J. Symbolic Computation (1990), **10**, 395-403

The Complexity of Almost Linear Diophantine Problems

V. WEISPFENNING

8390 *Passau, Universität Passau, Innstrasse* 33, *Postfach* 2540, *Germany*

(*Received* 15 *January* 1988)

We studied formulas of elementary number theory resulting from formulas of Presburger arithmetic PrA (additive elementary theory of integers with order) by substituting for some variables, polynomials and integer values of rational functions in a single new variable y, and quantifying over y. We show that the extension ALA (almost linear arithmetic) of PrA obtained in this way, has essentially the same upper and lower complexity bounds as the original theory. The same applies to the fragments of ALA obtained by restricting the number or type of quantifiers in formulas. We also show new upper complexity bounds for quantifier elimination in PrA and its fragments. The results form a common extension of known complexity bounds for PrA and for the existential almost linear problems studied by Gurari & Ibarra. The method is applicable also to other extensions of PrA without order, related to the famous bounds for binary forms of A. Baker.

1. Introduction

The elementary theory of integers with addition and order is of fundamental importance in theoretical computer science. Accordingly, algorithmic problems — in particular the decision problem — for this theory have received a great deal of attention, starting with the fundamental result of Presburger (1929). A long series of papers by Cooper (1972), Oppen (1973), Ferrante & Rackoff (1975, 1979), von zur Gathen & Sieveking (1978), Berman (1977, 1980), Fuerer (1982), Scarpellini (1984), Graedel (1987) has produced upper complexity bounds for Presburger arithmetic PrA and its fragments of bounded quantifier complexity. (Compare also Shostak (1977) for a partial decision method.) The famous result of Fischer & Rabin (1974) started a corresponding sequence of papers by Berman (1977, 1980), Fuerer (1982), Scarpellini (1984), Graedel (1987) on lower bounds.

By the negative solution to Hilbert's 10. problem, most extensions of PrA turn out to be undecidable, even if only existential problems are considered. This is the case, for example, if one admits arbitrary quadratic equations (comp. Gurari & Ibarra, 1979). If the order relation is replaced by the divisibility relation, then diophantine problems are still decidable, but problems with at least two quantifier-blocks are undecidable; moreover, even diophantine problems become undecidable, once quadratic polynomials are admitted (see Lipshitz, 1978). So it is rather surprising that Gurari & Ibarra (1979) were able to show that a large class of (existential) non-linear diphantine problems (not involving order and divisibility) can be solved in NP.

In this paper, we consider a similar extension of **arbitrary** sentences of PrA by admitting rational functions in **one additional variable.** To be more specific, an **almost linear formula** is obtained from a formula φ of Presburger arithmetic by substituting expressions of the form

$$p(y)+c_1\lfloor p_1(y)/q_1(y)\rfloor+\cdots+c_m\lfloor p_m(y)/q_m(y)\rfloor$$

0747-7171/90/110359+09 $03.00/0

with $p, p_i, q_i \in Z[y]$, $c_i \in Z$, for certain free variables of φ, and quantifying over the non-linear variable y. The resulting theory ALA (almost linear arithmetic) is an extension of PrA and hence satisfies the same lower complexity bounds.

The main purpose of this paper is to show that essentially all known upper complexity bounds for PrA and its fragments of bounded quantifier complexity are valid for ALA as well. Since the known upper and lower complexity bounds for PrA and many of its fragments are tight, the same applies to ALA.

In contrast to earlier studies of PrA that are based on effective Ehrenfeucht games (see Ferrante & Rackoff, 1979), we employ a fast quantifier elimination procedure for PrA. As a by-product, we get detailed upper complexity bounds for quantifier elimination in PrA. We also indicate how to obtain upper complexity bounds for a similar extension of additive arithmetic without order by binary irreducible forms, using the famous results of Baker (1968).

Section 2 provides a fast quantifier elimination method and upper complexity results for PrA refining the known results. Section 3 treats the case of a single non-linear variable, and section 4 combines both for a proof of the main results.

