Complexity and Uniformity of Elimination in Presburger Arithmetic

Volker Weispfenning
Universität Passau
D-94030 Passau, Germany
e-mail: weispfen@alice.fmi.uni-passau.de

January 29, 1997

MIP-9703

Abstract

The decision complexity of Presburger Arithmetic PA and its variants has received much attention in the literature. We investigate the complexity of quantifier elimination procedures for PA – a topic that is even more relevant for applications. First we show that the the author's triply exponential upper bound is essentially tight. This fact seems to preclude practical applications. By weakening the concept of quantifier elimination slightly to bounded quantifier elimination, we show, however, that the upper and lower bound for quantifier elimination in PA can be lowered by exactly one exponential. Moreover we gain uniformity in the coefficients, a property that we prove to be impossible for complete quantifier elimination in PA. Thus we have tight upper and lower complexity bounds for elimination theory in PA and uniform PA. The results are inspired by experimental implementations of bounded quantifier elimination that have solved non-trivial application problems e.g. in parametric integer programming.

1 Introduction

Presburger arithmetic PA is the first-order theory of the integers in the language L having $0, 1$ as constants, $+, -$ as binary operations, and equality $=$, order $\leq$ and congruences $\equiv_n$ modulo all integers $n \geq 1$ as binary relations. The fundamental paper of Presburger [P29] established an effective quantifier elimination procedure and a decision procedure for this "linear fragment" PA of number theory. The strength of his results could be appreciated only by 1931, when Gödel's incompleteness theorem showed that even the "quadratic fragment" of number theory is algorithmically undecidable (compare [GI79]).

The language of PA is rich enough to express many important application problems, such as solvability of (parametric) systems of linear Diophantine equations, integer feasibility of systems of (parametric) linear constraints, integer programming, and certain problems in program description and verification (compare [G85, SJ80]). This motivated an extensive study of the complexity of the decision problem for fragments and extensions of PA [Ber77, Ber80, Coo72, FR75, FR79, FiR74, F82, GS78, G87, GI79, GI81, L78, O73, RL78, Sc84, Sh77, V83]. While the decision problem is concerned with closed (i.e. parameter-free) formulas, the quantifier elimination problem deals with simplification of formulas involving free variables to a form that is easy to evaluate. It has turned out that for applications a quantifier eliminationprocedure is as a rule much more useful than a decision procedure. The reason is that a decision procedure gives a 'yes' or 'no' answer to a specific problem, while a quantifier elimination procedure describes for which integer values of the free variables an assertion holds; thus quantifier elimination provides a structural explanation in place of simple yes-no-answer. An upper bound for the worst-case complexity of the quantifier elimination problem in PA was obtained in [W90]: Let ℓ be the length of the input formula φ, n the number of quantified variables in φ and b the number of quantifier-blocks in φ. Then the bound is of the form $\exp(\ell^{(cn)^b})$ for some constant c. Moreover this bound holds no matter, whether integer constants are represented in unary or binary notation.

The first result of this note, Theorem 3.1, shows that the quantifier elimination problem for PA is inherently triply exponential. In fact the lower bound closely matches the upper bound in [W90].

This result seems to preclude any practical application of quantifier elimination in PA. In fact the situation can, however, be improved by exactly one exponential in exchange for a little sacrifice that is comparatively harmless in applications, namely an NP-search problem. The clue for this improvement is to abandon complete quantifier elimination in favour of bounded quantifier elimination, where one admits *bounded quantifiers* in the output formulas. This shift of viewpoint offers an extra advantage that is missing from complete quantifier elimination, namely *uniformity in the coefficients* of PA–terms and PA–formulas: We introduce uniform Presburger arithmetic UPA as an extension of PA, where we allow unquantified parameters in the coefficients of the integer variables. Formally this is achieved by introducing scalar terms of a new "scalar" sort that are built up from scalar parameters by certain scalar operations.

Our results on UPA are as follows: In Theorem 3.2 we show that complete quantifier elimination is impossible in UPA. This is in sharp contrast to a result of van den Dries and Holly [DH92] that proves quantifier elimination for UPA *without order*. The result of Theorem 3.2 was posed there as an open problem that "seems to be very hard". In theorem 3.3 we prove a lower bound for bounded quantifier elimination in PA (and hence in UPA) that is exactly one exponential lower than that of complete quantifier elimination in PA. In theorem 4.1 we describe an explicit bounded quantifier elimination procedure for UPA with an upper complexity bound again exactly one exponential lower than that of complete quantifier elimination in PA. As a corollary we can determine the infimum of the satisfaction set of an existential, parameter-free L formula in one free variable in polynomial space. Applications of the theorem and the corollary include a solution method for parametric mixed integer optimization problems with linear constraints and linear or quadratic objective function, and the problem of automatic loop parallelization in programs.

