Mixed Real-Integer Linear Quantifier Elimination

Volker Weispfenning

Fakultät für Mathematik und Informatik
Universität Passau
D-94030 Passau, Germany
e-mail: weispfen@uni-passau.de

Abstract

Consider the elementary theory T of the real numbers in the language L having 0,1 as constants, addition and subtraction and integer part as operations, and equality, order and congruences modulo natural number constants as relations. We show that T admits an effective quantifier elimination procedure and is decidable. Moreover this procedure provides sample answers for existentially quantified variables. The procedure comprises as special cases linear elimination for the reals and for Presburger arithmetic. We provide closely matching upper and lower bounds for the complexity of the quantifier elimination and decision problem for T.

Applications include a characterization of T-definable subsets of the real line, and the modeling of parametric mixed integer linear optimization, of continuous phenomena with periodicity, and the simulation and analysis of hybrid control systems.

We also consider the elementary theory of reals in variations of this language in view of quantifier elimination and decidability and provide positive and negative results for various variant languages.

1 Introduction

The design of quantifier elimination procedures for elementary algebraic theories is not only a fundamental problem of algebraic model theory, but also a fascinating problem of computer algebra. In recent years such quantifier elimination procedures have turned out to allow serious applications e.g. in simulation and optimization, control theory and applied computational geometry [1, 4, 6, 8, 14, 20, 21].

This applies in particular to the linear quantifier elimination procedures in [17, 12] for real algebra implemented in the REDLOG-package of REDUCE [2, 3], and to the linear quantifier elimination procedures in [18, 19] for the integers (Presburger Arithmetic) partially implemented in REDUCE [9]. The first quantifier elimination procedures for these theories were developed by A. Tarski in the 1930s and by M. Presburger in 1929 [16, 13] without emphasis on efficiency.

There are several types of applications, where one wants to eliminate two sorts of linear variables namely variables ranging over the reals and variables ranging over integers.

This situation occurs e.g.: in mixed linear optimization problem (see [22]), in the analysis of hybrid control systems (compare [10]), and in the simulation of continuous phenomena that have some periodicity such as train schedules (compare also example 21 of circling planes at an airport in [15]). For the first case one can simply combine the elimination procedures in [12] and [18] as sketched in [22] provided all parameters range only over integers. The reason for this possibility is that mixed linear optimization problems can be modelled as purely existential linear formulas; so quantifiers referring to real variables can be eliminated first, leaving a pure Presburger type linear integer elimination task.

For the other applications this restriction to purely existential problems without real parameters is too strong. Here we need both real parameters as well as arbitrary quantifier alternations. This is the quantifier elimination problem tackled in this paper. As a first result we show that the language L of Presburger arithmetic together with a sort-distinction between real and integer variables does not allow quantifier elimination. This result suggests a natural language extension L' by the unary integer part operation $[a]$ of the taking the greatest integer smaller or equal to the real number a.

The main result is then an algorithmic description of real linear quantifier elimination in this language L'. An explicit sort-distinction for integer variables is now superfluous, since $\mathbf{Z} = \{a \in \mathbf{R} \mid a = [a]\}$. Moreover we prove an additional feature of our quantifier elimination, that corresponds to [12, 19], namely the fact that we get "answers" for all variables in the outermost existential quantifier block. This means that the algorithm provides sample solutions for these variables depending on the parameters of the formula. This feature is of decisive importance for most applications. We provide an explicit example illustrating the quantifier elimination algorithm and the construction of answers.

As a corollary we show that the main result extends to a language L'', where we admit scalar multiplication by arbitrary rational constants. So the elementary theory of the reals in this language is decidable. Moreover we get closely matching upper and lower complexity bounds for the quantifier elimination and decision problem, and a structural characterization of L''-definable subsets of the real line. By way of contrast, quantifier elimination definitely breaks down if one admits scalar multiplication by a real parameter or integer divisibility in the language. In the latter case the elementary theory of real is in fact undecidable. The same applies if one admits scalar multiplication by a non-recursive real constant.

As indicated above, special cases of quantifier elimination for the L''-theory of reals have been implemented in REDUCE, [2, 3, 9] and in MAPLE [22], and have proven to be very valuable in practice [5]. Implementation of the full quantifier elimination for the L''-theory of reals is planned in an extension of the REDLOG-package.

2 An impossibility result

A first attempt to achieve quantifier elimination for mixed real and integer variables may consider the following language L adapted from Presburger arithmetic. We have two sorts of variables: real variables and integer variables; the latter are considered as a subsort of the former. The constants are 0, 1, operations are $+$ (binary), $-$ (unary), and the relations are equality $=$, order $<$, and congruences $\equiv_n$ for each natural number n. The semantics of this language is as in the reals, with integer variables ranging only over the integers and a congruence $s \equiv_n t$ between reals s, t being defined by $s - t \in n\mathbf{Z}$.

The following theorem asserts that quantifier elimination is impossible in this language.