2. Fast Quantifier Elimination for Presburger Arithmetic

We represent formulas of Presburger arithmetic as follows: terms are linear expressions $n_0 + n_1 x_1 + \cdots + n_k x_k$ in variables x_i with integer coefficients n_i in binary. *Atomic formulas* are expressions of the form $t\, r\, t'$ where t, t' are terms and r is one of the relations $=$, $<$, $>$, $\equiv (m)$ (congruence modulo m). Formulas are obtained from atomic formulas by means of the propositional connectives $\wedge$, $\vee$, $\neg$, and quantifications $\exists x$, $\forall x$ over variables. A formula, in which every variable x is bound by corresponding quantifier $\exists x$ or $\forall x$, is called a **sentence.** A formula φ is **quantifier-free** (q.f.) if it contains no quantifier $\exists x$, $\forall x$. φ is **prenex** if it is of the form $Q_1 x_1 \ldots Q_k x_k \varphi$, where each Q_i is a quantifier $\exists$ or $\forall$ and φ is q.f. A sequence $\exists x_1 \ldots \exists x_n$ or $\forall x_1 \ldots \forall x_n$ of quantifiers of the same kind is called a **quantifier-block;** n is the **length** of the block.

A **quantifier elimination** (q.e.) **procedure** for PrA is an algorithm assigning to any formula φ a q.f. formula φ' such that φ and φ' are equivalent in **Z**. Since any formula φ can be put into an equivalent prenex form in polynomial time, it suffices to define a q.e. procedure on prenex formulas.

Our q.e. procedure refines the method developed by Cooper (1972), Oppen (1973), Ferrante & Rackoff (1975, 1979), Reddy & Loveland (1978) in the context of Ehrenfeucht games and provides new upper complexity bounds for quantifier elimination and more specific complexity bounds for the decision problem. The main results of this section can be stated as follows.

THEOREM 2.1. *There exists a* q.e. *procedure assigning to any prenex formula φ an equivalent* q.f. *formula φ'. If φ has at most a quantifier-blocks each of length at most b, then the algorithm runs in time and space bounded by* $\exp(c \cdot \mathit{length}(\varphi)^{(4b)^a})$ *for some positive constant c.* (*Here and in the following,* $\exp(x) = 2^x$.)

For the statement of the following theorem, it will be convenient to introduce **bounded quantifiers** over integers: $(\exists x, \text{length}(x) \leq M)(\psi(x))$ will be an abbreviation of the finite disjunction

$$\bigvee_{k \in \mathbf{Z}, |k| < \exp(M-1)} \psi(k).$$

Similarly, $(\forall x, \text{length}(x) \leq M)(\psi(x))$ will stand for the finite conjunction

$$\bigwedge_{k \in \mathbf{Z}, |k| < \exp(M-1)} \psi(k).$$

THEOREM 2.2. *Let φ be a prenex sentence with at most a quantifier-blocks each of length at most b. For a constant c, let φ'_c, be the sentence resulting from φ by replacing each quantifier $\exists x$, $\forall x$ in φ by a corresponding bounded quantifier*

$$(\exists x, \mathit{length}(x) \leq (c \cdot \mathit{length}(\varphi)^{(3b)^a})$$

and

$$(\forall x, \mathit{length}(x) \leq (c \cdot \mathit{length}(\varphi)^{(3b)^a}),$$

respectively. Then there exists a positive constant c such that φ'_c is equivalent to φ.

Recall the definition of the complexity class $STA(*, -, -)$ in Berman (1980): $STA(*, f(n), g(n))$ is the class of all sets accepted by an alternating Turing machine running in time $f(n)$ which may make only $g(n)$ alternations of universal and existential states, where n is the length of the input. $STA(*, f(n), g(n))$ is a subclass of the class $SPACE(f(n))$ of all sets accepted by a deterministic Turing machine in space $f(n)$.

Then the following is an immediate consequence of Theorem 2.2 and the characterization of $STA(*, f(n), g(n))$ in terms of bounded quantifiers (comp. also Volger, 1983).

