A Survival Guide to Presburger Arithmetic

Christoph Haase, University of Oxford, UK

The first-order theory of the integers with addition and order, commonly known as Presburger arithmetic, has been a central topic in mathematical logic and computer science for almost 90 years. Presburger arithmetic has been the starting point for numerous lines of research in automata theory, model theory and discrete geometry. In formal verification, Presburger arithmetic is the first-choice logic to represent and reason about systems with infinitely many states. This article provides a broad yet concise overview over the history, decision procedures, extensions and geometric properties of Presburger arithmetic.

1. A VERY SHORT HISTORY OF PRESBURGER ARITHMETIC

Around the 1920s of the last millennium, David Hilbert together with his doctoral student Wilhelm Ackermann began to pursue what is nowadays known as *Hilbert's program*. The goal of this program was to create a formal system that would allow for providing solid foundations for all of mathematics. The means to achieve this goal was to use mathematical logic as an unambiguous language in which all mathematical statements could be formalised and manipulated according to a well-defined axiomatic system. In addition to asking for consistency and completeness, Hilbert also required that it should be possible to verify or falsify the truth of any given mathematical statement in a finite number of steps within this formal system. This requirement gave rise to the *Entscheidungsproblem (decision problem)* that was introduced by Hilbert and Ackermann in their book *Grundzüge der Theoretischen Logik (Principles of Mathematical Logic)* published in 1928, see [Hilbert and Ackermann 1950] for an English translation. The Entscheidungsproblem demands an algorithm that given a sentence in first-order logic together with a finite number of axioms allows for deciding whether that sentence is valid, i.e., holds in any structure satisfying the given axioms.

After studying the *Principles of Mathematical Logic* and related work, Alfred Tarski approached his student Mojżesz Presburger and asked him to investigate the completeness of a particular theory capturing a limited fragment of number theory. A couple of months later, Presburger showed in his Master's thesis the completeness

Fig. 1. Presburger's student card from the University of Warsaw, Poland.

of $\mathrm{Th}(\mathbb{Z}, +, 0, 1)$, the first-order theory of the integers with addition, equality and the standard axioms of arithmetic. He achieved this result by developing a quantifier-elimination procedure, an approach that Tarski had suggested to him. To this end, he extended $\mathrm{Th}(\mathbb{Z}, +, 0, 1)$ by infinitely many divisibility predicates $c|\cdot$, $c > 0$, since $\mathrm{Th}(\mathbb{Z}, +, 0, 1)$ by itself does not admit quantifier elimination. Presburger presented and published his results in the proceedings of the First Congress of Mathematicians in the Slavic Countries [Presburger 1929]. In his article, he remarked that his quantifier-elimination method can be adapted to work for the extended theory $\mathrm{Th}(\mathbb{Z}, 0, 1, +, <)$, which is nowadays commonly known as *Presburger arithmetic*. Legend has it that Presburger was awarded a Master's instead of Ph.D. degree for his work, since Tarski considered his results to be too simple for constituting a Ph.D. thesis. As of now, there is, however, not sufficient evidence supporting this legend [Zygmunt 1991].

Presburger's results imply that $\mathrm{Th}(\mathbb{Z}, 0, 1, +, <)$ possesses all the requirements laid down by Hilbert, except that the theory is not expressive enough to reason about all of number theory. Nevertheless, some basic statements can be expressed in it. [Smoryński 1991, Chap. 3] gives as an example the well-known *Frobenius problem*: Given positive integers $m_1, \ldots, m_n$, what is the largest number that cannot be obtained as a non-negative linear combination of those numbers? The Frobenius number, if it exists, is the smallest element of all satisfying assignments of the following formula:

$$\Phi(x) \equiv \forall y.\, x < y \rightarrow (\exists z_1 \cdots \exists z_n.\, y = z_1 m_1 + \cdots + z_n m_n \wedge z_1 \geq 0 \wedge \cdots \wedge z_n \geq 0)$$

Hilbert became aware of Presburger's work and viewed it as a first step towards the successful completion of his program. Shortly after, Kurt Gödel, Alan Turing and Alonzo Church shattered all of Hilbert's hopes. A simplified version of Presburger's quantifier elimination procedure made its way into Hilbert's and Bernay's *Grundlagen der Mathematik (Foundations of Mathematics)*, and Presburger arithmetic is nowadays a topic found in many introductory courses on mathematical and computational logic.

With the advent of automata theory in the 1950s, several authors began to relate Presburger arithmetic to formal language theory. In 1960, J. Richard Büchi developed an automata-based decision procedure for Presburger arithmetic [Büchi 1960]. Given a relation $R \subseteq \mathbb{N}^m$ defined by a formula in Presburger arithmetic, Büchi showed how to construct a finite-state automaton whose language encodes R. The idea of generating the solutions of a formula of a logical theory by a finite-state automaton later gave rise to the more general concept of *automatic structures* [Hodgson 1982; Khoussainov and Nerode 1994; Blumensath and Grädel 2000]. In the mid 1960s, Seymor Ginsburg and Edwin H. Spanier investigated the geometry of the sets of integers definable in Presburger arithmetic. They showed that Presburger-definable sets coincide with *semi-linear sets* that had been discovered by Rohit Parikh in the early 1960s [Ginsburg and Spanier 1964; Parikh 1966]. Semi-linear sets are generalisations of ultimately periodic sets to higher dimensions, and Parikh had introduced them when studying context-free grammars. He showed that the commutative closure of a context-free language is a semi-linear set. From the mid 1990s on-wards, Büchi's automata-based decision procedure received renewed interest. [Wolper and Boigelot 1995] and [Boudet and Comon 1996] investigated how to efficiently construct the finite automaton for a given Presburger formula. Later, [Klaedtke 2008] established precise upper bounds on the size of the minimal deterministic finite state automaton for a given formula. [Durand-Gasselin and Habermehl 2010] went on to continue Klaedtke's work and showed that Büchi's automata constructions runs in triply-exponential time.

The 1970s and 1980s then saw a focus on the algorithmic and computational complexity aspects of Presburger arithmetic. [Cooper 1972] investigated practical aspects

of Presburger's quantifier elimination procedure and developed several improvements that allowed for applying it to non-trivial examples for the first time. Specifically, he showed how to avoid the translation into disjunctive normal form that Presburger required. [Oppen 1978] later showed that Cooper's algorithm runs in deterministic triply exponential time. Coopers quantifier-elimination procedure nowadays provides the basis for most introductory texts on quantifier elimination for Presburger arithmetic. In 1974, [Fischer and Rabin 1998] gave the first hardness result for Presburger arithmetic and showed a non-deterministic doubly-exponential time lower bound for full Presburger arithmetic, see also [Kozen 2006, Lect. 21ff] for a comprehensive summary of their approach. [Berman 1980] observed that the complexity-theoretic framework at the time was insufficient to accurately capture the complexity of Presburger arithmetic. To overcome this problem, he introduced a combined space-time-alternation (STA) complexity measure. A problem is decidable in STA($s(n)$, $t(n)$, $a(n)$) if it can be solved by an alternating Turing machine that uses on every computation branch at most space $s(n)$, time $t(n)$ and makes at most $a(n)$ alternations. For the complexity of Presburger arithmetic, allowing for a finer control on the number of alternations is essential. Building upon the work of [Fischer and Rabin 1998] and [Ferrante and Rackoff 1975], Berman showed that Presburger arithmetic is complete for STA($*$, $2^{2^{p(n)}}$, $O(n)$), where p is some fixed polynomial and "$*$" indicates an unbounded availability of a resource (which may of course be implicitly bounded). Since $\mathrm{A2EXPTIME} \subseteq \mathrm{2EXPSPACE}$ [Chandra et al. 1981], Berman's result consequently yields a doubly-exponential space upper bound for Presburger arithmetic. One should bear in mind that the high lower bounds of Presburger arithmetic require formulas with an unbounded number of alternations. For many purposes, this is rarely the case, and often existential or fragments with few quantifier alternations and much lower complexity suffice.

