Effective Quantifier Elimination for Presburger Arithmetic with Infinity

Aless Lasaruk[1] and Thomas Sturm[2]

[1] FORWISS, Universität Passau, 94030 Passau, Germany
lasaruk@uni-passau.de
[2] Departamento de Matemáticas, Estadística y Computación, Facultad de Ciencias, Universidad de Cantabria, 39071 Santander, Spain
sturmt@unican.es

Abstract. We consider Presburger arithmetic extended by infinity. For this we give an effective quantifier elimination and decision procedure which implies also the completeness of our extension. The asymptotic worst-case complexity of our procedure is bounded by a function that is triply exponential in the input word length, which is known to be a tight bound for regular Presburger arithmetic. Possible application areas include quantifier elimination and decision procedures for Boolean algebras with cardinality constraints, which have recently moved into the focus of computer science research for software verification, and deductive database queries.

1 Introduction

The systematic investigation of the additive theory of integers with congruences started in 1929 with the pioneering work of Presburger [1]. The title of Presburger's original work is an understatement. It only mentions the completeness of Presburger arithmetic. For his proof Presburger gave a decision procedure proving every sentence equivalent to either "true" or "false." That is, the result is much more algorithmic than can be expected from complete theories in general. Even more important, from a modern point of view Presburger even gave a quantifier elimination procedure for a slightly extended language containing congruences. This on the one hand has considerable model theoretic consequences besides completeness, viz. substructure completeness, and on the other hand it considerably extends the power of a pure decision procedure with respect to possible practical applications.

For a long time already, Presburger arithmetic has been in the focus of mathematical as well as computer science research [2,3,4,5,6,7,8]. Quite recently the authors of the present note have extended quantifier elimination for Presburger arithmetic to parametric multiplicative constants [9] and furthermore to certain nonlinear input formulas [10].

Applications quite naturally arise in many areas of science and engineering. This might explain also the remarkable historical fact that already in 1954 Davis had implemented Presburger's original algorithm on a digital computer [11]. In

V.P. Gerdt, E.W. Mayr, and E.V. Vorozhtsov (Eds.): CASC 2009, LNCS 5743, pp. 195–212, 2009.

computer science many array subscript calculations fall within the region of problems decidable by Presburger arithmetic. This observation plays a prominent role in several proof of correctness systems for computer programs, beginning with the Stanford Pascal Verifier [12] and recently including Microsoft's Spec#. Further recent applications include elimination procedures for Boolean algebras with cardinality constraints in the context of deductive database queries [13].

Our present work extends classical Presburger arithmetic PA to PAI by adding a single infinite number with trivial arithmetic. This is inspired by the idea to include statements on the infinity of certain sets in deductive database queries [13]. Independently, Boolean algebras in combination with Presburger arithmetic have recently been considered for software verification. Within that framework there has even been considered our idea of including infinity. This was, however, realized in the Boolean algebra sort in contrast to the Presburger sort [14,15,16].

Some additional mathematical applications of our work might arise from the fact that in elimination procedures for valued fields, field quantifiers are often eliminated in favour of quantifiers over the value group [17]. Such procedures can possibly be simplified by not treating 0, which has value ∞, specially. Notice that the value group of the important class of p-adic valuations is in fact the ordered additive group of the integers such that the set of possible values ranges over $\mathbb{Z} \cup \{\infty\}$.

The outline of our paper is as follows: In Section 2 we make precise our extension of Presburger arithmetic by infinity and its relation to Presburger's original work. In Section 3 we introduce essential equivalence transformations on and normal forms of formulas in our extended framework, which are fundamental on the one hand for our elimination procedure and on the other hand for any serious attempt of an implementation. Section 4 states our main result, which is an effective quantifier elimination procedure for PAI and the model theoretic consequences of this. Section 5 gives asymptotic upper bounds on the worst-case complexity of our procedure. These bounds are known to be tight for PA. Section 6 give some examples for quantifier elimination in PAI in order to illustrate the procedure, to give an intuition of the semantics, and to point at possible applications. In Section 7 we finally summarize our results and indicate future research directions.

2 Presburger Arithmetic with Infinity

From a precise model-theoretic point of view, Presburger arithmetic is the model class of the axioms originally given by Presburger [1]. Presburger had considered congruences $a \equiv_\alpha b$ as abbreviations for first-order sentences $\exists x(\alpha \odot x + a = b)$, which he—besides atomic formulas—referred to as "ground formulas." This allowed him on the one hand to use the finite and apparently more natural language $(0, 1, +, \leq)$ of additive ordered groups and on the other hand not to emphasize too much the role of congruences in his procedures as they were considered only intermediate objects for his *decision procedure*. It is noteworthy that Presburger's presentation does not explicitly treat the ordering "$\leq$" at all.

There is only a remark in the appendix that the procedure can be generalized accordingly. This generalization has been made explicit e.g. in a textbook by Monk [18].

From a modern quantifier elimination point of view it is exactly the formal manifestation of congruences in an extended language

$$L = (0, 1, +, -, \leq, \equiv)$$

that straightforwardly exhibits that Presburger's decision procedure is actually even a quantifier elimination procedure over L. Notice that for convenience we have also added a function "$-$" for the additive inverse. We are now going to list Presburger's set of axioms with some slight modifications: We drop six axioms referring to the semantics of logical connectives and equality as their semantics is usually fixed on the meta-mathematical level in modern algebraic model theory. We use congruences in contrast to their existentially quantified equivalents described above. We add one axiom for our additional function symbol "$-$." Concerning notation, we use the symbol "$\odot$" to emphasize that any "multiplication" $\alpha \odot a$ occurring here is in fact an abbreviated notation for a corresponding addition $a + \cdots + a$ (α times). Furthermore, we use modern logical symbols and infix notation, and we save parentheses by following common conventions that the precedence of our logical operators decreases in the order "$\leq$," "$=$," "$\neg$," "$\wedge$," "$\vee$," "$\longrightarrow$," "$\longleftrightarrow$:"

(π_1) $a + c = b + c \longrightarrow a = b$
(π_2) $a + b = b + a$
(π_3) $a + (b + c) = (a + b) + c$
(π_4) $a + 0 = a$
(π_5) $\exists b(a + b = c)$
(π_6) $\alpha \odot a = \alpha \odot b \longrightarrow a = b$ for $\alpha = 2, 3, \ldots$
(π_7) $a \equiv_\alpha 0 \vee a \equiv_\alpha 1 \vee \cdots \vee a \equiv_\alpha (\alpha - 1) \odot 1$ for $\alpha = 2, 3, \ldots$
(π_8) $\neg\, \alpha \odot 1 = 0$ for $\alpha = 2, 3, \ldots$
(π_9) $a + (-a) = 0$.

