J. Symbolic Computation (1988) **5**, 3–27

The Complexity of Linear Problems in Fields

VOLKER WEISPFENNING

University of Heidelberg, Mathematisches Institut,
Im Neuenheimer Feld 288, *D*-6900 *Heidelberg, FRG*

(*Received* 20 *November* 1984)

We consider linear problems in fields, ordered fields, discretely valued fields (with finite residue field or residue field of characteristic zero) and fields with finitely many independent orderings and discrete valuations. Most of the fields considered will be of characteristic zero. Formally, linear statements about these structures (with parameters) are given by formulas of the respective first-order language, in which all bound variables occur only linearly. We study symbolic algorithms (*linear elimination procedures*) that reduce linear formulas to linear formulas of a very simple form, i.e. quantifier-free linear formulas, and algorithms (*linear decision procedures*) that decide whether a given linear sentence holds in all structures of the given class. For all classes of fields considered, we find linear elimination procedures that run in double exponential space and time. As a consequence, we can show that for fields (with one or several discrete valuations), linear statements can be transferred from characteristic zero to prime characteristic p, provided p is double exponential in the length of the statement. (For similar bounds in the non-linear case, see Brown, 1978.) We find corresponding linear decision procedures in the Berman complexity classes $\bigcup_{c\in\mathbb{N}} STA(*, 2^{cn}, dn)$ for $d = 1, 2$. In particular, all these procedures run in exponential space. The technique employed is quantifier elimination via Skolem terms based on Ferrante & Rackoff (1975). Using ideas of Fischer & Rabin (1974), Berman (1977), Fürer (1982), we establish lower bounds for these problems showing that our upper bounds are essentially tight. For linear formulas with a bounded number of quantifiers all our algorithms run in polynomial time. For linear formulas of bounded quantifier alternation most of the algorithms run in time $2^{O(n^k)}$ for fixed k.

Introduction

Elementary statements about fields, ordered fields and valued fields play an important rôle in symbolic algebraic computations. On the one hand, their expressive power is strong enough to cover a good deal of commutative algebra, geometry and number theory, in particular most polynomial manipulations. On the other hand, one knows since the pioneering work of Tarski, A. Robinson and Ax–Kochen–Ershov, that these statements are amenable to computational methods, when considered in certain fields such as the reals, the complex numbers, the p-adics and certain power series fields.

Two methods are of prime importance in this connection:

(1) *Decision procedures*, i.e. symbolic manipulations for deciding the validity of formal elementary statements in certain classes of structures.

(2) *Quantifier elimination procedures*, i.e. symbolic manipulations reducing formal elementary statements with parameters equivalently in a class of structures to particularly simple such statements (quantifier-free formulas).

While a great number of recursive and even primitive recursive procedures of this kind have been established (cf. van den Dries, 1981; Macintyre *et al.*, 1983), only few of them,

0747–7171/88/010003+25 $03.00/0

as e.g. for real algebra (cf. Collins, 1983; Ben-Or *et al.*, 1986), complex algebra (cf. Heintz, 1983), boolean algebra (cf. Kozen, 1980), are known to be elementary recursive, i.e. to run in time bounded by a finite iteration of the exponential function applied to the size of the input.

In this paper, we restrict our attention mostly to linear statements with parameters in fields, ordered fields, discretely valued fields and fields with several orderings and valuations. Roughly speaking, these are formulas of the respective elementary language, in which all essential variables, i.e. the variables x bound by a quantitier $\exists x$, $\forall x$, occur only linearly. This is, of course, a severe restriction in expressive power; on the other hand, it allows us to dispense with closure conditions such as real or p-adic closedness. The following two examples may illustrate the kind of problems that can be handled in this framework:

(1) Solvability of finite systems of linear equations, linear order inequalities, and linear p-adic divisibilities for variable prime p in the field $\mathbb{Q}$ of rationals.

(2) Solvability of finite systems of linear equations and in equations with specified orders of poles and zeros at finitely many places in the rational function field $\mathbb{Q}(t)$. Moreover, if t is specified as a transcendental real, linear order inequalities may be added.

(3) Elementary problems in computational geometry such as movability problems to the extent that they concern (not necessarily convex) polyhedra and translations (see section 6 for an example). In all examples, the parameters of the problem may be indeterminate.

The existence of quantifier elimination procedures for linear formulas (*linear elimination*, for short) has been studied in Macintyre *et al.*, 1983; Point, 1983; van den Dries, 1981. None of the procedures exhibited there is better than primitive recursive.

The purpose of this paper is to determine the exact complexity of linear elimination and the decision of linear sentences in the classes of fields mentioned above. Somewhat surprisingly, the outcome is essentially the same for all these classes of fields:

Except for the case of multiordered, multivalued fields, the decision problem for linear sentences in complete (under polynomial time reductions) for the Berman complexity class $\bigcup_{c\in\mathbb{N}} STA(*, 2^{cn}, n)$ (see Berman, 1977, 1980). So all these decision problems are computationally equivalent to the decision problem for real addition (see Berman, 1977) and for boolean algebras (see Kozen, 1980). In the exceptional case the problem is $\cup STA(*, 2^{cn}, n)$-hard and in $\cup STA(*, 2^{cn}, 2n)$. So in every case, the problem can be solved in exponential space and double exponential time.

We find linear elimination procedures running in double exponential space and time, and prove that any such procedure does, indeed, require double exponential space on infinitely many formulas. So the linear elimination problem for these classes of fields is of the same complexity as the quantifier elimination problem for torsion-free abelian groups and for algebraically closed fields (cf. section 5 and Heintz, 1983). Moreover, we show that any quantifier elimination procedure for the reals or p-adics requires double exponential space. So the quantifier elimination problem for arbitrary formulas and for linear formulas in the theory of real numbers are essentially of the same complexity.

We show in section 6 that the number of quantifiers (the *dimension*) of a linear formula is the prime source of computational complexity; the number of quantifier alternations is of secondary importance and the length of the formula enters only polynomially. Thus, for bounded dimension all our algorithms run in polynomial time; for bounded quantifier alternation many of them run in exponential time (with a polynomial exponent).

As a by-product, we find that the transfer of linear statements φ in fields and fields with one or several independent discrete valuations from characteristic zero to large positive characteristic p works for p double exponential in the length of φ, and does in fact require a lower bound of this size (see sections 2.7, 3.5, 4.3, 5.2′ below).

The upper bounds are established by the method of quantifier elimination via Skolem terms, based on ideas of Ferrante & Rackoff (1975). The lower bounds use results of Fischer & Rabin (1974), Berman (1977, 1980) and Fürer (1982), in particular the construction of short linear formulas defining large finite sets.

The *plan of the paper* is as follows: Section 1 provides the logical background and presents the general method. Section 2 treats the case of fields and ordered fields, and section 3 the case of discretely valued fields. Section 4 combines the results of the previous sections with the appropriate approximation theorem for independent valuations and orders to treat the case of multivalued, multiordered fields. Section 5 establishes the lower bounds. Section 6 studies the modifications of these results for linear formulas with a bounded number of quantifiers or quantifier blocks.

1. The General Method

We begin with a short sketch of the logical background. A reader familiar with elementary logic may skip this paragraph.

We consider elementary languages L given by a finite set of constants and finitary operation and relation symbols. From these symbols together with an infinite supply V of variables $x, y, \dots$, the equality sign "$=$", the logical symbols $\wedge$, $\vee$, $\neg$, $\exists$, $\forall$ and brackets $($, $)$, the terms and formulas of L are built up: *terms* $t, t', \dots$ are formed from constants and variables by superposition of operation symbols; *atomic formulas* are equations $(t=t')$ or formal relations $R(t_1, \dots, t_n)$ between terms; arbitrary *formulas* $\varphi, \psi, \dots$ are obtained from atomic formulas by closure under $\wedge$, $\vee$, $\neg$ and quantifiers $\exists\, x$, $\forall\, x$. $\varphi \rightarrow \psi$ and $\varphi \leftrightarrow \psi$ are abbreviations for $\neg\varphi \vee \psi$ and $(\varphi\rightarrow\psi)\wedge(\psi\rightarrow\varphi)$. An occurrence of a variable x in a formula φ is *bound*, if it is in the scope of a quantifier $\exists\, x$ or $\forall\, x$; otherwise, it is *free*. A formula containing no quantifier is *quantifier-free*. A formula containing no variable free is a *sentence*. A *theory* T in L is a set of L-sentences. An *L-structure* A is a non-empty set, where the constants, operation symbols and relation symbols of L are interpreted as elements, operations and relations of the appropriate arity. If $\varphi(\mathbf{x})$ is an L-formula with all free variables in the string $\mathbf{x}$, A is an L-structure and $\mathbf{a}$ is a string of elements of A matching $\mathbf{x}$, then $A \models \varphi(\mathbf{a})$ means "φ *holds* in A for the parameters $\mathbf{x}=\mathbf{a}$". For a sentence φ the parameters are deleted. A is a *model* of an L-theory T, if $A \models \varphi$ for all sentences $\varphi \in T$. A sentence φ is a *consequence* of T, $T \models \varphi$, if φ holds in all models of T. Let T be a theory in L and Φ a set of L-formulas. Then a *decision procedure* for Φ, T is a procedure that decides for any sentence $\varphi \in \Phi$ whether $T \models \varphi$ or not. A *quantifier elimination* for Φ, T is a procedure $\varphi \mapsto \varphi'$ assigning to any formula $\varphi \in \Phi$ a quantifier-free formula $\varphi' \in \Phi$ such that φ and φ' are T-equivalent. If in these definitions Φ is the set $Fo(L)$ of all L-formulas, then the reference to Φ is omitted.

Quantifier elimination procedures are an important tool in model theory; in particular, they reduce the decision problem for T to the decision of quantifier-free sentences with respect to T. The latter is solvable for many algebraic theories. Therefore, a great variety of techniques has been developed to prove the existence of quantifier elimination procedures (cf. Weispfenning, 1984). They yield—as a rule—only general recursive, at best primitive recursive procedures, and hence are far from being feasible. On the other hand, one knows from the work of Fischer & Rabin (1974) that the decision problem even for simple algebraic theories like real addition requires non-deterministic exponential time. The same technique can be applied to show that quantifier elimination for this theory requires double exponential space (see 5.1′). So the best time and space bound that can be expected in these matters is a finite iteration 2**2** . . . 2**n of the exponential function 2**$n = 2^n$. Functions computable on a Turing machine with such a time (or space) bound are called *elementary recursive*. Traditional quantifier elimination procedures violate such a bound for a rather trivial logical reason: They eliminate one quantifier at a time, and solve the quantifier elimination problem for a formula $\exists x(\varphi)$ with quantifier-free φ by reduction to the case that φ is simple enough to express a mathematically well-known problem of the respective theory T. This invariably involves an application of the distributive law for $\wedge$, $\vee$, in order to eliminate disjunctions from φ. But any such application may increase the length of the formula exponentially. So, for an unbounded number of quantifiers the length of the resulting formula surpasses any elementary recursive bound.

For some theories T, this problem can be circumvented in the following way: One disregards the internal structure of the formula $\exists x(\varphi)$, and tries instead to find a finite set of terms (depending on the free variables of this formula) to act as witnesses for the existence of an element x satisfying φ. This device dates back to the early work of Skolem. It was taken up by Cooper (1972) and Ferrante & Rackoff (1975) to find elementary recursive quantifier elimination procedures for Presburger arithmetic and for addition of reals with order (cf. also Weispfenning, 1986).

In the rest of this section, we present a uniform, abstract version of this method, suited for application to linear problems. A novel element—multiple substitution of Skolem terms—is introduced in order to cover the case of fields with several orderings and valuations in section 4. A corresponding method for finding elementary recursive *decision* procedures via finite sets of Henkin constants has received a uniform treatment in Ferrante & Rackoff (1979).