2. ABOUT THIS ARTICLE

The purpose of this article is to give an introductory overview over Presburger arithmetic, and to exhibit in some more detail some technical aspects of the concepts introduced and discussed in the previous section. Section 3 provides the main ideas underlying decision procedures for Presburger, Section 4 then exhibits the connection between Presburger arithmetic and semi-linear sets. A detailed account on the computation complexity of Presburger arithmetic and decision problems for semi-linear sets is given in Section 5. Finally, decidable extensions of Presburger arithmetic are discussed in Section 6. Throughout this article, many references to the literature are provided, a reader not familiar with Presburger arithmetic or aspects of it may use this article as a starting point.

For presentational convenience, except for Section 3.1 which presents Cooper's quantifier elimination procedure, we work in the theory $\mathrm{Th}(\mathbb{N}, 0, 1, +)$, i.e., first-order variables quantify over the natural numbers and no explicit order relation is present. Note that the order relation can be expressed without any problems, since $x < y$ if and only if $\exists z\, x + z = y - 1$. Moreover, by representing integers as differences of natural numbers, it is easily seen that a decision procedure for this theory allows for deciding $\mathrm{Th}(\mathbb{Z}, 0, 1, +, <)$.

3. DECISION PROCEDURES

We present two approaches to deciding full Presburger-arithmetic: first a quantifier-elimination approach, and second an automata-based approach. We will not discuss SMT-based approaches that are typically used for deciding the existential fragment. The interested reader is referred to an introduction by [de Moura and Bjørner 2011].

3.1. Quantifier Elimination

The basis of the quantifier-elimination procedure presented in this section is the algorithm of [Cooper 1972], which itself is a variant of Presburger's seminal quantifier-elimination procedure. One can even further trace back the core of Presburger's quantifier-elimination approach to the work of [Fourier 1826], who gave a quantifier-elimination procedure for systems of linear inequalities over the reals. His approach was rediscovered multiple times, most famously but not only by Theodore Motzkin, see [Williams 1986].

Recall that we are working in the structure $\mathrm{Th}(\mathbb{Z}, 0, 1, +, <)$. It is well-known that in order to show that a logical theory admits quantifier elimination it is sufficient to show how to eliminate a single existentially quantified variable from a conjunction of atomic formulas, see e.g. [Enderton 1972, Chap. 3]. In order to gently approach Cooper's quantifier-elimination procedure, let us consider the following simple example in which we aim for eliminating the variable z ranging over the reals:

$$2x + 4y - 3z < 7 \ \wedge \ 3x - y + 2z < -4 \tag{1}$$

Both inequalities yield lower and upper bounds on a satisfying z, which can be seen by re-arranging the inequalities to:

$$2x + 4y - 7 < 3z \ \wedge \ 2z < -3x + y - 4$$

For a solution for z to exist, we have to ensure that the interval between the greater-than and less-than constraints is non-empty. To this end, we scale all inequalities such that z has the same coefficient everywhere:

$$4x + 8y - 14 < 6z \ \wedge \ 6z < -9x + 3y - 12 \tag{2}$$

It is now obvious that (1), over the reals, is logically equivalent to the single constraint $4x + 8y - 14 < -9x + 3y - 12$, which is equivalent to

$$13x + 5y - 2 < 0.$$

If we can find a solution for x and y such that this inequality holds, we are guaranteed to find a satisfying z over the reals. However, there is no guarantee that an *integral* satisfying z will exist. What we have to ensure is that there is some integer divisible by 6 in the interval defined by (2). In fact, if an integral z exists we will find it in the intervals $(4x + 8y - 14, 4x + 8y - 8]$ and $[-9x + 3y - 18, -9x + 3y - 12)$. Therefore, over the integers we find that (1) is equivalent to the constraint $13x - 5y - 2 < 0$ together with one of

$$\bigvee_{1 \le m \le 6} 6 \mid 4x + 8y - 14 + m \ \text{ or } \ \wedge \bigvee_{1 \le m \le 6} 6 \mid -9x + 3y - 12 - m.$$

This simple example illustrates all the ingredients we need in order to eliminate a variable in a conjunction of linear inequalities over the integers: isolate the variable to be eliminated, scale all obtained inequalities, add additional divisibility constraints and discard the variable to be eliminated. It also demonstrates why Presburger introduced the additional divisibility predicates. Without them, we could, for instance, not eliminate x from the formula $\Phi(y) \equiv \exists x\, y = 2x$, since the property of a number being even cannot be expressed in terms of linear inequalities only.

Let us now generalise the previous example in order to obtain Cooper's quantifier elimination procedure. Given a conjunction of linear inequalities and divisibility constraints $\Phi(\boldsymbol{y}) = \exists x\, \varphi(x, \boldsymbol{y})$ from which we wish to eliminate the existentially quantified x, rewrite Φ as

$$\Phi \equiv \exists x \bigwedge_{i \in G} q_i(\boldsymbol{y}) < a_i \cdot x \wedge \bigwedge_{j \in L} a_j \cdot x < p_j(\boldsymbol{y}) \wedge \bigwedge_{k \in D} c_k \mid a_k \cdot x + r_k(\boldsymbol{y}) \wedge \theta, \tag{3}$$

where L, G, D are finite sets of disjoint indices, and q_i, p_j, r_k are linear polynomials in $\boldsymbol{y}$, and x does not occur in θ. For readability, in the following we will assume that θ is equivalent to *true*, i.e., that x occurs in all conjuncts of Φ. Note that, as above, x occurs isolated in (3), but with different coefficients. Now set

$$b := \mathrm{lcm}\{a_i \mid i \in G \cup L \cup D\}.$$

We have that Φ in (3) is equivalent to

$$\Psi \equiv \exists x \bigwedge_{i \in G} \frac{b}{a_i} \cdot q_i(\boldsymbol{y}) < x \wedge \bigwedge_{j \in L} x < \frac{b}{a_j} \cdot p_j(\boldsymbol{y}) \wedge \bigwedge_{k \in D} \frac{b}{a_k} \cdot c_k \mid x + \frac{b}{a_k} \cdot r_k(\boldsymbol{y}) \wedge b \mid x. \quad (4)$$

To see this, suppose $x \in \mathbb{Z}$ is such that it satisfies (3). We claim that $b \cdot x$ satisfies (4). This is indeed easily seen for all atomic formulas except for the divisibility constraints in (3). But note that $c \mid a \cdot x + r$ for some $c, r \in \mathbb{N}$ if and only if there exists $k \in \mathbb{N}$ such that

$$k \cdot c = a \cdot x + r \iff b \cdot k \cdot c = b \cdot a \cdot x + b \cdot r \iff \frac{b}{a} \cdot k \cdot c = b \cdot x + \frac{b}{a} \cdot r \iff \frac{b}{a} \cdot c \mid b \cdot x + \frac{b}{a} \cdot r.$$

By the same argument, if x satisfies (4) then x/b satisfies (3).