2 PA and uniform PA

Recall the Presburger arithmetic PA is the first-order theory of integers in the language $L = \{0, 1, +, -, \leq, \{\equiv_m\}_{m\in\mathbf{N}}\}$. So L-terms in PA can be written in the form

$$t = \sum_{i=1}^{k} n_i x_i + n_0 1,$$

where x_i are variables and and n_1 are integers. Atomic formulas containing a distinguished variable x can be written in the following normal form

$$nx = a, nx \leq a, nx \geq a, nx \equiv_m a$$

where $m, n \in \mathbf{N}$ and a is a term that does not contain the variable x, and $nx \geq a$ stands for $n(-x) \leq -a$. Formulas are obtained from atomic formulas by composition with the propositional operators $\wedge, \vee, \neg$ and quantifiers $\exists x, \forall x$. Formally, integer coefficients of variables and the constant 1 as well as moduli of congruences are written in unary notation. We reserve, however, the option to write these integers also in binary notation. Whenever necessary, we will indicate which notation is used. An L-formula is *quantifier-free*, if it contains no quantifiers. Using the properties of discrete order and of congruences in $\mathbf{Z}$ (viz. $\neg a \equiv_n 0 \iff \bigvee_{i=1}^{n} a \equiv_n i \cdot 1$) negation can be eliminated from quantifier-free L-formulas φ in PA. An L-formula is *prenex*, if it is of the form $Q_1 x_1 \ldots Q_n x_n \varphi$, where φ is a quantifier-free formula and Q_i are quantifiers. In such a prenex formula φ the quantifiers $Q_i x_i$ can be grouped into *blocks* of similar quantifiers (i.e. all existential or all universal). An *existential formula* is a prenex formula with a single block of existential quantifiers in its prefix.

A quantifier elimination procedure for PA is an algorithm that assigns to every L-formula φ a quantifier-free L-formula φ' that is equivalent to φ in $\mathbf{Z}$.

PA can be axiomatized by axioms saying that $\mathbf{Z}$ is a discretely ordered abelian group with smallest positive element 1 and that $|\mathbf{Z}\ /nZ| = n$ for all natural numbers n. As a consequence, any lexicographical product $G = H \times \mathbf{Z}$ of a divisible ordered abelian group H with $\mathbf{Z}$ is a model of PA. We will have occasion to consider models of this type in the next section.

Uniform Presburger arithmetic UPA is a generalization of PA: We extend the language L to a two-sorted language L^*. The new *scalar sort* will have the scalar constant 1, scalar variables $\alpha, \beta, \ldots$ and a set ScOp of finitary operation symbols acting on these variables. The old sort with constants $0, 1$, operations $+, -$ and relations $0, \leq, \equiv_m$ $(m \in \mathbf{N}\ )$ will be called the *vector sort* in L^*. The two sorts a tied together by the binary operation of scalar multiplication $(\alpha, x) \mapsto \alpha \cdot x$. Note that scalar variables are intended to range over the integers, while vector variables may range over more general models of PA. Scalar L^*-terms are obtained from scalar variables and scalar constants by superposition of the scalar operations in ScOp.

Vector terms in L^* are of the form

$$t = \sum_{i=1}^{k} a_i \cdot x_i + a_0 \cdot 1,$$

where a_i are scalar terms and x_i are vector variables. Atomic L^*-formulas are of the form $s\ \rho\ t$, where s, t are vector terms and $\rho \in \{=, \leq\} \cup \{\equiv_m\}_{m \in \mathbf{N}}$. L^*-formulas are obtained from atomic L^*-formulas similar as in PA. This means in particular that quantification is allowed L^* only with respect to vector variables. Quantifier-free formulas and quantifier elimination are defined for UPA similar as for PA, replacing L-formulas by L^*-formulas. A *parameter-free* L^*-formula is an L^*-formula containing no scalar variables.

In L^* we consider quantification of a special form: Let φ be an L^*-formula, x a vector variable, and let t be a scalar term. Then we write

$$(\exists x, |x| \leq t)\varphi \text{ for } \exists x(t \cdot (-1) \leq x \leq t \cdot 1\ \wedge\ \varphi)$$

$$(\forall x, |x| \leq t)\varphi \text{ for } \forall x(x \leq t \cdot (-1) - 1)\ \ \vee\ t \cdot 1 + 1 \leq\ x\ \vee\ \varphi).$$

We refer to the expressions

$$(\exists x, |x| \leq t),\ (\forall x, |x| \leq t)$$

as *bounded quantifiers* with *bound* t.