Note that in (π_6)–(π_8) we have countably infinite subsets of axioms and, consequently, the entire set of axioms is countably infinite. For reasons discussed above this system does not include any axioms for the ordering. Since for our work here it is not necessary to refer to explicit axioms at all, we pragmatically switch to the countably infinite set $\Pi = \{\, \varphi \mid \varphi$ is L-formula and $\mathbb{Z} \models \varphi \,\}$, which obviously comprises $\pi_1, \ldots, \pi_9$. We define PA to denote the *model class* of Π:

$$\mathrm{PA} = \mathrm{Mod}(\Pi) = \{\, \mathbb{A} \mid \mathbb{A}\ L\text{-structure and } \mathbb{A} \models \Pi \,\}.$$

We obviously have $\mathbb{Z} \in \mathrm{PA}$, and thus Π is consistent. The main result stated by Presburger was the fact that Π is even *complete*. That is, every L-sentence is either valid or invalid in all L-structures in PA simultaneously. In the former case, one writes $\mathrm{PA} \models \varphi$ or—since PA is completely determined by Π—shortly $\Pi \models \varphi$. Since Π is first-order and recursively enumerable, it follows from this completeness that PA is *decidable*. That is, there is an algorithm with input a first-order L-formula φ and output either $\top$ or $\bot$, which always terminates and which returns $\top$ if and only if $\mathrm{PA} \models \varphi$.

We would like to remind the reader at this point that there is no simple correspondence between completeness and decidability in the sense defined above. For instance, the theory of algebraically closed fields is decidable but not complete while the theory axiomatized by all first-order $(0, s)$-sentences valid in $\mathbb{N}$ is complete but not decidable.

From a modern point of view, Presburger has even shown that PA is *substructure complete*. That is, for any two L-structures $\mathbb{A}$ and $\mathbb{B}$ in PA that have a common substructure one may add to L constants for all elements of this common substructure yielding L'. When then viewing $\mathbb{A}$ and $\mathbb{B}$ as L'-structures in a natural way even all L'-formulas will be either valid or invalid in both $\mathbb{A}$ and $\mathbb{B}$ simultaneously. Substructure completeness is equivalent to the existence of a quantifier elimination procedure, which Presburger has implicitly given for PA.

Since variable-free atomic formulas are decidable in PA, any quantifier elimination procedure yields a decision procedure via successive elimination of all variables. In fact, it does even more: Since every formula algorithmically turns out to be equivalent to either "true" or "false," a return value $\bot$ for input φ of such a decision procedure may be interpreted not only as the existence of $\mathbb{A}_0 \in \mathrm{PA}$ with $\mathbb{A}_0 \not\models \varphi$ but it even follows that *for all* $\mathbb{A} \in \mathrm{PA}$ we have $\mathbb{A} \not\models \varphi$. In other words, this exhibits also the completeness of PA.

To get a more precise picture of PA, recall the famous upward Löwenheim–Skolem Theorem [19,20,21]: From the existence of the infinite model $\mathbb{Z} \in \mathrm{PA}$, it follows that PA contains models of arbitrary infinite cardinality. In particular, PA is a proper class in contrast to a set.

We are now going to modify and extend Presburger's axioms Π to describe the integers with infinity in an extended language

$$L_\infty = (0, 1, \infty, +, -, \leq, \equiv).$$

We obtain (ι_1) by restricting the axioms in Π to finite numbers, and we add (ι_2)–(ι_8) to axiomatize ∞. Let $V(\pi)$ denote the finite set of variables occurring freely in an L-formula π:

(ι_1) $\bigwedge_{v \in V(\pi)} \neg\, v = \infty \longrightarrow \pi$ for $\pi \in \Pi$
(ι_2) $a + \infty = \infty$
(ι_3) $\infty + a = \infty$
(ι_4) $-\infty = \infty$
(ι_5) $a \leq \infty$
(ι_6) $\neg\, a = \infty \longrightarrow \neg\, \infty \leq a$
(ι_7) $a \equiv_\alpha \infty$ for $\alpha = 2, 3, \ldots$
(ι_8) $\infty \equiv_\alpha a$ for $\alpha = 2, 3, \ldots$

We refer to this new countably infinite set of axioms as I and to its model class as PAI.

It is not hard to see that $\mathbb{Z} \cup \{\infty\}$ with trivial arithmetic on infinity as defined in (ι_2)–(ι_4) and relations as defined in (ι_5)–(ι_8) is in PAI and thus I is consistent: Since (ι_1) collects assertions about $\mathbb{Z} \cup \{\infty\}$ explicitly excluding ∞ the validity of these assertions for $\mathbb{Z} \cup \{\infty\}$ follows from the validity of Π for $\mathbb{Z}$. Axioms (ι_2)–(ι_4) straightforwardly complement the definitions of binary "+" and unary "−" at points involving infinity. Axioms (ι_5) and (ι_6) define the binary relation "$\leq$" at points involving infinity. They cannot contradict each other since the former refers to infinite right hand sides while the latter excludes this. Axioms (ι_7) and (ι_8) straightforwardly give a trivial definition of the congruence relation at points involving infinity. Observe that there are no axioms combining "+," "−" involving infinity on the one hand with "$\leq$" or "$\equiv$" involving infinity on the other hand.

In analogy to PA our new model class PAI is a proper class containing models of arbitrarily large cardinality. In the next section we are going to devise a quantifier elimination procedure for PAI. This exhibits the substructure completeness of PAI. Since our axioms (ι_2)–(ι_8) obviously admit to decide variable-free atomic formulas involving infinity, it will follow that PAI is furthermore complete and decidable and our quantifier elimination procedure yields a corresponding decision procedure.

3 Normal Forms

As a preparation for our quantifier elimination procedure for PAI we are going to discuss in this section normal forms for L_∞-formulas, the contained atomic formulas, and the terms in these atomic formulas.

3.1 Formulas

Our first goal is to isolate all occurrences of the L_∞-constant ∞. We call an L_∞-formula in *normal form* if ∞ occurs there exclusively in equations $x = \infty$, where x is a variable. The following lemma guarantees that such normal forms generally exist:

Lemma 1 (Normalization of L_∞-formulas). *Let φ be an atomic L_∞-formula containing the L_∞-constant ∞. Then φ can be equivalently transformed into "true" or into an L-formula*

$$\bigvee_{x \in X} x = \infty,$$

where X is a subset of the variables occurring in φ.