Let L be an elementary language and let T be a theory in L. Let $X \subset V$ be an infinite set of variables, Z a set of L-terms, θ a set of atomic L-formulas, and Φ the closure of θ under $\wedge$, $\vee$, $\neg$ and quantifiers $\exists x$, $\forall x$ with $x \in X$. Assume, moreover:

1.1 (i) All terms occurring in formulas $\vartheta \in \theta$ are in Z.

(ii) There is a modified substitution procedure assigning to variables $x \in X$ and terms $t, t' \in Z$ a term $t(x//t') \in Z$ such that $T \models t(x//t') = t(x/t')$, where $t(x/t')$ denotes the term obtained from t by substituting t' for x in the usual sense.

(iii) For $\vartheta \in \theta$, $x \in X$, $t' \in Z$, let $\vartheta(x//t')$ denote the expression resulting from ϑ by replacing every term t in ϑ by $t(x//t')$. Then $\vartheta(x//t')$ is a formula in θ.

If t is a term, φ is a formula, then $X(t)$, $X(\varphi)$ denote the set of variables $x \in X$ occurring in t and φ respectively. If Ψ is a finite subset of θ, $x \in X$, S is a finite set of terms $t \in Z$ with $x \notin X(t)$, then we say, *S is a set of Skolem terms for x, Ψ* if

$$T \models \forall x\Big(\bigvee_{t \in S} \bigwedge_{\psi \in \Psi} (\psi \leftrightarrow \psi(x//t))\Big).$$

We call T a *Skolem theory* with respect to X, Z, θ, if for every $x \in X$ and every finite $\Psi \subseteq \theta$, x, Ψ has a set of Skolem terms.

Lemma 1.2. *Let T be a Skolem theory with respect to X, Z, θ.*

(*i*) *If $\varphi \in \Phi$ is quantifier-free, Ψ is the set of atomic subformulas of φ, $x \in X$, and S is a set of Skolem terms for x, Ψ, then*

(*) $$T \models \exists\, x(\varphi) \leftrightarrow \bigvee_{t \in S} \varphi(x//t)$$

and

(**) $$T \models \forall\, x(\varphi) \leftrightarrow \bigwedge_{t \in S} \varphi x//t).$$

(*ii*) *Suppose modified substitution $(x, t, t') \mapsto t(x//t')$, and the assignment of sets S of Skolem terms to pairs (x, Ψ) is recursive for the theory T. Then there is a recursive quantifier elimination procedure for Φ, T.*

Proof. (i) (*) is obvious from the definitions; (**) follows from (*) by replacing $\forall\, x(\varphi)$ by $\neg \exists\, x \neg(\varphi)$. (ii) Notice that the formulas on the right-hand side of (*) and (**) are in Φ. So the following describes a recursive quantifier elimination procedure for Φ, T:

```
Input: $\varphi$
Output: $\varphi'$
$\varphi'$: = $\varphi$;
while $\varphi'$ contains a quantifier do
  begin find the first quantifier $\exists\, x$ or $\forall\, x$ in $\varphi'$, whose scope $\psi$ is quantifier-free; replace
        $\exists\, x(\psi)$ or $\forall\, x(\psi)$ in $\varphi'$ by the corresponding right-hand side of (*) or (**),
        respectively.
  end
end.
```

The following technical lemma will be useful in sections 2 and 3 to avoid explicit case distinctions on the parameters of linear problems.

Lemma 1.3. *Let $x \in X$, let Ψ, Ψ' be finite subsets of θ, and assume for every $\varphi \in \Psi$ there exists a finite set J_φ of pairs of formulas such that*

(*i*) *$x \notin X(\rho)$ and $\sigma \in \Psi'$ for all $(\rho, \sigma) \in J_\varphi$;*

(*ii*) $T \models \bigvee_{(\rho,\sigma) \in J_\varphi} \rho;$

(*iii*) $T \models \bigwedge_{(\rho,\sigma) \in J_\varphi} \rho \rightarrow (\sigma \leftrightarrow \varphi).$

Then any set S of Skolem terms for x, Ψ' is also a set of Skolem terms for x, Ψ.

Proof. Let all the variables of formulas in Ψ, Ψ' be interpreted in a model A of T. Then for any $\varphi \in \Psi$ there exists $(\rho_\varphi, \sigma_\varphi) \in J_\varphi$ such that $A \models \rho_\varphi$, and so $A \models \sigma_\varphi \leftrightarrow \varphi$. Furthermore, there exists $t \in S$ with

$$A \models \bigwedge_{\varphi \in \Psi} \sigma_\varphi \leftrightarrow \sigma_\varphi(x//t).$$

Since $x \notin X(\rho_\varphi)$, $A \models \rho_\varphi(x//t)$, and so $A \models \sigma_\varphi(x//t) \leftrightarrow \varphi(x//t)$ for any $\varphi \in \Psi$. Consequently,

$$A \models \bigwedge_{\varphi \in \Psi} \varphi \leftrightarrow \varphi(x//t).$$

Our next goal is to compute upper bounds on the complexity of the quantifier elimination procedure described in lemma 1.2. To this end, we assume that we have a notion of *rank* for terms $t \in Z$ with the following properties:

1.4 There is a positive constant c such that for all $x \in X$, $t, t' \in Z$,

(i) $\mathrm{rank}(t)$ is a positive integer;
(ii) $\mathrm{rank}(t) \leqslant \mathrm{length}(t) \leqslant c \cdot \mathrm{rank}(t) \cdot |X(t)|$;
(iii) $\mathrm{rank}(t(x//t')) \leqslant c \cdot \mathrm{rank}(t) + \mathrm{rank}(t')$.

For $\varphi \in \Phi$, we let *rank*$(\varphi) = \max(\mathrm{rank}(t): t$ occurs in $\varphi)$; *atom*(φ) is the number of atomic subformulas of φ, and *quant*(φ) is the number of quantifiers in φ. If $S \subseteq Z$, $\Psi \subseteq \Phi$ are finite, then *rank*(S), *rank*(Ψ) is the maximum of all ranks of terms (formulas) in S, Ψ, respectively.

Lemma 1.5. *Let g, h be weakly monotonic functions from $\mathbb{N}$ in $\mathbb{N}$, and put $g_1(n) = g(n) \cdot n$, $h_1(n) = h(n) + cn$ with c as in* 1.4. *Let T be a Skolem theory with respect to X, Z, θ and assume that for $x \in X$, Ψ a finite subset of θ, a set S of Skolem terms for x, Ψ can be found with $|S| \leqslant g(|\Psi|)$,* $\mathrm{rank}(S) \leqslant h(\mathrm{rank}(\Psi))$. *Let $\varphi \mapsto \varphi'$ be the quantifier elimination procedure of* 1.2(*ii*). *Then*

(*i*) $\mathrm{atom}(\varphi') \leqslant g_1^{(\mathrm{quant}(\varphi))}(\mathrm{atom}(\varphi))$,
(*ii*) $\mathrm{rank}(\varphi') \leqslant h_1^{(\mathrm{quant}(\varphi))}(\mathrm{rank}(\varphi))$,
(*iii*) $\mathrm{length}(\varphi') \leqslant c' \cdot |X(\varphi)| \cdot g_1^{(\mathrm{quant}(\varphi))}(\mathrm{length}(\varphi)) \cdot h_1^{(\mathrm{quant}(\varphi))}(\mathrm{length}(\varphi))$ *for a positive constant c'.*

Proof. Notice that

$$\mathrm{atom}\Big(\bigvee_{t \in S} \varphi(x//t)\Big) = |S| \cdot \mathrm{atom}(\varphi),$$

and by 1.4,

$$\mathrm{rank}\Big(\bigvee_{t \in S} \varphi(x//t)\Big) = c \cdot \mathrm{rank}(\varphi) + \mathrm{rank}(S).$$

From this remark and the proof of 1.2, (i) and (ii) follow now by induction on $\mathrm{quant}(\varphi)$. For (iii), let k be the maximal arity of a relation symbol in L. For $\vartheta \in \theta$, we have by 1.4,

$$\begin{aligned}\mathrm{length}(\vartheta) &\leqslant (k+2) \cdot \max(\mathrm{length}(t): t \text{ occurs in } \vartheta)\\ &\leqslant (k+2) \cdot c \cdot \mathrm{rank}(\vartheta) \cdot |X(\vartheta)|.\end{aligned}$$

In 1.2(i), we may assume that $X(t) \subseteq X(\varphi)$ for all $t \in S$. So by (i) and (ii), we get

$$\begin{aligned}\mathrm{length}(\varphi') &\leqslant \mathrm{atom}(\varphi') \cdot (k+2) \cdot c \cdot \mathrm{rank}(\varphi') \cdot |X(\varphi')|\\ &\leqslant c' \cdot g_1^{(\mathrm{quant}(\varphi))}(\mathrm{length}(\varphi)) \cdot h_1^{(\mathrm{quant}(\varphi))}(\mathrm{length}(\varphi)) \cdot |X(\varphi)|,\end{aligned}$$

for $c' = (k+2)c$.

Specialising 1.5 to the case of a polynomial bound $g(n) = c_1 \cdot n^k$ and a linear bound $h(n) = c_1 \cdot n$ with $c_1 > 0$, we obtain:

Corollary 1.6. *Assume the hypothesis of* 1.5 *for g, h as specified above. Then*

(*i*) $\mathrm{atom}(\varphi') \leqslant (1+\mathrm{atom}(\varphi))**2**d*\mathrm{quant}(\varphi)$,
(*ii*) $\mathrm{rank}(\varphi') \leqslant (2**d*\mathrm{quant}(\varphi))*\mathrm{rank}(\varphi)$,
(*iii*) $\mathrm{length}(\varphi') \leqslant 2**2**d*\mathrm{length}(\varphi)$,

for some positive constant d.

Theorem 1.7. *Let T be a Skolem theory with respect to X, Z, θ, and suppose that modified substitution $(x, t, t') \mapsto t(x//t')$ and the assignment of sets S of Skolem terms to pairs (x, Ψ)*

can be performed in polynomial time. Let $\varphi \mapsto \varphi'$ *be the quantifier elimination procedure of* 1.2. *Then* φ' *can be constructed from* φ *in* $\mathrm{TIME}_{qe}(\varphi) \leqslant 2^{**}2^{**}d^{*}\mathrm{length}(\varphi)$ *for some positive constant* d.

Proof. By the hypothesis, the elimination of one quantifier according to 1.2(i) can be performed in polynomial time. So by induction on quant(φ), the construction of a quantifier-free equivalent φ' for a formula in 1.2 requires at most double exponential time.

Corollary 1.8. *Assume the hypothesis of* 1.7, *and suppose in addition that the question whether* $T \models \varphi$ *for a quantifier-free sentence* $\varphi \in \Phi$ *can be decided in time* $\mathrm{TIME}_{\mathrm{dec}}(\varphi)$ *polynomial in* length(φ). *Then for an arbitrary sentence* $\varphi \in \Phi$, $\mathrm{TIME}_{\mathrm{dec}}(\varphi) \leqslant 2^{**}2^{**}d^{*}\mathrm{length}(\varphi)$ *for some positive constant* d.

Proof. Apply 1.7 to pass from φ *to* φ', and decide φ'.

With respect to the space required to decide $T \models \varphi$ for $\varphi \in \Phi$, we get the following simple exponential bound.

Corollary 1.9. *Assume the hypothesis of* 1.6, *and suppose in addition that the question whether* $T \models \varphi$ *for a quantifier-free sentence* $\varphi \in \Phi$ *can be decided in space* $\mathrm{SPACE}_{\mathrm{dec}}(\varphi)$ *polynomial in* length(φ). *Then for an arbitrary sentence* $\varphi \in \Phi$, $\mathrm{SPACE}_{\mathrm{dec}}(\varphi) \leqslant 2^{**}d^{*}\mathrm{length}(\varphi)$ *for a positive constant* d.