A *bounded quantifier* formula in L^* is an L^*-formula in which all quantifiers are bounded. A bounded quantifier formula is *prenex* if it is of the form

$$(Q_1 x, |x| \leq t_1) \ldots (Q_n x, |x| \leq t_n)\varphi$$

with $Q_i \in \{\exists, \forall\}$ and φ quantifier-free.

A *bounded quantifier elimination* procedure for UPA is an algorithm that assigns to every prenex L^*-formula φ a bounded quantifier formula φ' in L^* such that φ and φ' are equivalent in $\mathbf{Z}$ for all integer values of the scalar parameters in these formulas. In particular, quantifier elimination procedure is a bounded quantifier elimination procedure. We refer to quantifier elimination in contrast to bounded quantifier elimination as *complete quantifier elimination.* Notice that we may construe every L-term as a parameter-free L^*-term, and conversely every parameter-free L^*-term as an L-term by evaluating the scalar subterms as integers. Hence we may identify L-formulas with parameter-free L^*-formulas.

So the definition of bounded quantifier formulas and of bounded quantifier elimination applies to L-formulas and PA as well.

In the following, atom(φ) denotes the number of atomic subformulas of a formula φ in L or in L^*.

3 Impossibilities and lower bounds

Theorem 3.1 *There is a sequence of L-formulas $\{\varphi_n\}$ of lengths growing linearly in n such that for any sequence of quantifier-free L-formulas $\{\varphi'_n\}$ with the property that φ_n and φ'_n are equivalent in $\mathbf{Z}$ the length of φ'_n grows triply exponentially in n and hence in length(φ_n).*

Proof By a famous result of Fischer and Rabin ([FiR74], Theorem 13) there is a function $g : \mathbf{N} \longrightarrow \mathbf{N}$ such that

$$\text{for almost all } n \;\; g(n) \geq 2^{2^{2^{n+1}}}$$

and a sequence of L-formulas $\{\mu_n(x, y, z)\}$ of lengths growing linearly in n such that for all integers x, y, z, $\mu_n(x, y, z)$ holds in $\mathbf{Z}$ iff $0 \leq x, y, z < g(n)$ and $x \cdot y = z$. Thus the L-formulas $\{\mu_n(x, y, z)\}$ encode multiplication on large initial segments of $\mathbf{N}$.

Put $\varphi_n(z) := \mu_n(1, z, z)$ and $\psi_n(z) := \exists x \mu_n(x, x, z)$. Then $\varphi_n(z)$ holds in $\mathbf{Z}$ for an integer z iff $z < g(n)$ and $\psi_n(z)$ holds in $\mathbf{Z}$ for an integer z iff z is a square and $z < g(n)$. Suppose now that $\{\varphi'_n\}$ is a sequence of quantifier-free L-formulas with the property that φ_n and φ'_n are equivalent in $\mathbf{Z}$. Put

$$M_n := \{z \in \mathbf{Z} |\ \varphi'_n(z) \text{ holds in } \mathbf{Z}\}$$

Then M_n is a finite set in $\mathbf{N}$ bounded from above by $g(n)$. We may assume without restriction that the formulas $\varphi'_n(z)$ contain no equations and no negated inequalities, and that the atomic subformulas of $\varphi'_n(z)$ have been put into normal form with respect to the variable z. It is now easy to see that $\varphi'_n(z)$ must contain an inequality of the form $kz \leq b$, where $k \in \mathbf{N}$ and b is a variable-free L-term such that the evaluation of b/k in $\mathbf{R}$ is greater than or equal to $g(n)$. If integers in L are written in unary, this implies that length$(\varphi'_n) >$ length$(b) \geq g(n)$, which proves the theorem. $\square$

This argument fails, when integers in L are written in binary; in this case we still conjecture that atom(φ'_n) grows triply exponential in n. The idea is to use the set

$$N_n := \{z \in \mathbf{Z} | \ \psi_n(z) \text{ holds in } \mathbf{Z}\}$$

of all squares below $g(n)$ in place of M_n, and to argue that $\#(N_n)$ grows triply exponential in n and that the distribution of integers in N_n is sufficiently irregular in order that it can not be described by few inequalities and congruences.