COROLLARY 2.3 (Berman). *The decision problem for sentences in PrA is in the class*

$$\bigcup_{c>0} STA(*, 2^{c^n}, n), \text{ and hence in } \bigcup_{c>0} SPACE(2^{c^n}).$$

COROLLARY 2.4 (Graedel). *The decision problem for prenex sentences in PrA with a fixed bound on the number of quantifiers and at most a quantifier-blocks beginning with a block of existential (universal) quantifiers is in the class Σ_a^p (Π_a^p) of the polynomial time hierarchy (see Stockmeyer, 1977).*

Theorems 2.1 and 2.2 will be proved by induction on the number of quantifiers in the formula φ. The most important step is the elimination of a single (existential) quantifier.

Here one could use the quantifier elimination procedure implicit in Ferrante & Rackoff (1975). This would result in an enormous duplication of identical atomic formulas in the resulting quantifier-free formula. In the context of effective Ehrenfeucht games, considered in earlier papers, this if of no relevance. For quantifier elimination, however, the length of the output formula is of decisive importance. We avoid these unnecessary duplications by treating terms as "similar" that differ only in their variable-free part.

We need the following definitions: Two terms t, t' are associated, $t \sim t'$, if all variables x_i have the same coefficient in t and t'. (So t and t' differ at most in their "absolute term".) Two atomic formulas $t\, r\, t'$ and $s\, r'\, s'$ are associated, if $t \sim s$, $t' \sim s'$ and $r = r'$. In each set S of atomic formulas one can select canonical representatives for the classes of associated formulas in S. For any formula φ, we let $int(\varphi)$ denote the maximal absolute value of an integer multiple of 1 occurring in some term in φ.

Consider now a formula $\exists x \psi(x)$ where ψ is q.f. We let $S = \{n_i x\, r_i\, a_i : i \in I\}$ be the set of all atomic subformulas of ψ containing x, where n_i are positive integers and a_i are terms not containing x. Let $J = \{i \in I : r_i \in \{=, <, >\}\}$ and let $K = I \backslash J$. $I' = \{i \in I : n_i x\, r_i\, a_i$ is a canonical representative within S of a class of associated atomic subformulas of $\psi\}$. J' and K' are defined similarly. m denotes a common multiple of all moduli m_i, $i \in K'$.

LEMMA 2.5. *Let $\exists x\psi(x)$ be as described above, assume all n_i $(i \in I)$ are equal and put $n = n_i$. Let $\psi(j, k)$ result from ψ by replacing nx in ψ by $a_j + k$. Then $\exists x\psi(x)$ is equivalent in $\mathbf{Z}$ to*

$$\bigvee_{j \in J'} \bigvee_{-t \leq k \leq t} [\psi(j, k) \wedge a_j + k \equiv 0(n)],$$

where $t = 2s + mn$, $s = int(\psi)$.

PROOF. We regard the a_i as fixed integers. Then the implication from right to left is obvious. To prove the converse, let c be an integer such that $\psi(c)$ holds in $\mathbf{Z}$, and assume without restriction that $J = (1, \ldots, q)$ with $a_1 \leq \cdots \leq a_q$.

CASE 1. $nc > a_q$. Choose $j \in J'$ with $a_q \sim a_j$. Then $a_j + 2s \geq a_q$. Choose $2s < k \leq t$ with $nc \equiv a_j + k(nm)$. Then $\psi(j, k) \wedge a_j + k \equiv 0(n)$ holds in $\mathbf{Z}$.

CASE 2. $nc < a_1$, is similar.

CASE 3. $|nc - a_h| \leq nm$ for some $h \in J$. Then there exists $j \in J'$ such that $|nc - a_j| \leq t$. Pick $-t \leq k \leq t$ with $nc = a_j + k$. Then $\psi(j, k) \wedge a_j + k \equiv 0(n)$ holds in $\mathbf{Z}$.