Theorem 2.1 *Let $\varphi(x)$ be the following L-formula*

$$x \geq 0 \ \wedge\ \exists \xi (0 < 2(x - \xi) < 1),$$

where x is a real variable and ξ is an integer variable. Then there is **no** *quantifier-free L-formula $\varphi'(x)$ equivalent to φ in the reals.*

Proof Assume for a contradiction that such a $\varphi'(x)$ exists and let M be the set of reals x described by $\varphi(x)$. Then $M = \{k + r \mid k \in \mathbf{N}, 0 < r < \frac{1}{2}\}$ is unbounded from above in $\mathbf{R}$. Let $\bigvee_{i=1}^{n} \varphi_i(x)$ be a disjunctive normal form of $\varphi'(x)$, where each $\varphi_i(x)$ is a conjunction of equations, inequalities, congruences and incongruences. (Notice that negations in front of equations and inequalities can be eliminated.) Let M_i be the set of reals described by $\varphi_i(x)$. Let $\emptyset \neq J \subseteq I$ be the set of all $i \in I$ such that the set M_i is unbounded from above. Each M_i is an intersection of an interval M_i' and a set M_i'' defined by a conjunction of congruences and incongruences of the form $hx \equiv_m k1$ or $hx \not\equiv_m k1$. Moreover for $i \in J$, M_i' is unbounded from above. Pick an integer a such that the interval $[a, \infty)$ is contained in all M_i' with $i \in J$, and such that $a - 1$ is an upper bound for all M_i' with $i \in I \setminus J$. It is easy to see that each M_i'' is either dense or nowhere dense in $[a, \infty)$. Hence $M \cap [a, \infty) = (\bigcup_{i \in J} M_i'') \cap [a, \infty)$ is either dense or nowhere dense in $[a, \infty)$. This contradicts the description of M given above. □

3 The main theorem

In view of the negative result concerning quantifier elimination in L, it is natural to look for a slightly extended language L', where the counterexample $\varphi(x)$ does not work. For this purpose we extend L by a unary operation-symbol $[\,]$ for the integer part of a real argument. Then indeed our counterexample fails, since $\varphi(x)$ is equivalent in the reals to

$$x \geq 0 \ \wedge\ 0 < 2(x - [x]) < 1.$$

We are going to show that the reals admit quantifier elimination in L'; in fact we even show that in L' we have quantifier elimination with answers.

Theorem 3.1 *There is an algorithm assigning to a given L'-formula a quantifier-free L'-formula φ' that is equivalent to φ in $\mathbf{R}$. Moreover this quantifier elimination procedure yields answers to existential questions, i.e. the elimination provides as a byproduct for a given quantifier-free formula $\varphi(x, \underline{y})$ a finite set T of symbolic expressions $t(\underline{y})$ depending on the parameters $\underline{y}$ such that*

$$\exists x \varphi(x, \underline{y})$$

implies

$$\bigvee_{t \in T} \varphi(t(\underline{y}), \underline{y})$$

in the reals.

Notice that we have not exactly specified the "symbolic expressions" in this theorem. The nature of these expressions will become clear in the proof; at any rate, each $t(\underline{y})$ will determine a real function, or a non-standard real function.

Notice also that in L' there is no need to distinguish explicitly integer variables from real variables, since an integer variable x is characterized by the condition $x = [x]$. In the following, we abbreviate the *truncation* $x - [x]$ of a real x by x^*. For the purpose of linear quantifier elimination we will consider quantifiers ranging over the integers and quantifiers ranging over the half-open interval $[0, 1)$. The notation $\exists \xi (\varphi(\xi))$ will stand for $\exists x (x = [x] \ \wedge\ \varphi(x))$ (similarly for other variables η, ζ denoting integers).

The notation $\exists u (\varphi(u))$ will stand for $\exists x (0 \leq x < 1 \ \wedge\ \varphi(x))$ (similarly for other *truncated variables* v, w ranging over reals in the interval $[0, 1)$).

In order to perform quantifier elimination in L' it suffices iteratively to eliminate a single existential quantifier $\exists x$ in front of a quantifier-free formula $\varphi(x, \underline{y})$. Since we can write any real x as a sum $[x] + x^*$ with $[x] \in \mathbf{Z}$, $x^* \in [0, 1)$, it follows that $\exists x \varphi(x, \underline{y})$ is equivalent in $\mathbf{R}$ to $\exists \xi \exists u (\varphi(\xi + u, \underline{y}))$.

So our original task of eliminating the quantifier $\exists x$ is reduced to two more specialized tasks, namely the elimination of a quantifier $\exists \xi \varphi_1(\xi, \underline{y})$ and $\exists u \varphi_2(u, \underline{y})$ in front of quantifier-free formulas φ_1, φ_2.

As a first technical step, we show how to prepare a variable for elimination by removing it from the scope of the the integer-part operation.

Lemma 3.2 *Let ξ be an integer variable. Then any term $t(\xi, \underline{y})$ can be written in the form $n\xi + s(\underline{y})$, for some integer n and a term $s(\underline{y})$ not containing ξ.*

Proof By induction on the length of t: If t is a variable or a constant, then there is nothing to prove. The cases $t = t_1 + t_2$ and $t = -t_1$ are obvious. In the case $t = [t_1]$, put t_1 in the form $n\xi + s(\underline{y})$; then $t = n\xi + [s(\underline{y})]$, since ξ is supposed to be integer. □

Lemma 3.3 *Let u be a real variable in the range $[0, 1)$ and let $t(u, \underline{y})$ be a term. Then there is a finite disjoint case distinction given by quantifier-free formulas $\varphi_i(u, \underline{y})$ $(i \in I)$ that covers all cases, and a corresponding system $s_i(\underline{y})$ of terms not containing u and integers n_i $(i \in I)$, such that* *for all $i \in I$, $\varphi_i(u,\underline{y})$ implies $t(u,\underline{y}) = n_i u + s_i(\underline{y})$. Moreover the variable u does not occur in the scope of an integer part operation in the formulas $\varphi_i(u,\underline{y})$.*