Supplement to Theorem 3.1 Using the refinement of the Fischer–Rabin result due to Fürer [F82], one can easily modify Theorem 3.1 for prenex input formulas φ_n with at most a quantifier blocks. The the lower bound for quantifier elimination in PA restricted to input formulas of this type is then of the form $2^{2^{(\frac{n}{a})^{ca}}}$ for some positive constant c. In particular, the quantifier elimination problem for existential input formulas is still *inherently doubly exponential* in PA.

Theorem 3.2 *For arbitrary choice of scalar operations Uniform Presburger Arithmetic does not admit quantifier elimination.*

Proof. Consider the following formula with one free variable x and one parameter a in the language L^* of UPA:

$$\varphi(\alpha, x) \ := \ \exists y \ (0 \leq 2y \leq \alpha \cdot 1 \ \wedge \ x \equiv_\alpha y)$$

We claim that there is no quantifier-free L^*-formula $\psi(\alpha, x)$ that is equivalent to $\varphi(\alpha, x)$ in $\mathbf{Z}$. In order to prove this we require the following fact on quantifier-free L^*-formulas $\psi(\alpha, x)$ that is easy to prove by induction on the length of ψ:

Fact: For every quantifier-free L^*-formula $\psi(\alpha, x)$ there exists a natural number k and scalar terms $s(\alpha), t(\alpha)$ such that for any fixed value of α in $\mathbf{Z}$, there exists a set $N_\alpha \subset \mathbf{Z}$ consisting of at most k elements such that

$$M_\alpha := \{x \in \mathbf{Z} \ \ | \ |x| \geq s(\alpha), \ \psi(\alpha, x) \text{ holds in } \mathbf{Z} \ \} \ = \bigcup_{b \in N_\alpha} \{x \in \mathbf{Z} \ \ | \ \ |x| \geq s(\alpha), \ x \equiv_{t(\alpha)} b\}$$

or

$$\mathbf{Z} \ \setminus M_\alpha = \bigcup_{b \in N_\alpha} \{x \in \mathbf{Z} \ \ | \ \ |x| \geq s(\alpha), \ x \equiv_{t(\alpha)} b\}$$

Roughly speaking this means that the set of all integers x described by $\psi(\alpha, x)$ for fixed value of α equals up to a finite error set either a union of at most k congruence classes wrt to some modulus or the complement of such a union.

Assume now for a contradiction that $\psi(\alpha, x)$ is a quantifier-free L^*-formula equivalent to $\varphi(\alpha, x)$ in $\mathbf{Z}$. Let k be determined from ψ as in the fact and fix the value of α as an integer $\alpha > 4k$. It is now easy to see that the set

$$M_\alpha := \{x \in \mathbf{Z} \quad | \, |x| \geq s(\alpha), \ \varphi(\alpha, x) \text{ holds in } \mathbf{Z} \ \}$$

violates the fact above since it comprises about $\frac{\alpha}{2}$ "consecutive" congruence classes modulo α. Indeed, pick $\lfloor \frac{\alpha}{2} \rfloor$ consecutive integers in M_α. Then by the fact mentioned above, two different such numbers must be congruent modulo $t(\alpha)$, and so $t(\alpha) < \lfloor \frac{\alpha}{2} \rfloor$. But this contradicts the definition of M_α. □

Remark Theorem 3.2 is in sharp contrast to a result of van den Dries and Holly in [DH92]: They prove that UPA in a language *without order* admits complete quantifier elimination by a model theoretic, non-effective argument. The result in theorem 3.2 is posed there as an one of two open problems that "seem to be very hard".

Theorem 3.3 *There is a sequence of L-formulas $\{\varphi_n\}$ of lengths growing linearly in n such that for any sequence of bounded quantifier L-formulas $\{\varphi'_n\}$ with the property that φ_n and φ'_n are equivalent in $\mathbf{Z}$ the length of φ'_n grows doubly exponentially in n and hence in length(φ_n). This is even the case if integers are coded in unary notation in φ_n and in binary notation in φ'_n.*

Proof. Let ω be a new constant. By a slight extension of a result of Fischer-Rabin [FiR74] (see [W88], Lemma 5.5) there is a sequence of formulas $\{\varphi_n(x)\}$ in the language $L'_\omega = \{0, \omega, +, -\}$ such that in any additive, abelian group G with a distinguished element ω of infinite order: $\varphi_n(x)$ holds in G iff $x = i\omega$ for some $0 \leq i < 2^{2^n}$. Moreover the length of $\varphi_n(x)$ grows linearly in n.