Proof. It suffices to produce in a suitable systematic fashion the tuples of variable-free Skolem terms corresponding to the quantifiers in the given sentence φ, and to decide the validity in T of the sentences φ^* obtained from φ by substituting (in the modified sense) these tuples for the corresponding bound variables. Since by 1.6(ii),

$$\mathrm{rank}(t) \leqslant (2^{**}d' \cdot \mathrm{quant}(\varphi)) \cdot \mathrm{rank}(\varphi),$$

we get from 1.4,

$$\begin{aligned}\mathrm{length}(\varphi^*) &\leqslant \mathrm{atom}(\varphi) \cdot c' \cdot (2^{**}d' \cdot \mathrm{length}(\varphi)) \cdot \mathrm{rank}(\varphi) \cdot |X(\varphi)|^2 \\ &\leqslant 2^{**}d'' \cdot \mathrm{length}(\varphi)\end{aligned}$$

for certain constants d', c', d''. So these decisions together with a suitable record of their outcome can be made in space bounded by $2^{**}d \cdot \mathrm{length}(\varphi)$ for some constant d.

A tighter complexity bound for the decision problem for Φ, T under the hypothesis of 1.8 is given by the *Berman complexity class* $\bigcup_{c \in \mathbb{N}} STA(*, 2^{cn}, n)$. $STA(*, 2^{cn}, dn)$ may be described as the class of all sets accepted by an alternating Turing machine running in time 2^{cn} which may make only $d \cdot n$ alternations of universal and existential states, where n is the length of the input (see Berman, 1977, 1980; Kozen, 1980). For any $d \in \mathbb{N}$, this class is contained in EXPSPACE. Then the argument given for 1.9 shows (comp. Kozen, 1980, pp. 234, 235):

Theorem 1.10. *Assume the hypothesis of* 1.6 *and* 1.8. *Then the decision problem for* Φ, T *is in the class* $\bigcup_{c \in \mathbb{N}} STA(*, 2^{cn}, n)$.

The framework outlined so far is sufficient for handling linear problems in fields, ordered fields and valued fields. For multi-ordered, multi-valued fields, we now introduce a method of quantifier elimination via *multiple substitution of Skolem terms*.

Let L_0 be an elementary language, let L_i $(1 \leqslant i \leqslant r)$ be extensions of L_0 by new relation symbols such that $L_i \cap L_j = L_0$ for $i \neq j$, and let $L = \cup L_i$. Let $X \subseteq V$, Z a set of L_0-terms, and θ_i $(0 \leqslant i \leqslant r)$ pairwise disjoint sets of atomic L_i-formulas such that each triple X, Z, θ_i satisfies 1.1.

Let $\bar{\theta}_i$ be the closure of θ_i under $\wedge$, and let Φ be the closure of $\bigcup_{0 \leqslant i \leqslant r} \theta_i$ under $\wedge$, $\vee$, $\exists x$, $\forall x$ with $x \in X$ (note the absence of the negation). Then we define the *multiple substitution* of an $(r+1)$-tuple $(t_0, t_1, \ldots, t_r)$ of terms $t_i \in Z$ for a variable $x \in X$ in a quantifier-free formula $\varphi \in \Phi$ as follows: $\varphi(x//t_0, t_1, \ldots, t_r)$ is obtained from φ by replacing any term t occurring in an atomic subformula ψ of φ in θ_i by $t(x//t_i)$ for $0 \leqslant i \leqslant r$. If T_i are theories in L_i and

$$T \supseteq \bigcup_{0 \leqslant i \leqslant r} T_i,$$

then we say T satisfies the *abstract approximation theorem* (AAT) for $\theta_1, \ldots, \theta_r$, if for all $\vartheta_i \in \bar{\theta}_i$,

$$T \models \bigwedge_{1 \leqslant i \leqslant r} \exists x \vartheta_i \rightarrow \exists x \Big(\bigwedge_{1 \leqslant i \leqslant r} \vartheta_i \Big).$$

LEMMA 1.11. *Let T_i be Skolem theories in L_i with respect to X, Z, θ_i for $0 \leqslant i \leqslant r$, and assume*

$$T_0 \models \forall x\, \vartheta \vee \forall x\, \forall y\, ((\vartheta \wedge \vartheta(x//y)) \rightarrow x = y)$$

for $x, y \in X$, $\vartheta \in \theta_0$. Let

$$T \supseteq \bigcup_{0 \leqslant i \leqslant r} T_i,$$

and assume T has only infinite models and satisfies AAT with respect to $\theta_1, \ldots, \theta_r$.

(*i*) *Let $\varphi \in \Phi$ be quantifier-free, let Ψ_i be the set of atomic subformulas of φ in θ_i, and let S_i be a set of Skolem terms in L_0 for x, Ψ_i. Then*

$$(*) \qquad T \models \exists x(\varphi) \leftrightarrow \bigvee_{t_0 \in S_0} \varphi(x//t_0) \vee \bigvee_{t_1 \in S_1} \cdots \bigvee_{t_r \in S_r} \bigwedge_{t_0 \in S_0} \varphi(x//t_0, t_1, \ldots, t_r).$$

(*ii*) *Assume in addition:*

(1) *There are quantifier-free formulas $\nu_=$, $\nu_{R(\mathrm{x})}$ for any atomic formula $R(x_1, \ldots, x_n)$ in L with $x_i \in X$, such that $T \models x_1 \neq x_2 \leftrightarrow \nu_=$, $T \models \neg R(\mathrm{x}) \leftrightarrow \nu_R$. Moreover, $\nu_=$, $\nu_{R(\mathrm{x})}$ contain no negation.*

(2) *Modified substitution $(x, t, t') \mapsto t(x//t')$ and the assignment of sets S_i of Skolem terms to pairs x, Ψ_i with $\Psi_i \subseteq \theta_i$ is recursive.*

Then there exists a recursive quantifier elimination procedure for Φ, T.

PROOF. (i) Let A be a model of T in which all the free variables of $\exists x(\varphi)$ are interpreted. "$\Rightarrow$": Suppose $A \models \varphi$ when x is interpreted by $a \in A$. If $a = t_0$ for some $t_0 \in S_0$, we are done. Otherwise, for every $\psi \in \Psi_0$, either $A \models \neg \psi$ or $A \models \forall x \psi$, and so for every $t_0 \in S_0$, $A \models \psi \rightarrow \psi(x//t_0)$. For $1 \leqslant i \leqslant r$, find $t_i \in S_i$ with

$$A \models \bigwedge_{\psi \in \Psi_i} \psi \leftrightarrow \psi(x//t_i).$$

Then

$$A \models \bigwedge_{t_0 \in S_0} \varphi(x//t_0, t_1, \ldots, t_r).$$

"$\Leftarrow$": If $A \models \varphi(x//t_0)$ for some $t_0 \in S_0$, we are done. Otherwise, there exist $t_i \in S_i$ $(1 \leqslant i \leqslant r)$ such that

$$A \models \bigwedge_{t_0 \in S_0} \varphi(x//t_0, t_1, \ldots, t_r).$$

By choice of S_0, there exists $t_0 \in S_0$ such that for every $\psi \in \Psi_0$, $A \models \neg \psi(x//t_0) \vee \forall x\psi$. Let Ψ_i' be the set of all $\psi \in \Psi_i$ with $A \models \psi(x//t_i)$, and let $\mu_i = \wedge \Psi_i'$ for $1 \leqslant i \leqslant r$. By the AAT there exists $a \in A$ such that, when x is interpreted by a,

$$A \models \bigwedge_{1 \leqslant i \leqslant r} \mu_i.$$

So $A \models \psi(x//t_i) \to \psi$ for all $\psi \in \Psi_i$, $0 \leqslant i \leqslant r$, and so $A \models \varphi$.

(ii) We define a recursive map $\varphi \mapsto \varphi_{\text{neg}}$ assigning to every quantifier-free formula $\varphi \in \Phi$ a quantifier-free formula φ_{neg} with $T \models \neg\varphi \leftrightarrow \varphi_{\text{neg}}$: φ_{neg} is obtained from φ by interchanging $\wedge$ and $\vee$ in φ and replacing any atomic subformula $R(t_1, \ldots, t_n)$ of φ by $\nu_R(x_1//t_1, \ldots, x_n//t_n)$, and any equation $t_1 = t_2$ in φ by $\nu_=(x_1//t_1, x_2//t_2)$. A quantifier elimination procedure for Φ, T can now be described as follows:

```
Input: $\varphi$; Output: $\varphi'$; $\varphi' :=$ a negation-free formula equivalent to $\varphi$;
while $\varphi'$ contains a quantifier do
  begin find the first quantifier $\exists x$ or $\forall x$ in $\varphi'$, whose scope $\psi$ is quantifier-free;
  if this quantifier is existential
  then replace $\exists x(\psi)$ in $\varphi'$ by the corresponding right-hand side of (*)
  else begin compute $\psi_{\text{neg}}$; compute the corresponding right-hand side $\psi'$ of (*) for
      $\exists x(\psi_{\text{neg}})$; compute $\psi'_{\text{neg}}$; replace $\forall x(\psi)$ in $\varphi'$ by $\psi'_{\text{neg}}$ end
  end
end.
```

Upper bounds for the complexity of the quantifier elimination procedure $\varphi \mapsto \varphi'$ provided by 1.11 and a resulting decision procedure for Φ, T can now be computed similar as for 1.5–1.10. Two additional complications occur:

(1) Due to the double formation of formulas ψ_{neg} during the elimination of one universal quantifier, the number of atoms of the resulting formula is additionally increased by a constant factor determined by the maximum of all numbers atom($\nu_=$), atom($\nu_{R(x)}$). In the final outcome, this increase is absorbed in the double exponential growth of atom(φ') given by 1.6.

(2) For each existential quantifier, (*) introduces an additional alternation of a disjunction and a conjunction. This leads to a doubling of the last parameter in the Berman complexity class, yielding $STA(*, 2^{cn}, 2n)$ instead of $STA(*, 2^{cn}, n)$.

We leave the details of the verification to the reader and state only the results required for section 4.

THEOREM 1.12. *Let L, T be as in* 1.11(*ii*). *Assume in addition:*

(1) *Modified substitution* $(x, t, t') \mapsto t(x//t')$ *can be performed in polynomial time.*

(2) *For every pair* x, Ψ_i $(\Psi_i \subseteq \theta_i)$ *a set* S_i *of Skolem terms can be computed in polynomial time such that* $\operatorname{rank}(S_i)$ *is linear in* $\operatorname{rank}(\Psi_i)$.

(3) *For quantifier-free sentences* $\varphi \in \Phi$, "$T \models \varphi$" *can be decided in polynomial time.*

Then:

(*i*) *There is a quantifier elimination procedure* $\varphi \mapsto \varphi'$ *for* Φ, T *with*

$$\operatorname{length}(\varphi') \leqslant 2{**}2{**}d{*}\operatorname{length}(\varphi), \quad \mathrm{TIME}_{\mathrm{qe}}(\varphi) \leqslant 2{**}2{**}d{*}\operatorname{length}(\varphi)$$

for some positive constant d.