Proof. To start with, observe that for L-terms u with variables $x_1, \dots, x_n$ we have

$$\mathrm{PAI} \models u = \infty \longleftrightarrow \bigvee_{i=1}^{n} x_i = \infty.$$

Our atomic L_∞-formula φ is of the form $s \varrho t$, where s, t are L_∞-terms and ϱ is one of $=$, $\leq$, $\equiv_\alpha$. From our observation above it follows that s or t can be equivalently replaced by ∞ when containing the L_∞-constant ∞. Next, congruences containing ∞, atomic formulas $s \leq \infty$, and equations $\infty = \infty$ can be equivalently replaced by "true." Atomic formulas $\infty \leq t$ can be equivalently replaced by $t = \infty$. So unless we have already evaluated to "true" we finally arrive at an equation of the form $u = \infty$ where u is an L-term, and we can once more apply our above observation. □

It is interesting to observe that the use of the L_∞-constant ∞ can in fact be avoided entirely: According to Lemma 1, we may assume w.l.o.g. that ∞ occurs exclusively in equations $x = \infty$, where x is a variable.

Lemma 2. *Let t be an L-term. Then* $\mathrm{PAI} \models t = \infty \longleftrightarrow \neg\, t - t = 0$. □

Furthermore, our language admits to bring quantifier-free L_∞ formulas into *positive normal form*, i.e., the only logical operators occurring are "$\wedge$" and "$\vee$." All Boolean connectives can be equivalently expressed by means of "$\wedge$," "$\vee$," and "$\neg$." Using de Morgan's laws and involution, all "$\neg$" can be moved inside until they cancel or directly precede some atomic formula. Then we have:

Lemma 3 (Positive normal form). *Let s, t be L_∞-terms. Then the following holds:*

(i) $\mathrm{PAI} \models \neg\, s \equiv_\alpha t \longleftrightarrow \bigvee_{\beta=1}^{\alpha-1} s \equiv_\alpha t + \beta \wedge s - s = 0 \wedge t - t = 0$
(ii) $\mathrm{PAI} \models \neg\, s \leq t \longleftrightarrow t + 1 \leq s \wedge t - t = 0$
(iii) $\mathrm{PAI} \models \neg\, s = t \longleftrightarrow (t + 1 \leq s \wedge t - t = 0) \vee (s + 1 \leq t \wedge s - s = 0)$. □

In particular from Lemma 2 and Lemma 3(iii) we obtain

$$t = \infty \longleftrightarrow \neg t - t = 0 \longleftrightarrow 1 \leq t - t.$$

Finally, notice that our Lemmas 1–3 are compatible in the following sense: for quantifier-free L_∞-formulas one can obtain positive normal forms not containing the L_∞-constant ∞.

3.2 Terms

Recall from Lemma 1 that we can bring all L_∞-formulas into a normal form where the L_∞-constant ∞ occurs exclusively in equations of the form $x = \infty$ where x is a variable, and all other atomic formulas are L-formulas. So for the discussion of normal forms of our terms it is sufficient to consider L-terms.

Notice that even for L-terms common transformations fail. At the first place, "$-$" does not generally yield an additive inverse in PAI since $\infty + (-\infty) = \infty + \infty = \infty$. Consequently, simplifications of terms like replacing $x + (-x)$ by 0 are not sound.

The following lemma lists some relevant axioms in Π which remain valid in PAI and mentions some further arithmetic rules valid for PAI, which we are going to use in the sequel. When referring to elements $\alpha \in \mathbb{Z}$ occurring in some term, we consider α an abbreviated notation for the corresponding term of the form $\pm(1 + \cdots + 1)$ or 0.

Lemma 4 (Arithmetic in PAI). *Presburger's axioms* (π_2)*–*(π_4)*,* (π_6)*–*(π_8) *remain valid in* PAI*. This includes the laws of commutativity and associativity and the neutrality of* 0 *for addition and the involutivity of "−." Furthermore the following arithmetic rules hold:*

(i) $\mathrm{PAI} \models \alpha \odot 0 = 0$ *for* $\alpha \in \mathbb{N}$
(ii) $\mathrm{PAI} \models -0 = 0$
(iii) $\mathrm{PAI} \models -(-a) = a$
(iv) $\mathrm{PAI} \models -\alpha \odot a = \alpha \odot (-a)$ *for* $\alpha \in \mathbb{N}$
(v) $\mathrm{PAI} \models \alpha \odot a + (-\beta \odot a) = (\alpha - \beta) \odot a$ *for* $\alpha, \beta \in \mathbb{N}, \alpha > \beta$
(vi) $\mathrm{PAI} \models \alpha \odot a + (-\alpha \odot a) = a - a$ *for* $\alpha \in \mathbb{N}$
(vii) $\mathrm{PAI} \models a + \alpha = b + \alpha \longrightarrow a = b$ *for* $\alpha \in \mathbb{Z}$
(viii) $\mathrm{PAI} \models \alpha \odot (a + b) = \alpha \odot a + \alpha \odot b$ *for* $\alpha \in \mathbb{Z}$*.* □

When using n-ary addition in the sequel, we tacitly assume that "+" is right-associative. Due to Lemma 4(π_2) this assumption is only of syntactic relevance. Furthermore, we are going to use $s - t$ as a short notation for terms $s + (-t)$.

Lemma 5 (Normal form of L-terms). *Let t be an L-term with variables x_1, …, x_n. Then there exist $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n \in \mathbb{N}$ and $\alpha \in \mathbb{Z}$ such that*

$$\mathrm{PAI} \models t = \alpha + \sum_{i=1}^{n} \alpha_i x_i - \sum_{i=1}^{n} \beta_i x_i.$$

Proof. Use Lemma 4(iv,viii) to move all occurrences of "−" inside until all such occurrences are nested occurrences in front of constants or variables. Use Lemma 4(iii) to reduce each such nested occurrence to at most one. Use Lemma 4(ii) and Lemma 4(π_4) to eliminate all occurrences of 0. Use Lemma 4(π_3) to obtain a right-associative n-ary sum of variables and the constant 1 possibly preceded by "−." Use Lemma 4(π_2, π_3) to reorder this n-ary sum as required by our normal form. Finally use (ι_9) and Lemma 4(π_2, π_3, iv) to rewrite the initial sequence $\pm 1 \pm \cdots \pm 1$ in this n-ary sum as $\pm(1 + \cdots + 1)$. □

Lemma 6 (Unique normal form of L-terms). *Consider an L-term t with variables $x_1, \ldots, x_n$, which we assume to be ordered $x_1 \prec x_2 \prec \cdots \prec x_n$. Then there is an enumeration $y_1, \ldots, y_k, \ldots, y_n$ of $\{x_1, \ldots, x_n\}$ with $y_1 \prec \cdots \prec y_k$ and $y_{k+1} \prec \cdots \prec y_n$, there is $\alpha \in \mathbb{Z}$, and there are $\alpha_1, \ldots, \alpha_k \in \mathbb{Z}$ such that*

$$\mathrm{PAI} \models t = \alpha + \sum_{i=1}^{k} \alpha_i y_i + \sum_{i=k+1}^{n} y_i - \sum_{i=k+1}^{n} y_i.$$

Furthermore, there is only one such choice $y_1, \ldots, y_k, \ldots, y_n, \alpha, \alpha_1, \ldots, \alpha_k$. □

Notice that the normal form in the previous lemma depends on the considered set $\{x_1, \ldots, x_n\}$ of variables. A *unique normal form* that does not depend on $x_1, \ldots, x_n$ is obtained by deleting summands $\alpha_i y_i$ where $\alpha_i = 0$. In addition, we agree to delete α if $\alpha = 0$.