CASE 4. Note case 3 and $a_h < nc < a_{h+1}$ for some $h \in J$. Then there exists $j \in J'$ such that $|a_j - a_h| \leq 2s$. Pick $0 < k' \leq nm$ such that $nc = a_h + k'(nm)$, and put $k = a_h - a_j + k'$. Then $|k| \leq t$ and $a_j + k = a_h + k'$ and so $\psi(j, k) \wedge a_j + k \equiv 0(n)$ holds in $\mathbf{Z}$.

Next, we treat the general case.

LEMMA 2.6. *Let $\exists x\psi(x)$ be as described above, let $\bar{\psi}(j, k)$ result from ψ by replacing each atomic subformula $n_i x\, r_i\, a_i$ by $n_i a_j + n_i k\, r_i\, n_j a_i$, if $r_i \in (=, <, >)$, and by $n_i a_j + n_i k \equiv n_j a_i (m_i n_j)$ if r_i is the relation $\equiv (m_i)$. Let m, s be as in Lemma 2.5, let*

$$n' = \prod_{i \in I'} n_i,$$

and let $t_j = n_j(2s + n'm)$. Then $\exists x\psi$ is equivalent in $\mathbf{Z}$ to

$$\bigvee_{j \in J'} \bigvee_{-t_j \leq k \leq t_j} [\bar{\psi}(j, k) \wedge a_j + k \equiv 0(n_j)].$$

PROOF. Let

$$n' = \prod_{i \in I'} n_i,\ a_i' = (n'/n_i)a_i, \qquad m_i' = m_i n'/n_i,$$

for $i \in I$, and let $m' = n'm$. Then each m_i' divides m'. Notice that $n_i x\, r_i\, a_i$ is equivalent to $n' x\, r_i\, a_i'$ for $r_i \in (=, <, >)$, and $n_i x \equiv a_i(m_i)$ is equivalent to $n' x \equiv a_i'(m_i')$. Let ψ' result from ψ by replacing each atomic subformula by its equivalent of the form $n' x\, r_i\, a_i'$. Then $s' = int(\psi') \leq n's = n' \cdot int(\psi)$. So we may conclude with Lemma 2.5 that $\exists x\psi$ is equivalent to $\exists x\psi'$, and this in turn to

$$\bigvee_{j \in J'} \bigvee_{l' \leq k' \leq t'} [\psi'(j, k') \wedge a_j' + k' \equiv 0(n')],$$

where $t' = 2n's + n'm' = n'(2s + m')$.

By definition of a_j', $a_j' \equiv 0(n'/n_j)$; so we may equivalently restrict the second disjunction to k' of the form $k' = k \cdot n'/n_j$, where $-t_j \leq k \leq t_j$. Dividing finally each of the atomic subformulas $a_j' + k' r_i' a_i'$ of $\psi'(j, k')$ by $n'/n_i n_j$, and each $a_j' + k' \equiv 0(n')$ by n'/n_j, we obtain the desired result.

Next, we estimate the size of the formula obtained in Lemma 2.6. For this purpose, we introduce the following complexity measures:

$atom(\varphi) = |I|$, the number of atomic formulas in φ;
$atom'(\varphi) = |I'|$, the number of canonical representatives of atomic formulas in φ;
$coef(\varphi)$ = the maximal absolute value of all coefficients of variables in φ;
$mod(\varphi)$ = the absolute value of $lcm(m_i: i \in K')$. As before, we put
$int(\varphi)$ = the maximal absolute value of all coefficients of 1 in φ.

Denote in Lemma 2.6 $\exists x \psi$ by φ and the right hand side of the equivalence by

$$\varphi' = \bigvee_{j \in J'} \psi_j.$$

Then we get:

LEMMA 2.7
$atom'(\psi_j) \leq atom'(\varphi) + 1$,
$atom'(\varphi') \leq (2\ atom'(\varphi))^2$,
$coef(\varphi') \leq (2\ coef(\varphi))^2$,
$mod(\varphi') \leq mod(\varphi) \cdot coef(\varphi)^{(atom'(\varphi))}$,
$int(\varphi') \leq coef(\varphi) \cdot [2\ int(\varphi) + mod(\varphi) \cdot coef(\varphi)^{(atom'(\varphi))}]$.