(*ii*) *The decision problem for* Φ, T *is in the Berman complexity class* $\bigcup_{c\in\mathbb{N}} STA(*, c^{cn}, 2n)$. *In particular, it can be solved in exponential space and double exponential time.*

2. Linear Problems in Fields and Ordered Fields

We let $L_F = \{0, 1, +, -, \cdot, {}^{-1}\}$ be the elementary language of fields, and $L_{OF} = L_F \cup \{<\}$ the language of ordered fields. We treat $(\,)^{-1}$ as a total operation with the convention that $0^{-1} = 0$. V is the set of variables for formulas in L_F and L_{OF}. We fix an infinite subset X of V and a linear order $\prec$ of X. The variables in X will be denoted by $x, x', x_1, x_2, \ldots$, and called *linear variables*. A term t of L_F is *linear* if t is of the form $a_0 + a_1x_1 + \ldots + a_nx_n$ with $x_i \in X$, $x_i \prec x_j$ for $i<j$, and a_i terms containing no linear variable. The *rank* of t is then defined as

$$\operatorname{rank}(t) = \max(\operatorname{length}(a_i) : 0 \leqslant i \leqslant n).$$

Deviating from the usual definition of addition, subtraction, multiplication and substitution for terms in L_F, we define these operations on linear terms in such a way that linearity is preserved. Let

$$t = a_0 + a_1x_1 + \ldots + a_nx_n, \qquad t' = a'_0 + a'_1x'_1 + \ldots + a'_{n'}x'_{n'}$$

be linear terms, and let c be a term containing no linear variable. Then

$$-t = -a_0 + -a_1x_1 + \ldots + -a_nx_n, \qquad t + t' = a''_0 + a''_1x''_1 + \ldots + a''_mx''_m,$$

where

$$\{x''_1, \ldots, x''_m\} = \{x_1, \ldots, x_n\} \cup \{x'_1, \ldots, x'_{n'}\}$$

ordered according to $\prec$, and $a''_0 = (a_0 + a'_0)$,

$$a''_h = \begin{cases} a_i & \text{if } x''_h = x_i \notin \{x'_1, \ldots, x'_{n'}\}, \\ a'_i & \text{if } x''_h = x'_i \notin \{x_1, \ldots, x_n\}, \\ (a_i + a'_j) & \text{if } x''_h = x_i = x'_j, \end{cases} \qquad \text{for } 1 \leqslant h \leqslant m.$$

$$c \cdot t = t \cdot c = ca_0 + ca_1x_1 + \ldots + ca_nx_n.$$

Modified substitution for linear terms is defined as follows:

$$t(x//t') = t \quad \text{if } x \notin \{x_1, \ldots, x_n\};$$

$$t(x_j//t') = b_0 + b_1x''_1 + \ldots + b_mx''_m$$

with

$$\{x''_1, \ldots, x''_m\} = (\{x_1, \ldots, x_n\} \backslash \{x_j\}) \cup \{x'_1, \ldots, x'_{n'}\}$$

ordered according to $\prec$, $b_0 = a_0 + a_ja'_0$,

$$b_h = \begin{cases} a_i & \text{if } x''_h = x_i \notin \{x'_1, \ldots, x'_{n'}\}, \\ a_ja'_i & \text{if } x''_h = x'_i \notin \{x_1, \ldots, x_n\}, \\ (a_i + a_ja'_k) & \text{if } x''_h = x_i = x'_k, \end{cases} \qquad \text{for } 1 \leqslant h \leqslant m.$$

Then the following properties are obvious:

Lemma 2.1.

(*i*) $\operatorname{rank}(-t) = \operatorname{rank}(t) + 1$,

(*ii*) $\operatorname{rank}(t + t') \leqslant \operatorname{rank}(t) + \operatorname{rank}(t') + 3$,

(*iii*) $\operatorname{rank}\ (c \cdot t) \leqslant \operatorname{length}(c) + \operatorname{rank}(t) + 1$,

(*iv*) $\operatorname{rank}(t(x//t') \leqslant 2\operatorname{rank}(t) + \operatorname{rank}(t') + 3$,

(*v*) *all these operations can be performed in polynomial time,*
(*vi*) $\mathrm{rank}(t) \leqslant \mathrm{length}(t) \leqslant (\mathrm{rank}(t)+1)\cdot|X(t)|$, *and so* 1.3. *holds*

We call a formula φ in $L_F(L_{OF})$ *linear*, if

(i) every atomic subformula of φ is of the form $t=0$ (or $t>0$) for a linear term t;
(ii) every bound variable in φ is linear.

If φ is a quantifier-free linear formula, x is a linear variable and t' is a linear term, then we denote by $\varphi(x//t')$ the formula obtained from φ by replacing any term t in φ by $t(x//t')$. Then $\varphi(x//t')$ is again linear, and in any field (ordered field) F, $\varphi(x//t')$ is equivalent to the formula $\varphi(x/t')$ obtained from φ by substituting t' for x in the usual manner.

We now have the following result on linear elimination in fields of characteristic zero and ordered fields.

Theorem 2.2. *Let T be the theory T_{FO} of fields of characteristic* 0 *in L_F, or the theory T_{OF} of ordered fields in L_{OF}. There is a quantifier elimination procedure $\varphi \mapsto \varphi'$ for linear formulas with respect to T such that*

$$\mathrm{length}(\varphi') \leqslant 2{*}{*}2{*}{*}c{*}\mathrm{length}(\varphi) \quad \textit{and} \quad \mathrm{TIME}_{qe}(\varphi) \leqslant 2{*}{*}2{*}{*}c{*}\mathrm{length}(\varphi)$$

for some positive constant c.

In the light of the general results 1.2, 1.6, 1.7, where Z is now the set of linear terms, $\Phi(\theta)$ is the set of (atomic) linear formulas, it suffices to prove the following facts.

Lemma 2.3. *There exists a positive constant c and a natural number k such that for any finite set Ψ of atomic linear formulas and any linear variable x, Ψ, x has a set S of linear Skolem terms with respect to T with the following properties:*

(*i*) $|S| \leqslant c\cdot|\Psi|^k$,
(*ii*) $\mathrm{rank}(t) \leqslant c\cdot\mathrm{rank}(\Psi)$ *for any* $t\in S$,
(*iii*) *S can be constructed from Ψ, x in polynomial time.*

Proof. By permuting summands, we may write $\psi\in\Psi$ in the form $ax+b\,_{(\overset{=}{>})}0$ where $X(a)=\emptyset$, b is linear, $x\notin X(b)$. So we may assume that Ψ is of the form $\{ax+b\,_{(\overset{=}{>})}0 : (a,b)\in I\}$, with linear terms b, $x\notin X(b)$, $X(a)=\emptyset$.

Case 1: *Fields of characteristic* 0. *Since*

$$a=0\to(ax+b=0\leftrightarrow b=0),$$
$$a\neq 0\to(ax+b=0\leftrightarrow x=-b/a),$$

it suffices by 1.4 *to find a set of Skolem terms for* $\{x=-b/a : (a,b)\in I\}$. *We claim that*

$$S=\{-b/a,\ -b/a+1 : (a,b)\in I\}$$

is such a set. This is a consequence of the following lemma.

Lemma 2.4. *Let F be a field, C a finite subset of F and let* $\mathrm{char}(F)=0$ *or* $\mathrm{char}(F)>|C|$. *Then* $\{c+1 : c\in C\}\nsubseteq C$.

Proof. $\{c+1 : c\in C\}\subseteq C$ implies that for any $c\in C$ there exist $h<k\leqslant|C|$ with $c+h=c+k$. So $\mathrm{char}(F)$ divides $k-h$, and so $0<\mathrm{char}(F)\leqslant|C|$.

The proof of case 1 is now completed by the observation that $|S| \leqslant 2|\Psi|$,

$$\operatorname{rank}(t) \leqslant 10 \max(\operatorname{rank}(ax+b) : (a, b) \in I),$$

and that all terms in S are linear.

Case 2: *Ordered fields. Since*

$$a \gtrless 0 \to (ax+b > 0 \leftrightarrow x \gtrless -b/a),$$

it suffices by 1.4 *to find a set of Skolem terms for*

$$\{x = -b/a,\ x \gtrless -b/a : (a, b) \in I\}.$$

We claim that

$$S = \{-b/a+1, -b/a-1 : (a, b) \in I\} \cup \{(-b'/a' - b/a)/2 : (a, b), (a', b') \in I\}$$

is such a set. This follows from the following observation due to Ferrante & Rackoff (1975):

Lemma 2.5. *Let C be a finite subset of an ordered field (or a 2-divisible ordered abelian group) F, and let $d \in F$. Then there exists*

$$e \in \{c+1, c-1 : c \in C\} \cup \{(c+c')/2 : c, c' \in C\}$$

such that for all $c \in C$, $d \overset{=}{\gtrless} c$ iff $e \overset{=}{\gtrless} c$.

Proof. Let $C = \{c_1, \ldots, c_n\}$ with $c_1 \leqslant c_2 \leqslant \ldots \leqslant c_n$. If $d = c_i$, pick $e = c_i$; if $d < c_1$, pick $e = c_1 - 1$; if $d > c_n$, pick $e = c_n + 1$; if $c_i < d < c_{i+1}$, pick $d = (c_i + c_{i+1})/2$.

To complete the proof of 2.3, we notice that all terms in S are linear, $|S| \leqslant 3|I|^2$,

$$\operatorname{rank}(t) \leqslant 10 \max(\operatorname{rank}(ax+b) : (a, b) \in I)$$

for $t \in S$.

Theorem 2.6. *The decision problem for linear sentences in the theory T_{FO} of fields of characteristic 0 and in theory T_{FO} of ordered fields is in the Berman complexity class $\cup STA(*, 2^{cn}, n)$. In particular, it can be solved in exponential space and double exponential time.*

Proof. By 1.8–1.10, it suffices to verify that the validity of an equation $t = 0$ and an inequality $t > 0$ for variable-free t can be tested in the field $\mathbb{Q}$ of rationals in polynomial time. For this purpose, one evaluates t as a quotient m/n of integers in binary expansion, and observes that the number of digits required for m and n can be bounded by 2 length(t).

Corollary 2.7. *There exists a positive constant c such that any linear sentence φ that holds in some field of characteristic 0, also holds in any field of characteristic p with $p > 2$**2**c*length(φ).*

Proof. Reduce φ equivalently in T_{FO} to a quantifier-free linear sentence φ'. Then by 2.2, length(φ') $\leqslant$ 2**2**c*length(φ), and by 2.4, the reduction holds in all fields of characteristic > length(φ'). By the proof of 2.6, the atomic subformulas $t = 0$ of φ' may be written in the form $m/n = 0$, where the number of binary digits required for m and n is bounded by

$$\text{length}(t) = \text{rank}(t) \leqslant \text{rank}(\varphi').$$

So by 1.6(ii),

$$m, n \leqslant 2^{**}\text{rank}(\varphi') \leqslant 2^{**}2^{**}d^{*}\text{length}(\varphi)$$

for some positive constant d. So the truth-value of $m/n = 0$ will be the same in all fields of characteristic 0 or characteristic $>2^{**}2^{**}c'^{*}\text{length}(\varphi)$ for $c' = \max(c, d)$.

3. Linear Problems in Discretely Valued Fields

A *discretely valued field* (F, v, Γ) is a field F with a Krull valuation $v: F \to \Gamma \cup \{\infty\}$, where the value group Γ has a smallest positive element $1 = 1_\Gamma$. We treat discretely valued fields as one-sorted structures for the language $L_{DVF} = L_F \cup \{\pi, \text{div}\}$, where π is a field constant of value 1_Γ (i.e. a uniformising parameter) and div is a *strict linear divisibility* relation, i.e. a div b iff $va < vb$ (cf. Macintyre *et al.*, 1983).[†] Accordingly, we define a *linear formula* in L_{DVF} as a formula φ of L_{DVF} such that

(i) every atomic subformula of φ is of the form $t = 0$ or t div t' with linear terms t, t';
(ii) every bound variable in φ is linear.

LEMMA 3.1. *The following hold in any valued field.*

(*i*) $$vd \geqslant 0 \to (vx + vd < v(x+c) \leftrightarrow v(cd) < v(x+c)),$$

(*ii*) $$vd < 0 \to (vx + vd < v(x+c) \leftrightarrow vx + vd < vc),$$

(*iii*) $$v(ax+b) < v(a'x+b') \leftrightarrow \begin{cases} vb < vb' & \text{if } a = a' = 0, \\ v(b/a') < v(x+b'/a') & \text{if } a = 0,\ a' \neq 0, \\ v(x+b/a) < v(b'/a) & \text{if } a \neq 0,\ a' = 0, \\ v(a/a'(b'/a' - b/a) < v(x + (b'/a' - b/a)), & \text{if } a, a' \neq 0,\ va \geqslant va', \\ v(x+b/a) < v(a'/a(b'/a' - b/a)), & \text{if } a, a' \neq 0,\ va < va'. \end{cases}$$

PROOF. (i) By the strong triangle inequality, $vd \geqslant 0$ and $vx + vd < v(x+c)$ implies $vx = vc$, and so $v(cd) < v(x+c)$; conversely, this implies $vc < v(x+c)$, and so $vx = vc$, and so $vx + vd < v(x+c)$.

