Linear Problems in Valued Fields

THOMAS STURM[†]

Fakultät für Mathematik und Informatik, Universität Passau, 94030 Passau, Germany

MIP 9815

3 November 1998

A first-order formula over a valued field is called linear if it contains no products or reciprocals of quantified variables. We give quantifier elimination procedures based on test term ideas for linear formulas in the following classes of valued fields: discretely valued fields, discretely valued fields with a $\mathbb{Z}$-group as value group over a language containing predicates stating divisibility in the value group, and non-discretely valued fields. From the existence of the elimination procedures, it follows that the corresponding decision problems are in an alternating single exponential time-space (Berman) complexity class. We exhibit the substructure completeness of the considered classes of valued fields wrt. linear formulas.

[†] E-mail: `sturm@uni-passau.de`

1. Introduction

A *quantifier elimination procedure* for a class $\mathfrak{M}$ over a language L is an algorithm that given an L-formula φ computes a quantifier-free L-formula φ' such that $\mathfrak{M} \models \varphi' \longleftrightarrow \varphi$. An L-formula is called *linear* if it contains no products or reciprocals of quantified variables.

Quantifier elimination methods for valued fields have been extensively investigated in the past, cf. Weispfenning (1984) and the references there. The procedures given there are primitive recursive, but far beyond feasibility.

Based on ideas of Ferrante and Rackoff (1979) for decision problems, quantifier elimination by *elimination sets* containing test terms has been introduced for linear formulas by Weispfenning (1988). This technique is very attractive due to its comparatively low complexity $a^{q^{O(c)}}$, where a is the number of atomic formulas, q is the number of quantifiers, and c is the number of quantifier type changes in a prenex input formula. For ordered fields these algorithms have turned out feasible, and implementations including powerful simplification algorithms (Dolzmann and Sturm, 1997b) are applicable to a wide range of both academic and non-academic problems, cf. Dolzmann and Sturm (1997a), Dolzmann *et al.* (1997, 1998), Sturm (1996, 1997), Sturm and Weispfenning (1998).

Weispfenning (1988) has already given elimination sets for discretely valued fields the residue fields of which are either finite or of characteristic zero. This paper extends the elimination set technique to arbitrary valued fields.

The plan of the paper is as follows. It will turn out that different types of residue fields can uniformly be handled only by means of some extra field constant ζ. Section 2 contains the algebraic foundations for the interpretation of ζ, and indicates its role within test terms. We furthermore show how to do without ζ for classes of valued fields the residue fields of which are prime. This covers the important class of p-adic valuations.

Section 3 introduces the underlying languages for the various classes of fields considered. Section 4 describes some elementary equivalence transformations on the input formulas.

Section 5 extends Weispfenning's (1988) notion of Skolem sets to that of "CS sets." This more sophisticated concept makes use of the negation structure of the original formula leading to smaller elimination sets and simpler proofs.

Section 6 introduces a concept for treating equations independently from all other atomic formulas. In Section 7 we describe the application of improper test terms containing dummy symbols, a technique introduced by Loos and Weispfenning (1993) for decreasing the complexity of the elimination sets for ordered fields.

Section 8 exhibits elimination sets and thus a quantifier elimination procedure for linear formulas in discretely valued fields. Restricting to linear formulas where there are not both upper and lower restrictions on the value of terms wrt. any quantified variable, we can give an elimination procedure for linear formulas in the class of *all* valued fields. Section 9 focuses on discretely valued fields with a $\mathbb{Z}$-group as value group. For this class, we can permit an extended language containing predicates $D_n(x)$ that state divisibility of $v(x)$ by $n \in \mathbb{N}$ in the value group.

Section 10 establishes elimination sets and thus a quantifier elimination procedure for linear formulas non-discretely valued fields. From the elimination procedures for the various classes of valued fields, we derive in Section 11 corresponding decision procedures that are in an alternating single exponential time-space complexity class, cf. Berman (1980).

In Section 12 we point on some model theoretic consequences of the existence of our elimination procedures. Section 13 finally summarizes our results.

2. Avoiding Residue Classes

Given a valued field (K, v), we want to solve the following problem: Consider a finite set $C \subseteq K$ of field elements all of the same value μ. Assume further that we know there is some $a \in K$ with $v(a) = \mu$ such that $v(a - c) = v(c) = \mu$ for all $c \in C$. Our aim is to find by testing finitely many field elements some $t \in K$ that can play the role of a, i.e.,

$$v(t - c) = v(t) = v(c) = \mu \quad \text{for all } c \in C.$$

For $\mu = \infty$ the problem is trivial. For finite μ, division of all the c and a by any fixed $c_0 \in C$ allows us to restrict our attention to the case $\mu = 0$. We can then restate the problem as follows. Given a finite set $\overline{C} \subset K_v^\times$ of non-zero residue fields elements find $\overline{t} \in K_v^\times$ such that $\overline{t} \neq \overline{c}$ for all $c \in C$. In other words, find $t \in K$ that *avoids the residue classes* of the $c \in C$. In case that $|K_v^\times| > |C|$, in particular for infinite K_v, one simply has to try $|C| + 1$ elements applying the pigeon hole principle. Else one has to try all elements of $K_v^\times$. Notice that the problem is stated in such a way that there is a suitable residue class, namely that of a. The following lemma encodes these different cases into a field element $\zeta \in K$.