We are now fully prepared to eliminate x. To this end, let

$$c := \mathrm{lcm} \left\{ b, \frac{b}{a_k} \cdot c_k : k \in D \right\},$$

where $c := 1$ if $D = \emptyset$. We now claim that (4) is equi-satisfiable with of the following formulas:

$$\begin{cases} \bigvee_{j \in G} \bigvee_{1 \leq m \leq c} \Psi[((b/a_j) \cdot q_j(\boldsymbol{y}) + m)/x] & \text{if } G \neq \emptyset \\ \bigvee_{j \in L} \bigvee_{1 \leq m \leq c} \Psi[((b/a_j) \cdot p_j(\boldsymbol{y}) - m)/x] & \text{if } G = \emptyset \text{ and } L \neq \emptyset \\ \bigvee_{0 \leq m < c} \Psi[m/x] & \text{otherwise.} \end{cases} \quad (5)$$

Let us first consider the case in which $G \cup L = \emptyset$. If the divisibility constraints in Ψ have a solution then by the Chinese remainder theorem, see e.g. [Jones and Jones 1998, Thm. 3.12] they have a solution amongst $\{0, \ldots, c-1\}$ as x is not constrained by any inequality constraints. Thus we can just try out by brute-force all values for x between $\{0, \ldots, c-1\}$ in order to obtain an equi-satisfiable formula. If, for instance $G \neq \emptyset$ then x is constrained from below by some greater-than constraint indexed by G. But then some term $((b/a_j) \cdot q_j(\boldsymbol{y}) + m)$ will be the largest amongst all others in a satisfying assignment, and hence we can use a long disjunction in order to "simulate" guessing which assignment is going to be the largest, and then additionally add some number in $\{1, \ldots, c\}$ giving a smallest solution, if it exists. The case $G = \emptyset$ and $L \neq \emptyset$ follows analogously.

We have thus shown how to eliminate a single variable from a conjunction of atomic formulas. What is presented here is the essence of Cooper's algorithm. We have omitted additional technicalities that Cooper had to obey in order to avoid a translation into disjunctive normal form. As stated in the introduction, [Oppen 1978] showed that Cooper's algorithm runs in deterministic triply-exponential time, which is the optimal complexity for a deterministic algorithm deciding Presburger arithmetic.

3.2. Automata-Based Decision Procedures

An alternative approach to deciding Presburger arithmetic is based on constructing a finite-state automaton whose language encodes all satisfying assignments of a given formula. This approach was introduced by [Büchi 1960], and we will give the main ideas below.

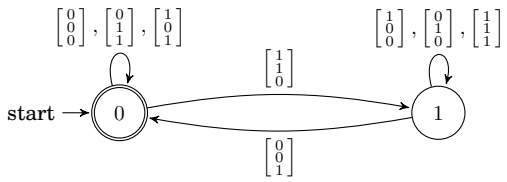

Fig. 2. Basis for a finite-state automaton accepting the addition relation L.

Recall that we work in the structure $\mathrm{Th}(\mathbb{N}, 0, 1, +)$. The decidability of Presburger arithmetic by automata-based methods follows from the fact that the structure underlying Presburger arithmetic is an automatic structure [Hodgson 1982; Khoussainov and Nerode 1994; Blumensath and Grädel 2000]. For a structure to be automatic, it is required that its universe is isomorphic to a regular language. For the natural numbers, this can easily be achieved by representing a number by its binary expansion. For instance, by using a least-significant-bit-first encoding, $\mathbb{N}$ is isomorphic to

$$N := (\{0,1\}^*1) \cup \{0\}.$$

The second requirement for a structure to be automatic is that all its relations are regular languages over a suitable alphabet that allows for encoding tuples of strings of the universe. For Presburger arithmetic, this requires that we give a regular language L that encodes the addition relation of natural numbers represented as words from N. To this end, consider the finite-state automaton depicted in Figure 2. This automaton reads the binary representation of three numbers i, j, k digit-by-digit as triples over $\{0,1\}$, and accepts if $i + j = k$. In state 0, all triples of bits not leading to a carry are read. Once a carry occurs, the automaton switches to state 1 and only accepts once the carry has been resolved.

A problem with the automaton in Figure 2 is that it allows representations of numbers to have an arbitrary number of tailing zeros. In automatic structures, this problem is circumvented by introducing a special marker $\#$ that indicates that a word has ended. Words of the domain of an automatic structure of different lengths can then be glued together using a *convolution function*, and the automata defining a relation of a structure can then take the special marker $\#$ into account. While the details are not difficult, they are not relevant to this article. The interested reader is referred to the literature cited above.

Once the domain and the relations of a structure have been represented by suitably chosen regular languages, deciding the first-order theory of this structure becomes easy. The closure of regular languages under inverse homomorphisms allows for making the languages of relations involving different variables compatible. Conjunction, disjunction and negation can be handled by application of the closure of regular languages under intersection, union and complement, respectively. Existential quantification can be dealt with by applying the closure of regular languages under homomorphisms. Again, for the specific technical details see the literature cited above.

A priori, the automata-based approach to deciding Presburger arithmetic is non-elementary due to the possibility of repeated complementation. However, [Durand-Gasselin and Habermehl 2010] showed that the automata resulting from Presburger arithmetic have a special structure that prevents this non-elementary blow-up from happening. In fact, in terms of runtime the automata-based construction matches the optimal deterministic triply-exponential time upper bound of quantifier elimination. While to the best of the author's knowledge the automata-based approach is not widely applied in practice these days, it is worth mentioning that it can empirically be more

efficient compared to quantifier elimination. For instance, even on small instances of the Frobenius problem presented in the introduction, a straight-forward implementation of the automata-based decision procedure outperforms the quantifier-elimination procedure implemented in the SMT-solver Z3 [de Moura and Bjørner 2008] by orders of magnitudes [Blondin 2018].

4. SEMI-LINEAR SETS

We will now present an exposition of the result of [Ginsburg and Spanier 1964] that the sets of integers definable in Presburger arithmetic coincide with semi-linear sets. Given a *base vector* $\boldsymbol{b} \in \mathbb{Z}^d$ and a finite set of *period vectors* $P = \{\boldsymbol{p}_1, \dots, \boldsymbol{p}_n\} \subseteq \mathbb{Z}^d$, the *linear set* $L(\boldsymbol{b}, P)$ is defined as

$$L(\boldsymbol{b}, P) = \boldsymbol{b} + \{\lambda_1 \boldsymbol{p}_1 + \cdots + \lambda_n p_n : \lambda_i \geq 0, 1 \leq i \leq n\}.$$

A *semi-linear set* is a finite union of linear sets. Observe that semi-linear sets are trivially closed under projection.

Given $\boldsymbol{v} \in \mathbb{Z}^d$ and $1 \leq i \leq d$, write $\boldsymbol{v}(i)$ for the i-th component of $\boldsymbol{v}$. It is easily seen that every linear set is definable in Presburger arithmetic, since $\boldsymbol{x} \in L(\boldsymbol{b}, P)$ if and only if $\boldsymbol{x}$ is a solution of

$$\Phi(\boldsymbol{x}) \equiv \exists \lambda_1 \cdots \exists \lambda_n \bigwedge_{1 \leq i \leq d} \boldsymbol{x}(i) = \boldsymbol{b}(i) + \lambda_1 \boldsymbol{p}_1(i) + \cdots + \lambda_n \boldsymbol{p}_n(i).$$

It follows that semi-linear sets are Presburger-definable.

Showing that Presburger-definable sets are semi-linear requires some more efforts. From Section 3.1, we know that Presburger arithmetic admits quantifier elimination. Hence in order to show that Presburger-definable sets are semi-linear, it suffices to show that the sets of solutions to systems of linear inequalities and linear congruences are semi-linear, and that semi-linear sets are closed under intersection.