(ii) "$\to$": Assume $vx + vd \geqslant vc$. Then $vx > vc$, and so $v(x+c) = vc \leqslant vx + vd$, a contradiction. "$\leftarrow$": If $vx \geqslant vc$, then $vx + vd < vc = v(x+c)$; if $vx < vc$, then $vx + vd < vx = v(x+c)$.

(iii) The first three equivalences are obvious; for the last two, observe that for $a, a' \neq 0$, $v(ax+b) < v(a'x+b')$ is equivalent to

$$v(x+b/a) + v(a/a') < v((x+b/a) + (b'/a' - b/a)),$$

and apply (i) and (ii).

Next, let T_{DVF_p} be the theory of discretely valued fields F with residue class field F_v of characteristic p (p zero or prime) in the language L_{DVF}.

LEMMA 3.2. *Let x be a linear variable, let I be a finite set of pairs (c, d) of linear terms, and put*

$$\Psi = \{x + c \text{ div } d,\ d \text{ div } x + c : (c, d) \in I\}.$$

[†] The reason for taking this relation rather than $va \leqslant vb$ as basic is technical: it guarantees that the relation is open in F^2 under the valuation topology. This will be useful in the next section.

Then

$$S = \{-c, d-c, \pi d-c, \pi(c'-c)-c, \pi^{-1}d-c, \pi^{-1}(c'-c)-c, c-c'-c'' : (c,d), (c',d'), (c'',d'')\in I\}$$

is a set of linear Skolem terms for Ψ, x *with respect to* T_{DVFp}, *provided* $p=0$ *or* $p>|I|$.

PROOF. Let F be a model of T_{DVFp}, $a\in F$, and let all c, d with $(c,d)\in I$ be interpreted in F. We are going to show that for some $a'\in S$,

$$F\models\psi(a) \text{ iff } F\models\psi(a') \text{ for all } \psi(x)\in\Psi. \qquad (*)$$

Choose $(c_0,d_0)\in I$ such that $v(a+c_0)=\max(v(a+c):(c,d)\in I)$.

CASE 1. *For all* $(c,d)\in I$, $v(c-c_0)\neq v(a+c_0)$.

SUBCASE 1.1. There is $(c,d)\in I$ with $vd\leqslant v(a+c_0)$. Pick $(c_1,d_1)\in I$ with

$$vd_1=\max(vd:(c,d)\in I, vd\leqslant v(a+c_0)).$$

SUBSUBCASE 1.1.1. There is no $(c,d)\in I$ with $vd_1<v(c-c_0)\leqslant v(a+c_0)$. Then we may put $a'=d_1-c_0$ if $vd=v(a+c_0)$, and $a'=\pi d_1-c_0$, if $vd_1<v(a+c_0)$. Then the triangle inequality guarantees that

$$v(a+c)\gtreqless vd \text{ iff } v(a'+c)\gtreqless vd \text{ for all } (c,d)\in I.$$

SUBSUBCASE 1.1.2. There exists $(c_2,d_2)\in I$ such that

$$vd_1<v(c_2-c_0)=\max(v(c-c_0):v(c-c_0)<v(a+c_0)).$$

Then we put $a'=\pi(c_2-c_0)-c_0$ and again use the triangle inequality.

SUBCASE 1.2. $v(a+c_0)<vd$ for all $(c,d)\in I$. Pick $(c_1,d_1)\in I$ with

$$vd_1=\min(vd:(c,d)\in I).$$

SUBSUBCASE 1.2.1. There is no $(c,d)\in I$ with $v(a+c_0)\leqslant v(c-c_0)<vd_1$. Then we put $a'=\pi^{-1}d_1-c_0$.

SUBSUBCASE 1.2.2. There exists $(c_2,d_2)\in I$ with

$$v(a+c_0)<v(c_2-c_0)=\min(v(c-c_0):(c,d)\in I)<vd_1.$$

Then we put $a'=\pi^{-1}(c_2-c_0)-c_0$. Again, the triangle inequality proves (*) in both subsubcases.

CASE 2. *There exist* $(c_1,d_1)\in J\subseteq I$ *such that for all* $(c,d)\in J$,

$$v(a+c_0)=v(c-c_0).$$

SUBCASE 2.1. $a=-c_0$; then we put $a'=-c_0$.

SUBCASE 2.2. $a\neq -c_0$, and hence $c\neq c_0$ for all $(c,d)\in J$. Put

$$J'=\{c-c_0:(c,d)\in J\}$$

and notice that $0\neq J'$.

CLAIM. *There exists* $(c_2, d_2) \in J$ *such that with* $e_2 = c_2 - c_0$, $e_1 = c_1 - c_0$,

$$v(e_2 + e_1 - e) = ve_1$$

for all $e \in J'$.

PROOF of the claim: If the claim fails, there exists a finite sequence $e_1, e_2, \ldots, e_k$ of elements of J' and $1 \leqslant j < k \leqslant |J'|+1$ such that $e_j = e_k$ and $v(e_i + e_1 - e_{i+1}) > ve_1$ for $1 \leqslant i \leqslant k$. Let $f_i = \operatorname{res}(e_i/e_1) \neq 0$ be the residues of e_i/e_1 in the field F_v. Then $f_i + 1 = f_{i+1}$ for $1 \leqslant i \leqslant k$ and $f_j = f_k$. So $f_j + (k-j)1 = f_j$, and so $(k-j)1 = 0$, and so $p = \operatorname{char}(F_v)$ divides $(k-j)$, and so $0 \neq p \leqslant |I|$, a contradiction.

We now put

$$a' = -(e_2 + e_1 + c_0) = -(c_2 + c_1 - c_0).$$

Then for every $(c, d) \in J$,

$$v(a' + c) = v((c - c_0) - e_2 - e_1) = ve_1 = v(a + c),$$

and for $(c, d) \notin J$, $v(a' + c) = v(a + c)$ by the triangle inequality.

This completes the proof of lemma 3.2.

We can now prove a counterpart to theorem 2.2.

THEOREM 3.3. *There is a quantifier elimination procedure* $\varphi \mapsto \varphi'$ *for linear formulas in* L_{DVF} *with respect to* T_{DVFO} *such that*

$$\operatorname{length}(\varphi') \leqslant 2^{**}2^{**}c^{*}\operatorname{length}(\varphi), \qquad \operatorname{TIME}_{qe}(\varphi) \leqslant 2^{**}2^{**}c^{*}\operatorname{length}(\varphi)$$

for some positive constant c. *Moreover, the equivalence* $\varphi \leftrightarrow \varphi'$ *holds in* T_{DVFp} *for any* $p > 2^{**}2^{**}c^{*}\operatorname{length}(\varphi)$.

PROOF. By 1.2, 1.6, 1.7, it suffices to verify the hypothesis of lemma 2.3 for the language L_{DVF} and the theory T_{DVFO}. Since $t = 0$ is equivalent to $\neg(t \operatorname{div} 0)$, we may assume that Ψ consists entirely of linear atomic formulas of the form $ax + b \operatorname{div} a'x + b'$, say

$$\Psi = \{ax + b \operatorname{div} a'x + b' : (a, b, a', b') \in I\}.$$

By 1.4 and 3.1(iii), it suffices to consider instead Ψ', x with

$$\Psi' = \{x + c \operatorname{div} d,\ d \operatorname{div} x + c : (c, c) \in I'\}$$

with

$$I' = \{(b'/a', b/a'), (b/a, b'/a), ((b'/a' - b/a), a/a'(b'/a' - b/a)), (b/a, a'/a(b'/a' - b/a)) : (a, b, a', b') \in I\}.$$

By 3.2, S can now be taken as

$$\{-c, d - c, \pi d - c, \pi(c' - c) - c, \pi^{-1}d - c, \pi^{-1}(c' - c) - c, c - c' - c'' : (c, d), (c', d'), (c'', d'') \in I'\}.$$

Notice that I' consists entirely of pairs of linear terms; so all the terms in S are linear. Furthermore,

$$|S| \leqslant 4|I'| + 2|I'|^2 + |I'|^3 \leqslant 7|I'|^3 \leqslant 28|I|^3 = 28|\Psi|^3; \text{ for } t \in S,$$

$$\operatorname{rank}(t) \leqslant 10 \max(\operatorname{rank}(c), \operatorname{rank}(d) : (c, d) \in I') \leqslant 100 \operatorname{rank}(\Psi).$$

S is obviously constructible in polynomial time. The last statement of the theorem follows from the fact that in the equivalence proof for φ and φ', lemma 3.2 is applied to sets I of pairs of terms with

$$|I| \leqslant \text{length}(\varphi') \leqslant 2^{**}2^{**}c^{*}\text{length}(\varphi).$$

THEOREM 3.4. *The decision problem for linear sentences in the theory T_{DVFO} is in the Berman complexity class $\cup STA(*, 2^{cn}, n)$. In particular, it can be solved in exponential space and double exponential time.*

PROOF. Any model F of T_{DVFO} contains the rational function field $\mathbb{Q}(\pi)$, and for $f(X) = \Sigma f_i X^i \in \mathbb{Q}[X]$, the valuation v induced by F on $\mathbb{Q}(\pi)$ is determined by

$$vf(\pi) = k1_\Gamma \text{ iff } f_0 = \ldots = f_{k-1} = 0 \neq f_k.$$

Since any variable-free term t in L_{DVF} can be rewritten as a rational function term $f(\pi)/g(\pi)$ with $\deg(f), \deg(g) \leqslant \text{length}(t)$, equations $t=0$ and relations $t \operatorname{div} t'$ can be decided in time polynomial in the length of t and t'. By 1.8–1.10, this proves the theorem.

COROLLARY 3.5. *There is a positive constant c, such that for any linear sentence φ in L_{DVF}, φ has the same truth-value in any model of T_{DVFp} with $p=0$ or $p > 2^{**}2^{**}c^{*}\text{length}(\varphi)$.*

PROOF. Similar to the proof of 2.7.

Next, we consider discretely valued fields with finite residue fields.

Let $L_{DVF\alpha}$ be L_{DVF} extended by a constant α. For k a positive integer, p prime, we let $T_{DVFp,k}$ be the theory of all models F of T_{DVFp} in the language $L_{DVF\alpha}$, whose residue field F_v has p^k elements and is obtained from the prime field $\mathbb{F}_p$ by adjunction of α. Furthermore, we assume that for each (p, k), the irreducible polynomial $f_\alpha(X)$ of α is specified with coefficients in $\{0, \ldots, p-1\}$. In particular for $k=1$, we assume $\alpha = 1$.

THEOREM 3.6. *Let p, k be fixed. There is a quantifier elimination procedure $\varphi \mapsto \varphi'$ for linear formulas in $L_{DVF\alpha}$ with respect to $T_{DVFp,k}$ such that*

$$\text{length}(\varphi') \leqslant 2^{**}2^{**}c^{*}\text{length}(\varphi), \qquad \text{TIME}_{qe}(\varphi) \leqslant 2^{**}2^{**}c^{*}\text{length}(\varphi)$$

for some positive constant c.

PROOF. For the proof, it suffices to replace the application of lemma 3.2 in the proof of 3.3 by the following lemma.

LEMMA 3.7. *Under the hypothesis of 3.2,*

$$S = \{-c, d-c, \pi d - c, \pi(c'-c)-c, \pi^{-1}d - c, \pi^{-1}(c'-c)-c, g(\alpha)(c'-c)-c : \\ (c, d), (c', d') \in I, g(X)$$

polynomial of degree $<k$ with coefficients in $\{0, \ldots, p-1\}\}$ is a set of linear Skolem terms for Ψ, x with respect to $T_{DVFp,k}$.