Proof By induction on the length of t: If t is a variable or a constant, then there is nothing to prove. The cases $t = t_1 + t_2$ and $t = -t_1$ are obvious. In the case $t = [t']$, let $\varphi'_i(u,\underline{y}), s'_i(\underline{y}), n'_i$ $(i \in I)$ be associated with t' by induction assumption. Then we put for each $i \in I, 0 \leq j \leq n'_i, \varphi_{ij}(u,\underline{y}) = (\varphi'_i(n,\underline{y}) \ \wedge\ [s'_i(\underline{y})] + j \cdot 1 \leq n'_i u + s'_i(\underline{y}) < [s'_i(\underline{y})] + (j+1) \cdot 1)$. Then we obtain for each i and j that $\varphi_{ij}(u,\underline{y})$ implies $t(u,\underline{y}) = j \cdot 1 + [s'_i(\underline{y})]$. So we can put $n_{ij} = 0$ and $s_{ij}(\underline{y}) = j \cdot 1 + [s'_i(\underline{y})]$. □

After these preparations we can now prove the first claim of the theorem, i.e. that **R** admits quantifier elimination in L'. As observed above, it suffices to eliminate quantifiers of the form $\exists \xi \varphi, \exists u \varphi$, where φ is quantifier-free.

Case 1 $\exists \xi \varphi$. By lemma 3.2 we may assume that the atomic formulas in φ are of the form

$n\xi = s$, or $n\xi < s$, or $n\xi \equiv_k s$, with ξ not in s. These formulas can be equivalently rewritten in the following respective forms:

- $n\xi = [s] \ \wedge\ s = [s]$,
- $n\xi < [s] \ \vee\ (n\xi = [s] \ \wedge\ [s] < s)$,
- $n\xi \equiv_k [s] \ \wedge\ s = [s]$,

After the rewriting all atomic formulas involving ξ are of the Presburger type. Hence the quantifier $\exists \xi$ can now be eliminated by any quantifier elimination procedure for Presburger arithmetic.

Case 2 $\exists u \varphi$. By lemma 3.3 and an interchange between an existential quantifier and a disjunction, we may assume that each atomic formula in φ is of the form $nu = s$, or $nu < s$, or $nu \equiv_k s$, with u not in s. Formulas of the last type can be equivalently rewritten in the form

$$\bigvee_{i=0}^{n-1} (nu = s^* + i1 \ \wedge\ i1 \equiv_k [s]).$$

Now the quantifier $\exists u \varphi$ can be eliminated by any linear quantifier elimination procedure for **R**. □

Finally we show how to get answers for an existentially quantified variable $\exists \xi$ or $\exists u$. In the first case the quantifier elimination procedure for Presburger arithmetic in [18] provides as a byproduct answers that are terms in a slight extension of L'. Suppose we introduce for every rational number r a corresponding unary operation σ_r for scalar multiplication by r, i.e. $\sigma_r(x) = r \cdot x$ as real number. Call the resulting extension language L''. Then the answers obtained for an integer variable ξ are terms in L''. The same applies to the answers for a variable u ranging over $[0,1)$ by inspection of [12]. A more efficient alternative (see also [12]) will in addition yield also answers for u of the form $t \pm \varepsilon$, where t is an L''-term and ε is a symbol for a positive infinitesimal. □

Notice also that congruences can be eliminated in L'' as follows: $x \equiv_k y \iff [k^{-1}(y-x)] = k^{-1}(y-x)$. So we may assume from now on that congruences have been eliminated from L''.

Next we show that the main theorem can in fact be extended to the larger language L''.

Corollary 3.4 *There is an algorithm assigning to a given L''-formula a quantifier-free L''-formula φ' that is equivalent to φ in* **R**. *Moreover this quantifier elimination procedure yields answers to existential questions, i.e. the elimination provides as a byproduct for a given quantifier-free formula $\varphi(x,\underline{y})$ a finite set T of L''-terms $t(\underline{y})$ depending on the parameters $\underline{y}$ such that*

$$\exists x \varphi(x,\underline{y})$$

implies

$$\bigvee_{t \in T} \varphi(t(\underline{y}),\underline{y})$$

in the reals.

Proof It suffices to perform quantifier elimination for L''-formulas of the form $\exists x(\varphi(x,\underline{y}))$, where φ is quantifier-free. Moreover, we may assume as in the proof of theorem 3.1 that x is either an integer variable or a truncated real variable. Let k be the lcm of all denominators of scalar multipliers σ_r occurring in φ , and distribute scalar multiplication over addition in φ. Then the substitution $x' := k^{-1}x$ in φ, and the application of lemma 3.2 and lemma 3.3 result in a quantifier-free L''-formula $\varphi^*(x',\underline{y})$ such that in $\varphi^*(x',\underline{y})$ x' is not in the scope of an integer-part operation, and all scalar multipliers of x' in φ^* are integers. Hence the quantifier elimination for $\exists x(\varphi(x,\underline{y})$ is reduced to the quantifier elimination for $\exists x'(\varphi^*(x',\underline{y})$ which can be performed as in the proof of the main theorem. □

As a consequence we obtain the following decidability result.