LEMMA 2.1. *Let (K, v) be a valued field, and let $n \in \mathbb{N}$. There is $\zeta \in K$ such that defining $Z(n) = \{1, \zeta, \ldots, \zeta^{n-1}\}$ we have $|\overline{Z(n)}| = |Z(n)| = n$ or $\overline{Z(n)} = K_v^\times$.*

PROOF. In case that $\mathrm{char}(K_v) = 0$, we have also $\mathrm{char}(K) = 0$, and we can set $\zeta = 2$.

Let now $\mathrm{char}(K_v) = p \neq 0$. If K_v is finite, we have $|K_v| = p^k$. Set ζ to the preimage of a $(p^k - 1)$-st root of unity. An infinite K_v is either an infinite algebraic extension of its prime field $\mathbb{Z}/p$ or it is obtained by adjunction of at least one transcendental X. In the former case, K_v contains an m-th root of unity for some $m > n$. We set ζ to a preimage of this. In the latter case, we set ζ to a preimage of X. $\square$

Notice that ζ depends on n only in the case of K_v being an infinite algebraic extension of a finite prime field.

The following proposition formally states our problem and its solution using the sets $Z(n)$ introduced in Lemma 2.1. Notice once more that in most cases the selection of ζ will not depend on $|C|$.

PROPOSITION 2.2. *Let (K, v) be a valued field. Let $\mu \in v(K^\times)$ and let $|C| \subseteq K$ be finite such that $v(c) = \mu$ for all $c \in C$. Let further $a \in K$ with $v(a) = \mu$ such that $v(a - c) = \mu$ for all $c \in C$. Fix $c_0 \in C$, and set*

$$T = \{\, z c_0 \mid z \in Z(|C| + 1) \,\}.$$

Then there is $t \in T$ such that $v(t - c) = \mu$ for all $c \in C$.

Lemma 2.1 provides sets $Z(n)$ which make Proposition 2.2 uniformly correct for the class of *all* valued fields. We are going to sketch how simpler sets $Z(n)$ solve the problem for restricted classes of valued fields. Restricting our attention to valued fields with finite residue class fields up to some fixed cardinality allows to cut off higher powers of ζ.

Corollary 2.3. *For $c \in \mathbb{N}$ let (K, v) be a valued field such that $|K_v^\times| \leqslant c$. There is $\zeta \in K$ such that defining $Z(n) = \{1, \zeta, \dots, \zeta^{\min(n-1,c)}\}$, we have $|\overline{Z(n)}| = |Z(n)| = n$ or $\overline{Z(n)} = K_v^\times$.*

Notice that in the above corollary $|Z(n)|$ is, asymptotically, not longer linear but constant in n. Its depends only on the considered class of valued fields given by c.

If the residue class field is prime both its elements and their preimages are natural numbers. This special case covers the important class of p-adic valuations on the rationals.

Corollary 2.4. *Let (K, v) be a valued field such that K_v is prime, and let $n \in \mathbb{N}$. There is $\zeta \in K$ such that defining $Z(n) = \{1, \dots, n\}$ we have $|\overline{Z(n)}| = |Z(n)| = n$ or $\overline{Z(n)} = K_v^\times$. If moreover $|K_v^\times| \leqslant c$, we can set $Z(n) = \{1, \dots, \min(n, c)\}$.*

Finally notice that we have actually solved a slightly more general problem than stated in the beginning: The strong triangle inequality guarantees that also

$$v(t - d) = v(a - d) = v(d)$$

for all $d \in K$ with $v(d) < \mu$. Moreover, we have $v(t - d) = \mu$ for all $d \in K$ with $v(d) > \mu$.

3. The Underlying Languages

We will use the language of fields, which in contrast to the language of rings includes multiplicative inverses. For completeness, we define $0^{-1} := 0$, a selection which is not relevant for the correctness of our procedures. The valuation is encoded in binary predicates $s \mid t :\longleftrightarrow v(s) \leqslant v(t)$ and $s \parallel t :\longleftrightarrow v(s) < v(t)$. A constant ζ plays the role described in Section 2. We assume ζ not to be present in the input formulas. Then for the critical case of valued fields K where the residue class field K_v is an infinite algebraic extension of some prime field, the interpretation of ζ in the quantifier elimination result can be determined from information obtained during the elimination process. Summarizing, we have the one-sorted language

$$L_\zeta = \{0, 1, \zeta, +, \cdot, -, {}^{-1}, |, \|\}.$$

This language L_ζ will be used for non-discretely valued fields. For discretely valued fields we start out with the language

$$L_{\zeta,\pi} = L_\zeta \cup \{\pi\}$$

where the constant π is interpreted as a field element of minimal positive value. For the restricted class of discretely valued fields the value group of which is a $\mathbb{Z}$-group, we will discuss elimination in the extension

$$L_{\zeta,\pi,D} = L_{\zeta,\pi} \cup \{\, D_n, \bar{D}_n \mid n \in \mathbb{N}\},$$

which contains divisibility predicates $D_n(a) :\longleftrightarrow n \mid_{\mathbb{Z}} v(a)$ stating integer divisibility of the value of their argument by $n \in \mathbb{N}$, and their negated counterparts $\bar{D}_n$.

Most of the methods described throughout this paper need not distinguish between strict and weak divisibilities. For the sake of a more convenient notation, we use the symbol "$\Diamond$," which consistently stands for either "$|$" or "$\|$."