3.3 Atomic Formulas

Notice that even for the atomic L-formulas in our normal form according to Lemma 1 and even when subtracting terms "carefully" in the sense of the previous section, some familiar equivalence transformations are not valid in PAI. For instance, $x = x+y$ is not equivalent to $y = 0$ as the interpretation $x = \infty$ admits arbitrary interpretations of y in the former equation. Normalization of right-hand sides to 0 in atomic L-formulas can, however, be achieved when making on the syntactic level case distinctions similar to those in the proof of Lemma 1.

Lemma 7 (Normal form of atomic L-formulas). *Let s, t be L-terms. Denote by $V(s)$ and $V(t)$ the finite sets of variables occurring in s and t, respectively. Then*

(i) $\mathrm{PAI} \models s \equiv_\alpha t \longleftrightarrow s - t \equiv_\alpha 0$
(ii) $\mathrm{PAI} \models s \leq t \longleftrightarrow s - t \leq 0 \vee \bigvee_{x \in V(t)} x = \infty$
(iii) $\mathrm{PAI} \models s = t \longleftrightarrow s - t = 0 \vee \Big(\bigvee_{x \in V(s)} x = \infty \wedge \bigvee_{x \in V(t)} x = \infty\Big)$.

Proof. Fix an interpretation of all variables so that s, $t \in \mathbb{Z} \cup \{\infty\}$. Recall from the proof of Lemma 1 that s, $t = \infty$ if and only if at least one variable in s, t, resp., is interpreted as infinity.

(i) If one of $s = \infty$ or $t = \infty$, then $s - t = \infty$ and both $s \equiv_\alpha t$ and $s - t \equiv_\alpha 0$ are true. Otherwise s, $t \in \mathbb{Z}$, where our transformation is known to be correct.
(ii) If $t = \infty$, then both sides of our equivalence are true. Assume now that $t \neq \infty$. If $s = \infty$ then both sides of our equivalence are false. Otherwise s, $t \in \mathbb{Z}$, where subtraction on both sides of the atomic formula is known to be correct, and our big disjunction is false.
(iii) If $s = t = \infty$, then both sides of our equivalence are true. If w.l.o.g. $s = \infty$ and $t \neq \infty$, then both sides of our equivalence are false. Otherwise s, $t \in \mathbb{Z}$, where subtraction on both sides of the equation is known to be correct, and our big disjunctions are both false. □

This normal form for atomic formulas is very convenient for practical purposes. Recall that the practical applicability of quantifier elimination by virtual substitution crucially depends on powerful methods for simplification of intermediate results, and these methods in turn are typically based on atomic formulas with right-hand sides normalized to 0 [22].

For Presburger quantifier elimination, one temporarily renormalizes to $sx = t$ where x is the variable currently considered for elimination. The following lemma describes a corresponding normal form for PAI:

Lemma 8 (Normal form of atomic L-formulas w.r.t. a variable). *Let $t\ \varrho\ 0$ be an atomic L-formula in normal form according to Lemma 7, let t be in unique normal form, and let x be a variable occurring in t. That is*

$$t = \alpha + \sum_{i=1}^{k} \alpha_i y_i + \sum_{i=k+1}^{n} y_i - \sum_{i=k+1}^{n} y_i,$$

and $y_j = x$ *for one and only one* $j \in \{1, \dots, n\}$*. Then*

$$\mathrm{PAI} \models t \varrho 0 \longleftrightarrow \eta,$$

where η *is a quantifier-free* L_∞*-formula, where* x *occurs in* η *exclusively in atomic* L*-formulas* $s \varrho u$ *with*

$$s = \begin{cases} \alpha_j x & \text{for } j \leq k \\ x - x & \text{for } j > k \end{cases} \quad \text{and} \quad u = -\alpha + \sum_{\substack{i=1 \\ i \neq j}}^{k} -\alpha_i y_i + \sum_{\substack{i=k+1 \\ i \neq j}}^{n} y_i - \sum_{\substack{i=k+1 \\ i \neq j}}^{n} y_i.$$

Proof. To start with, it is easy to see that $\mathrm{PAI} \models t \varrho 0 \longleftrightarrow s - u \varrho 0$. We are now going to distinguish cases on ϱ:

$$\begin{aligned}
&\mathrm{PAI} \models s - u \equiv_\alpha 0 \longleftrightarrow s \equiv_\alpha u \\
&\mathrm{PAI} \models s - u \leq 0 \longleftrightarrow s \leq u \land x - x = 0 \land u - u = 0 \\
&\mathrm{PAI} \models s - u = 0 \longleftrightarrow s = u \land (x - x = 0 \lor u - u = 0).
\end{aligned}$$

Recall that $\mathrm{PAI} \models r - r = 0 \longleftrightarrow \neg r = \infty$. □

3.4 Relevant Combinations of Normal Forms

Consider a quantifier-free L_∞-formula φ. To put φ into *general normal form*, we apply Lemma 1 to isolate all occurrences of the L_∞-constant ∞, then apply Lemma 7 to normalize all right hand sides of contained atomic L-formulas to 0, and finally bring the left hand side terms of the contained atomic L-formulas into unique normal form.

Recall from Section 3.1 that we can bring our φ into positive normal form. Since none of the transformations leading to the general normal form defined above introduces any Boolean connectives except "$\land$" and "$\lor$," we can obtain *positive general normal forms* by computing positive normal forms and subsequently computing general normal forms.

An *elimination normal form* with respect to some variable x is obtained from a general normal form of φ by applying Lemma 8 to equivalently replace all contained atomic L-formulas containing x. Notice that this preserves positivity as well. Hence we can obtain a *positive elimination normal form* with respect to x from a positive general normal form.