Corollary 3.5 *The elementary theory T'' of the real numbers as an L''-structure is decidable. Morover, T'' is also the elementary theory of any subfield of the reals as an L''-structure.*

Proof It has been shown in [12] that the algorithmic linear quantifier elimination for the reals in the language $L_0 = \{0, 1, +, -, <\}$ is in fact valid for every subfield of the reals. The proof of our main theorem and corollary 3.4 shows that this fact extends to mixed real-integer in the language L''. Using this fact, it suffices to decide variable-free L''-formulas uniformly in arbitrary subfields of **R**. By means of truth-tables this problem is reduced to deciding atomic variable-free L''-formulas. Since 0 and 1 are the only constants in L'' every L''-term can easily be evaluated as a rational number. Hence evaluation of an atomic variable-free L''-formula amounts to simple sign evaluations of rational numbers. □

4 An example

We illustrate the quantifier elimination method described in the proof of the main theorem by an explicit example. Consider the following L'-formula

$$\varphi(y) \ := \ \exists x(0 < y - x \ \wedge\ 4(y-x) < 1 \ \wedge\ 2x \equiv_2 1)$$

In a first step the quantifier $\exists x$ ranging over the reals is replaced by quantifiers over an integer variable ξ and a truncated variable u; this results in an equivalent formula $\exists \xi \exists u(\varphi_1)$, with

$$\varphi_1(\xi,u,y) \ :=$$

$$(0 < y - \xi - u \ \wedge\ 4(y - \xi - u) < 1 \ \wedge\ 2(\xi - u) \equiv_2 1),$$

where x is replaced by $\xi + u$. In order to eliminate the quantifier in $\exists u(\varphi_1)$, we separate the truncated variable u on the left hand side of the atomic formulas, and obtain

$$\exists u(u < y - \xi \ \wedge\ 4u > 4(y - \xi) - 1 \ \wedge\ 2u \equiv_2 2\xi - 1)$$

Next we eliminate the occurrence of u in a congruence as in case 2 of the proof of the main theorem by noting that $2u \equiv_2 2\xi - 1$ is equivalent to

$$(2u = (2\xi - 1)^* \ \wedge\ 0 \equiv_2 [2\xi - 1]) \vee$$

$$(2u = (2\xi - 1)^* + 1 \ \wedge\ 1 \equiv_2 [2\xi - 1]).$$

Since ξ is an integer variable, we have $[2\xi - 1] = 2\xi - 1 \equiv_2 1$, and $(2\xi - 1)^* = 0$. Hence $2u \equiv_2 2\xi - 1$ is equivalent to $2u = 1$, and so by Gauss elimination $\exists u(\varphi_1)$ is equivalent to

$$2\xi < 2y - 1 \ \wedge\ 4\xi > 4y - 3 \ \wedge\ 2\xi \equiv_2 0.$$

Moreover $u = 1/2$ is the unique answer for the variable u in the existential formula $\exists u(\varphi_1)$. As a consequence, $\exists\xi\exists u(\varphi_1)$ is equivalent to

$$\exists\xi(2\xi < 2y - 1 \ \wedge\ 4\xi > 4y - 3).$$

In order to prepare the elimination of the quantifier $\exists\xi$, we proceed is in case 1 of the proof of the main theorem, and obtain the equivalent formula

$$\bigvee_{i=1}^{4} \exists\xi(\psi_i),$$

where

$$\psi_1 := \ (2\xi < [2y - 1] \ \wedge\ -4\xi < [3 - 4y]),$$

$$\psi_2 := \ (2\xi = [2y - 1] \ \wedge\ -4\xi < [3 - 4y] \ \wedge\ [2y - 1] < 2y - 1),$$

$$\psi_3 := \ (2\xi < [2y - 1] \ \wedge\ -4\xi = [3 - 4y] \ \wedge\ [3 - 4y] < 3 - 4y),$$

$$\psi_4 := \ (2\xi = [2y - 1] \ \wedge\ -4\xi = [3 - 4y]$$
$$\wedge\ [2y - 1] < 2y - 1 \ \wedge\ [3 - 4y] < 3 - 4y).$$

In the last three cases the quantifier elimination can be performed by a simple Gauss elimination, introducing a new congruence in each case: $\exists\xi(\psi_2)$ is equivalent to

$$-2[2y - 1] < [3 - 4y] \ \wedge\ [2y - 1] < 2y - 1 \ \wedge\ [2y - 1] \equiv_2 0.$$

$\exists\xi(\psi_3)$ is equivalent to

$$-[3 - 4y] < 2[2y - 1] \ \wedge\ [3 - 4y] < 3 - 4y \ \wedge\ [3 - 4y] \equiv_4 0.$$

$\exists\xi(\psi_4)$ is equivalent to

$$-2[2y-1] = [3-4y] \wedge [2y-1] < 2y-1 \wedge [3-4y] < 3-4y \wedge$$
$$[2y - 1] \equiv_2 0.$$

In the first case we apply the quantifier elimination method for Presburger arithmetic in [18] and find that $\exists\xi(\psi_1)$ is equivalent to

$$\bigvee_{i=1}^{3} -[3 - 4y] + i1 < 2[2y - 1] \ \wedge\ [3 - 4y] \equiv_4 i1.$$

In summary φ is equivalent in $\mathbf{R}$ to the quantifier-free L'-formula

$$\varphi'(y) \ := \ \bigvee_{i=1}^{3} (-[3 - 4y] + i1 < 2[2y - 1] \ \wedge\ [3 - 4y] \equiv_4 i1) \ \vee$$

$$(-2[2y - 1] < [3 - 4y] \ \wedge\ [2y - 1] < 2y - 1 \ \wedge\ [2y - 1] \equiv_2 0) \ \vee$$

$$(-[3 - 4y] < 2[2y - 1] \ \wedge\ [3 - 4y] < 3 - 4y \ \wedge\ [3 - 4y] \equiv_4 0) \ \vee$$

$$(-2[2y-1] = [3-4y] \wedge [2y-1] < 2y-1 \wedge [3-4y] < 3-4y \wedge$$
$$[2y - 1] \equiv_2 0).$$

So we see e. g. that φ holds for $y = 5/8$ or $y = 13/8$, and fails for $y = -5/8$ or $y = 7/8$ or $y = 3/2$.