The *proof* is the same as for 3.2, except in subcase 2.2: There is $(c_1, d_1) \in J \subseteq I$ such that for all $(c, d) \in J$,

$$\infty > v(a+c_0) = v(c-c_0) = \max(v(a+c) : (c, d) \in I).$$

Then $v((a+c_0)/(c-c_0)) = 0$, and so there is a polynomial $g(X)$ of degree $<k$ with coefficients in $\{0, \ldots, p-1\}$ such that

$$v((a+c_0)/(c-c_0)-g(\alpha)) > 0,$$

and so

$$v(a+c_0-(c-c_0)g(\alpha)) > v(a+c_0).$$

So with $a' = (c-c_0)g(\alpha)-c_0$, we find that $v(a+c) \gtrless vd$ iff $v(a'+c) \gtrless vd$.

Concerning the decision of linear sentences in models of $T_{DVFp,k}$, the situation is somewhat more intricate than in the characteristic zero case (cf. Weispfenning, 1985).

THEOREM 3.8. *Let F be a model of $T_{DVFp,k}$ such that for all polynomials $f(X, Y)$, $g(X, Y) \in \mathbb{Z}[X, Y]$ the relation $f(\pi, \alpha) \operatorname{div} g(\pi, \alpha)$ can be decided in polynomial time. Then the decision problem for linear sentences in F is in the Berman complexity class $\cup STA(*, 2^{cn}, n)$, and hence solvable in exponential space and double exponential time.*

PROOF. It suffices to remark that any variable-free term t in L_{DVF} can be rewritten in polynomial time as a rational function term $f(\pi, \alpha)/g(\pi, \alpha)$ with integer coefficients. The result follows now from the hypothesis and 1.10.

The hypothesis of 3.8 is satisfied, e.g. in the following cases:

3.9 (i) $\operatorname{char}(F) = 0$, $\alpha = 1$, $\pi = p$; in particular for the p-adic valuation on $\mathbb{Q}$.

(ii) $\operatorname{char}(F) = p$ and the residue field F_v is embedded in F. Then $vf(\pi, \alpha)$ is determined as the index of the lowest non-vanishing coefficient of $f(\pi, \alpha)$, when regarded as polynomial in π; in particular this is the case for any rational function field or Laurent series field over a finite field.

4. Linear Problems in Multiordered, Multivalued Fields

In this section, we consider fields with a finite number of independent orderings and discrete valuations. We describe such fields as structures for a language L^* formed as follows: $L^* = L(\mathrm{Ord}, \mathrm{Val})$ is obtained from the language L_F of fields by adding a finite set Ord of binary relation symbols $<, <', <_1, \ldots$ for orders, and finite families $\{\operatorname{div}_v : v \in \mathrm{Val}\}$ of binary relation symbols for strict linear divisibilities and $\{\pi_v, \alpha_v : v \in \mathrm{Val}\}$ of field constants. The case that Ord or Val is empty is admitted.

Let us call a theory T in L^* *distinguished* if for any model F of T:

(i) F is a field of characteristic zero;
(ii) every $< \in \mathrm{Ord}$ is a field ordering of F;
(iii) for every $v \in \mathrm{Val}$, div_v is the strict linear divisibility associated with a discrete valuation v of F with uniformising parameter π_v;
(iv) for every $v \in \mathrm{Val}$, *either* $\operatorname{char}(F_v) = 0$ and $\alpha_v = 1$ *or* $F_v = \mathbb{F}_p(\alpha_v)$ is finite and T specifies p and an irreducible polynomial f_{α_v} for α_v over F_p; moreover, this decision is made uniformly for all models of T (but may vary with $v \in \mathrm{Val}$).

If F is a model of a distinguished theory T in L^*, we let $\tau_<, \tau_v$ be the topologies associated with the orders $< \in \mathrm{Ord}$ and the valuations $v \in \mathrm{Val}$. We call these topologies *independent* if for every family

$$\{U_< : < \in \mathrm{Ord}\} \cup \{U_v : v \in \mathrm{Val}\}$$

of non-empty subsets of F such that $U_<$ is $\tau_<$-open and U_v is τ_v-open, it follows that

$$\bigcap_{<\in \mathrm{Ord}} U_< \cap \bigcap_{v\in \mathrm{Val}} U_v$$

is non-empty. By Stone's approximation theorem for V-topologies on fields (see Macintyre *et al.*, 1983), this is the case iff the topologies $\{\tau_<: <\in \mathrm{Ord}\}\cup\{\tau_v: v\in \mathrm{Val}\}$ are pairwise different. The independence of these topologies can be expressed by the following (linear) sentence IND in L^*: Let

$$\mathrm{Ord} = \{<_1, \ldots, <_n\}, \qquad \mathrm{Val} = \{v_1, \ldots, v_m\}.$$

Then IND is the sentence

$$\forall x_1 \ldots x_{n+m} \forall y_1 \ldots y_{n+m}\Big(\bigwedge_{1\leqslant i\leqslant n} y_i > 0 \wedge \bigwedge_{n<i\leqslant n+m} y_i \neq 0\Big)$$
$$\to \exists z \Big(\bigwedge_{1\leqslant i\leqslant n} x_i - y_i \underset{i}{<} z \underset{i}{<} x_i + y_i \wedge \bigwedge_{n<i\leqslant n+m} y_i \,\mathrm{div}_{v_{i-n}} z - x_i\Big).$$

Next, we describe how distinguished theories T in L^* fit into the framework of multiple Skolem terms and the abstract approximation theorem presented in section 1 (last part): L_0 is the language of fields extended by the constants π_v, α_v for $v\in \mathrm{Val}$. If Ord and Val are as above, then $L_i = L_0\cup\{\underset{i}{<}\}$ for $1\leqslant i\leqslant n$, and $L_i = L_0\cup\{\mathrm{div}_{v_i}\}$ for $n<i\leqslant n+m$. X is an infinite subset of V and Z is the set of linear terms (with respect to X) in L_0. θ_0 is the set of all linear equations $t=0$ in L_0; for $1\leqslant i\leqslant n$, θ_i is the set of all linear inequalities $t \underset{i}{>} 0$ in L_i, and for $n<i\leqslant n+m$, θ_i is the set of all strict divisibilities $t\,\mathrm{div}_{v_{i-n}} t'$ between linear terms in L_i. T_0 is the theory T_{FO} in L_0; for $1\leqslant i\leqslant n$, T_i is T_{OF} in L_i; for $n<i\leqslant n+m$, T_i is T_{DVFO} or $T_{DVFp,k}$ in L_i. To complete the picture, we now show:

LEMMA 4.1. *Let T be a distinguished theory in L^*. Then $T\models IND\leftrightarrow AAT$, where AAT is the abstract approximation theorem of section* 1.

PROOF. "$\to$": Let $F\models T$, $\vartheta_i(x)\in\bar{\theta}_i$, $x\in X$. Let the free variables of ϑ_i, except x, be interpreted in F and let $\vartheta_i^F = \{a\in F: F\models \vartheta_i(a)\}\neq\emptyset$. Observe that terms in $\vartheta_i(x)$ are interpreted as linear functions in $F[x]$, and hence are continuous (with respect to all order and valuation topologies) at any point in F. So (by the way div_{v_i} are defined) all φ_i^F are open in their respective topology τ_i. Hence, by INT their intersection is non-empty, which proves AAT.

"$\leftarrow$": Suppose $F\models T$ and A_i are non-empty subsets of F that are open in the topology τ_i induced by $\underset{i}{<}$ for v_{i-n} for $1\leqslant i\leqslant n+m$. Pick $a_i\in A_i$ and a basic τ_i-open neighbourhood U_i of a_i (i.e. an interval or a circle) with $U_i\subseteq A_i$. Then there exist formulas $\vartheta_i(x)\in\bar{\theta}_i$ and an interpretation of the free variables of ϑ_i except x in F, such that $U_i = \vartheta_i^F$. Since

$$F\models \bigwedge_{1\leqslant i\leqslant n+m} \exists x\vartheta_i(x),$$

AAT entails

$$F\models \exists x\Big(\bigwedge_{1\leqslant i\leqslant n+m} \vartheta_i\Big),$$

and so

$$\bigcap_{1\leqslant i\leqslant n+m} A_i \neq \emptyset.$$

We are now in a position to apply theorem 1.12.

THEOREM 4.2. *Let T be a distinguished theory in L^* satisfying IND. Suppose that for every $v \in \mathrm{Val}$, for which F_v is finite in any model F of T, the relations $f(\pi_v, \alpha_v)\ \mathrm{div}_v\ g(\pi_v, \alpha_v)$ with $f(X, Y), g(X, Y) \in \mathbb{Z}[X, Y]$ are decidable in polynomial time. Then the following hold:*

(*i*) *There is a quantifier elimination procedure $\varphi \mapsto \varphi'$ for linear formulas in L^* with respect to T such that* $\mathrm{length}(\varphi') \leqslant 2^{**}2^{**}c^*\mathrm{length}(\varphi)$, $\mathrm{TIME}_{qe}(\varphi) \leqslant 2^{**}2^{**}c^*\mathrm{length}(\varphi)$ *for some positive constant c.*

(*ii*) *The decision problem for linear sentences in L^* with respect to T is in the Berman complexity class $\cup STA(*, 2^{cn}, 2n)$, and hence solvable in exponential space and double exponential time.*

For the case Ord $= \emptyset$, we have a characteristic transfer principle similar to 2.7 and 3.5:

THEOREM 4.3. *Let $L^* = L(\emptyset, \mathrm{Val})$. Then there exists a positive constant c such that for every linear sentence φ in L^*, φ has the same truth-value in all fields F with independent discrete valuations $v \in \mathrm{Val}$ such that* $\mathrm{char}(F_v) = 0$ *or* $\mathrm{char}(F_v) > 2^{**}2^{**}c^*\mathrm{length}(\varphi)$.

PROOF. 1.6(ii) remains valid for the quantifier elimination procedure of 4.2(i), when T specifies $\mathrm{char}(F_v) = 0$ for all $v \in \mathrm{Val}$. The argument is now as for 2.7 and 3.5.

5. Lower Complexity Bounds

In the previous sections, we have shown that for various classes of fields with additional structure:

5.1 Quantifier elimination for linear formulas can be performed in double exponential space and time.

5.2 Transfer of linear statements φ from fields of characteristic zero to fields of prime characteristic p works for p at least double exponential in length(φ).

5.3 The decision problem for linear sentences is in the Berman complexity class $\cup STA(*, 2^{cn}, n)$ or $\cup STA(*, 2^{cn}, 2n)$.

The purpose of this section is to show that these upper complexity bounds are tight in the following sense:

5.1′ Any quantifier elimination procedure for linear formulas in any of the fields considered so far requires double exponential space on a set of linear formulas of unbounded length in L_F.

5.2′ There is a sequence ρ_n of linear sentences of unbounded length in L_F and a positive constant c such that ρ_n holds in any field of characteristic zero, but fails in fields of prime characteristic $< 2^{**}2^{**}c^*\mathrm{length}(\varphi)$.

5.3′ The decision problem for linear sentences in fields of characteristic zero is $\cup STA(*, 2^{cn}, n)$—hard under polynomial time reductions. (So, for linear problems in multiordered, multivalued fields there remains a potential gap between upper and lower complexity bounds.)