4. Positive Formulas and Bounds

We may wlog. assume our input formulas to be prenex. We refer to $\wedge$-$\vee$-combinations of atomic formulas as *positive formulas.* Including both "$|$" and "$\|$" in L_ζ allows to compute positive equivalents for given formulas according to the equivalences $\neg(s = 0) \longleftrightarrow s \parallel 0$, $\neg(s \mid t) \longleftrightarrow t \parallel s$, and $\neg(s \parallel t) \longleftrightarrow t \mid s$.

With elimination sets the quantifiers are eliminated starting with the innermost. Elimination of universal quantifiers can be reduced to that of existential quantifiers using the equivalence $\forall x\varphi \longleftrightarrow \neg\exists x\neg\varphi$. We hence have to establish a method for the elimination of one existential quantifier in front of a positive formula.

An atomic formula of the form $ax + b \mathrel{\Diamond} a'x + b'$ can be substituted by an equivalent positive formula in which each atomic formula containing x is of the form $x - c \mathrel{\Diamond} d$ or $e \mathrel{\Diamond} x - f$ where the $c, \ldots, f$ are terms not containing x: Provided that $a,\ a' \neq 0$, we have the equivalence

$$ax + b \mathrel{\Diamond} a'x + b' \longleftrightarrow a/a'(x + b/a) \mathrel{\Diamond} x + b/a + (b'/a' - b/a).$$

On the other hand, we can derive the following equivalence from a corresponding result for "$\|$" given by Weispfenning (1988):

$$st \mathrel{\Diamond} s + u \longleftrightarrow \bigl(\neg(t \mathrel{\Diamond} 1) \wedge tu \mathrel{\Diamond} s + u\bigr) \vee \bigl(t \mathrel{\Diamond} 1 \wedge st \mathrel{\Diamond} u\bigr).$$

Application of the this equivalence to the former one yields the non-trivial cases of the following equivalence:

$$\begin{aligned} ax + b \mathrel{\Diamond} a'x + b' \quad \longleftrightarrow \quad & (a = 0 \wedge a' = 0 \wedge b \mathrel{\Diamond} b') \vee \\ & (a = 0 \wedge a' \neq 0 \wedge b/a' \mathrel{\Diamond} x + b'/a') \vee \\ & (a \neq 0 \wedge a' = 0 \wedge x + b/a \mathrel{\Diamond} b'/a) \vee \\ & \bigl(a \neq 0 \wedge a' \neq 0 \wedge \neg(a \mathrel{\Diamond} a') \wedge a/a'(b'/a' - b/a) \mathrel{\Diamond} x + b'/a\bigr) \vee \\ & \bigl(a \neq 0 \wedge a' \neq 0 \wedge a \mathrel{\Diamond} a' \wedge x + b/a \mathrel{\Diamond} a'/a(b'/a' - b/a)\bigr). \end{aligned}$$

At this point, we need multiplicative inverses. Notice, however, that the equivalence does not depend on the definition of 0^{-1}.

We refer to atomic formulas of the form $x - c \mathrel{\Diamond} d$ as *upper bounds* and to those of the form $e \mathrel{\Diamond} x - f$ as *lower bounds.* Both this transformation and the computation of positive formulas above are of linear time-space complexity.

5. Conjunctive Satisfiability

For finding elimination sets it would be convenient to restrict to 1-primitive formulas by computing DNF's and then moving the quantifier inside the disjunction. This should, however, not be done due to complexity reasons. Successive dual normal form computations with every change of the quantifier type would lead to a non-elementary recursive procedure.

On the other hand, the matrices of the 1-primitive formulas obtained above are subconjunctions of the conjunction of all atomic formulas contained in the positive input formula. Our idea is to consider the latter conjunction for the elimination set computation. We then may draw conclusions from the absence but not from the presence of certain atomic formulas.

DEFINITION 5.1. Let A be a finite set of atomic formulas. Then a set of terms T is a *test set for conjunctive satisfiability* (CS set) for A and the variable x if for any $\mathrm{A}' \subseteq \mathrm{A}$ the following holds: For all interpretations of x there is $t \in T$ such that

$$\bigwedge \mathrm{A}' \longrightarrow \bigwedge \mathrm{A}'[x/t].$$

PROPOSITION 5.2. *Let φ be a positive quantifier-free formula, let x be a variable. Then any* CS *set T for the atomic formulas contained in φ and x is an elimination set for $\exists x \varphi$, in other words:*

$$\exists x \varphi \longleftrightarrow \bigvee_{t \in T} \varphi[x/t].$$

PROOF. Let $a \in K$ such that $\varphi(a)$ holds. There is a DNF $\bigvee_{i=0}^{n} \psi_i$ of φ which contains only atomic formulas already present in φ. Assume wlog. that $\psi_0(a)$ holds. Then there is $t \in T$ such that $\psi_0[x/t]$ and hence $\varphi[x/t]$ holds. The converse is obvious. □

The Skolem sets introduced by Weispfenning (1988) have the following property: After fixing an interpretation for all parameters and a quantified variable x, there is a term that, when substituted for x, exactly simulates the truth values of all atomic formulas.

With CS sets in contrast, the situation is as follows: Choose a subset of the atomic formulas, and fix an interpretation for all parameters. For each satisfying interpretation of the quantified variable x, there is a term that, when substituted for x, satisfies all atomic formulas that hold. This will be the structure of our proofs.