Moreover we have the following set of answers for the variable ξ in the existential formula $\exists\xi\exists u(\varphi_1)$:

$$\xi \in \{ \ \frac{-[3 - 4y] + i1}{4} \ \mid\ i = 1, 2, 3 \ \} \cup \{ \ \frac{[2y - 1]}{2}, \frac{-[3 - 4y]}{4} \ \}$$

As a result we get the following set of answers for the variable x in our original existential formula $\varphi(y)$:

$$x \in \{ \ \frac{-[3 - 4y] + i1}{4} + \frac{1}{2} \ \mid\ i = 1, 2, 3 \ \} \cup$$

$$\{ \ \frac{[2y - 1]}{2} + \frac{1}{2}, \frac{-[3 - 4y]}{4} + \frac{1}{2} \ \}$$

5 Complexity of the Quantifier Elimination and the Decision Problem

The complexity of quantifier elimination for Presburger arithmetic has been studied in [18, 19]. For prenex input formulas of length ℓ with n quantified variables grouped into a blocks of alternating quantifiers quantifier elimination in Presburger arithmetic can be performed in deterministic time and space $2^{\ell^{n^{O(a)}}}$. Moreover there is a worst-case lower bound of the same type. For linear real quantifier elimination in the language $L_0 = \{0, 1, +, - <\}$ the corresponding upper and lower bound is one exponential lower, i. e. of the form $\ell^{n^{O(a)}}$. Since mixed real-integer quantifier elimination in L' or in L'' includes quantifier elimination for both Presburger arithmetic and for the linear theory of reals as special case, the worst-case lower bound for quantifier elimination in Presburger arithmetic applies here as well. We claim that a similar upper bound holds too:

Theorem 5.1 *Quantifier elimination for the reals and prenex formulas in L' or in L'' can be performed in deterministic time and space $2^{\ell^{n^{O(a)}}}$.*

Sketch of the proof. The case of quantifier elimination in L'' is reduced to quantifier elimination in L' as in the proof of corollary 3.4. The decisive observation for L'-quantifier elimination is the fact that both the elimination of an integer variable and the elimination of a truncated real variable is almost uniform with respect to formulas, whose atomic parts differ only by additive integer constants. For Presburger arithmetic this is proved in [18]; for the linear theory of reals it follows by inspection from [12]. As a preparatory step one replaces every block of quantifiers in the prefix of the input formula by corresponding blocks of quantifiers w. r. t. integer variables and truncated real variables as in the proof of theorem 3.1. Then one observes that the introduction of new integer-part operations during the elimination of variables does by lemma 3.2 not affect the other integer variables. Finally one observes that the removal of a truncated real variable u from all scopes of the integer-part operation and from all congruences in a given formula can be achieved by a single disjunction on the size of $[ku]$ for a suitable, large enough positive integer k. Armed with these observations, the calculation of the upper bound proceeds essentially as for Presburger arithmetic in [18]. □

As in [17, 18] we conclude from the fact that quantifier elimination in L' is achieved via answers provided by test terms in L'' the following complexity bound for the corresponding decision problem:

Corollary 5.2 *A closed prenex formula φ of length ℓ with n quantified variables grouped into a blocks of alternating quantifiers in L' or in L'' can be decided in the reals in deterministic space $\ell^{n^{O(a)}}$ and deterministic time $2^{\ell^{n^{O(a)}}}$; more specifically, φ can be decided by an alternating Turing machine in time $\ell^{n^{O(a)}}$ using at most a alternations.*

6 Definable Sets

The following structural characterizations of L-definable subsets of the set of the integers is well-known and an easy consequence of quantifier elimination for Presburger arithmetic: A subset A of $\mathbf{Z}$ is L-definable iff it is ultimately periodic, i.e. differs from a periodic subset of $\mathbf{Z}$ only by a finite set. For the linear theory of the reals in the language $L_0 = \{0, 1, +, -, <\}$ the corresponding characterization reads as follows: A subset A of $\mathbf{R}$ is L_0-definable iff it is a finite union of intervals with rational endpoints (compare [12]). Let us call subsets of this type *simple*. This means in particular that the linear theory of the reals in L_0 is *o-minimal* (see [7]). We will now characterize the L''-definables subsets of the real line structurally by a kind of composition of these two structural properties.

Call a subset A of $\mathbf{R}$ *periodically simple* if it is of the form $A = \bigcup_{n=-\infty}^{\infty}(np + B)$ for some simple set B contained in an interval $[0, p)$ for some rational number p. Call a subset A of $\mathbf{R}$ *ultimately periodically simple* if it is of the form $(A' \setminus B) \ \cup \ C$ for a periodically simple set A' and simple sets B, C.

Theorem 6.1 *A subset A of $\mathbf{R}$ is L''-definable iff it is ultimately periodically simple.*

Proof Every simple set B is obviously L''-definable. Next suppose A is periodically simple, say $A = \bigcup_{n=-\infty}^{\infty}(np + B)$ for the simple set B contained in the interval $[0, p)$ for the rational number p , where B is defined by the L''-formula $\psi(x)$. Then A is defined by the L''-formula $\varphi(x) := \exists y(y = [y] \ \wedge \ \psi(x + py))$. Finally if A is ultimately periodically simple, say $A = (A' \setminus B) \ \cup \ C$ for a periodically simple set A' and simple sets B, C defined by $\varphi'(x), \psi(x), \rho(x)$, respectively. Then A is defined by $\varphi(x) := (\varphi'(x) \ \wedge \ \neg\psi(x)) \ \vee \ \rho(x)$.