In order to apply the topological technique of [W88] we have to pass to a non-standard model of PA with modified topology: Let $G := \mathbf{R} \times \mathbf{Z}$ be the lexicographical product of the ordered additive abelian groups $\mathbf{R}$ and $\mathbf{Z}$ and put $\omega := (1, 0)$, $1 := (0, 1)$. Then by Presburgers axioms, G is a model of PA. For fixed n put $\varphi(x) := \varphi_n(x)$ and let $\varphi'(x)$ be a bounded quantifier formula in $L_\omega = \{0, 1, \omega, +, -, <\}$ equivalent to $\varphi(x)$ in G. We claim that at$(\varphi') \geq 2^{2^n}$. This will prove the theorem.

In order to prove the claim, let m be the least common multiple of all moduli of congruences occuring in φ', and put $S = \{0, \ldots, m-1\}$. We furnish $\mathbf{R}$ with the order topology, S with the discrete topology, $\mathbf{R} \times S$ with the product topology, and finally G with the topology induced by the map $\pi : G \longrightarrow \mathbf{R} \times S$, $(x, y) \mapsto (x, i)$, where $i \equiv_m x$. In other words, a subset A of G is open iff $\pi(A)$ is open in $\mathbf{R} \times S$. We let $\delta(A)$ denote the boundary of the set A in this topology and recall the *rules*

$$\delta(A \cup B),\ \delta(A \cap B) \subseteq \delta(A) \cup \delta(B) \text{ and } \delta(G \setminus A) = \delta(A)$$

For an L_ω-formula $\psi(x)$ in one free variable x we let ψ^G denote the set of all $x \in G$ satisfying $\psi(x)$ in G.

The following *fact* is easy (but somewhat tedious) to verify:
For every atomic subformula $\psi(x)$ of $\varphi'(x)$, $\delta(\psi^G)$ is either empty, or of the form $\{a\} \times \mathbf{Z}$, or of the form $\{a\} \times C$ for a single congruence class C modulo m in $\mathbf{Z}$, and some $a \in \mathbf{R}$.

Regarding the bounded quantifiers in $\varphi'(x)$ as finite disjunctions or conjunctions, we may assume that $\varphi'(x)$ is in fact a quantifier-free formula in L_ω. Then by the rules for the boundary, $\delta(\varphi'^G)$ is the contained in the union of all $\delta(\psi^G)$, where ψ ranges over all atomic subformulas of φ'. On the other hand, $\varphi'^G = \{\ i\omega \mid 0 \leq i < 2^{2^n}\ \}$, and so $\delta(\varphi'^G) = \bigcup\{\ \{i\} \times \{0\} \mid 0 \leq i < 2^{2^n}\ \}$

In view of the fact above, this means that φ', regarded as quantifier-freeformula has at least 2^{2^n} many atomic subformulas ψ, such that $\delta(\psi^G)$ have pairwise different first entries. This in turn means that φ' regarded as bounded quantifier formula has at least 2^{2^n} different atomic subformulas. This proves the claim, and hence the theorem. $\square$

Supplement to Theorem 3.3 Using again the refinement of the Fischer–Rabin result due to Fürer [F82], one can modify Theorem 3.3 for prenex input formulas φ_n with at most a quantifier blocks. The the lower bound for bounded quantifier elimination in PA restricted to input formulas of this type is then of the form $2^{(\frac{n}{a})^{ca}}$ for some positive constant c. In particular, the bounded quantifier elimination problem for existential input formulas is still *inherently exponential* in PA.

4 Efficient quantifier elimination in UPA

Theorem 4.1 *There is a bounded quantifier elimination procedure in UPA assigning to every prenex L^*-formula φ a bounded quantifier formula φ' in L^*. If φ has at most a blocks of unbounded quantifiers each of length at most b, then the bounded quantifier elimination procedure runs in time and space $O(length(\varphi)^{(4b)^a})$. The only scalar operations required for the procedure are $+, \cdot$, lcm, max.*

Proof. By induction on the number of unbounded quantifiers in φ, it suffices to eliminate a single unbounded existential quantifier $\exists x$ in front of a bounded quantifier formula in L^*. So we may suppose that the input formula φ is of the form $\exists x \psi(\alpha_1, \ldots, \alpha_m, x, y_1, \ldots, y_n)$, where ψ is a bounded quantifier formula, α_i are the scalar parameters and x, y_i are the free variables of ψ. Notice that for *fixed integer values* of the parameters α_i, the formula ψ can be regarded as a quantifier-free L-formula ψ_1, by rewriting the bounded existential and universal quantifiers as finite disjunctions and conjunctions. Next the fast quantifier elimination procedure in [W90] can be applied to $\varphi_1 := \exists x \psi_1$ in order to obtain an equivalent quantifier-free L-formula φ_1'. The important point is to show now that the parameters α_i can be recovered in φ_1', *provided* we admit an additional bounded existential quantifier in rewriting φ_1' as a bounded quantifier L^*-formula φ'. In other words, the quantifier elimination procedure of [W90] is *uniform in the parametric coefficients* provided it is rearranged as a bounded quantifier elimination procedure.