6. Treatment of Equations

The next lemma shows how equations can be handled separately from all other predicates. At this point, mind that our languages are supersets of the language of fields including reciprocals.

PROPOSITION 6.1. *Given a variable x and a finite set of atomic formulas* A, *split the latter into linear equations $E = \{\, m_i x + b_i = 0 \mid i \in I \,\}$ and all others $\overline{\mathrm{A}}$. Let T be a* CS *set for $\overline{\mathrm{A}}$ and x. Then $T \cup \{\, -m_i/b_i \mid i \in I \,\}$ is a* CS *set for $\mathrm{A} = \overline{\mathrm{A}} \cup E$ and x.*

PROOF. Consider a subset $\mathrm{A}' \subseteq \mathrm{A}$. Fix an interpretation for all variables except x. Let $a \in K$ such that $\bigwedge \mathrm{A}'(a)$ holds. If A' contains at least one non-trivial linear equation $mx + b = 0$, it follows that $a = -b/m$ is contained in our considered set. Else T is already a CS set, and so is hence any superset. □

The technique given in the lemma does, of course, work for any predicate for which there are at most finitely many satisfying points provided that the considered language allows to substitute these points.

7. Substitution of Dummy Symbols

In addition to proper terms, elimination sets can include certain terms containing dummy symbols $\sigma_1, \ldots, \sigma_n$, which are not part of the underlying language. Such symbols stand for elements of an elementary extension $(K, v) \preccurlyeq (K^*, v^*)$. We will use elements of infinite negative value and elements of infinitesimal positive value. The terms are substituted via a *modified substitution* $[x/\!/t(\underline{\sigma})]$ mapping atomic formulas to quantifier-free formulas containing only proper terms.

The logical background for this is as follows: We expand (K^*, v^*) extending the original language to $L_{\underline{\sigma}} = L \cup \{\sigma_1, \dots, \sigma_n\}$. Consider an L-formula $\exists x\varphi(x, y_1, \dots, y_m)$ with φ quantifier-free. We find a set T of $L_{\underline{\sigma}}$-terms such that for any choice of $a_1, \dots, a_m \in K$ we have

$$(K^*, v^*) \models \Big(\exists x\varphi(x, \underline{y}) \longleftrightarrow \bigvee_{t\in T} \varphi[x/t](\underline{y}) \longleftrightarrow \bigvee_{t\in T} \varphi[x/\!/t](\underline{y})\Big)(\underline{a}).$$

Notice that the last constituent of the equivalence is an L-formula. Since the extension was elementary, we obtain $(K, v) \models \exists x\varphi \longleftrightarrow \bigvee_{t\in T} \varphi[x/\!/t]$.

It easy to see that using a suitable modified substitution Definition 5.1 and Proposition 5.2 can be extended to sets T of terms possibly containing dummy symbols.

8. Elimination in Discretely Valued Fields

We are now going to construct CS sets wrt. a variable x for sets of linear atomic formulas in discretely valued fields over the language $L_{\zeta,\pi}$. The introduction of π would actually allow to drop "$|$" from the language using the equivalence $\neg(s \parallel t) \longleftrightarrow s = 0 \vee t \parallel \pi s$ for the computation of positive formulas. For our purposes, however, it will be advantageous to keep both strong and weak divisibility.

Handling equations as described in Section 6, and transforming all divisibilities into upper and lower bounds, it suffices to construct a CS set for a set

$$\{\, x - c \diamondsuit d,\; e \diamondsuit x - f \mid (c, d) \in I,\; (e, f) \in J \,\}$$

of upper and lower bounds wrt. x. In the sequel, we will use the following convention for denoting the first and second projections of I and J:

$$C = \mathrm{pr}_1(I), \quad D = \mathrm{pr}_2(I), \quad E = \mathrm{pr}_1(J), \quad F = \mathrm{pr}_2(J).$$

First consider the special case that there are no lower bounds. This is surprisingly easy:

LEMMA 8.1. (CS SETS FOR UPPER BOUNDS) *Let x be a variable, and let* $\mathrm{A} = \big\{\, x - c \diamondsuit d \;\big|\; (c, d) \in I \,\big\}$ *with x not occurring in the c, d. Then $\bigwedge \mathrm{A}$ is satisfiable wrt. x, and* $T = \{\, 1, \pi^{-1}c, \pi^{-1}d \mid (c, d) \in I \,\}$ *is a* CS *set for* A *and* x.

PROOF. Fix an interpretation for all variables except x. Choose $m \in C \cup D$ of minimal value. If $m = 0$ we set $t = 1 \in T$, else we set $t = \pi^{-1}m \in T$. In both cases $\bigwedge \mathrm{A}'[x/\!/t]$ holds for all $\mathrm{A}' \subseteq \mathrm{A}$. $\square$

Lemma 8.1 substitutes several terms in order to ensure that there is one term of sufficiently small value among them. This observation suggests to introduce a dummy symbol with infinite negative value.