For the converse we use the fact that by quantifier elimination every L''-definable subset A of $\mathbf{R}$ is definable by a quantifier-free L''-formula $\varphi(x)$. We show that every atomic subformula of $\varphi(x)$ defines a simple set or a periodically simple set. From this fact we see that all L''-definable subsets are ultimately periodically simple, since the class of these sets is closed under boolean operations.

For this purpose we need the following lemma that characterizes the real functions defined by L''-terms.

Lemma 6.2 *Let $t(x)$ be a univariate L''-term. Then there exist rational numbers m, q and positive integers p, c such that*

1. *for all $x \in \mathbf{R}$, $mx + q \leq t(x) \leq mx + q - c$,*
2. *$t(x) - (mx + q)$ is a p-periodic real function,*
3. *the interval $[0, p)$ can be partitioned into finitely many subintervals with rational endpoints such that $t(x)$ is a linear function on each subinterval.*

The lemma is proved by a syntactic analysis of terms.

Based on the lemma we can now study the set A defined by an atomic L''-formula $t(x) = 0$ or $t(x) > 0$. With notations as in the lemma, we see that if $m \neq 0$ then A is a simple set. If $m = 0$ then $t(x)$ is p-periodic and $A \cap [0, p)$ is a simple set; so A is periodically simple. □

We illustrate the theorem by revisiting the example of section 4, and determining the set of real numbers defined by

$$\varphi(y) \ := \ \exists x(0 < y - x \ \wedge \ 4(y - x) < 1 \ \wedge \ 2x \equiv_2 1)$$

By the quantifier elimination performed in section 4, this formula is equivalent over the reals to the following quantifier-free formula

$$\varphi'(y) \ := \ \bigvee_{i=1}^{3}(-[3 - 4y] + i1 < 2[2y - 1] \ \wedge \ [3 - 4y] \equiv_4 i1) \ \vee$$

$$(-2[2y - 1] < [3 - 4y] \ \wedge \ [2y - 1] < 2y - 1 \ \wedge \ [2y - 1] \equiv_2 0) \ \vee$$

$$(-[3 - 4y] < 2[2y - 1] \ \wedge \ [3 - 4y] < 3 - 4y \ \wedge \ [3 - 4y] \equiv_4 0) \ \vee$$

$$(-2[2y-1] = [3-4y] \wedge [2y-1] < 2y-1 \wedge [3-4y] < 3-4y \ \wedge$$

$$[2y - 1] \equiv_2 0).$$

In order to simplify this formula we observe that for $y^* < \frac{1}{4}$, $[3 - 4y] = 2 - 4[y]$, for $\frac{1}{4} \leq y^* < \frac{1}{2}$, $[3 - 4y] = 1 - 4[y]$, for $\frac{1}{2} \leq y^* < \frac{3}{4}$, $[3 - 4y] = -4[y]$, and for $y^* \geq \frac{3}{4}$, $[3 - 4y] = -1 - 4[y]$. For $y^* < \frac{1}{2}$, $[2y - 1] = 2[y] - 1$, and for $y^* \geq \frac{1}{2}$, $[2y - 1] = 2[y]$. Using these facts, the formula $\varphi'(y)$ simplifies by case distinction to $\frac{1}{2} < y^* < \frac{3}{4}$. So the set of reals defined by $\varphi(y)$ is the periodically simple set $\mathbf{Z} + (\frac{1}{2}, \frac{3}{4})$.

We close this section by a hint at the enormous complexity of definable sets that can arise if we allow scalar multiplication by an irrational number.

Let α be an irrational number and let L'_α be the extension of L' by one scalar multiplier σ_α for multiplication by α.

Theorem 6.3 *Let $1 < \alpha$ be an irrational number, and let $\varphi_\alpha(y)$ be the following $L'_{\alpha^{-1}}$-formula:*

$$0 < y = [y] \ \wedge \ \exists x(0 < x = [x] \ \wedge$$

$$x \equiv_2 1 \ \wedge \ [\alpha^{-1}(x + 1)] = -[-\alpha^{-1}x] = y)$$

Then for all positive integers n, the formula $\varphi_\alpha(2^n)$ holds in the reals iff the n-th digit in the binary expansion of α^* equals 1.

Proof For positive integers x, y we have the following equivalences:

$$[\alpha^{-1}(x+1)] = y \iff 0 < \alpha^{-1}(x+1) - y < 1 \iff$$

$$\frac{1}{y} > \alpha - \frac{x}{y} > \frac{1-\alpha}{y}$$

$$[-\alpha^{-1}x] = -y \iff 0 < -\alpha^{-1}x + y < 1 \iff$$

$$0 < \alpha - \frac{x}{y} < \frac{\alpha}{y}$$

Hence $[\alpha^{-1}(x+1)] = -[-\alpha^{-1}x] = y$ implies

$$0 < \alpha - \frac{x}{y} < \frac{1}{y}.$$

Conversely,

$$0 < \alpha - \frac{x}{y} < \frac{1}{y}$$

implies

$$\frac{1}{y} > \alpha - \frac{x}{y} > \frac{1-\alpha}{y},$$

and so $[\alpha^{-1}(x+1)] = y$, and

$$0 < \alpha - \frac{x}{y} < \frac{\alpha}{y},$$

and so $-[-\alpha^{-1}x] = y$. Consequently $\varphi_\alpha(2^n)$ holds in the reals for a positive integer n iff there exists a positive, odd integer x such that

$$0 < \alpha - \frac{x}{2^n} < \frac{1}{2^n}.$$

This in turn is the case iff the n-th digit in the binary expansion of α^* equals 1.