4 Quantifier Elimination

We are going to reuse here an essential part of our existing quantifier elimination procedure for regular Presburger arithmetic [9]. At least for complexity considerations it is going to be essential that this is a *virtual substitution* method [23,24,25,26,27,9,10]. Let us recall some basic facts on virtual substitution: The key idea for the elimination of a quantifier $\exists x$ from $\exists x \varphi$ is to compute a finite *elimination set* E such that

$$\exists x \varphi \longleftrightarrow \bigvee_{t \in E} \varphi[t/x],$$

i.e., there are finitely many terms substituted for x into φ, where E is constructed such that for any choice of parameters the following holds: If there exists some satisfying choice for x at all, then at least one $t \in E$ evaluates to a satisfying choice for x. The notion *virtual* refers to the following generalization:

1. The elimination set E need not exclusively contain regular terms but possibly also some *pseudo-terms*. A typical example are pseudo-terms containing division with real quantifier elimination [24]. Since elimination sets can comprise both regular terms and pseudo-terms, one often refers to their elements as test *points*.
2. Instead of regular substitution one uses a *modified substitution*, which does not map terms to terms but more generally atomic formulas to quantifier-free formulas. This happens in such a way that the substitution result, in contrast to the substituted test point t, generally does not contain any symbols not in the considered language.
3. The generalized test points are paired with *guards*, which ascertain their validity. For instance, for a test point containing division we would add the guard that the denominator is not zero. The guards are added conjunctively when substituting.

Altogether our substitution idea given above generalizes as follows:

$$\exists x \varphi \longleftrightarrow \bigvee_{(\gamma,t)\in E} \gamma \wedge \varphi[t /\!/ x].$$

Our elimination procedure is going to make use of our main technical Lemma for uniform Presburger arithmetic [9, Lemma 8]. This lemma uses a more general form of virtual substitution introducing bounded quantifiers. For the special case of classical Presburger arithmetic it can be adapted to the classical virtual substitution framework discussed above [9, Lemma 2(ii)]. We explicitly formulate this adapted result:

Lemma 9 (Regular Presburger elimination set). *Consider an L-formula $\exists x \varphi$ where φ is quantifier-free and in positive normal form. Let the set of all atomic formulas of φ that contain x be*

$$A = \{\, \alpha_i x \; \varrho_i \; r_i \mid i \in I_1 \mathbin{\dot{\cup}} I_2 \,\}.$$

We have $\alpha_i \in \mathbb{Z} \setminus \{0\}$, and the r_i do not contain the variable x. For $i \in I_1$, we have $\varrho_i \in \{=, \leq\}$. For $i \in I_2$, we have that ϱ_i is a congruence $\equiv_{m_i}$. Define $m = \operatorname{lcm}\{\, |m_i| \,:\, i \in I_2 \,\}$ where $\operatorname{lcm} \emptyset := 1$. Then

$$E = \bigcup_{i\in I_1} \bigcup_{-|\alpha_i|m \leq k \leq |\alpha_i|m} \{(\gamma_i, t_i)\} \cup \bigcup_{0\leq k<m} \{(\mathrm{true}, k)\},$$

where $\gamma_i = (r_i + k \equiv_{|\alpha_i|} 0)$ and $t_i = \dfrac{r_i + k}{\alpha_i}$, is an elimination set for $\exists x \varphi$. $\square$

For our purposes here it is important to know that the elimination set E is computed essentially from the set of atomic formulas contained in φ in such a way that the following holds:

Remark 10. Fix an interpretation v of all variables into $\mathbb{Z}$ for all variables, and consider the subset $A^+ = \{\, \psi \in A \mid (\mathrm{PA}, v) \models \psi \,\}$ of all atomic formulas that hold with respect to this interpretation. Then there is $(\gamma, t) \in E$ such that the following holds:

(i) $(\mathrm{PA}, v) \models \gamma$ and $(\mathrm{PA}, v) \models \psi[t /\!/ x]$ for all $\psi \in A^+$.
(ii) All variables in (γ, t) occur also in A^+. □

So with respect to any interpretation of variables where $x = z$, the relevant test term satisfies *at least* those atomic formulas that are satisfied by z—possibly more. This is the reason behind working with positive formulas when devising elimination sets.

Weispfenning originally had used *Skolem sets*, which exactly simulated the truth values of all atomic formulas [23]. He switched to positive formulas in the subsequent work on the reals [24]. In the context of valued fields, the second author introduced *CS-sets*, which further generalize the positive formula approach used here [26]. There has been also some research on taking into account the Boolean structure of φ for computing smaller elimination sets [24,28].

Remark 10(ii) is a quite natural property, which in fact holds for elimination sets for numerous theories. Nevertheless, it is not generally true but closely related to the question whether or not there are several atomic formulas combined to obtain some test point. This happened for example in the first elimination sets for the reals, where there were arithmetic means of interval boundaries computed in order to hit open intervals [23]. In elimination sets for discretely valued fields there are even up to three atomic formulas combined [26].

Lemma 11. *Consider an atomic L-formula $s \varrho t$ in normal form with respect to x:*

$$s \in \{\beta x, x - x\} \quad \textit{and} \quad t = \alpha + \sum_{i=1}^{k} \alpha_i y_i + \sum_{i=k+1}^{n} y_i - \sum_{i=k+1}^{n} y_i.$$

Fix an interpretation $v : \{y_1, \dots, y_n\} \to \mathbb{Z} \cup \{\infty\}$. If $\infty \in v[\{y_1, \dots, y_n\}]$, then one and only one of the following two assertions is true:

$$(\mathrm{PAI}, v \cup \{x = z\}) \models s \varrho t \quad \textit{iff} \quad z = \infty, \qquad (\mathrm{PAI}, v) \models s \varrho t.$$

That is, with respect to v either $x = \infty$ is the only satisfying choice for $s \varrho t$ or any choice from $\mathbb{Z} \cup \{\infty\}$ will do.

Proof. With respect to v we obtain $s = \infty$, $s \leq \infty$, or $s \equiv_\alpha \infty$ depending on ϱ. In the first case, $x = \infty$ is the only solution. In the other cases any choice for x is valid. □

Lemma 12 (Elimination of one existential quantifier). *Let φ be a quantifier-free L_∞-formula in positive elimination normal form with respect to x. Compute the set A of all those atomic L-formulas containing x, where the left hand side is not $x - x$. Compute an elimination set E for A according to Lemma 9. Then $E' := E \cup \{(\mathrm{true}, 0), (\mathrm{true}, \infty)\}$ is an elimination set for $\exists x \varphi$.*

Proof. Fix an interpretation into $\mathbb{Z} \cup \{\infty\}$ for all parameters, i.e. all variables except x. Assume that there is a satisfying interpretation $z \in \mathbb{Z} \cup \{\infty\}$ for x. Since φ is positive it suffices to substitute some test point for x such that at least those atomic formulas A^+ become true that contain x and hold for the choice $x = z$. Notice that in general A^+ is neither a subset nor a superset of A. If $z = \infty$, then $(\mathrm{true}, \infty) \in E'$ is a suitable choice.