4.1. Systems of linear inequalities

Given a $d \times n$ integer matrix A, we first show that the set of non-negative integer solutions to the homogeneous system of equations $A \cdot \boldsymbol{x} = 0$ is semi-linear. Observe that the set of all solutions to this system forms a monoid. In fact, this monoid is generated by a finite set of minimal elements $P \subseteq \mathbb{N}^n$ with respect to the ordering $<$. To the contrary, assume that P was infinite. Then Dickson's lemma gives $\boldsymbol{v}, \boldsymbol{w} \in P$ such that $\boldsymbol{v} < \boldsymbol{w}$. But then $\boldsymbol{w} - \boldsymbol{v} > \boldsymbol{0}$, contradicting minimality of P. Thus P is finite and the set of non-negative integer solutions of $A \cdot \boldsymbol{x} = 0$ is $L(\boldsymbol{0}, P)$, a linear set.

For an arbitrary system $A \cdot \boldsymbol{x} = \boldsymbol{b}$, consider the homogeneous system of linear equations obtained from augmenting A with $-\boldsymbol{b}$:

$$(A \mid -\boldsymbol{b}) \cdot \left[\begin{smallmatrix} \boldsymbol{x} \\ y \end{smallmatrix}\right] = 0.$$

Let $B \subseteq \mathbb{N}^n$ be the finite set obtained from the minimal elements generating the solutions of the augmented system whose last component corresponding to y equals one. Then the set of solutions of $A \cdot \boldsymbol{x} = \boldsymbol{b}$ is the semi-linear set $L(B, P) = \bigcup_{\boldsymbol{b} \in B} L(\boldsymbol{b}, P)$, where P is as above. Semi-linear sets of the form $L(B, P)$ are called *hybrid linear sets* [Chistikov and Haase 2016]. They form a convenient subclass of semi-linear sets that lie between linear and arbitrary semi-linear sets.

Finally, semi-linearity of the set of solutions of a system of linear inequalities $A \cdot \boldsymbol{x} \geq b$ follows a similar pattern. Consider the system of equations

$$(A \mid -I_d) \cdot \left[\begin{smallmatrix} \boldsymbol{x} \\ \boldsymbol{y} \end{smallmatrix}\right] = \boldsymbol{b},$$

where I_d is the $d \times d$ identity matrix, and let $L(C, Q) \subseteq \mathbb{N}^{n+d}$ be a hybrid linear set generating its solutions such that Q generates the solutions of the associated homo-

geneous system of equations as above. Let $B, P \subseteq \mathbb{N}^n$ be obtained from projecting the elements of C and Q onto the first n components. Then $L(B, P)$ generates the set of all solutions of $A \cdot \boldsymbol{x} \geq \boldsymbol{b}$, and also observe that $L(\mathbf{0}, P)$ generates all solutions of the homogeneous system of linear inequalities $A \cdot \boldsymbol{x} \geq \mathbf{0}$.

4.2. Systems of linear congruences

We now continue showing that the set of solutions of a system of divisibility constraints is a hybrid linear set. Consider such a system

$$\Phi(\boldsymbol{x}) \equiv \bigwedge_{1 \leq i \leq d} c_i \mid p_i(\boldsymbol{x}),$$

where the p_i are linear polynomials in $\boldsymbol{x} = (x_1, \ldots, x_n)$ with constant term zero. Let $c = \operatorname{lcm}(c_1, \ldots, c_d)$ and set

$$B = \{\boldsymbol{v} \in \{0, \ldots, c-1\}^n : \Phi(\boldsymbol{v}/\boldsymbol{x}) \text{ is true}\}.$$

Now the Chinese remainder theorem gives that for any $\boldsymbol{v} \in \mathbb{N}^n$,

$$\bigwedge_{1 \leq i \leq d} c_i \mid p_i(\boldsymbol{v}) \iff \bigwedge_{1 \leq i \leq d} c_i \mid p_i(\boldsymbol{v}) + c.$$

Consequently, letting $\boldsymbol{e}_i \in \mathbb{N}^n$ denote the i-th unit vector and defining $P = \{c \cdot \boldsymbol{e}_i : 1 \leq i \leq n\}$, we get that $L(B, P)$ is the set of non-negative solutions of $\Phi(\boldsymbol{x})$.

4.3. Intersection of semi-linear sets

It remains to show that semi-linear sets are closed under intersection. Due to the distributivity of union and intersection, it suffices to show that the intersection of two linear sets is a semi-linear set.

Let $L(\boldsymbol{c}, Q)$ and $L(\boldsymbol{d}, R)$ be linear sets. We can view the sets of vectors Q and R as matrices. Then $\boldsymbol{v} \in L(\boldsymbol{c}, Q) \cap L(\boldsymbol{d}, R)$ if and only if there are $\boldsymbol{\lambda}, \boldsymbol{\gamma} \geq \mathbf{0}$ such that

$$\begin{aligned} & \boldsymbol{v} = \boldsymbol{c} + Q \cdot \boldsymbol{\lambda} \text{ and } \boldsymbol{v} = \boldsymbol{d} + R \cdot \boldsymbol{\gamma} \\ \iff & \boldsymbol{c} + Q \cdot \lambda = \boldsymbol{d} + R \cdot \boldsymbol{\gamma} \\ \iff & (Q \mid -R) \left[\begin{smallmatrix} \boldsymbol{\lambda} \\ \boldsymbol{\gamma} \end{smallmatrix}\right] = \boldsymbol{d} - \boldsymbol{c}. \end{aligned}$$

The latter is a system of linear equations whose set of solutions is a hybrid linear set. Let $L(E, S)$ be the hybrid linear set obtained from projecting the solution set onto the components corresponding to $\boldsymbol{\lambda}$. Setting $B = \boldsymbol{c} + Q \cdot E$ and $P = Q \cdot S$, we have

$$\begin{aligned} L(\boldsymbol{c}, Q) \cap L(\boldsymbol{d}, R) &= \boldsymbol{c} + \{Q \cdot \boldsymbol{w} : \boldsymbol{w} \in L(E, S)\} \\ &= \boldsymbol{c} + Q \cdot L(E, S) \\ &= \boldsymbol{c} + Q \cdot \{E + S \cdot \boldsymbol{\xi} : \boldsymbol{\xi} \geq \mathbf{0}\} \\ &= L(\boldsymbol{c} + Q \cdot E, Q \cdot S) \\ &= L(B, P). \end{aligned}$$

Hence, semi-linear sets are closed under intersection.

4.4. Decompositions of semi-linear sets

When working with semi-linear sets, it is often helpful being able to assume with no loss of generality some structural properties on the constituting linear sets.

We first mention that one may assume that all linear sets have linearly independent period vectors. Essentially, this requires establishing a discrete analogue of Carathéodory's theorem. This theorem states that the convex cone generated by a finite set of vectors P can be decomposed into a union of cones generated by linearly

independent subsets of P, see e.g. [Schrijver 1986, p. 94]. A fully discrete analogue of Carathéodory's theorem cannot be obtained since we may need additional base vectors in order to preserve the discrete periodic structure of a linear set. It was first shown by [Ginsburg and Spanier 1964] that a linear set $L(\boldsymbol{b}, P)$ decomposes as

$$L(\boldsymbol{b}, P) = \bigcup_{i \in I} L(\boldsymbol{b}_i, P_i),$$

where the $P_i \subseteq P$ are linearly independent vectors.

An even stronger property is that of unambiguity. [Eilenberg and Schützenberger 1969] and [Ito 1969] independently showed that every semi-linear set M is equivalent to a semi-linear set

$$M = \bigcup_{i \in I} L(\boldsymbol{b}_i, P_i)$$

such that all P_i are linearly independent and $L(\boldsymbol{b}_i, P_i) \cap L(\boldsymbol{b}_j, P_j) = \emptyset$ for all $i \neq j$.