In eliminating one block of existential quantifiers of length b, one may interchange the existential quantifiers with the disjunctions arising from the applications of Lemma 2.6, in order to decrease the complexity of the resulting formulas. (This was observed in Reddy & Loveland, 1978.) Suppose, for example, we are given the formula $\exists y \exists x \psi(x, y)$, where ψ is q.f. Suppose the elimination of the quantifier $\exists x$ in the formula $\exists x \psi(x, y)$, using Lemma 2.6, yields the disjunction $\bigvee_{i=1}^{m} \psi_i(y)$. Then $\exists y \exists x \psi(x, y)$ is equivalent to $\exists y (\bigvee_{i=1}^{m} \psi_i(y))$, and hence to $\bigvee_{i=1}^{m} (\exists y \psi_i(y))$. So we may apply Lemma 2.6 to each of the formulas $\exists y \psi_i(y)$ instead of the formula $\exists y (\bigvee_{i=1}^{m} \psi_i(y))$.

Using this device and Lemma 2.7, the complexity of the resulting formula φ' can be estimated by induction on b as follows:

LEMMA 2.8
$atom'(\varphi') \leq (2\ atom'(\varphi))^{(2^b)}$,
$coef(\varphi') \leq (2\ coef(\varphi))^{(2^b)}$,
$mod(\varphi') \leq mod(\varphi) \cdot (2\ coef(\varphi))^{(atom'(\varphi) \cdot 2^{2b})}$,
$int(\varphi') \leq int(\varphi) \cdot mod(\varphi) \cdot (2\ coef(\varphi))^{(atom'(\varphi) \cdot 2^{3b})}$.

Finally, after eliminating a quantifier blocks, we get:

LEMMA 2.9
$atom'(\varphi') \leq (2\ atom'(\varphi))^{((2^b)^a)}$,
$coef(\varphi') \leq (2\ coef(\varphi))^{(2^{ba})}$,
$mod(\varphi') \leq mod(\varphi) \cdot (2\ coef(\varphi))^{((2\ atom'(\varphi))^{(3b)^a})}$,
$int(\varphi') \leq int(\varphi) \cdot (mod(\varphi)) \cdot (2\ coef(\varphi))^{((2\ atom'(\varphi))^{(3b)^a})}$.

Since
$atom(\varphi') \leq atom'(\varphi') \cdot 2 \cdot int(\varphi')$, and
$length(\varphi') \leq atom(\varphi') \cdot 2 \cdot log\, int(\varphi') \cdot log\, coef(\varphi') \cdot f(\varphi)$,
where $f(\varphi)$ is the number of free variables in φ, we get:

COROLLARY 2.10. *There exists a positive constant c such that*
$length(\varphi') \leq exp[(c \cdot length(\varphi))^{(4b)^a}]$,
$int(\varphi') \leq exp[(c \cdot length(\varphi))^{(3b)^a}]$.

Since the running time of the q.e. procedure is polynomial in $length(\varphi')$, this proves Theorem 2.1.

Theorem 2.2 is proved by induction on the number of quantifiers in φ. The case that φ is q.f. is trivial. Let now φ be the prenex sentence $\exists x \psi(x)$ with at most a quantifier-blocks each of length at most b. By Theorem 2.1, $\psi(x)$ is equivalent to the quantifier-free formula $\psi'(x)$, having x as the only variable.

By Lemma 2.6, $\exists x \psi'(x)$ is equivalent to

$$\bigvee_{j \in J'} \bigvee_{-t_j \leq k \leq t_j} [\bar{\psi}'(j, k) \wedge a_j + k \equiv 0(n_j)].$$

Since a_j is an integer, this is equivalent to

$$\bigvee_{j \in J'} \bigvee_{-t_j \leq k \leq t, n_j | k + a_j} \psi'((a_j + k)/n_j).$$

Plugging in the bounds in Lemma 2.9, we find that $|(a_j + k)/n_j|$ is bounded by $4\, int(\psi')$. We may now apply the induction assumption to each $\psi((a_j + k)/n_j)$ to bound the quantifiers in these formulas. This proves Theorem 2.2.

