline{y})\}$ is a definable set. Using the quantifier elimination in ACF, we can represent B as $\{\overline{y} \in K^n \mid K \models \psi(\overline{y}, \overline{b})\}$, where formula ψ is without quantifiers and parameters $\overline{b}$ are among $\overline{a}$ and coefficients of f. Thus B is constructible. □

References

[1] S. Lang, *Algebra*, Addison–Wesley, 1965

[2] F. Marić, M. Borovčanin, M. Marić, *Quantifier elimination in fields*, Proc. XLVIII ETRAN Conference, Čačak, June 2004, to appear

[3] F. Marić, M. Marić, Ž. Mijajlović, A. Jovanović, *Theorem provers based on the quantifier elimination method*, Proc. XLVII ETRAN Conference, Herceg Novi, June 8–13, 2003, Vol. 3

[4] D. Marker, *Model theory–an introduction*, Springer–Verlag 2002.

[5] D. Marker, M. Messmer, A. Pilay, *Model theory of fields*, Springer–Verlag 1996.

[6] Ž. Mijajlović, *An introduction to model theory*, University of Novi Sad, 1987.

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

[8] M. Milošević, M. Udovičić, D. Doder, D. Ilić, *Quantifier elimination in mathematical theories*, Proc. XLVIII ETRAN Conference, Čačak, June 2004, to appear