The last statement 5.3′ was essentially proved by Berman (1977, 1980) by analysing Fischer & Rabin (1974). He shows that $\cup STA(*, 2^{cn}, n)$ is polynomial-time reducible to the decision problem for the theory of reals in the language $\{0, 1, +, -, <\}$. His proof—as well as that of Fischer & Rabin—makes no essential use of the order relation, and hence holds for the language $L_{G1} = \{0, 1, +, -\}$. In this language, the theory of reals can be completely axiomatised by the axioms for torsion-free, divisible, abelian groups and the axiom $0 \neq 1$. This yields the following version of Berman's result which covers 5.3′:

THEOREM 5.4. *Let G be a torsion-free, divisible, abelian group with distinguished element $1 \neq 0$. G may carry additional structure for a language L extending L_{G1}. Then the decision problem for elementary sentences in the L-theory of G is $\cup STA(*, 2^{cn}, n)$—hard under polynomial time reductions.*

The proof of 5.1′ and 5.2′ also employs a construction of Fischer & Rabin (1974, thm. 8, cor. 9) in a somewhat extended setting.

LEMMA 5.5 (Fischer–Rabin). *There is a positive constant c and a sequence $\mu_n(x)$ of L_{G1}-formulas with one free variable x such that:*

(*i*) *In any abelian group G, where 1 is an element of infinite order,*

$$\mu_n^G = \{a \in G : G \models \mu_n(a)\} = \{0, 1, 2, \ldots, 2**2**n-1\}.$$

(*ii*) *In any abelian group G with distinguished element* 1,

$$\{0, 1, 2, \ldots, 2**2**n-1\} \subseteq \mu_n^G.$$

(*iii*) $\text{length}(\mu_{n+1}) \leqslant c(n+1)$.

PROOF. Fischer & Rabin define a sequence of L_{G1}-formulas $M_n(x, y, z)$ such that in the field of reals—and in fact in any abelian group G with a distinguished element 1 of infinite order, $G \models M_n(a, b, c)$ iff $a \in \{0, 1, \ldots, 2**2**n-1\}$ and $a . b = c$ (when a is regarded as a natural number). Moreover, $\text{length}(M_{n+1}) \leqslant c(n+1)$ for a suitable constant c, and M_n can be equivalently expressed by a positive existential formula. So the formulas $\mu_n(x) = M_n(x, 0, 0)$ satisfy the lemma.

We prove 5.2′ in the following more general form:

THEOREM 5.6. *There is a sequence ρ_n of sentences of unbounded length in L_{G1} and a positive constant c such that ρ_n holds in any abelian group, where 1 is an element of infinite order, and ρ_n fails in any abelian group, where 1 has order $\leqslant 2**2**c*\text{length}(\rho_n)$ for $n > 0$.*

PROOF. Let ρ_n be the sentence $\forall x(\mu_n(x) \to x+1 \neq 0)$. Then for some constant $c > 0$, 5.5(iii) shows that length $(\rho_{n+1}) \leqslant c(n+1)$. By 5.5(i), ρ_n holds if 1 has infinite order. If

$$m = \text{order}(1) \leqslant 2**2**c^{-1}\text{length}(\rho_{n+1}) \leqslant 2**2**(n+1),$$

then by 5.5(ii), $G \models \mu_{n+1}(m-1)$, and so $G \models \neg \rho_{n+1}$.

Finally, 5.1′ will be a consequence of the following very general, but somewhat technical result 5.7. As in section 4, we call a finite, non-empty set Top of topologies τ on a set G *independent*, if whenever $\mathcal{U}$ is a set of non-empty subsets of G, then $\cap\mathcal{U} \neq \emptyset$, provided there is an injective map $\mathcal{U} \to \text{Top}$, $U \mapsto \tau_U$ such that U is τ_U-open. For $A \subseteq G$, $\tau \in \text{Top}$, $\delta_\tau(A) = cl_\tau(A) \cap cl_\tau(G \backslash A)$ denotes the *τ-boundary* of A.

THEOREM 5.7. *Let G be an abelian group with distinguished element 1 of infinite order. G may carry additional structure for a language L extending L_{G1}. Let* Top *be a finite independent* *set of T_1-topologies on G, such that for any $\tau \in \mathrm{Top}$, no $a \in G$ is τ-isolated. Assume, furthermore, that there is a positive constant d and a map $\psi(x) \mapsto \tau_\psi$ assigning to any atomic L-formula $\psi(x)$ in one variable x a topology $\tau_\psi \in \mathrm{Top}$ such that $|\delta_\tau(\psi^G)| \leqslant d \cdot \mathrm{length}(\psi)$. Let c and $\{\mu_n(x)\}$ be as in lemma 5.5. Then for any sequence $\{\sigma_n(x)\}$ of quantifier-free L-formulas with $G \models \mu_n \leftrightarrow \sigma_n$, we have $d \cdot \mathrm{length}(\sigma_n) \geqslant 2{**}2{**}c^{-1}\mathrm{length}(\mu_n)$ for positive n.*

Proof. By 5.5, we know that $\mu_n^G = \{0, 1, \ldots, 2{**}2{**}n-1\}$, and that $\mathrm{length}(\mu_{n+1}) \leqslant c\,.(n+1)$ for some positive constant c. So it suffices to prove the following claim:

Claim 5.8. *Let $\sigma(x)$ be a quantifier-free L-formula in one variable x, and let Ψ be the set of all atomic subformulas of σ. If σ^G is finite, then*

$$\sigma^G \subseteq \cup\{\delta_{\tau_\psi}(\psi^G) : \psi \in \Psi\}.$$

Assuming the claim, we argue as follows: If $G \models \mu_n \leftrightarrow \sigma$ for a quantifier-free σ, then

$$\{0, \ldots, 2{**}2{**}n-1\} = \mu_n^G = \sigma^G \subseteq \cup\{\delta_{\tau_\psi}(\psi^G) : \psi \in \Psi\},$$

and so

$$\begin{aligned} 2{**}2{**}c^{-1}\mathrm{length}(\mu_{n+1}) &\leqslant 2{**}2{**}(n+1) \leqslant \Sigma\,\{|\delta_{\tau_\psi}(\psi^G)| : \psi \in \Psi\} \\ &\leqslant d \cdot \Sigma(\mathrm{length}(\psi) : \psi \in \Psi) = d \cdot \mathrm{length}(\sigma). \end{aligned}$$

Proof of the claim. Assume for a contradiction that σ^G is finite

$$a \in \sigma^G \backslash \cup\{\delta_{\tau_\psi}(\psi^G) : \psi \in \Psi\}.$$

Then $a \in \mathrm{int}_{\tau_\psi}(\psi^G) \cup \mathrm{int}_{\tau_\psi}(\neg\,\psi^G)$ for every $\psi \in \Psi$. By the hypothesis on Top, we find τ_ψ-open sets U_ψ with $U_\psi \subseteq ((\neg)\psi)^G$, $U_\psi \cap \sigma^G = \{a\}$. Let $V_\psi = \cap\{U_{\psi'} : \tau_{\psi'} = \tau_\psi\}$. Then $V_\psi \cap \sigma^G = \{a\}$, $V_\psi \subseteq ((\neg)\psi)^G$ and $V_\psi \neq V_{\psi'}$ implies $\tau_\psi \neq \tau_{\psi'}$. Since a is not τ_ψ-isolated, we find for each V_ψ a non-empty τ_ψ-open subset V'_ψ with $a \notin V'_\psi$. Since Top is independent, there exists $b \in \cap\{V'_\psi\}$. But then $b \in \psi^G$ iff $a \in \psi^G$ for all $\psi \in \Psi$. Consequently, $b \in \sigma^G$, since $a \in \sigma^G$, and so

$$b \in \sigma^G \cap \bigcap\{V'_\psi\} \subseteq \sigma^G \cap \bigcap\{U_\psi \backslash \{a\}\} = \emptyset.$$

This completes the proof of theorem 5.7.

Verification of 5.1′ by means of theorem 5.7:

Notice to begin with at any L_F-term $t(x)$ in one variable can be rewritten as a rational function term $f(x)/g(x)$ with integer coefficients and $\deg f$, $\deg g \leqslant \mathrm{length}(t)$.

If G is a field of characteristic zero, we may take $\mathrm{Top} = \{\tau\}$, where τ is the cofinite topology on G, and $d = 2$. This gives us a new proof of the fact (see Heintz, 1983) that no algebraically closed field admits quantifier elimination in less than double exponential space, for the characteristic zero case.

If G is an ordered field, we take $\mathrm{Top} = \{\tau_<\}$, where $\tau_<$ is the order topology, and observe that $\delta_{\tau_<}(t(x) > 0)^G \subseteq (t(x) = 0)^G$. This shows in particular that no real closed field admits quantifier elimination in less than double exponential space.

If G is a valued field, regarded as structure for a sublanguage of $LDVF$, possibly with additional constants, then we take $\mathrm{Top} = \{\tau_v\}$ with the valuation topology τ_v, and observe that

$$\delta_{\tau_v}(t(x) \text{ div } t'(x))^G \subseteq (t(x) = 0)^G \cup (t'(x) = 0)^G.$$

So we may take $d = 4$. The same argument is valid for languages including in addition nth root predicates $W_n(x) \leftrightarrow \exists\, z(z^n = x)$, provided G satisfies Hensel's lemma. For Hensel's lemma guarantees that $\delta_{\tau_v}(W_n(t(x))^G \subseteq (t(x) = 0)^G$. So none of the following fields admits quantifier elimination in its natural language (see Macintyre *et al.*, 1983; Weispfenning, 1985) in less than double exponential space: Algebraically closed valued fields of characteristic zero, p-adic fields, fields of Laurent series $F((t))$ over a real closed or algebraically closed field F of characteristic zero.

Finally, if G is a field with finitely many orderings $< \in \mathrm{Ord}$ and finitely many valuations $v \in \mathrm{Val}$ inducing different topologies on G, we take

$$\mathrm{Top} = \{\tau_< : < \in \mathrm{Ord}\} \cup \{\tau_v : v \in \mathrm{Val}\}$$

and argue as before.

6. Linear Problems of Bounded Dimension or Bounded Quantifier Alternation

We have defined the concept of a linear problem very broadly; accordingly, the upper and lower bounds on the complexity of these problems have turned out to be quite high. So it is natural to look for more restricted classes of linear problems that are still comprehensive enough for applications but computationally less complex.

Recall from 1.5 and 1.6 that the number of quantifiers quant(φ) occurring in a linear formula φ is the most decisive parameter for the computational complexity of φ. Since quant(φ) measures the number of essential variables of the problem φ, we refer to quant(φ) as the *dimension* of φ. A first obvious restriction on linear problems is thus to bound the dimension q of the problems considered. This has the drastic effect that all problems considered so far become solvable in polynomial time. More precisely, we have the following result.

THEOREM 6.1. *Let T be any of the theories of fields considered in sections* 2, 3, 4 *and let q be a fixed non-negative integer. Then the following hold:*

(*i*) *There is a quantifier elimination procedure $\varphi \mapsto \varphi'$ for linear formulas of dimension $\leqslant q$ with respect to T such that*

$$\mathrm{length}(\varphi') \leqslant c^*(\mathrm{length}(\varphi))k \quad \textit{and} \quad \mathrm{TIME}_{qe}(\varphi) \leqslant c^*(\mathrm{length}(\varphi))^k$$

for some constants $c, k \in \mathbb{N}$.

(*ii*) *The decision problem for linear sentences of dimension $\leqslant q$ in the theory T is solvable in polynomial time.*

PROOF. The upper bounds in sections 2–4 are all based on the inequalities in 1.6, in particular the very generous bound in 1.6(iii) on the increase of length of a formula during quantifier elimination. Using the tighter inequality 1.5(iii) together with the uniform bound $\mathrm{quant}(\varphi) \leqslant q$, we immediately obtain $\mathrm{length}(\varphi') \leqslant c^*(\mathrm{length}(\varphi))^k$ for some constants $c, k \in \mathbb{N}$. This bound applies to the quantifier elimination by multiple substitutions of Skolem terms in 1.12 as well, and thus proves (i). (ii) follows from (i) and the fact that for all theories considered, quantifier-free linear sentences can be decided in polynomial time.