Assume now that $z \neq \infty$ and note that then $x = \infty \notin A^+$. Let A' be the subset of all atomic formulas in A not containing any parameter that is interpreted as ∞. If $A' \cap A^+ \neq \emptyset$, then according to Remark 10(i) the regular Presburger elimination set E provides a test point t rendering true all atomic formulas in $A' \cap A^+$. Using Remark 10(ii) it follows that $t \in \mathbb{Z}$ with respect to our fixed interpretation. If, in contrast, $A' \cap A^+ = \emptyset$, then we may consider $t = 0$ as we have explicitly added $(\mathrm{true}, 0)$ to E'. In either case for all atomic L-formulas in $A^+ \setminus A$, i.e., where the left hand side is $x - x$, the satisfying value z is exactly simulated by t yielding 0 in both cases. By Lemma 11 all atomic formulas in $(A \setminus A') \cap A^+$ are satisfied by any choice for x since they are satisfied by $z \neq \infty$. $\square$

Theorem 13. PAI *admits effective quantifier elimination.*

Proof. Let $\hat{\varphi} = Q_1 x_1 \ldots Q_n x_n \varphi$ be an L_∞-formula, which is w.l.o.g. in prenex normal form, i.e., φ is quantifier-free. We proceed by induction on the number n of quantifiers in $\hat{\varphi}$. If $n = 0$, then $\hat{\varphi}$ is already quantifier-free. So there is nothing to do. Consider now the case $n > 0$. We then either have $Q_n x_n = \forall x_n$ or $Q_n x_n = \exists x_n$. The former case can be reduced to the latter one by means of the equivalence $\forall x_n \varphi \longleftrightarrow \neg \exists x_n \neg \varphi$. In the latter case we equivalently transform φ into elimination normal form $\bar{\varphi}$ with respect to x_n. By Lemma 12, there exists an elimination set E for $\exists x_n \bar{\varphi}$. That is

$$\mathrm{PAI} \models \exists x_n \varphi \longleftrightarrow \exists x_n \bar{\varphi} \longleftrightarrow \bigvee_{(\gamma,t) \in E} \gamma \wedge \bar{\varphi}[t /\!/ x_n] \longleftrightarrow \bigvee_{(\gamma,t) \in E} \gamma \wedge \varphi[t /\!/ x_n].$$

We obtain $\hat{\varphi}^*$ from $\hat{\varphi}$ by equivalently replacing $\exists x_n \varphi$ with the last disjunction above, and we can eliminate the remaining quantifiers from $\hat{\varphi}^*$ by our induction hypothesis. $\square$

Corollary 14. PAI *is substructure-complete, complete, and decidable.*

Proof. Admitting quantifier elimination is known to be equivalent to substructure completeness. For deciding an L_∞-sentence in PAI we eliminate all quantifiers according to Theorem 13, then decide all atomic formulas in $\mathbb{Z} \cup \{\infty\}$, and finally obtain an equivalent truth value via propositional calculus. This exhibits also the completeness. $\square$

5 Complexity

All complexity bounds discussed in the sequel are based on the assumption that the integers in the input formulas are binary coded. Notice that our formal language L_∞ would actually require to code them unary as sums of L_∞-constants 1 possibly preceded by the unary function symbol "$-$." Taking this into account, however, might improve the bounds by one exponential step but would not appropriately describe practical computations.

Notice that from a complexity point of view it is absolutely essential to have ternary predicates symbols for the congruences. When considering, in contrast, countably infinitely many binary ones—one for each modulus—our procedure is not elementary recursive as by increasing moduli the number of test points can by arbitrarily increased without increasing the input length. Again, our choice of ternary predicate symbols, where the (logarithm of the) size of the modulus contributes to the input length, establishes an appropriate model for practical computations.

Our write-up of our elimination procedure in the previous two sections is driven by the idea to use a small and natural language L_∞ and to separate mathematical foundations from implementation issues. Turning to complexity we have to discuss and revise one detail of this procedure: The application of Lemma 3(i) for making positive logically negated congruences introduces a number of atomic formulas, which is linear in the modulus. Since that modulus is represented in binary, this causes an exponential blow-up, which can however be easily avoided: one simply leaves negated congruences, which are directly preceded by logical negation, unchanged. One could call this a *weakly positive* formula. This is correct due to the following observation: The role of congruences in the elimination set computation in Lemma 9 is only that their modulus contributes to some least common multiple computation, and applying Lemma 3(i) would introduce several new congruences but no new moduli.

Since the size of our elimination set in Lemma 12 is essentially that of the part obtained via Lemma 9 for the regular Presburger case, we obtain the asymptotic upper bounds given by Weispfenning for a similar procedure [8]. That is, the procedure is triply exponential in the input word length. More precisely, it is triply exponential in the number of quantifiers. This bound is known to be tight for regular Presburger arithmetic [4].

Weispfenning observed, however, that this result still can be improved in several ways [23,8]. First, consider the elimination of several consecutive existential quantifiers in the proof of Theorem 13: When proceeding like

$$\exists x_{n-1}\exists x_n\varphi \longleftrightarrow \exists x_{n-1} \bigvee_{(\gamma,t)\in E} \gamma \wedge \varphi[t/\!/x_n] \longleftrightarrow \bigvee_{(\gamma,t)\in E} \exists x_{n-1}\big(\gamma \wedge \varphi[t/\!/x_n]\big)$$

and independently eliminating $\exists x_{n-1}$ from several smaller subproblems, one achieves that test points originating from a certain subproblem are not substituted within other subproblems. An analogue observation holds with consecutive universal quantifiers. This way, the quantifier elimination procedure is triply exponential in the number of quantifier alternations but only doubly exponential in the number of quantifiers for a bounded number of alternations.

Second, one can gain one exponential step by introducing big disjunction symbols "$\bigvee$" as an abbreviated notation for regular disjunctions following common mathematical practice. These big disjunctions can be used for substituting the big unions of elimination terms ranging over k in Lemma 9. The crucial observation is that this is compatible with the elimination procedure in the sense that these big disjunctions need not be expanded for the elimination of subsequent quantifiers. Our original main technical Lemma for *uniform* Presburger arithmetic [9, Lemma 8], is in fact a formalization of this approach, since for regular Presburger arithmetic the bounded quantifiers considered there represent such big disjunctions, and this approach is compatible with our extension considered here.

6 Elimination Examples

We start with two examples for quantifier elimination in PAI in order to illustrate the procedure and to give an intuition of the semantics. Then we turn to a more complex example pointing at one possible application of our work.