3. Eliminating One Non-linear Quantifier

We consider now a new kind of quantifier-free formulas $\varphi(y)$ involving only one variable y, which may occur non-linearly. $\varphi(y)$ is a propositional combination of atomic formulas of the form $t(y)\ r\ 0$, where r is one of the relations $=$, $<$, $>$, $\equiv(m)$, and $t(y)$ is a term of the form

$$p(y) + c_1 \lfloor p_1(y)/q_1(y) \rfloor + \cdots + c_m \lfloor p_m(y)/q_m(y) \rfloor,$$

where c_i are integers and p, p_i, q_i are polynomials in y with integer coefficients. (We assume that all polynomials $q(y)$ are presented in such a way that the degree $d(q)$ of q is polynomial in the length $l(q)$ of q. This is the case, for example, for the dense representation of q.)

Our goal is to show the following theorem:

THEOREM 3.1. *There is a function $\varphi \mapsto s(\varphi) \in \mathbf{N}$, defined on all* q.f. *formulas φ in one variable y and computable in polynomial time such that $\exists y \varphi(y)$ is equivalent in the ordered ring $\mathbf{Z}$ of integers to $\exists y(-s(\varphi) < y < s(\varphi) \wedge \varphi(y))$.*

The proof follows well-known lines (comp. the article of Mignotte in Buchberger *et al.* (1982/3) and the arguments in Gurari & Ibarra (1979). So it will suffice to provide an outline of arguments.

LEMMA 3.2. *Let $f(y)=\sum_{i=0}^{d} f_i y^i$ be a polynomial of positive degree d in y with integer coefficients, and let $k \geq 1$ be an integer. Then for any real number a with*

$$|a| \geq \max\{1, k \cdot d \cdot |f_i|/|f_d| : 0 \leq i < d\},$$
$$(k-1)/k \cdot |f_d| \cdot |a|^d \leq |f(a)| \leq (k+1)/k \cdot |f_d| \cdot |a|^d;$$

moreover,

$$f(a) > 0 \Leftrightarrow f_d a^d > 0.$$

The proof is similar to the proof of Cauchy's inequality in Buchberger *et al.* (1982/3). Applying Lemma 3.2 to the numerator and denominator of a rational function, we obtain:

LEMMA 3.3. *Let*

$$f(y) = \sum_{i=0}^{d} f_i y^i, \qquad g(y) = \sum_{j=0}^{d'} g_j y^j$$

be the polynomials in y with integer coefficients of positive degrees d in d', respectively, and let k be an integer >1. Then for any real number a with

$$|a| \geq max\{1, k \cdot d \cdot |f_i|/|f_d|, \quad k \cdot d' \cdot |g_j|/|g_{d'}| : 0 \leq i < d, 0 \leq j < d'\},$$
$$\frac{(k-1)|f_d| \cdot |a|^{d-d'}}{(k+1)|g'_d|} \leq \left|\frac{f(a)}{g(a)}\right| \leq \frac{(k+1)|f_d| \cdot |a|^{d-d'}}{(k-1)|g_{d'}|};$$

moreover,

$$f(a)/g(a) > 0 \Leftrightarrow f_d a^{d-d'}/g_{d'} > 0.$$

COROLLARY 3.4. *Let f, g, k, a be as above, and assume in addition that $d < d'$ and a is an integer with $|a| > (k+1)|f_d|/|g_{d'}|$. Then*

1. $|f(a)/g(a)| < 1/(k-1)$.
2. *For any polynomial $h(y)$ with integer coefficients, $\lfloor h(a)+f(a)/g(a) \rfloor = h(a)$ or $\lfloor h(a)+f(a)/g(a) \rfloor = h(a)-1$.*

Recall that polynomial division with remainder can be performed in polynomial time. Combining this fact with Lemmas 3.2 and 3.3 and Corollary 3.4 and an appropriate choice of the integers k, we get:

LEMMA 3.5. *There are functions $t \mapsto s(t) \in \mathbf{N}$, $t \mapsto P(t)(y)$ in $\mathbf{Z}[y]$ that are defined on all terms $t = t(y)$ and computable in polynomial time, such that for all integers a with $|a| \geq s(t)$,*

1. $t(a) = P(t)(a)$.
2. *For any relation*

$$r \in \{=, <, >\},\ t(a)\ r\ 0 \Leftrightarrow P(t)(\mathrm{sgn}(a) \cdot s(t))r0.$$

COROLLARY 3.6. *Let t, $s(t)$, $P(t)$, a be as in 3.5, and let k, m be positive integers. Then $t(a) \equiv k(m) \Leftrightarrow$ for some $1 \leq j \leq m$, $a \equiv j(m)$ and $P(t)(j) \equiv k(m)$.*

Theorem 3.1 is now an easy consequence of Lemma 3.5 and Corollary 3.6. It suffices to put $s(\varphi) = 1 + max\{s(t)$: t occurs in some atomic subformula of $\varphi\} + max\{m$: m is the modulus of some congruence in $\varphi\}$.

4. Main Results

Almost linear formulas arise by a combination of the formulas considered in sections 2 and 3: Let $\varphi(z_1, \ldots, z_k)$ be a formula of Presburger arithmetic with distinguished free variables z_i, let y be a variable distinct from all variables occurring in φ, and let $t_1(y), \ldots, t_k(y)$ be terms in y in the sense of section 3. Let $\varphi^* = \varphi(t_1, \ldots, t_k)$ result from φ by substituting $t_i(y)$ for z_i. Then φ^* is an almost linear formula (a.l. formula) with non-linear variable y. Further a.l. formulas ρ, σ are obtained from φ^* by quantifying over y, $\rho = \exists y \varphi^*$, $\sigma = \forall y \varphi^*$. Thus we may assume without restriction that the atomic subformulas of an a.l. formula ψ with non-linear variable y are of the form $n_0 + n_1 x_1 + \cdots + n_k x_k \, r \, t(y)$, where n_i are integers, $t(y)$ is a term in y in the sense of section 3, and r is one of the relations $=, <, >, \equiv(m)$. Almost linear arithmetic (ALA) is the set of all a.l. sentences true in the ordered ring $\mathbf{Z}$ of integers.

THEOREM 4.1. *Let φ be a prenex* a.l. *sentence with at most a quantifier-blocks each of length at most b. For a constant c, let φ'_c be the sentence resulting from φ by replacing each quantifier $\exists x$, $\forall x$ in φ by*

$$[\exists x, \mathit{length}(x) \leq \mathit{length}(\varphi)^{((cb)^a)}]$$

and

$$[\forall x, \mathit{length}(x) \leq \mathit{length}(\varphi)^{((cb)^a)}],$$

respectively. Then there exists a positive constant c such that φ'_c is equivalent to φ in $\mathbf{Z}$.

The proof is exactly the same as for Theorem 2.2, using Theorem 3.1 for the non-linear quantifier in φ.

COROLLARY 4.2. *The decision problem for* a.l. *sentences in* ALA *in the Berman complexity class*

$$\bigcup_{c>0} \mathit{STA}(*, 2^{c^n}, n),$$

and hence in

$$\bigcup_{c>0} \mathit{SPACE}(2^{c^n}).$$

In particular, the decision problem for existential a.l. *sentences in ALA is in $\mathit{NTIME}(2^{c^n})$.*

By Berman (1980), the decision problem for PrA is also complete in this class; consequently, the same applies to ALA.

COROLLARY 4.3. *The decision problem for prenex a.l. sentences in ALA with a fixed bound on the number of quantifiers and at most a quantifier-blocks beginning with a block of existential (universal) quantifiers is in the class $\sum_a^p$ ($\prod_a^p$) of the polynomial time hierarchy.*

Notice that for $a = 1$ and unbounded number of quantifiers, Theorem 4.1 yields only a non-deterministic **exponential** time bound for the complexity of deciding existential ALA-sentences. Using the technique of von zur Gathen & Sieveking (1978) and Gurari & Ibarra (1979), it is, however, possible to get an NPTIME bound for this case as well.