Finally, if we are only interested in decreasing the cardinality of a set of period vectors without introducing new base vectors, we can apply a theorem of [Eisenbrand and Shmonin 2006]. Given $P \subseteq \mathbb{Z}^d$ and $\boldsymbol{v} \in L(\boldsymbol{0}, P)$, this theorem states that there exists $Q \subseteq P$ such that $\boldsymbol{v} \in L(\boldsymbol{0}, Q)$ and $|Q| \leq 2d \log(4dm)$, where m is the maximum absolute value of all constants appearing in P.

4.5. Complementation of semi-linear sets

Closure of semi-linear sets under complement follows from the equivalence between semi-linear and Presburger-definable sets. However, it is less commonly known that, using the decompositions of previous section, it is not difficult to give a direct proof of this result. Due to closure of semi-linear sets under union and intersection, it suffices to show that the complement of a linear set is semi-linear.

To this end, let $M = L(\boldsymbol{b}, P) \subseteq \mathbb{Z}^d$ be a linear set, and with no loss of generality assume that P is linearly independent. As before, we can view P as a $d \times n$ integer matrix. Let $\widetilde{M} \subseteq \mathbb{R}^d$ denote the convex hull of M. By the Minkowski-Weyl theorem, there is a system of linear inequalities $A \cdot \boldsymbol{x} \geq \boldsymbol{c}$ defining $\widetilde{M}$. Let the rows of $A \cdot \boldsymbol{x} \geq \boldsymbol{c}$ be $\{\boldsymbol{a}_i \cdot \boldsymbol{x} \geq c_i\}_{1 \leq i \leq m}$. Then $\mathbb{R}^d \setminus \widetilde{M}$ can be obtained as the union over the set of solutions of all systems of linear inequalities $\boldsymbol{a}_i \cdot \boldsymbol{x} < c_i$. It thus remains to show how to define $\widetilde{M} \setminus M$. For every $\boldsymbol{v} \in L(\boldsymbol{b}, P)$, there is a unique $\boldsymbol{\lambda} \in \mathbb{N}^n$ such that $\boldsymbol{v} = \boldsymbol{b} + P \cdot \boldsymbol{\lambda}$. Any $\boldsymbol{w} \in \widetilde{M} \setminus M$ is therefore obtained as $\boldsymbol{w} = \boldsymbol{b} + P \cdot \boldsymbol{\gamma}$ for some $\boldsymbol{\gamma} \in \mathbb{R}^n$ with the property that some component of $\boldsymbol{\gamma}$ is not integral. Defining $C := \boldsymbol{b} + (\{\boldsymbol{v} \in P \cdot \boldsymbol{\lambda} \cap \mathbb{Z}^d : \boldsymbol{\lambda} \in [0,1)^n\} \setminus \boldsymbol{0})$, we thus have $L(C, P) = \widetilde{M} \setminus M$. In summary, we obtain $\mathbb{Z}^d \setminus M = ((\mathbb{R}^d \setminus \widetilde{M}) \cap \mathbb{Z}^d) \cup L(C, P)$, which is a semi-linear set.

4.6. Descriptional complexity

So far, we have only looked at definability, closure and decomposition properties of semi-linear sets. When manipulating semi-linear sets, in many applications scenarios we want to keep track of the growth of constants and the number of generators. A building block is a result of [Pottier 1991] which provides bounds on the constants of the generators P of the set of non-negative solutions of a homogeneous system of linear equations $A \cdot \boldsymbol{x} = \boldsymbol{0}$, where A is an integer matrix or rank r. Pottier shows that the largest absolute value $||P||$ in P is bounded by

$$||P|| \leq (1 + ||A||_{1,\infty})^r.$$

Bootstrapping from this base case as done in Sections 4.1–4.5 then allows for obtaining bounds on the effect on the descriptional complexity of Boolean operations and decom-

Table I. Complexity of Presburger arithmetic

number of quantifier alternations	fixed number of variables in quantifier blocks	variable number of variables in quantifier blocks
existential fragment	P-complete [Scarpellini 1984]	NP-complete [Borosh and Treybing 1976] [von zur Gathen and Sieveking 1978]
fixed $i > 1$	STA$(*, n^{O(1)}, i-1)$-complete [Grädel 1988]	STA$(*, 2^{n^{O(1)}}, i-1)$-complete [Haase 2014]
variable	STA$(*, 2^{2^{n^{O(1)}}}, O(n))$-complete [Berman 1980]	

positions. Following this simple approach yields in some cases optimal bounds, but not in all. Rigorous estimations have recently been established by [Chistikov and Haase 2016], and also [Beier et al. 2017] who established the descriptional complexity of the constructions given by [Ginsburg and Spanier 1964].

5. COMPUTATIONAL COMPLEXITY

A short account on the computational complexity of Presburger arithmetic has already been given in Section 1. The purpose of this section is to give a full account on the complexity of the various fragments of Presburger arithmetic together with references to the literature. Subsequently, we provide a similar overview of the complexity of decision problems for semi-linear sets.

5.1. Presburger arithmetic

Table I gives an overview over the complexity of Presburger arithmetic, broken down according to the number of quantifier alternations and the number of variables in every quantifier block. The complexity results stated are for formulas beginning with an existential quantifier, analogous results hold for formulas beginning with a universal quantifier.

An NP upper bound for the existential fragment can be obtained from NP upper bounds for integer programming, which were independently established by [Borosh and Treybing 1976] and [von zur Gathen and Sieveking 1978]. Based on Lenstra's polynomial-time algorithm for integer programming in a fixed dimension [Lenstra Jr 1983], [Scarpellini 1984] showed that existential Presburger arithmetic with a fixed number of variables can be decided in polynomial time. The key observation is that when fixing the number of variables, one can translate a quantifier-free Presburger formula in polynomial time into disjunctive normal form [Woods 2015, Prop. 5.1].

For quantified fragments, the complexity is given in terms of the STA complexity measure. If the number of alternations is fixed, those complexity classes correspond to standard oracle complexity classes. Presburger arithmetic with a fixed number of quantifier alternations $i > 1$ and a fixed number of variables in every quantifier block is complete for $\Sigma^{\mathrm{P}}_{i-1}$, i.e., every level of the polynomial time hierarchy. The reason for "saving" one oracle call is that, as seen in Table I, in the presence of a fixed number of variables the existential (and thus universal) fragment of Presburger is in P. If instead we allow for an arbitrary number of variables in every quantifier block, Presburger arithmetic becomes complete for $\Sigma^{\mathrm{EXP}}_{i-1}$, i.e., every level of the weak EXP hierarchy. The first level of this hierarchy is NEXP, the second $\mathrm{NEXP}^{\mathrm{NP}}$, etc. Again, we can "save" one oracle call, the reason being that integer linear programming is fixed-parameter tractable in the number of variables [Frank and Tardos 1987].

Recalling the example of the Frobenius problem given in Section 1, we observe that, regardless of the instance of the Frobenius problem, the number of quantifier alternations and even the number of inequalities in the formula is fixed. If in addition the number of integers in an instance of the Frobenius problem is fixed, [Kannan 1992] showed that the Frobenius number can be computed in polynomial time. Observe that in this case also the number of variables in the corresponding Presburger formula becomes fixed. Kannan's result led to the more general question of whether *short Presburger arithmetic*, i.e. Presburger arithmetic with a fixed number of quantifier alternations, variables and inequalities, is polynomial-time decidable. [Schöning 1997] showed that already for an $\exists x \forall y$-quantifier prefix, Presburger arithmetic is NP-hard, so fixing the number of linear inequalities is crucial. Affirmative answers were given only recently. [Woods 2015] showed that the Π_2-fragment of short Presburger arithmetic is decidable in polynomial time. In contrast, [Nguyen and Pak 2017] showed that the Σ_{i+2}-fragment of short Presburger arithmetic is complete for Σ_i^{P}, already for instances of quantified integer programming, i.e., short Presburger formulas in which no disjunction appears. Finally, if we allow for an unbounded number of variables in every quantifier block, quantified integer programming with i quantifier alternations becomes complete for Σ_i^{P} [Chistikov and Haase 2017].