Example 15 (There is a maximum). Consider the sentence $\exists x \forall y (y \leq x)$, which in regular Presburger arithmetic is equivalent to "false." We start with the elimination of the inner quantifier $\forall y$ using the equivalence $\forall y(y \leq x) \longleftrightarrow \neg\exists y(\neg\, y \leq x)$. We bring $\neg\, y \leq x$ into positive elimination normal form with respect to y by applying Lemma 3(ii), Lemma 7(ii), and Lemma 8:

$$\begin{aligned}\neg\, y \leq x &\longleftrightarrow x + 1 \leq y \wedge x - x = 0\\ &\longleftrightarrow (x - y + 1 \leq 0 \vee y = \infty) \wedge x - x = 0\\ &\longleftrightarrow \big((-y \leq -x - 1 \wedge y - y = 0 \wedge x - x = 0) \vee y = \infty\big) \wedge x - x = 0.\end{aligned}$$

Applying Lemma 12 we compute $A = \{-y \leq -x - 1\}$ and obtain from Lemma 9 the following elimination set with respect to y:

$$E = \big\{(\mathrm{true}, x), (\mathrm{true}, x + 1), (\mathrm{true}, x + 2)\big\}.$$

To simplify our discussion here, we observe that all guarded points except for $(\mathrm{true}, x + 1)$ can be dropped from E without violating Remark 10. This yields

$$E' = \big\{(\mathrm{true}, x + 1), (\mathrm{true}, 0), (\mathrm{true}, \infty)\big\}.$$

The application of this E' yields

$$\begin{aligned}\forall y(y \leq x) &\longleftrightarrow \neg\exists y(\neg\, y \leq x)\\ &\longleftrightarrow \neg \bigvee_{(\gamma,t)\in E'} \gamma \wedge \big((x - y + 1 \leq 0 \vee y = \infty) \wedge x - x = 0\big)[t /\!/ y]\\ &\longleftrightarrow \neg(x - x = 0 \vee x + 1 \leq 0 \vee x - x = 0)\\ &\longleftrightarrow \neg\, x - x = 0.\end{aligned}$$

Now $\neg\, x - x = 0$ is equivalent to $x = \infty$ so that for the elimination of the outer quantifier $\exists x$ we obtain "true" via (true, ∞), which is generally contained in our elimination sets. $\square$

Example 16 (There is a minimum). Consider the sentence $\exists x \forall y (x \leq y)$, which is dual to our previous example. Again we construct a positive elimination normal form with respect to y of $\neg\, x \leq y$ to eliminate the inner quantifier:

$$\neg\, x \leq y \longleftrightarrow y \leq x - 1 \wedge y - y = 0.$$

For $A = \{y \leq x - 1\}$ Lemma 9 essentially yields $\{(\text{true}, x - 1)\}$, and according to Lemma 12 we obtain the elimination set

$$E' = \{(\text{true}, x - 1), (\text{true}, 0), (\text{true}, \infty)\}.$$

The application of E' yields

$$\forall y (y \leq x) \longleftrightarrow \neg(x - x = 0 \vee 0 \leq x - 1 \vee \text{false}) \longleftrightarrow \text{false},$$

and it follows that $\exists x \forall y (y \leq x) \longleftrightarrow \text{false}$. $\square$

Recently, computer science research has focussed on decidable fragments of Boolean algebras of power sets with cardinality constaints where the interpretation of the 1 is a finite or countably infinite set [14,15]. This resulted in a theory called BAPA combining Boolean algebra and Presburger arithmetic in a two-sorted approach. The decision procedure for BAPA is based on quantifier elimination. It reduces an input BAPA formula to an L-formula in our sense. This method still yields a decision procedure when combined with any decidable extension of Presburger arithmetic. In particular the results in [14,15] are compatible with our extension PAI. We are now going to demonstrate by means of an example how PAI can be combined with Boolean algebras.

Example 17 (Boolean algebra with cardinality). Consider the following problem: We are looking for a non-empty set which is a subset of every infinite element of the powerset of some countable ground set. In the language of Boolean algebras with cardinality constraints a first-order formulation is given by

$$|A| > 0 \wedge \forall X (|X| = \infty \longrightarrow A \cap X = A).$$

Notice that we have $|X| = \infty$ as a constraint, which in BAPA is only first-order definable, e.g. $\exists k (|\overline{A}| = k)$. Notice furthermore that we do not have a decision problem but a quantifier elimination problem here.

We are going to transform the quantified part of the given formula into an L_∞-formula. To start with,

$$\forall X (|X| = \infty \longrightarrow A \cap X = A) \longleftrightarrow \neg \exists X (|X| = \infty \wedge \overline{A} \cup X \neq 1).$$

We can equivalently repace $\overline{A} \cup X \neq 1$ by $A \cap \overline{X} \neq \emptyset$. The latter can be transformed into a cardinality constraint $|A \cap \overline{X}| > 0$. Analogously $|X| = \infty$ can be expressed by $|X \cap A| + |X \cap \overline{A}| = \infty$. We additionally introduce two tautological constraints

$$|A| - |X \cap A| - |\overline{X} \cap A| = 0 \quad \text{and} \quad |A| - |X \cap \overline{A}| - |\overline{X} \cap \overline{A}| = 0.$$

We replace each cardinality by a variable ranging over $\mathbb{Z} \cup \{\infty\}$ as follows:

$$|A| = x, \quad |X \cap A| = a, \quad |\overline{X} \cap A| = b, \quad |X \cap \overline{A}| = c, \quad |\overline{X} \cap \overline{A}| = d.$$

This finally yields

$$\neg\exists a \exists b \exists c \exists d (x \geq 0 \land a \geq 0 \land b \geq 0 \land c \geq 0 \land d \geq 0 \land \\ x - a - b = 0 \land x - c - d = 0 \land a + c = \infty \land c > 0).$$

Eliminating the quantified variables a, b, c, d we would obtain the formula $x = 0$. The solution set with respect to x describes the cardinality of all sets A which satisfy our condition. In our case the result $x = 0$ contradicts the condition $|A| > 0$ outside the scope of the quantifier in the original problem. Consequently there is no such set A. $\square$

7 Conclusions and Further Work

We have given a quantifier elimination procedure and a corresponding decision procedure for Presburger arithmetic with infinity. The asymptotic worst-case complexity is not worse than that of corresponding procedures for regular Presburger arithmetic, which are widely accepted as an important and useful tool. The next reasonable step is to implement our procedure in the computer logic system REDLOG [29], which already features an implementation of quantifier elimination for regular Presburger Arithmetic [9,10], the essential part of which can be reused as a subroutine. One can then address quantifier elimination for Boolean algebras with cardinality constraints and examine the practical applicability of our approach to problems from deductive databases or software verification [13,14,15]. For Boolean algebras with cardinality constraints it is a promising idea to adopt for PAI the concept of *positive quantifier elimination* restricting to variables that describe positive or non-negative numbers including infinity. For applications of real quantifier elimination to problems in algebraic biology this brought a considerable progress [30]. Finally note that our approach can be expected to admit also *extended quantifier elimination*, where one obtains satisfying sample values for existentially quantified variables if such values exist [31].

Acknowledgment

We thank Peter Revesz, who pointed us at his work on deductive databases and quantifier elimination for certain Boolean algebras via reduction to Presburger formulas. Peter also pointed us at the option to extend this to considering infinite sets on the basis of a potential Presburger implementation with infinity.