Corollary 6.4 *Let $1 < \alpha$ be an irrational number with a non-recursive binary expansion. Then the set*

$$\{\ n \in \mathbf{N} \ \mid \ \varphi_\alpha(2^n) \textit{ holds in } \mathbf{R}\ \}$$

is not recursive. As a consequence, the theory of reals in the language $L'_{\alpha^{-1}}$ is undecidable.

7 More impossibility results

Consider the following extension L^* of the language L', obtained by allowing one scalar multiplier σ_α for multiplication by a real parameter α that ranges over arbitrary real values.

Then we have the following impossibility result:

Theorem 7.1 *Let $\varphi(\alpha)$ be the following L^*-formula*

$$\neg\exists x \exists y (x = [x] \ \wedge \ y = [y] \ \wedge \ y > 0 \ \wedge \ \alpha y = x).$$

Then there is **no** *quantifier-free L^*-formula $\varphi'(\alpha)$ equivalent to φ in the reals.*

Proof By definition, $\varphi(\alpha)$ holds for a given real value a of α iff a is irrational.

Assume now for a contradiction that such a variable-free equivalent $\varphi'(\alpha)$ for $\varphi(\alpha)$ exists and let M be the set of reals a such that $\varphi'(\alpha)$ holds in $\mathbf{R}$. Fix a transcendental real number b.

Claim. For any variable-free term $t(\alpha)$ in L^* there exists a neighborhood U of b such that $t(\alpha)$ describes a polynomial function of α with integer coefficients on U.

The claim is proved easily by induction on the length of t.

Based on this claim we see that there is some neighborhood U of b such that $M \cap U = S \cap U$ for some semialgebraic set S of reals. So for some neighborhood V of b contained in U, it follows that $M \cap U$ is an interval. This contradicts the fact that $M \cap U$ consists of all irrational numbers in V. □

Next we consider two other natural languages L_{div} and $L_{div'}$ for mixed real-integer linear problems: L_{div} is obtained from the language L by dropping the order relation and all congruences, and by adding a divisibility relation $s|t$. We interpret this relation in $\mathbf{R}$ as follows: $a|b \iff b$ is an integer multiple of a. Similarly, $L_{div'}$ is obtained from L by dropping the order relation and all congruences, and by adding the divisibility relation $s \parallel t$ defined by $a \parallel b \iff b$ is an integer multiple of a and a is an integer. Then we have the following negative result:

Theorem 7.2 *The elementary theory of* $\mathbf{R}$ *in L_{div} and in $L_{div'}$ is undecidable and* $\mathbf{R}$ *does not admit quantifier elimination in L_{div} or in $L_{div'}$.*

Proof As the relation $s \| t$ is definable in L_{div} by $(1|s \ \wedge\ s|t)$, it suffices to prove the result for $L_{div'}$. As remarked in [11], integer multiplication is definable in the $L_{div'}$-structure $\mathbf{Z}$. (By the first binomial formula it suffices to define squaring of positive integers; this can be done by the equivalence $y = x^2 \iff y + x = \mathrm{lcm}(x, x+1)$.) So, the elementary theory of the integers in $L_{div'}$ is undecidable. Since $\mathbf{Z}$ is definable in the $L_{div'}$-structure $\mathbf{R}$ by a quantifier-free formula, the same applies to $\mathbf{R}$. If $\mathbf{R}$ would admit quantifier elimination in $L_{div'}$ then by a similar argument as in the previous proof, the elementary theory of $\mathbf{R}$ as $L_{div'}$-structure would be decidable. As remarked in [11] the unsolvability of Hilbert's tenth problem even implies that prenex $L_{div'}$-formulas with on block of existential quantifiers followed by a single universal are undecidable in $\mathbf{Z}$ and hence in $\mathbf{R}$. □

By way of contrast we have the following positive result for the extension $L'_{div'}$ of $L_{div'}$ by the integer-part operation:

Theorem 7.3 *The positive existential theory of* $\mathbf{R}$ *in $L'_{div'}$ is decidable.*

Sketch of the proof. We have to decide a positive (i.e. negation-free) existential $L'_{div'}$-formula φ without free variables in $\mathbf{R}$. As in the proof of the main theorem, we may assume that the prefix of φ consists of a block of existential quantifiers ranging over the integers followed by a block of existential quantifiers ranging over the interval $[0, 1)$. We show that the latter quantifiers can be eliminated successively. For this purpose we can first replace any atomic formula $s \| t$ in φ equivalently by $[s] \parallel [t] \ \wedge\ s = [s] \ \wedge\ t = [t]$. Next a variable u ranging over $[0, 1)$ can be eliminated from the scope of the integer-part operation as in Lemma 3.3. Next a corresponding quantifier $\exists u$ can be eliminated as in the proof of the main theorem, case 2.

So we may assume from now on that the prefix of φ contains only existential quantifiers ranging over the integers. Moreover - by forming a disjunctive normal form and distributing the existential quantifiers over disjunctions - we may assume that the matrix of φ is a conjunction of equations and divisibility relations between linear polynomials in these variables with integer coefficients. Next we can perform integer linear transformations on the variables and the equations in order to put the system of equations into Hermite normal form. At this point the equations can be used to eliminate certain of the variables by introducing new divisibility relations between the remaining variables. So we end up with a conjunction of divisibility relations between linear polynomials in the remaining variables. By the main result of Lipshitz in [11], the solvability of such a system in the integers is decidable. □

Remark. We do not know whether a corresponding theorem holds in the analogous language L'_{div}.