5.2. Semi-linear sets

The decision problems relevant to semi-linear sets are the standard decision problems from formal language theory. The parameters on which the complexity of those decision problems depends on are the dimension and the encoding of numbers in unary or binary.

Given a semi-linear set $M \subseteq \mathbb{Z}^d$ and a point $\boldsymbol{v} \in \mathbb{Z}^d$, the *word problem* asks whether $\boldsymbol{v} \in M$. In general, this problem is NP-complete. The upper bound follows from the NP upper bound of integer programming [Borosh and Treybing 1976; von zur Gathen and Sieveking 1978]. An NP lower bound for $d = 1$ and numbers encoded in binary can, for instance, be derived from a variant of the classical subset sum problem in which elements can be chosen multiple times, see e.g. [Haase 2012, p. 70]. If the dimension is variable and numbers are encoded in unary, the word problem remains NP-complete [Kopczynski and To 2010]. Finally, the word problem is decidable in polynomial time if both the dimension is fixed and numbers are encoded in unary [Kopczynski and To 2010].

The second important decision problem for semi-linear sets is the *inclusion problem*, i.e., deciding whether $M \subseteq N$ holds for two given semi-linear sets $M, N \subseteq \mathbb{Z}^d$. Obtaining upper bounds for the inclusion problem entails showing upper bounds on the size of the constants of smallest elements in the set-theoretic difference of two semi-linear sets. [Huynh 1982] showed that the bit size of the smallest such elements is polynomial, which places the inclusion problem in Π_2^{P}. He later gave a simplified proof of this result [Huynh 1986]. Regarding lower bounds, the inclusion problem is hard for Π_2^{P} already for linear sets in dimension one with numbers encoded in binary [Simon 2018], and also for linear sets in variable dimension with numbers encoded in unary [Chistikov et al. 2018, Thm. 15]. If both the dimension is fixed and numbers are encoded in unary, the inclusion problem is decidable in polynomial time [Kopczynski and To 2010].

It should be noted that those complexity results hold for semi-linear sets which are given explicitly. This is rarely the case, and often only the largest constant in an implicitly given semi-linear set is known. In such situations, the following result can be helpful: Suppose we are given semi-linear sets $M, N \subseteq \mathbb{Z}^d$ with largest absolute value

is m. [Chistikov and Haase 2016] showed that if $M \setminus N$ is non-empty then there is some $\boldsymbol{v} \in M \setminus N$ whose largest absolute value is bounded by $2^{m^{O(d^2)}}$.

6. DECIDABLE EXTENSIONS

Even very basic extensions of Presburger arithmetic with additional functions and predicates render Presburger arithmetic undecidable. Most prominently, Gödel's incompleteness theorem implies that the extension of Presburger arithmetic with multiplication is undecidable, which was shown by [Church 1936]. Many further such undecidable extensions are surveyed in the paper by [Bès 2002]. The goal of this section is to give examples, references to the literature and main ideas underlying decidable extensions of Presburger arithmetic.

6.1. Büchi arithmetic

When developing his automata-based decision procedure for Presburger arithmetic, [Büchi 1960] observed that the extension of Presburger arithmetic with a binary predicate V_k for any *fixed* $k \geq 2$ such that $V_k(x, y)$ holds if x is the largest power of k dividing y is decidable. The family of such extensions of Presburger arithmetic is known as *Büchi arithmetic*. The crucial observation is that, when writing y in base k, $V_k(x, y)$ holds if the first non-zero digit of y is x. From this observation, it is easy to derive a finite-state automaton accepting tuples of words in base k such that $V_k(x, y)$ holds, analogously to the automaton in Figure 2. As outlined in Section 3.2, this in turn gives a decision procedure for Büchi arithmetic for any fixed $k \geq 2$. The converse also holds: the sets of tuples of natural numbers $\mathbb{N}^n$ encoded in base k and accepted by a finite-state automaton coincides with the sets definable in Büchi arithmetic with the additional V_k predicate, see e.g. [Bruyère et al. 1994].

Extending Presburger arithmetic with multiple predicates V_k is in general not possible. If j and k are multiplicatively independent, i.e., $j^a = k^b$ with $a, b \in \mathbb{N}$ implies $a = b = 0$, then the first-order theory of Presburger arithmetic extended with predicates V_j, V_k becomes undecidable [Villemaire 1992].

6.2. Counting

Another decidable extension of Presburger arithmetic allows for counting the number of solutions for a given variable in a subformula. Formally, *Presburger arithmetic with counting* has an additional unary *counting quantifier* $\exists^{=x} y$. A formula $\exists^{=x} y\, \varphi(x, y, \boldsymbol{z})$ evaluates to true for $x = a$ and $\boldsymbol{c} \in \mathbb{N}^n$ iff

$$a = \#\{b \in \mathbb{N} : \varphi[x/a, b/y, \boldsymbol{c}/\boldsymbol{z}] \text{ holds}\},$$

i.e., the number of satisfying assignments for y is bound to the variable x, provided that this number is finite. [Schweikardt 2005] gave a quantifier elimination procedure for this extension that translates a formula of Presburger arithmetic with counting to standard Presburger arithmetic. This translation involves a non-elementary blow-up. However, no harder lower bounds than those of standard Presburger arithmetic are known. A restriction of the counting quantifier has been studied by [Habermehl and Kuske 2015]. They considered counting modulo a constant and gave a quantifier-elimination procedure that runs in triply exponential time, i.e., is not more expensive than standard Presburger arithmetic.

[Barvinok 1994] gave a polynomial-time algorithm that counts the number points in polyhedra in fixed dimensions. Building upon this result, [Woods 2015] showed that the number of solutions of an existential Presburger formula with a fixed number of variables can be counted in polynomial time, thereby generalising the result of [Scarpellini 1984].

6.3. Non-linear extensions

In general, extensions of Presburger arithmetic with non-linear functions and predicates almost always lead to undecidability. Nevertheless, a few exceptions exist. [Weispfenning 1990] gave a quantifier-elimination procedure for an extension of Presburger arithmetic allowing for terms involving rational functions of the form

$$p(x) + \left\lfloor \frac{p_1(x)}{q_1(x)} \right\rfloor + \cdots + \left\lfloor \frac{p_k(x)}{q_j(x)} \right\rfloor$$

for arbitrary univariate polynomials p, p_i, q_i with integer coefficients. His quantifier-elimination procedure inherits the triply exponential-time upper bound for standard Presburger arithmetic. [Gurari and Ibarra 1979] showed NP-completeness of a non-linear integer programming problem. Given a $d \times n$ integer matrix A with row vector $\boldsymbol{a}_i$ and a dimension d vector σ consisting in every component of a rational function r_i, the problem is to find $\boldsymbol{v} \in \mathbb{N}^n$ and $w \in \mathbb{N}$ such that $\boldsymbol{a}_i \cdot \boldsymbol{v} = r_i(y)$ or $\boldsymbol{a}_i \cdot \boldsymbol{v} = \lfloor r_i(y) \rfloor$ for all $1 \leq i \leq d$. This problem is harder than classical integer programming, since determining whether the quadratic Diophantine equation $a \cdot x + b \cdot y^2 = c$ has a solution in the non-negative integers is already NP-hard [Manders and Adleman 1976].

[Robinson 1949] showed that the full first-order theory of the extension of Presburger arithmetic with a divisibility predicate is undecidable since it allows for defining multiplication. However, when restricting to the existential fragment, Presburger arithmetic with a full divisibility relation is still decidable [Lipshitz 1978; Lipshitz 1981], and known to be NP-hard and in NEXP [Lechner et al. 2015].