This fact is established by a careful analysis of the quantifier elimination procedure in [W90]. As a pleasant byproduct, the resulting bounded quantifier elimination procedure for UPA has an upper complexity bound that is exactly one exponential lower than the original bound for the quantifier elimination procedure.

In the following we provide the required steps for this analysis. The crucial point is to reinterpret the elimination lemma 2.6 in [W90] as a bounded quantifier elimination lemma in UPA. For this purpose, we introduce the corresponding notation: We assume that ψ has a prefix of k bounded quantifiers $(Q_1 z_1, |z_1| \leq s_1), \ldots, (Q_k z_k, |z_k| \leq s_k)$, where $Q_i \in \{\exists, \forall\}$; moreover we assume that negations and equations have been eliminated from ψ and that all atomic subformulas of ψ containing the variable x have been normalized to the form $\beta_i x \ r_i \ a_i$, where r_i is one of the relations $\leq, \equiv_{\mu_i}$ for some scalar terms μ_i and a_i terms in the remaining variables $y_1, \ldots, y_n, z_1, \ldots, z_k$ and the parameters $\alpha_1, \ldots, \alpha_m$. We let $J = \{i \in I \mid r_i \in \{\leq, \geq\}\}$ and put $K = I \setminus J$, asuume without restriction that $J, K \neq \emptyset$, and put $\mu = \mathrm{lcm}\{\mu_i \mid i \in K\}$, $s = \max\{s_1, \ldots, s_k\}$. With this notation the analogue of lemma 2.6 in [W90] reads as follows.

Lemma 4.2 *Let z be a new variable. For each $j \in J$ let ψ_j^+ and ψ_j^- be the bounded quantifier formulas obtained from ψ as follows: Replace each congruence $\beta_i x \equiv_{\mu_i} a_i$ $(i \in K)$ by $\beta_i a_j + \beta_i z \equiv_{\mu_i \beta_j} \beta_j \ a_i$ and replace each inequality $\beta_i x \leq a_i$ $(i \in J)$ by $\beta_i a_j + \beta_i z \ \rho \beta_j a_i$, where ρ is "$\leq$" for ψ_j^+ and ρ is "$\geq$" for ψ_j^-. Let t_j be the scalar term $t_j := \beta_j(2s + \prod_{i \in I} \beta_i \mu)$. Then $\varphi := \exists x \psi(x)$ is equivalent in UPA to the following bounded quantifier formula φ':*

$$\psi(0) \ \vee \ \bigvee_{j \in J} (\exists z, |z| \leq t_j)(a_j + z \equiv_{\beta_j} 0 \ \wedge$$

$$((\beta_j > 0 \ \wedge \ \psi_j^+) \ \vee \ (\beta_j < 0 \ \wedge \ \psi_j^-)))$$

The **proof** of this lemma is obtained by applying lemma 2.6 of [W90] to $\exists x \psi(x)$ with *fixed integer values of the parameters* $\alpha_1, \ldots, \alpha_m$. $\square$

The complexity analysis of the bounded quantifier elimination procedure induced by this lemma proceeds along the lines of Lemmas 2.7, 2.8, 2.9 and Corollary 2.10 in [W90], keeping in mind that the reduced number of atomic formulas

$\text{atom}'(\varphi')$ in [W90] corresponds to the actual number of atomic formulas $\text{atom}(\varphi')$ in the present bounded quantifier elimination setting. In particular, we get the bound of the theorem for $\text{length}(\varphi')$ and a bound of type $O(\text{length}(\varphi)^{(3b)^a})$ for the binary length of the scalar terms s bounding the quantifiers in φ'. □

The latter bound can, however, be improved dramatically by adapting the well-known observation of Bareiss [Bar68] about the growth of coefficients in integer Gauss elimination to our present setting: Notice that the iterated application of Lemma 4.2 above does roughly correspond to an iterated Gauss elimination on certain parameteric linear equations obtained from the inequalities of our input formula – except for the introduction of a new auxilliary variable z_i with a corresponding bounded quantifier in each elimination step. Hence the superfluous factors observed by Bareiss accumulate in the coefficients of the auxilliary variables only *with a retardation* of two elimination steps. Since, however, the quantifier elimination concerns only the originally quantified variables of φ, not the newly introduced auxilliary variables z_i, we can can still profit from the cancellation of the Bareiss-factors in iterated elimination, *provided* we keep our scalar terms *in non-expanded form.* As a result, the size of all scalar terms appearing in φ' as coefficients, moduli and quantifier bound, can be kept polynomial in the length of the input. This has the following important consequence:

Corollary 4.3 *Let φ be a purely existential L-formula with at most one free variable y. Let*

$$Y_\varphi = \mathit{inf}\{\ y \in \mathbf{Z}\ \mid \varphi \textit{ holds in } \mathbf{Z}\ \} \in \mathbf{Z}\ \cup \{\pm\infty\}.$$

Then Y_φ can be computed in polynomial space. Moreover, if φ has no free variable, then the validity of φ in $\mathbf{Z}$ constitutes an NP-search problem (compare [GS78] for the latter result).

Proof. We apply Lemma 4.2 iteratively in order to eliminate the unbounded quantifiers in φ successively. In each step the remaining existential quantifiers are interchanged with the disjunctions produced by earlier applications of the lemma. This results in a finite tree T of formulas, whose leaves are bounded quantifier formulas in the free variable y. The depth of the tree is the number of unbounded quantifiers in φ. The length of each leaf is polynomial in the length of φ, when integer coefficients and moduli are written in binary notation. The disjunction over all the leaves constitutes the output formula φ' that is equivalent to the input formula φ. We construct the tree T in a depth-first manner.

Suppose to begin with that φ has no free variable. Then the validity of φ in $\mathbf{Z}$ can be decided by guessing a leaf ψ of T and integer values for the variables occurring in ψ with bounded existential quantifiers. By the discussion above this search space is of size polynomial in the length of φ and the evaluation of a quantifier-free L-formula can be performed in polynomial time.

Next suppose that φ has the only free variable y. For each leaf $\psi(y)$ of T we can by the discussion above decide in space polynomial in the length of ψ and hence of φ, whether $\exists y \psi(y)$ holds in $\mathbf{Z}$. Moreover, if this is the case, then the proof of Lemma 4.2 will provide an explicit integer y_0 of polynomial binary length in the length of φ satisfying ψ in $\mathbf{Z}$. Next we decide in polynomial space, whether the formula $\exists y(y < y_0 1 \ \wedge \ \psi(y))$ holds in $\mathbf{Z}$. If the answer is 'no', then $Y = y_0$ and we are done. Otherwise, we iterate this procedure with $y_1 = y_0 - 1, y_2 = y_1 - 1, \ldots$, until the answer 'no' is reached. □

Remark Let φ be as in Corollary 4.3. Then in general any description of the set $\{ \ y \in \mathbf{Z} \ \mid \varphi \text{ holds in } \mathbf{Z} \ \}$ by a bounded quantifier formula φ' in L may require the length of φ' to be exponential in the length of φ even if integers in *varphi* are denoted in unary notation, and in φ' in binary notation. This is a consequence of the supplement to Theorem 3.3.

5 Conclusions and Applications

We have given tight upper and lower complexity bounds for quantifier elimination in Presburger arithmetic and for bounded quantifier elimination in uniform Presburger arithmetic. Moreover we have shown that quantifier elimination is impossible in uniform Presburger arithmetic, in contrast to a result in [DH92] for UPA without order. As a consequence, we have shown that for a parameter–free existential formula $\varphi(y)$ in uniform Presburger arithmetic with one free variable y, the minimum possible value of this free variable, such that $\varphi(y)$ holds in $\mathbf{Z}$, can be computed in polynomial space.

Besides their theoretical importance, these results have also practical significance. Two experimental implementations have been carried out at the University of Passau: A REDUCE-implementation of the bounded quantifier elimination procedure in Theorem 4.1 for PA (i.e. without parametric coefficients of variables) in [K91], a MAPLE-implementation of the applications of Theorem 4.1 and Corollary 4.3 to mixed integer programming with linear constraints, linear or quadratic objective function and additive parameters by Xue Rui (see [WX95]). An implementation of the full bounded quantifier elimination procedure in Theorem 4.1 in the REDLOG-package (compare [DS96]) is in preparation. The heuristic results of these implementations were quite encouraging: [K91] has produced necessary and sufficient conditions for the solvability of simultaneous congruences and for the existence of lattice points in parametrically described regions of the plane. [WX95] has solved among others (non totally unimodular) mixed integer programming problems with up to 11 real and 4 integer variables and 16 constraints in less than 2 minutes on a SUN Sparc-10. Moreover the implementation has turned out to be very useful in automatic parallelization of loops in programs (compare [L93] for the approach).