Reviewing the proofs of these results, we see that the essential fact used was the following; for the "right-hand side" t of any atomic formula $n_0 + n_1 x_1 + \cdots + n_k x_k \, r \, t(y)$, there are bounds $s(t, m)$ for the solutions of equations $t(y) = m (m \in \mathbf{Z})$, and the asymptotic behaviour of $t(y)$ is determined by the value of $t(s(t, m))$. The latter condition is required only in order to handle **inequalities.** Let now PrA^- be Presburger arithmetic **without** order.

Let T be a class of polynomials $p(y_1, \ldots, y_k)$ with integer coefficients. Then, we say T has **effective equation bounds**, if there exists a recursive function $s: \mathbf{N}^2 \to \mathbf{N}$, such that for any $p(\mathbf{y})$ in T, $m \in \mathbf{Z}$, $a_1, \ldots, a_k \in \mathbf{Z}$ with $p(\mathbf{a}) = m$, $|a_i| \leq s(\mathit{length}(p), m)$ for $1 \leq i \leq k$. Let ALA (**T**) be the class of all sentences obtained from PrA^--formulas φ by substituting some $p_j(\mathbf{y})$ in T for free variables z_j of φ, and adding a block of quantifiers $\exists y_1 \ldots \exists y_k$ or $\forall y_1 \ldots \forall y_k$. Then we have the following result:

THEOREM 4.4. *Suppose T has effective equation bounds. Then the decision problem for $ALA(T)$ is recursively solvable. Upper complexity bounds can be obtained as in Theorem* 4.1 *by combining the bound function s for T with the bounds for PrA in section* 2.

By the famous results of Baker (1968), Theorem 4.4 is applicable, for example, to the class T of irreducible binary forms $p(y_1, y_2)$.

References

Baker, A. (1968). Contributions to the theory of diophantine equations, I. On the representation of integers by binary forms, II. The Diophantine equation $y^2 = x^3 + k$. *Phil. Trans. Roy. Soc. London* (ser. A) **263,** 173-208.

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

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

Buchberger, B., Collins, G. E., Loos, R. (eds.) (1982/3) *Computer Algebra.* Berlin: Springer-Verlag.

Cooper, D. C. (1972). Theorem-proving in arithmetic without multiplication. In: *Machine Intelligence* Vol. 7, pp. 91-100. Edinburgh: University 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. *Lecture Notes in Mathematics* **718.**

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

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

Von zur Gathen, J., Sieveking, M. (1978). A bound on solutions of linear integer equations and inequalities. *Proc. AMS* **72,** 155-158.

Graedel, E. (1987). The complexity of subclasses of logical theories. Doctoral Dissertation, Basel.

Gurari, E. M., Ibarra, O. H. (1979). An NP-complete number-theoretic problem. *J. ACM* **26,** 567-581.

Lipshitz, L. (1978). The diophantine problem for addition and divisibility. *Trans. AMS* **235,** 271-283.

Oppen, D. C. (1973). Elementary bounds for Presburger arithmetic. *Proc. 5th ACM Symp. on Theory of Computing,* pp. 34-37.

Presburger, M. (1929). Über die Vollständigkeit eines gewissen Systems der Arithmetik ..., Comptes rendues du Ier Congres des Math. des Pays Slaves, Warsaw, **395,** pp. 92-101.

Reddy, C. R., Loveland, D. W. (1978). Presburger arithmetic with bounded quantifier alternation. *ACM STOC* 320-325.

Scarpellini, B. (1984). Complexity of subcases of Presburger arithmetic. *Trans. AMS* **284,** 203-218.

Shostak, R. E. (1977). On the SUP-INF method for proving Presburger formulas. *J. ACM* **24,** 529-543.

Stockmeyer, L. (1977). The polynomial time hierarchy. *Th. Comp. Sci.* **3,** 1-22.

Volger, H. (1983). Turing machines with linear alternation, theories of bounded concatenation and the decision problem of first order theories. *Th. Comp. Sci.* **23,** 333-337.