8 Conclusions

We have shown that effective linear quantifier elimination is possible for the reals in a language including the constants $0, 1$, the operations $+, -, [\ ]$ and the relations $=, <, \equiv_n$. Moreover we have quantifier elimination with answers in this language and also in the extension language L'', where scalar multiplication with arbitrary rational numbers is allowed. As a consequence the elementary theory of reals in this language is decidable. Moreover we have closely matching upper and lower bounds for the complexity of the quantifier elimination and decision problem for this theory. These result strongly generalize known facts about the linear theory of the reals and about Presburger arithmetic. As an application we obtain a structural characterization of definable subsets of the real line in this theory. Other applications in engineering and optimization are indicated. The elimination and decision algorithms are partially implemented, namely for the purely real and the purely integer case, and have shown to be of high practical value. A complete implementation of mixed integer-real quantifier elimination in the language L'' is planned in the REDLOG-package of REDUCE.

By way of contrast, quantifier elimination is impossible in the reals if we drop the integer part function from L' or if we extend L'' by scalar multiplication with a real parameter α. The same applies to an extension of L' by an integer divisibility relation. Moreover the elementary theory of reals in this extended language is undecidable, whereas the positive existential theory of the reals in a similar language with integer divisibility but without order is decidable.

References

[1] Abdallah, C. T., Dorato, P., Yang, W., Liska, R., and Steinberg, S. Applications of quantifier elimination theory to control system design. In *Proceedings of the 4th IEEE Mediterranean Symposium on Control and Automation* (1996), IEEE, pp. 340–345.

[2] Dolzmann, A., and Sturm, T. *Redlog User Manual.* FMI, Universität Passau, D-94030 Passau, Germany, Oct. 1996. Edition 1.0 for Version 1.0.

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

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

[5] Dolzmann, A., Sturm, T., and Weispfenning, V. Real quantifier elimination in practice. In *Algorithmic Algebra and Number Theory*, B. H. Matzat, G.-M. Greuel, and G. Hiss, Eds. Springer, Berlin, 1998, pp. 221–247.

[6] Dorato, P., Yang, W., and Abdallah, C. Robust multi-objective feedback design by quantifier elimination. *Journal of Symbolic Computation 24*, 2 (Aug. 1997), 153–159. Special issue on applications of quantifier elimination.

[7] Dries, L. v. d. *Tame Topology and o-minimal structures.* Cambridge University Press, 1998.

[8] Jirstrand, M. Nonlinear control system design by quantifier elimination. *Journal of Symbolic Computation 24*, 2 (Aug. 1997), 137–152. Special issue on applications of quantifier elimination.

[9] Köppl, C. Eine REDUCE-Implementierung eines Quantoreneliminationsverfahrens für die Presburger Arithmetik. Master's thesis, Universität Passau, Universität Passau, FMI, 1991.

[10] Lafferriere, G., Pappas, G. J., and Yovine, S. Decidable hybrid systems. Tech. rep., VERIMAG, Univ. of Grenoble, 1998.

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

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

[13] Presburger, M. Über die Vollständigkeit eines gewissen Systems der Arithmetik. In *Comptes rendues du 1er Congres des Mathematique des Pays Slaves* (Warsaw, 1929), vol. 395, pp. 92–101.

[14] Sturm, T., and Weispfenning, V. Rounding and blending of solids by a real elimination method. In *Proceedings of the 15th IMACS World Congress on Scientific Computation, Modelling, and Applied Mathematics (IMACS 97)* (Berlin, Aug. 1997), A. Sydow, Ed., vol. 2, IMACS, Wissenschaft & Technik Verlag, pp. 727–732.

[15] Sturm, T., and Weispfenning, V. Computational geometry problems in Redlog. In *Automated Deduction in Geometry*, D. Wang, Ed., vol. 1360 of *Lecture Notes in Artificial Intelligence (Subseries of LNCS).* Springer-Verlag, Berlin Heidelberg, 1998, pp. 58–86.

[16] Tarski, A. A decision method for elementary algebra and geometry. Tech. rep., RAND, Santa Monica, CA, 1948.

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

[18] Weispfenning, V. The complexity of almost linear diophantine problems. *Journal of Symbolic Computation 10*, 5 (Nov. 1990), 395–403.

[19] Weispfenning, V. Complexity and uniformity of elimination in Presburger arithmetic. In *International Symposium on Symbolic and Algebraic Computation, Maui, Hawaii* (New York, July 1997), W. W. Küchlin, Ed., ACM Press, pp. 48–53.

[20] Weispfenning, V. Simulation and optimization by quantifier elimination. *Journal of Symbolic Computation 24*, 2 (Aug. 1997), 189–208. Special issue on applications of quantifier elimination.

[21] Weispfenning, V. A new approach to quantifier elimination for real algebra. In *Quantifier Elimination and Cylindrical Algebraic Decomposition*, B. Caviness and J. Johnson, Eds., Texts and Monographs in Symbolic Computation. Springer, Wien, New York, 1998, pp. 376–392.

[22] Weispfenning, V., and Xue, R. Parametric mixed integer programming by elimination. Technical Report MIP-9503, Universität Passau, 1995. Poster presentation at ISSAC'95, Montreal.