Consider a valued field (K, v). By the Compactness Theorem of first-order logic, there is an elementary extension $(K, v) \preccurlyeq (K^*, v^*)$ where there is $\infty \in K^*$, not to be confused with $\infty = v(0)$, such that $v^*(\infty) < v^*(x)$ for all $x \in K$. There are suitable modified substitutions for ∞: For a, $b \in K$ an equation $a \cdot \infty + b = 0$ is equivalent in (K^*, v^*) to

$$(ax + b = 0)[x/\!/\infty] :\longleftrightarrow a = 0 \wedge b = 0.$$

For a, b, a', $b' \in K$, an atomic formula $a \cdot \infty + b \diamondsuit a' \cdot \infty + b'$ is equivalent in (K^*, v^*) to

$$(ax + b \diamondsuit a'x + b')[x /\!/ \infty] :\longleftrightarrow (a = 0 \land a' = 0 \land b \diamondsuit b') \lor (a \neq 0 \land a \diamondsuit a').$$

This allows us to treat pure upper bound problems with a constant CS set.

COROLLARY 8.2. (CS SETS FOR UPPER BOUNDS) *Let x be a variable, and let A be a set of upper bounds in x. Then $\bigwedge \mathrm{A}$ is satisfiable wrt. x, and $T = \{\infty\}$ is a CS set for A and x.*

Before turning to the main result of this section, we state an immediate consequence of the strict triangle inequality, which will be used in the proof of the theorem to follow.

LEMMA 8.3. *Let $v(a - c_0) = \mu$. Then from $v(a - s) < \mu$ it follows that $v(s - c_0) = v(a - s)$, and for $v(a - s) = \mu$ we obtain $v(s - c_0) \geqslant v(a - s) = \mu$.*

THEOREM 8.4. (CS SETS FOR MIXED BOUNDS) *Let x be a variable, and let*

$$\mathrm{A} = \{\, x - c \diamondsuit d,\ e \diamondsuit x - f \mid (c, d) \in I,\ (e, f) \in J \,\}$$

with x not occurring in the c, ..., f. Set

$$\begin{aligned} T_0 &= \{\, 1,\ \pi^{-1}c,\ \pi^{-1}d \mid c \in C,\ d \in D \,\} \\ T_1 &= \{\, e + c,\ \pi(c - c') + c' \mid c,\ c' \in C,\ c \neq c',\ e \in E \,\} \\ T_2 &= C \cup F \cup \{\, z(c - c') + c' \mid c,\ c' \in C,\ c \neq c',\ z \in Z(|C|) \,\}. \end{aligned}$$

Then $T_0 \cup T_1 \cup T_2$ is a CS set for A and x.

PROOF. Choose $\mathrm{A}' \subseteq \mathrm{A}$, and let I', J', C', ..., F' be corresponding subsets of I, J, C, ..., F. Fix an interpretation for all variables except x, and assume that $\exists x \bigwedge \mathrm{A}'$ holds with $a \in K$ being a satisfying element. If J' is empty, T_0 contains a suitable test term due to Lemma 8.1. Let now $J' \neq \emptyset$. The case $a \in C' \cup F'$ is captured by T_2. We may henceforth assume that

$$\mu := \max\{\, v(a - s) \mid s \in C' \cup F' \,\} < \infty.$$

If $v(a - c) < \mu$ for all $c \in C'$ there must be some $f_0 \in F'$ with $v(a - f_0) = \mu$. In this case $f_0 \in T_2$ is a suitable test term: We obtain $v(f_0 - c) = v\bigl(a - c - (a - f_0)\bigr) = v(a - c)$ for upper bounds, and $v(f_0 - f) = v\bigl(a - f - (a - f_0)\bigr) \geqslant v(a - f)$ for lower bounds.

Else let $c_0 \in C'$ such that $v(a - c_0) = \mu$. Let $C'' = \{\, c \in C' \mid v(c - c_0) = \mu \,\}$. Again, we have to consider two cases: If C'' is non-empty, we are in the situation discussed in Section 2: We know that

$$v\bigl(a - c_0 - (c - c_0)\bigr) = v(a - c) = \mu \quad \text{for all } c \in C'',$$

and Proposition 2.2 tells us that $\{\, z(c - c_0) \mid c \in C'',\ z \in Z(|C''| + 1) \,\}$ contains a term t that can serve as a substitute for $a - c_0$ in the atomic formulas captured by C''. Substitution of this t for $a - c_0$ actually works for all atomic formulas: For $s \in C' \cup F'$ with $v(a - s) < \mu$ we get $v\bigl(t - (s - c_0)\bigr) = v(a - s)$. For upper bounds with $v(a - c) = \mu$ but $v(c - c_0) > \mu$ we have $v\bigl(t - (c - c_0)\bigr) = \mu$. Finally, for lower bounds with $v(a - f) = \mu$ we obtain $v\bigl(t - (f - c_0)\bigr) \geqslant \mu$. Hence $t + c_0 \in T_2$ is a suitable test term.

Assume now that C'' is empty, i.e., from $v(a - c) = \mu$ we may conclude that $v(c - c_0) >$

μ. Choose a term $e_0 \in E'$ of maximal value. We certainly have $v(e_0) \leqslant \mu$. If there is no $c \in C'$ with $v(e_0) \leqslant v(c - c_0) < \mu$, we can test $e_0 + c_0 \in T_1$: For upper bounds we obtain

$$v\bigl(e_0 - (c - c_0)\bigr) = v(e_0) \leqslant \mu \quad \text{if } v(a - c) = \mu,$$

and $v\bigl(e_0 - (c - c_0)\bigr) = v(a - c)$ else. For lower bounds we have that

$$v\bigl(e_0 - (f - c_0)\bigr) \geqslant v(e_0) \quad \text{if } v(a - f) \geqslant v(e_0),$$

and $v\bigl(e_0 - (f - c_0)\bigr) = v(a - f)$ else. If there is $c_1 \in C'$ with $v(e_0) \leqslant v(c_1 - c_0) < \mu$ assume wlog. that $v(c_1 - c_0)$ is of maximal value with this property. Then $\pi(c_1 - c_0) + c_0 \in T_1$ can play the role of $e_0 + c_0$ above. $\square$

Using Corollary 8.2, we could alternatively set $T_0 = \{\infty\}$. Furthermore, in T_2 one does not have to check the whole set C but only the subset occurring with weak lower bounds because for any $d \in K$ certainly $0 \not\parallel d$.