References

[Bar68] E.H. Bareiss, Sylvester's identity and multistep integer preserving gaussian elimination, math. of Computation 22, 565-578 (1968).

[Ber77] L. Berman, Precise bounds for Presburger arithmetic and the reals with addition, IEEE Symp. FOCS 18, 95-99 (1977).

[Ber80] L. Bermann, The complexity of logical theories, Th. Comp. Sci. 11, 71-77 (1980).

[Coo72] D. C. Cooper, Theorem-proving in arithmetic without multiplication, Machine Intelligence Vol.7, 91-100 (1972).

[DS96] A. Dolzmann, T. Sturm, REDLOG, Computer algebra meets computer logic, preprint MIP-9603, Universität Passau (1996).

[DH92] L. van den Dries, J. Holly, Quantifier elimination for modules with scalar variables, Annals of Pure and Applied Logic, 57, 161-179 (1992).

[FR75] J. Ferrante, Ch. Rackoff, A Decision Procedure for the first Order Theory of Real Addition with Order, SIAM J. Comp. 4, 69-77 (1975).

[FR79] J. Ferrante, Ch. Rackoff, The computational complexity of logical theories, Springer Lecture Notes in Mathmatics, 718 (1979).

[FiR74] M.J. Fischer, M. Rabin, Super-exponential complexity of Presburger arithmetic, SIAM-AMS Proceedings 7, 27-41 (1974).

[F82] M. Fürer, The complexity of Presburger arithmetic with bounded quantifier alternation depth, Theor. Comp. Sci. 18, 105-111 (1982).

[GS78] J. von zur Gathen, M. Sieveking, A bound on solutions of linear integer equations and inequalities, Proc. AMS 72, 155-158 (1978).

[G87] E. Graedel, The complexity of subclasses of logical theories, Doctoral Dissertation, Basel (1987).

[G85] E.M. Gurari, Decidable problems for powerful programs, J. ACM 32, 466-483 (1985).

[GI79] E.M. Gurari, O.H. Ibarra, An NP-complete number-theoretic Problem, J. ACM 26, 567-581 (1979).

[GI81] E.M. Gurari, O.H. Ibarra, The complexity of the equivalence problem for two characterizations of Presburger sets Theor. Comp. Science 13, 295-314 (1981).

[K91] Ch. Köppl, Eine REDUCE-Implementierung eine Quantoreneliminationsverfahrens für die Presburger Arithmetik,Diploma Thesis, Universität Passau (1991).

[L93] Ch. Lengauer, Loop parallelization in the polytope model, CONCUR'93, Springer LNCS vol. 715 (1993)

[L78] L. Lipshitz, The Diophantine problem for addition and divisibility, Trans. AMS 235, 271-283 (1978).

[O73] D. C. Oppen, Elementary bounds for Presburger arithmetic, Proc. 5th ACM Symp. on Theory of Computing, 34-37 (1973).

[P29] M. Presburger, Über die Vollständigkeit eines gewissen Systems der Arithmetik..., Comptes rendues du premier Congres des Math. des Pays Slaves, Warsaw, 92-101, 395 (1929).

[RL78] C.R. Reddy, D.W. Loveland, Presburger arithmetic with bounded quantifier alternation, ACM STOC, 320-325 (1978).

[Sc84] B. Scarpellini, Complexity of subcases of Presburger arithmetic, Trans. AMS 284, 203-218 (1984).

[Sh77] B. Shostak, On the SUP-INF method for proving Presburger formulas, J. ACM 24, 529-543 (1977).

[SJ80] N. Suzuki, D. Jefferson, Verification decidability of Presburger array programs, J. ACM 27, 191-205 (1980).

[V83] H. Volger, Turing machines with linear alternation, theories of bounded concatenation and the decision problem of First Order Theories, Theor. Comp. Sci. 23, 333-337 (1983).

[W88] V. Weispfenning, The complexity of linear problems in fields, J. Symb. Comp. 5, 3-27 (1988).

[W90] V. Weispfenning, The complexity of almost linear Diophantine problems, J. Symb. Comp. 10, 395-403 (1990).

[W97] V. Weispfenning, Simulation and optimization by quantifier elimination, J. Symb. Comput. to appear, (1997).

[W97a] V. Weispfenning, Parametric linear, quadratic and hyperbolic optimization by elimination, J. Symb. Comput. to appear, (1997).

[WX95] V. Weispfenning, Xue Rui, Parametric mixed integer programming by elimination, Tech. Report MIP-9503, Universität Passau (1995), poster presentation at ISSAC'95, Montreal.