REFERENCES

Alexander I. Barvinok. 1994. A Polynomial Time Algorithm for Counting Integral Points in Polyhedra When the Dimension is Fixed. *Math. Oper. Res.* 19, 4 (1994), 769–779. DOI:http://dx.doi.org/10.1287/moor.19.4.769

Simon Beier, Markus Holzer, and Martin Kutrib. 2017. On the Descriptional Complexity of Operations on Semilinear Sets. In *Automata and Formal Languages (AFL) (EPTCS)*, Vol. 252. 41–55. DOI:http://dx.doi.org/10.4204/EPTCS.252.8

Leonard Berman. 1980. The complexity of logical theories. *Theor. Comput. Sci.* 11, 1 (1980), 71–77.

Alexis Bès. 2002. A survey of arithmetical definability. In *A tribute to Maurice Boffa*. Société Mathématique de Belgique, 1–54.

Michael Blondin. 2018. Personal communication. (2018).

Achim Blumensath and Erich Grädel. 2000. Automatic Structures. In *Logic in Computer Science (LICS)*. IEEE Computer Society, 51–62. DOI:http://dx.doi.org/10.1109/LICS.2000.855755

Itshak Borosh and Leon B. Treybing. 1976. Bounds on positive integral solutions of linear Diophantine equations. *Proc. Am. Math. Soc.* 55 (1976), 299–304. DOI:http://dx.doi.org/10.2307/2041711

Alexandre Boudet and Hubert Comon. 1996. Diophantine Equations, Presburger Arithmetic and Finite Automata. In *Trees in Algebra and Programming (CAAP) (Lect. Notes Comp. Sci.)*, Vol. 1059. Springer, 30–43. DOI:http://dx.doi.org/10.1007/3-540-61064-2_27

Véronique Bruyère, Georges Hansel, Christian Michaux, and Roger Villemaire. 1994. Logic and p-recognizable sets of integers. *Bull. Belg. Math. Soc. Simon Stevin* 1, 2 (1994), 191–238.

J. Richard Büchi. 1960. Weak Second-Order Arithmetic and Finite Automata. *Mathematical Logic Quarterly* 6, 1-6 (1960), 66–92. DOI:http://dx.doi.org/10.1002/malq.19600060105

Ashok K. Chandra, Dexter Kozen, and Larry J. Stockmeyer. 1981. Alternation. *J. ACM* 28, 1 (1981), 114–133. DOI:http://dx.doi.org/10.1145/322234.322243

Dmitry Chistikov and Christoph Haase. 2016. The Taming of the Semi-Linear Set. In *Automata, Languages, and Programming (ICALP) (LIPIcs)*, Vol. 55. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 128:1–128:13. DOI:http://dx.doi.org/10.4230/LIPIcs.ICALP.2016.128

Dmitry Chistikov and Christoph Haase. 2017. On the Complexity of Quantified Integer Programming. In *Automata, Languages, and Programming (ICALP) (LIPIcs)*, Vol. 80. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 94:1–94:13. DOI:http://dx.doi.org/10.4230/LIPIcs.ICALP.2017.94

Dmitry Chistikov, Christoph Haase, and Simon Halfon. 2018. Context-free commutative grammars with integer counters and resets. *Theor. Comput. Sci.* 735 (2018), 147–161. DOI:http://dx.doi.org/10.1016/j.tcs.2016.06.017

Alonzo Church. 1936. An unsolvable problem of elementary number theory. *Am. J. Math.* 58, 2 (1936), 345–363. https://projecteuclid.org:443/euclid.jsl/1183142123

David C. Cooper. 1972. Theorem proving in arithmetic without multiplication. *Mach. Intell.* 7 (1972), 91–99.

Leonardo Mendonça de Moura and Nikolaj Bjørner. 2008. Z3: An Efficient SMT Solver. In *Tools and Algorithms for the Construction and Analysis of Systems, TACAS (Lect. Notes Comp. Sci.)*, Vol. 4963. Springer, 337–340. DOI:http://dx.doi.org/10.1007/978-3-540-78800-3_24

Leonardo Mendonça de Moura and Nikolaj Bjørner. 2011. Satisfiability modulo theories: introduction and applications. *Commun. ACM* 54, 9 (2011), 69–77. DOI:http://dx.doi.org/10.1145/1995376.1995394

Antoine Durand-Gasselin and Peter Habermehl. 2010. On the Use of Non-deterministic Automata for Presburger Arithmetic. In *Concurrency Theory (CONCUR) (Lect. Notes Comp. Sci.)*, Vol. 6269. Springer, 373–387. DOI:http://dx.doi.org/10.1007/978-3-642-15375-4_26

Samuel Eilenberg and Marcel-Paul Schützenberger. 1969. Rational sets in commutative monoids. *J. Algebra* 13, 2 (1969), 173–191. DOI:http://dx.doi.org/10.1016/0021-8693(69)90070-2

Friedrich Eisenbrand and Gennady Shmonin. 2006. Carathéodory bounds for integer cones. *Oper. Res. Lett.* 34, 5 (2006), 564–568. DOI:http://dx.doi.org/10.1016/j.orl.2005.09.008

Herbert B. Enderton. 1972. *A mathematical introduction to logic*. Academic Press.

Jeanne Ferrante and Charles Rackoff. 1975. A Decision Procedure for the First Order Theory of Real Addition with Order. *SIAM J. Comput.* 4, 1 (1975), 69–76. DOI:http://dx.doi.org/10.1137/0204006

Michael J. Fischer and Michael O. Rabin. 1998. Super-Exponential Complexity of Presburger Arithmetic. In *Quantifier Elimination and Cylindrical Algebraic Decomposition*. Springer Vienna, 122–135. DOI:http://dx.doi.org/10.1007/978-3-7091-9459-1_5

Jean Baptiste Joseph Fourier. 1826. Solution d'une question particuliere du calcul des inégalités. *Nouveau Bulletin des Sciences par la Société philomatique de Paris* 99 (1826), 100.

András Frank and Éva Tardos. 1987. An application of simultaneous Diophantine approximation in combinatorial optimization. *Combinatorica* 7, 1 (1987), 49–65. DOI:http://dx.doi.org/10.1007/BF02579200

Seymor Ginsburg and Edwin H. Spanier. 1964. Bounded ALGOL-like languages. *T. Am. Math. Soc.* (1964), 333–368. DOI:http://dx.doi.org/10.2307/1994067

Erich Grädel. 1988. Subclasses of Presburger arithmetic and the polynomial-time hierarchy. *Theor. Comput. Sci.* 56, 3 (1988), 289–301. DOI:http://dx.doi.org/10.2307/2041711

Eitan M. Gurari and Oscar H. Ibarra. 1979. An NP-Complete Number-Theoretic Problem. *J. ACM* 26, 3 (1979), 567–581. DOI:http://dx.doi.org/10.1145/322139.322152

Christoph Haase. 2012. *On the Complexity of Model Checking Counter Automata*. Ph.D. Dissertation. University of Oxford.

Christoph Haase. 2014. Subclasses of Presburger arithmetic and the weak EXP hierarchy. In *Joint Meeting Computer Science Logic (CSL) and Logic in Computer Science (LICS), CSL-LICS*. ACM, 47:1–47:10. DOI:http://dx.doi.org/10.1145/2603088.2603092

Peter Habermehl and Dietrich Kuske. 2015. On Presburger Arithmetic Extended with Modulo Counting Quantifiers. In *Foundations of Software Science and Computation Structures (FoSSaCS) (Lect. Notes Comp. Sci.)*, Vol. 9034. Springer, 375–389. DOI:http://dx.doi.org/10.1007/978-3-662-46678-0_24

David Hilbert and Wilhelm Ackermann. 1950. *Principles of Mathematical Logic*. Chelsea Pub. Co.