As a special case of Theorem 8.4, the elimination set for a pure lower bound problem turns out to be linear in the number of bounds.

Corollary 8.5. (cs sets for lower bounds) *Let x be a variable, and let* $\mathrm{A} = \bigl\{\, e \lozenge x - f \bigm| (e, f) \in J \,\bigr\}$ *with x not occurring in the e, f. Then F is a* cs *set for* A *and x.*

9. Elimination in Discretely Valued Fields with Divisibility

For introducing divisibility predicates we restrict to discretely valued fields the value group $v\bigl(K \setminus \{0\}\bigr)$ of which is a $\mathbb{Z}$-group, i.e., it is elementary equivalent to $(\mathbb{Z}, +)$. It makes then sense to define unary predicates $D_n(a) :\longleftrightarrow n \mid_{\mathbb{Z}} v(a)$ stating integer divisibility of their argument's value by $n \in \mathbb{N}$. We also introduce negated counterparts $\bar{D}_n(a) :\longleftrightarrow \neg D_n(a)$, which yields the language

$$L_{\zeta,\pi,D} = L_{\zeta,\pi} \cup \{\, D_n, \bar{D}_n \mid n \in \mathbb{N} \,\}.$$

For quantifier elimination, D_n and $\bar{D}_n$ are treated the same way, so in the style of "$\lozenge$" above we write "Δ_n" for both of them. We have to find a cs set for a set containing upper and lower bounds together with *divisibilities*

$$\bigl\{\, \Delta_n(gx - h) \bigm| (n, g, h) \in L \,\bigr\},$$

where x is a variable, and g, h are terms not containing x. Under any fixed interpretation, we may assume that $g \neq 0$, possibly generating superfluous test points. The following lemma shows how the truth values of several divisibilities can be simulated simultaneously.

Lemma 9.1. *Let g, h, $a \in K$ with $g \neq 0$, and let n, $m \in \mathbb{N}$ such that $n \mid_{\mathbb{Z}} m$. Then for $t \in K$ such that $v(t - h/g) \equiv v(a - h/g) \bmod m$, it follows that $\Delta_n(gt - h) \longleftrightarrow \Delta_n(ga - h)$.*

In the proof of Theorem 8.4 notice that the cs set is organized in such a way that T_2 contains test terms simulating the values of the $a - c$ exactly while all others, in general, simulate only the truth values of the bounds. We construct a set

$$Q = \{\, h/g \mid (n, g, h) \in L \,\}.$$

If we now recompute T_2 with the set C replaced by $C \cup Q$, the new T_2 will also simulate the values of all $a - h/g$ exactly.

The new sets T_0 and T_1 will provide sequences of test points stepping into the right direction wrt. the ordering on the value group such that a suitable congruence class of the $a - g/h$ is met as required by Lemma 9.1. It is not hard to derive the following theorem from the proof of Theorem 8.4:

THEOREM 9.2. (CS SETS FOR MIXED BOUNDS WITH DIVISIBILITIES) *Let x be a variable and let*

$$\mathrm{A} = \{\, x - c \Diamond d,\ e \Diamond x - f,\ \Delta_n(gx - h) \mid (c, d) \in I,\ (e, f) \in J,\ (n, g, h) \in L \,\}$$

with x not occurring in the $c, \dots, h$. Set $m = \operatorname{lcm}\{\, n \mid (n, g, h) \in L \,\} > 0$. We define sets of linear terms:

$$\begin{aligned}
T_0 &= \{\, \pi^{-(i-1)},\ \pi^{-i}u,\ \pi^{-i}d \mid i \in \{1, \dots, m\},\ u \in C \cup Q,\ d \in D \,\} \\
T_1 &= \{\, \pi^{i-1}e + u,\ \pi^{i}(u - u') + u' \mid i \in \{1, \dots, m\},\ u,\ u' \in C \cup Q,\ u \neq u',\ e \in E \,\} \\
T_2 &= C \cup Q \cup F \cup \{\, z(u - u') + u' \mid u,\ u' \in C \cup Q,\ u \neq u',\ z \in Z(|C \cup Q|) \,\}
\end{aligned}$$

Then $T_0 \cup T_1 \cup T_2$ is a CS *set for* A *and x.*

With divisibility predicates, T_0 cannot be replaced by $\{\infty\}$ since for any choice the value of $\infty \in K^*$ is fixed to a certain congruence class modulo $\mathbb{Z}$. Applying the Compactness Theorem once more we may, however, assume that $\infty \equiv 0 \bmod n$ for all $n \in \mathbb{N}$. There is then the following modified substitution for terms of the form $\pi^k\infty$ into divisibilities:

$$\Delta_n(gx + h)[x /\!/ \pi^k\infty] :\longleftrightarrow \Delta_n(g\pi^k).$$

The modified substitutions of the $\pi^k\infty$ into equations and atomic formulas $ax+b \Diamond a'x+b'$ are the same as those of ∞.