For some applications, e.g. in computational geometry, a uniform bound on the dimension may be felt to be too restrictive. Consider, e.g. the following problem from robotics:

Input: $n, k \in \mathbb{N}$, a (not necessarily convex) polyhedron P in $\mathbb{R}^n$ with distinguished point $p \in P$, a polyhedral environment U of P in $\mathbb{R}^n$, a finite set D of vectors (directions) in $\mathbb{R}^n$ and a goal vector $g \in \mathbb{R}^n$.

Question: Does there exist a sequence of k translations of P along directions in D moving P into a position, where p coincides with g without collision with U?

The problem can be expressed by a linear formula φ in L_{OF} of the form $\exists x_1 \ldots \exists x_k \forall y_1 \ldots \forall y_{n+1} \psi$, where ψ is quantifier-free. So it is not sensible to bound k and hence quant(φ) in advance; on the other hand, φ will always contain only two *blocks* of quantifiers $\exists x_1 \ldots \exists x_k$ and $\forall y_1 \ldots \forall y_{n+1}$. A similar observation can be made with other problems from computational geometry. (In fact, no human being is likely to comprehend a linear sentence with, say, 10 alternating blocks of quantifiers, unless quantifiers can be "hidden" in defined concepts, for which a "higher level" intuition is available.) This motivates the study of linear formulas with a bounded number of alternating quantifier blocks.

A linear formula φ is *prenex* if it is of the form $Q_1\ x_1 \ldots Q_n x_n \psi$, where Q_i are quantifiers $\exists$, $\forall$ and ψ is quantifier-free. By collecting adjacent quantifiers of the same kind into blocks, we may write φ in the form $\mathbf{Q}_1\mathbf{x}_1 \ldots \mathbf{Q}_a\mathbf{x}_a\psi$, where each $\mathbf{Q}_i\mathbf{x}_i$ is a *block of quantifiers* $\exists x_{i_1} \ldots \exists x_{i_{b_i}}$ or $\forall x_{i_1} \ldots \forall x_{i_{b_i}}$. We let $\Phi_a(\Phi_{a,b})$ be the set of all linear sentences φ in the language considered such that φ is prenex with at most a blocks of quantifiers (each comprising at most b single quantifiers). For formulas in Φ_a, the upper complexity bounds derived in sections 2 and 3 can then be improved as follows.

THEOREM 6.2. *Let T be any of the theories considered in sections* 2 *and* 3, *and let* $0 < a, b \in \mathbb{N}$.

(*i*) *There is a quantifier elimination procedure $\varphi \mapsto \varphi'$ for formulas $\varphi \in \Phi_{a,b}$ with respect to T such that*

$$\text{length}(\varphi') \leqslant \text{length}(\varphi)\ {**}(a{*}(c{*}b){**}a)$$

and

$$\text{TIME}_{qe}(\varphi) \leqslant \text{length}(\varphi)\ {**}(a{*}(c{*}b){**}a)$$

for some constant $c \in \mathbb{N}$.

(*ii*) *Linear sentences $\varphi \in \Phi_{a,b}$ can be decided in T in*

$$\text{TIME}_{dec}(\varphi) \leqslant \text{length}(\varphi)\ {**}(a{*}(c{*}b){**}a)$$

for some constant $c \in \mathbb{N}$.

PROOF. Since quantifier-free linear sentences can be decided in T in polynomial time, (ii) is an immediate consequence of (i). To prove (i), we use an observation made by Reddy & Loveland (1978) for Presburger arithmetic: In all cases considered, the elimination of an existential quantifier is achieved via the equivalence

$$\exists x\varphi \leftrightarrow \bigvee_{t \in S} \varphi(x//t)$$

established in 1.2, where $S = S(x, \varphi)$ is a set of Skolem terms for x and the set Atom(φ) of atomic subformulas of φ. Let now y be a second linear variable,

$$\varphi_t = \varphi(x//t), \qquad \varphi' = \bigvee_{t \in S} \varphi_t.$$

Then we may replace the equivalence used so far

$$\exists y \exists x\varphi \leftrightarrow \exists y\varphi \leftrightarrow \bigvee_{t' \in S'} \varphi'(y//t'),$$

where $S' = S(y, \varphi')$, by the much more economical equivalence

$$\exists\, y \,\exists\, x\varphi \leftrightarrow \exists\, y\varphi' \leftrightarrow \bigvee_{t\in S} \exists\, y\varphi_t \leftrightarrow \bigvee_{t\in S}\ \bigvee_{t'\in S_t} \varphi_t(y//t'),$$

where $S_t = S(y, \varphi_t)$. The same applies to an arbitrary block of existential or universal quantifiers.

Suppose now $\varphi \in \Phi_{a,b}$ and φ' is obtained from φ by quantifier elimination in T employing the modified equivalence described above. Using the notation of 1.5, we then get the following bounds. Let

$$g_2^{(0)}(n, b) = n, \qquad g_2^{(m+1)}(n, b) = (g(g_2^{(m)}(n, b)))^b \cdot g_2^{(m)}(n, b).$$

Then

$$\text{atom}(\varphi') \leqslant g_2^{(a)}(\text{atom}(\varphi), b)$$

and

$$\text{length}(\varphi') \leqslant c' \cdot |X(\varphi)| \cdot g_2^{(a)}(\text{length}(\varphi), b) \cdot h_1^{(a\cdot b)}(\text{length}(\varphi)).$$

Specialising g and h as in 1.6, this yields

$$\text{atom}(\varphi') \leqslant \text{atom}(\varphi)^{(kb+1)^a} \quad \text{and} \quad \text{length}(\varphi') \leqslant \text{length}(\varphi)^{a(cb)^a}$$

for some constant $c \in \mathbb{N}$.

Remark. This proof does not work for the theories T of multivalued, multiordered fields considered in section 4, since here an existential quantifier is eliminated using a disjunction of conjunctions in place of a simple disjunction.

In Fürer (1982, theorem 5), is proved a lower bound for the decision of sentences of bounded quantifier alternation concerning real addition. His proof is valid for all the theories considered in sections 2–4:

Theorem 6.3 (Fürer). *Let T be any of the theories considered in sections 2–4, and let $a \in \mathbb{N}$. There exists a positive constant c such that $\varphi \in \Phi_a$ cannot be decided in T in*

$$\text{NTIME}_{\text{dec}}(\varphi) \leqslant (\text{length}(\varphi)/a)^{**}\lfloor c \cdot a \rfloor.$$

A lower space bound for quantifier elimination on Φ_a can be obtained by the following variant of 5.5, which results from Fürer's modification of the Fischer–Rabin trick (Fürer, 1982, theorem 1].

Lemma 6.3. *For all $0 < n, a \in \mathbb{N}$ there is a L_{G1}-formula $\mu_{n,a}(x)$ in Φ_{2a-1} such that:*

(*i*) *In any abelian group G, where 1 is an element of infinite order,*

$$\mu_{n,a}^G = \{0, 1, 2, \ldots, 2^{**}n^{**}a\}.$$

(*ii*) length$(\mu_{n,a}) \leqslant c(a \cdot n \cdot \log n + 1)$ *for some positive constant c.*

From 6.3(ii) we get $n \geqslant c'^{*}(\text{length}(\mu_{n,a})/a)^{**}(1-\delta)$ for some $c' > 0$ and arbitrary $\delta > 0$. As a consequence, theorem 5.7 holds with μ_n replaced by $\mu_{n,a}$ and the lower bound $2^{**}2^{**}c^{-1}\text{length}(\mu_n)$ by $2^{**}(c'(\text{length}(\mu_{n,a})/a))^{**}(\text{a}(1-\delta))$. This yields the following variant of 5.1′:

Theorem 6.4. *Let $0 < a \in \mathbb{N}$ and let T be any of the theories considered in sections 2–4. Then there is a set M of formulas of unbounded length in Φ_{2a-1} and a positive constant c such* *that any quantifier elimination procedure $\varphi \mapsto \varphi'$ on M requires space*

$$\text{length}(\varphi') \geqslant 2^{**}(c^{*}\text{length}(\varphi)/a)^{**}(\text{a}^{*}(1-\delta))$$

for arbitrary $\delta > 0$.

It is well known (see von zur Gathen & Sieveking, 1976) that *existential* linear sentences can be decided in the theory T_{OF} of ordered fields in non-deterministic polynomial time. A use of the approximation theorem shows that this fact holds for multiordered fields as well. Is the corresponding statement true for the theories of valued fields considered in section 3?

References

Ben-Or, M., Kozen, D., Reif, J. (1986). The complexity of elementary algebra and geometry. *ACM Symp. on Computing*, 457–464.

Berman, L. (1977). Precise bounds for Presburger arithmetic and the reals with addition (preliminary report). *Proc. 18 IEEE Symp. FOCS*, pp. 95–99.

Berman, L. (1980). The complexity of logical theories. *Theor. Comp. Sci.* **11**, 71–77.

Brown, S. S. (1978). Bounds on transfer principles for algebraically closed and complete, discretely valued fields. *AMS Memoirs* **204.**

Collins, G. E. (1983). Quantifier elimination for real closed fields, a guide to the literature. In: (Buchberger, B., Collins, G. E., Loos, R., eds) *Computer Algebra*, 2nd edn. Berlin: Springer.

Cooper, D. C. (1972). Theorem-proving in arithmetic without multiplication. In: (B. Meltzer & D. Michie, eds.) *Machine Intelligence* **7**, 91–100. Univ. of Edinburgh Press.

Ferrante, J., Rackoff, Ch. (1975). A decision procedure for the first order theory of real addition with order. *SIAM J. Comp.* **4**, 69–77.

Ferrante, J., Rackoff, Ch. (1979). The computational complexity of logical theories. *Springer Lec. Notes Math.* **718.**

Fischer, M. J., Rabin, M. O. (1974). Super-exponential complexity of Presburger arithmetic. *SIAM–AMS Proc.* **7**, 27–41.

Fürer, M. (1982). The complexity of Presburger arithmetic with bounded quantifier alternation depth. *Theor. Comp. Sci.* **18**, 105–111.

Heintz, J. (1983). Definability and fast quantifier elimination in algebraically closed fields. *Theor. Comp. Sci.* **24,** 239–277.

Kozen, D. (1980). Complexity of Boolean algebras. *Theor. Comp. Sci.* **10,** 221–247.

Macintyre, A., McKenna, K., van den Dries, L. (1983). Elimination of quantifiers in algebraic structures. *Adv. Math.* **47,** 74–87.

Point, F. (1983). *Quantifier elimination for projectable L-groups and linear elimination for rings.* Thèse, Mons, Belgium.

Prestel, A., Ziegler, M. (1978). Model theoretic methods in the theory of topological fields. *J. reine u. ang. Math.* **299/300,** 318–341.

Reddy, C. R., Loveland, D. W. (1978). Presburger arithmetic with bounded quantifier alternation. *Proc. 10 ACM Symp. Th. of Comp.*, pp. 320–325.

van den Dries. L. (1981). Quantifier elimination for linear formulas over ordered and valued fields. *Bull. Sos. Math. Belg.* **33,** ser. B, 19–32.

von zur Gathen, J., Sieveking, M. (1976). Weitere zum Erfüllungsproblem polynomial äquivalente kombinatorische Aufgaben. In: Komplexität von Entscheidungsproblemen. (Specker, E., Strassen, V., eds) *Springer Lec. Notes Comp. Sci.* 43.

Weispfenning, V. (1984). Aspects of quantifier elimination in algebra. In: *Universal Algebra and its Links.* Proc. 25. Arbeitstagung über Allgemeine Algebra, Darmstadt, 1983. Berlin: Heldermann.

Weispfenning, V. (1985). Quantifier elimination and decision procedures for valued fields. Proc. Logic Coll. '83, Aachen. Part I: Models and sets. (Müller, G. H., Richter, M. M., eds). *Springer Lec. Notes Math.* **1103,** 419–472.

Weispfenning, V. (1986). The complexity of elementary problems in archimedean ordered groups. Proc. EUROCAL '85, vol. 2. (Caviness, B. F., ed.) *Springer Lec. Notes Comp. Sci.* **204,** 87–88.