Bernard R. Hodgson. 1982. On direct products of automaton decidable theories. *Theor. Comput. Sci.* 19, 3 (1982), 331 – 335. DOI:http://dx.doi.org/10.1016/0304-3975(82)90042-1

Dung T. Huynh. 1986. A Simple Proof for the Σ_2^p Upper Bound of the Inequivalence Problem for Semilinear Sets. *Elektron. Inf.verarb. Kybern.* 22, 4 (1986), 147–156.

Thiet-Dung Huynh. 1982. The Complexity of Semilinear Sets. *Elektron. Inf.verarb. Kybern.* 18, 6 (1982), 291–338.

Ryuichi Ito. 1969. Every Semilinear Set is a Finite Union of Disjoint Linear Sets. *J. Comput. Syst. Sci.* 3, 2 (1969), 221–231. DOI:http://dx.doi.org/10.1016/S0022-0000(69)80014-0

Gareth A. Jones and J. Mary Jones Jones. 1998. *Elementary Number Theory*. Springer London. DOI:http://dx.doi.org/10.1007/978-1-4471-0613-5

Ravi Kannan. 1992. Lattice translates of a polytope and the Frobenius problem. *Combinatorica* 12, 2 (1992), 161–177. DOI:http://dx.doi.org/10.1007/BF01204720

Bakhadyr Khoussainov and Anil Nerode. 1994. Automatic Presentations of Structures. In *Logical and Computational Complexity (Lect. Notes Comp. Sci.)*, Vol. 960. Springer, 367–392. DOI:http://dx.doi.org/10.1007/3-540-60178-3_93

Felix Klaedtke. 2008. Bounds on the automata size for Presburger arithmetic. *ACM Trans. Comput. Log.* 9, 2 (2008), 11:1–11:34. DOI:http://dx.doi.org/10.1145/1342991.1342995

Eryk Kopczynski and Anthony Widjaja To. 2010. Parikh Images of Grammars: Complexity and Applications. In *Logic in Computer Science (LICS)*. IEEE Computer Society, 80–89. DOI:http://dx.doi.org/10.1109/LICS.2010.21

Dexter Kozen. 2006. *Theory of Computation*. Springer.

Antonia Lechner, Joël Ouaknine, and James Worrell. 2015. On the Complexity of Linear Arithmetic with Divisibility. In *Logic in Computer Science (LICS)*. IEEE Computer Society, 667–676. DOI:http://dx.doi.org/10.1109/LICS.2015.67

Hendrik W. Lenstra Jr. 1983. Integer programming with a fixed number of variables. *Math. Oper. Res.* 8, 4 (1983), 538–548. http://www.jstor.org/stable/3689168

Leonard M. Lipshitz. 1978. The Diophantine Problem for Addition and Divisibility. *T. Am. Math. Soc.* 235 (1978), 271–283. DOI:http://dx.doi.org/10.2307/1998219

Leonard M. Lipshitz. 1981. Some remarks on the Diophantine problem for addition and divisibility. In *Proc. Model Theory Meeting*, Vol. 33. 41–52.

Kenneth L. Manders and Leonard M. Adleman. 1976. NP-Complete Decision Problems for Quadratic Polynomials. In *Symposium on Theory of Computing (STOC)*. ACM, 23–29. DOI:http://dx.doi.org/10.1145/800113.803627

Danny Nguyen and Igor Pak. 2017. Short Presburger Arithmetic Is Hard. In *Foundations of Computer Science (FOCS)*. IEEE Computer Society, 37–48. DOI:http://dx.doi.org/10.1109/FOCS.2017.13

Derek C. Oppen. 1978. A $2^{2^{2^{pn}}}$ upper bound on the complexity of Presburger Arithmetic. *J. Comput. Syst. Sci.* 16, 3 (1978), 323 – 332. DOI:http://dx.doi.org/10.1016/0022-0000(78)90021-1

Rohit Parikh. 1966. On Context-Free Languages. *J. ACM* 13, 4 (1966), 570–581. DOI:http://dx.doi.org/10.1145/321356.321364

Loïc Pottier. 1991. Minimal solutions of linear Diophantine systems : bounds and algorithms. In *Rewriting Techniques and Applications (RTA)*. Lect. Notes Comp. Sci., Vol. 488. Springer, 162–173. DOI:http://dx.doi.org/10.1007/3-540-53904-2_94

Mojżesz Presburger. 1929. Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt. In *Comptes Rendus du I congres de Mathematiciens des Pays Slaves*. 92–101.

Julia Robinson. 1949. Definability and Decision Problems in Arithmetic. *J. Symb. Log.* 14, 2 (1949), 98–114. DOI:http://dx.doi.org/10.2307/2266510

Bruno Scarpellini. 1984. Complexity of subcases of Presburger arithmetic. *T. Am. Math. Soc.* 284 (1984), 203–218. DOI:http://dx.doi.org/10.2307/1999283

Uwe Schöning. 1997. Complexity of Presburger arithmetic with fixed quantifier dimension. *Theor. Comput. Syst.* 30, 4 (1997), 423–428. DOI:http://dx.doi.org/10.1007/BF02679468

Alexander Schrijver. 1986. *Theory of linear and integer programming*. John Wiley & Sons.

Nicole Schweikardt. 2005. Arithmetic, first-order logic, and counting quantifiers. *ACM Trans. Comput. Log.* 6, 3 (2005), 634–671. DOI:http://dx.doi.org/10.1145/1071596.1071602

Hans Ulrich Simon. 2018. On the Containment Problem for Linear Sets. In *Symposium on Theoretical Aspects of Computer Science (STACS) (LIPIcs)*, Vol. 96. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 55:1–55:12. DOI:http://dx.doi.org/10.4230/LIPIcs.STACS.2018.55

Craig Smoryński. 1991. *Logical number theory I: An introduction*. Springer.

Roger Villemaire. 1992. The Theory of $(\mathbb{N}, +, V_k, V_l)$ is Undecidable. *Theor. Comput. Sci.* 106, 2 (1992), 337–349. DOI:http://dx.doi.org/10.1016/0304-3975(92)90256-F

Joachim von zur Gathen and Malte Sieveking. 1978. A bound on solutions of linear integer equalities and inequalities. *Proc. Am. Math. Soc.* 72, 1 (1978), 155–158. DOI:http://dx.doi.org/10.2307/2042554

Volker Weispfenning. 1990. The Complexity of Almost Linear Diophantine Problems. *J. Symb. Comput.* 10, 5 (1990), 395–404. DOI:http://dx.doi.org/10.1016/S0747-7171(08)80051-X

H. Paul Williams. 1986. Fourier's Method of Linear Programming and Its Dual. *Am. Math. Mon.* 93, 9 (1986), 681–695. DOI:http://dx.doi.org/10.2307/2322281

Pierre Wolper and Bernard Boigelot. 1995. An Automata-Theoretic Approach to Presburger Arithmetic Constraints (Extended Abstract). In *Static Analysis (SAS) (Lect. Notes Comp. Sci.)*, Vol. 983. Springer, 21–32. DOI:http://dx.doi.org/10.1007/3-540-60360-3_30

Kevin Woods. 2015. Presburger arithmetic, rational generating functions, and quasi-polynomials. *J. Symbolic Logic* 80, 2 (2015), 433–449. DOI:http://dx.doi.org/10.1017/jsl.2015.4

Jan Zygmunt. 1991. Mojżesz Presburger: Life and Work. *Hist. Philos. Logic* 12, 2 (1991), 211–223. DOI:http://dx.doi.org/10.1080/014453409108837186