For problems combining only upper bounds with divisibilities the use of $\pi^k\infty$ again decreases the complexity of the elimination set. It then does not depend on the number of different bounds but only on the LCM of the divisibilities.

COROLLARY 9.3. (CS SETS FOR UPPER BOUNDS WITH DIVISIBILITIES) *Let x be a variable, and let $\mathrm{A} = \{\, x - c \Diamond d,\ \Delta_n(gx - h) \mid (c, d) \in I,\ (n, g, h) \in L \,\}$ with x not occurring in the $c, \dots, h$. Set $m = \operatorname{lcm}\{\, n \mid (n, g, h) \in L \,\} > 0$. Then $\{\, \infty,\ \pi^{-1}\infty,\ \dots,\ \pi^{-(m-1)}\infty \,\}$ is a* CS *set for* A *and x.*

The treatment of divisibility predicates is a reasonable first step towards including root predicates $P_n(a) :\longleftrightarrow \exists r(r^n) = a$, which play a crucial role for the general quantifier elimination problem (Macintyre, 1976).

10. Elimination in Non-Discretely Valued Fields

For quantifier elimination in non-discretely valued fields (K, v) we use the language L_ζ of Section 3. Our aim is to copy Theorem 8.4 though there is no analogue of π in a non-discretely valued field. Revision of the proof for Theorem 8.4 wrt. the role of π shows that the latter could be substituted by a dummy symbol, which we consider to be of positive infinitesimal value.

Applying the Compactness Theorem of first-order logic there is an elementary extension $(K, v) \preccurlyeq (K^*, v^*)$ containing both ∞ as in the previous section and $\pi^\varepsilon \in K^*$ such that for all $x \in K$ with $0 < v^*(x)$ we have $0 < v^*(\pi^\varepsilon) < v^*(x)$. The modified substitution of π^ε into an equation is the same as that for ∞. Given a, b, a', $b' \in K$, an atomic formula $a \cdot \pi^\varepsilon + b \mathrel{\Diamond} a' \cdot \pi^\varepsilon + b'$ is equivalent in (K^*, v^*) to

$$\begin{aligned}(ax + b \mathrel{\Diamond} a'x + b')[x/\!/\pi^\varepsilon] \quad :\longleftrightarrow \quad & (b \mid a \wedge b' \mid a' \wedge b \mathrel{\Diamond} b') \vee (b \mid a \wedge a' \parallel b' \wedge b \mid a') \vee \\ & (a \parallel b \wedge b' \mid a' \wedge a \parallel b') \vee (a \parallel b \wedge a' \parallel b' \wedge a \mathrel{\Diamond} a').\end{aligned}$$

Corollary 10.1. *Lemma 8.1, Corollary 8.2, and Corollary 8.5 hold for non-discretely valued fields over the language L. So does Theorem 8.4 with π replaced by π^ε.*

In contrast to the use of dummy terms by Loos and Weispfenning (1993) and to our use for discretely valued fields, there is no proper term counterpart to this elimination set. Thus the use of dummy terms here does not only improve the efficiency of the elimination procedure, but is necessary for transferring the results given for discretely valued fields to non-discretely valued fields.

11. Complexity of the Corresponding Decision Problems

Quantifier elimination on closed formulas yields a decision procedure, provided that variable-free atomic formulas can be evaluated to truth values. This is obviously the case in our context. Applying complexity results for elimination set methods by Weispfenning (1988) based on Berman (1980), we obtain the following Corollary:

Corollary 11.1. *The decision problems for linear problems in the following classes of valued fields are in an alternating single exponential time-space (Berman) complexity class:*

1 *non-discretely valued fields over the language L_ζ,*
2 *discretely valued fields over the language $L_{\zeta,\pi}$,*
3 *discretely valued fields with a $\mathbb{Z}$-value group over the language $L_{\zeta,\pi,D}$.*

12. Model Theoretic Consequences

Definition 12.1. Let $\mathfrak{K}$ be a class of valued fields over a language L. Let Λ be a set of L-formulas. We call $\mathfrak{K}$ *substructure complete* wrt. Λ if the following holds: Given K_1, $K_2 \in \mathfrak{K}$ containing a common L-substructure $K_0 \subseteq K_1$, K_2 we have that

$$K_1 \models \varphi(a_1, \dots, a_n) \Longleftrightarrow K_2 \models \varphi(a_1, \dots, a_n)$$

for all formulas $\varphi(x_1, \dots, x_n) \in \Lambda$ and all $a_1, \dots, a_n \in K_0$.

The existence of a quantifier elimination procedure implies substructure completeness. In general, the converse holds for elementary classes only. Since the following corollaries are based on the former direction, we obviously have both a quantifier elimination and substructure completeness even for the non-elementary classes in Corollary 12.3 below.

Corollary 12.2. 1 *The class of all non-discretely valued fields over the language L_ζ with an infinite residue class field is substructure complete wrt. linear L_ζ-formulas.*

2 The class of all discretely valued fields over the language $L_{\zeta,\pi}$ with an infinite residue class field is substructure complete wrt. linear $L_{\zeta,\pi}$-formulas.
3 The class of all discretely valued fields over the language $L_{\zeta,\pi,D}$ with a $\mathbb{Z}$-value group and an infinite residue class field is substructure complete wrt. linear $L_{\zeta,\pi,D}$-formulas.