References

1. Presburger, M.: Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt. In: Comptes Rendus du premier congrès de Mathématiciens des Pays Slaves, Warsaw, Poland, pp. 92–101 (1929)
2. Cooper, D.C.: Theorem proving in arithmetic without multiplication. Machine Intelligence 7, 91–99 (1972)
3. Ferrante, J., Rackoff, C.W.: The Computational Complexity of Logical Theories. Lecture Notes in Mathematics, vol. 718. Springer, Berlin (1979)
4. Fischer, M.J., Rabin, M.: Super-exponential complexity of Presburger arithmetic. SIAM-AMS Proceedings 7, 27–41 (1974)
5. Reddy, C.R., Loveland, D.W.: Presburger arithmetic with bounded quantifier alternation. In: STOC 1978: Proceedings of the Tenth Annual ACM Symposium on Theory of Computing, pp. 320–325. ACM, New York (1978)
6. Pugh, W.: The omega test: a fast and practical integer programming algorithm for dependence analysis. In: Supercomputing 1991: Proceedings of the 1991 ACM/IEEE Conference on Supercomputing, pp. 4–13. ACM, New York (1991)
7. Oppen, D.C.: A $2^{2^{2^{pn}}}$ upper bound on the complexity of Presburger arithmetic. J. Comput. Syst. Sci. 16(3), 323–332 (1978)
8. Weispfenning, V.: The complexity of almost linear Diophantine problems. Journal of Symbolic Computation 10(5), 395–403 (1990)
9. Lasaruk, A., Sturm, T.: Weak quantifier elimination for the full linear theory of the integers. A uniform generalization of Presburger arithmetic. Applicable Algebra in Engineering, Communication and Computing 18(6), 545–574 (2007)
10. Lasaruk, A., Sturm, T.F.: Weak integer quantifier elimination beyond the linear case. In: Ganzha, V.G., Mayr, E.W., Vorozhtsov, E.V. (eds.) CASC 2007. LNCS, vol. 4770, pp. 275–294. Springer, Heidelberg (2007)
11. Davis, M.: Final report on mathematical procedures for decision problems. Technical report, Institute for Advanced Study, Princeton, NJ (October 1954), Under Technical Supervision of Commanding General, Aberdeen Proving Ground. Work Performed During Period 1, to 31, Under Contract No. DA-36-034-ORD-1645. Department of Army Project No. 599-01-004 (1954)
12. Luckham, D.C., German, S.M., von Henke, F.W., Karp, R.A., Milne, P.W., Oppen, D.C., Polak, W., Scherlis, W.L.: Stanford Pascal verifier user manual. Technical report, Stanford University, Stanford, CA, USA (1979)
13. Revesz, P.Z.: Quantifier-elimination for the first-order theory of boolean algebras with linear cardinality constraints. In: Benczúr, A.A., Demetrovics, J., Gottlob, G. (eds.) ADBIS 2004. LNCS, vol. 3255, pp. 1–21. Springer, Heidelberg (2004)
14. Kuncak, V., Nguyen, H.H., Rinard, M.: An algorithm for deciding BAPA: Boolean algebra with presburger arithmetic. In: Nieuwenhuis, R. (ed.) CADE 2005. LNCS (LNAI), vol. 3632, pp. 260–277. Springer, Heidelberg (2005)
15. Kuncak, V., Nguyen, H.H., Rinard, M.: Deciding Boolean algebra with Presburger arithmetic. Journal of Automated Reasoning 36(3), 213–239 (2006)
16. Kuncak, V.: Quantifier-free Boolean algebra with Presburger arithmetic is NP-complete. Technical Report TR-2007-001, MIT Computer Science and AI Lab, Cambridge, MA (January 2007)
17. Weispfenning, V.: Quantifier elimination and decision procedures for valued fields. In: Mueller, G.H., Richter, M.M. (eds.) Models and Sets. Proceedings of the Logic Colloquium held in Aachen, July 18–23, 1983 Part I. Lecture Notes in Mathematics (LNM), vol. 1103, pp. 419–472. Springer, Heidelberg (1984)

18. Monk, J.D.: Mathematical Logic. Graduate Texts in Mathematics, vol. 37. Springer, Heidelberg (1976)
19. Löwenheim, L.: Über Möglichkeiten im Relativkalkül. Mathematische Annalen 76(4), 447–470 (1915)
20. Skolem, T.: Logisch-kombinatorische Untersuchungen über die Erfüllbarkeit oder Beweisbarkeit mathematischer Sätze nebst einem Theoreme über dichte Mengen. Videnskapsselskapet Skrifter, I. Matematisk-naturvidenskabelig Klasse 6, 1–36 (1920)
21. Malcev, A.: Untersuchungen aus dem Gebiete der mathematischen Logik. Rec. Math. [Mat. Sbornik] N.S. 1(43)(3), 323–336 (1936)
22. Dolzmann, A., Sturm, T.: Simplification of quantifier-free formulae over ordered fields. Journal of Symbolic Computation 24(2), 209–231 (1997)
23. Weispfenning, V.: The complexity of linear problems in fields. Journal of Symbolic Computation 5(1&2), 3–27 (1988)
24. Loos, R., Weispfenning, V.: Applying linear quantifier elimination. The Computer Journal 36(5), 450–462 (1993); Special issue on computational quantifier elimination
25. Weispfenning, V.: Quantifier elimination for real algebra—the quadratic case and beyond. Applicable Algebra in Engineering Communication and Computing 8(2), 85–101 (1997)
26. Sturm, T.: Linear problems in valued fields. Journal of Symbolic Computation 30(2), 207–219 (2000)
27. Sturm, T., Weispfenning, V.: Quantifier elimination in term algebras. The case of finite languages. In: Ganzha, V.G., Mayr, E.W., Vorozhtsov, E.V. (eds.) Computer Algebra in Scientific Computing. Proceedings of the CASC 2002, Institut für Informatik, Technische Universität München, Garching, Germany, pp. 285–300 (2002)
28. Dolzmann, A.: Algorithmic Strategies for Applicable Real Quantifier Elimination. Doctoral dissertation, Universität Passau, 94030 Passau, Germany (July 2000)
29. Dolzmann, A., Sturm, T.: Redlog: Computer algebra meets computer logic. ACM SIGSAM Bulletin 31(2), 2–9 (1997)
30. Sturm, T., Weber, A., Abdel-Rahman, E.O., El Kahoui, M.: Investigating algebraic and logical algorithms to solve Hopf bifurcation problems in algebraic biology. Mathematics in Computer Science 2(3), 493–515 (2009)
31. Weispfenning, V.: Simulation and optimization by quantifier elimination. Journal of Symbolic Computation 24(2), 189–208 (1997)