COROLLARY 12.3. *1 For a fixed field K_v, the class of all non-discretely valued fields over the language L_ζ with K_v as residue class field is substructure complete wrt. linear L_ζ-formulas.*
2 For a fixed field K_v, the class of all discretely valued fields over the language $L_{\zeta,\pi}$ with K_v as residue class field is substructure complete wrt. linear $L_{\zeta,\pi}$-formulas.
3 For a fixed field K_v, the class of all discretely valued fields over the language $L_{\zeta,\pi,D}$ with a $\mathbb{Z}$-value group and K_v as residue class field is substructure complete wrt. linear $L_{\zeta,\pi,D}$-formulas.

DEFINITION 12.4. For $L \supseteq L_\zeta$ we define the set $\Pi(L)$ of linear L-formulas φ containing only *pure bound conditions* as follows: $\varphi \in \Pi(L)$ if the occurrence of each quantified variable is restricted to one side of the predicates "$|$" and "$\|$."

COROLLARY 12.5. *1 The class of all valued fields over the language L_ζ is substructure complete wrt. $\Pi(L_\zeta)$.*
2 The class of all discretely valued fields over the language $L_{\zeta,\pi}$ is substructure complete wrt. $\Pi(L_{\zeta,\pi})$.
3 The class of all discretely valued fields with a $\mathbb{Z}$-value group over the language $L_{\zeta,\pi,D}$ is substructure complete wrt. $\Pi(L_{\zeta,\pi,D})$.

In their famous papers, Ax and Kochen (1965, 1966) and, independently, Ershov (1965) established various transfer principles for elementary properties of Henselian valued fields. Since substructure completeness implies model completeness one can derive analogue transfer principles for linear formulas that do not require the fields to be Henselian.

13. Conclusions

We have extended the Skolem sets introduced by Weispfenning (1988), to the more sophisticated concept of CS sets. On this basis, we have given elimination sets, and thus quantifier elimination procedures of comparatively moderate complexity for linear problems in various reasonable classes of valued fields. Some of the classes required the use of improper terms containing dummy symbols. Our use of this technique thus goes far beyond that of related work, where it was only used to slightly decrease the complexity. Our elimination procedures imply complexity results for the corresponding decision problems and substructure completeness wrt. linear formulas of the considered classes of valued fields.

References

Ax, J., Kochen, S. (1965). Diophantine problems over local fields. *American Journal of Mathematics*, **87**:605–648. Parts I and II.
Ax, J., Kochen, S. (1966). Diophantine problems over local fields. *Annals of Mathematics*, **83**:437–456. Part III.

Berman, L. (1980). The complexity of logical theories. *Theoretical Computer Science*, **11**:71–77.

Dolzmann, A., Sturm, T. (1997a). Redlog: Computer algebra meets computer logic. *ACM SIGSAM Bulletin*, **31**(2):2–9.

Dolzmann, A., Sturm, T. (1997b). Simplification of quantifier-free formulae over ordered fields. *Journal of Symbolic Computation*, **24**(2):209–231.

Dolzmann, A., Sturm, T., Weispfenning, V. (1997). Real quantifier elimination in practice. Technical Report MIP-9720, FMI, Universität Passau, D-94030 Passau, Germany.

Dolzmann, A., Sturm, T., Weispfenning, V. (1998). A new approach for automatic theorem proving in real geometry. *Journal of Automated Reasoning*, **21**(3):357–380.

Ershov, J. L. (1965). On elementary theories of local fields. *Algebra i Logika Sem.*, **4**(2):5–30.

Ferrante, J., Rackoff, C. W. (1979). *The Computational Complexity of Logical Theories.* Number 718 in Lecture Notes in Mathematics. Springer-Verlag, Berlin.

Loos, R., Weispfenning, V. (1993). Applying linear quantifier elimination. *The Computer Journal*, **36**(5):450–462. Special issue on computational quantifier elimination.

Macintyre, A. (1976). On definable subsets of p-adic fields. *Journal of Symbolic Logic*, **41**(3):605–610.

Sturm, T. (1996). Real quadratic quantifier elimination in Risa/Asir. Research Memorandum ISIS-RM-5E, ISIS, Fujitsu Laboratories Limited, 1-9-3, Nakase, Mihama-ku, Chiba-shi, Chiba 261, Japan.

Sturm, T. (1997). Reasoning over networks by symbolic methods. Technical Report MIP-9719, FMI, Universität Passau, D-94030 Passau, Germany.

Sturm, T., Weispfenning, V. (1998). Computational geometry problems in Redlog. In Wang, D., editor, *Automated Deduction in Geometry*, volume 1360 of *Lecture Notes in Artificial Intelligence (Subseries of LNCS)*, pages 58–86. Springer-Verlag, Berlin Heidelberg.

Weispfenning, V. (1984). Quantifier elimination and decision procedures for valued fields. In Müller, G. H., Richter, M. M., editors, *Models and sets (Aachen, 1983)*, volume 1103 of *Lecture Notes in Mathematics*, pages 419–472. Springer-Verlag, Berlin, Heidelberg.

Weispfenning, V. (1988). The complexity of linear problems in fields. *Journal of Symbolic Computation*, **5**(1–2):3–27.