Geometric decision procedures and the VC dimension of linear arithmetic theories

Dmitry Chistikov
d.chistikov@warwick.ac.uk
Centre for Discrete Mathematics and its Applications (DIMAP) & Department of Computer Science, University of Warwick
Coventry, UK

Christoph Haase
christoph.haase@cs.ox.ac.uk
Department of Computer Science, University of Oxford
Oxford, UK

Alessio Mansutti
alessio.mansutti@cs.ox.ac.uk
Department of Computer Science, University of Oxford
Oxford, UK

ABSTRACT

This paper resolves two open problems on linear integer arithmetic (LIA), also known as Presburger arithmetic. First, we give a triply exponential geometric decision procedure for LIA, i.e., a procedure based on manipulating semilinear sets. This matches the running time of the best quantifier elimination and automata-based procedures. Second, building upon our first result, we give a doubly exponential upper bound on the Vapnik–Chervonenkis (VC) dimension of sets definable in LIA, proving a conjecture of D. Nguyen and I. Pak [*Combinatorica* 39, pp. 923–932, 2019].

These results partially rely on an analysis of sets definable in linear real arithmetic (LRA), and analogous results for LRA are also obtained. At the core of these developments are new decomposition results for semilinear and $\mathbb{R}$-semilinear sets, the latter being the sets definable in LRA. These results yield new algorithms to compute the complement of ($\mathbb{R}$-)semilinear sets that do not cause a non-elementary blowup when repeatedly combined with procedures for other Boolean operations and projection. The existence of such an algorithm for semilinear sets has been a long-standing open problem.

CCS CONCEPTS

• **Theory of computation** → **Logic**; **Machine learning theory**.

KEYWORDS

semilinear sets, convex polyhedra, linear real arithmetic, linear integer arithmetic, Presburger arithmetic, VC dimension

ACM Reference Format:
Dmitry Chistikov, Christoph Haase, and Alessio Mansutti. 2022. Geometric decision procedures and the VC dimension of linear arithmetic theories. In *37th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS) (LICS '22), August 2–5, 2022, Haifa, Israel.* ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3531130.3533372

LICS '22, August 2–5, 2022, Haifa, Israel

ACM ISBN 978-1-4503-9351-5/22/08…$15.00
https://doi.org/10.1145/3531130.3533372

Acknowledgments. This work is part of a project that has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme – Grant agreement No. 852769, *Advanced Reasoning in Arithmetic Theories* (*ARiAT*).

1 INTRODUCTION

Linear arithmetic theories are first-order theories over numerical domains, such as $\mathbb{R}$ or $\mathbb{Z}$, and the signature $\langle 0, 1, +, \leq \rangle$ whose constant and relation symbols are interpreted in their natural semantics. For $\mathbb{R}$ and $\mathbb{Z}$, these theories are commonly referred to as *linear real arithmetic (LRA)* and *linear integer arithmetic (LIA)*, respectively, the latter also known as *Presburger arithmetic*. The expressiveness and computational complexity of these theories have been studied for decades. From the perspective of computational logic, an appealing aspect of arithmetic theories is a troika of decision procedure paradigms for both LRA and LIA: quantifier elimination procedures [12, 32, 36, 46], automata-based procedures [4, 5, 9, 47], and geometric (generator-based) procedures [6, 15].

The main focus of this paper is on the algorithmic and descriptional complexity of Boolean operations on sets definable in LRA and LIA and their geometric properties. The fact that both LRA and LIA admit quantifier elimination (in case of LIA in the extended structure with additional unary divisibility predicates $c \mid \cdot$ for all $c > 0$ [36]) immediately enables us to understand the geometry of the sets they define. For LRA, a quantifier-free formula is a Boolean combination of linear inequalities, and hence the sets definable in LRA are finite unions of copolyhedra, which are convex polyhedra possibly with some faces removed. We refer to such sets as $\mathbb{R}$*-semilinear sets*. The sets definable in LIA are commonly known as *semilinear sets*, which are finite unions of intersections of a convex polyhedron with an integer lattice.

Semilinear sets admit a generator representation as finite unions of *hybrid linear sets* [6, 15]. Given finite sets of *generators* $B, P \subseteq \mathbb{Z}^d$, the hybrid linear set $M \subseteq \mathbb{Z}^d$ (in dimension d) generated by B and P is the set

$$L(B, P) := \{\boldsymbol{b} + \lambda_1 \cdot \boldsymbol{p}_1 + \cdots + \lambda_k \cdot \boldsymbol{p}_k : \boldsymbol{b} \in B, k \geq 0, \lambda_i \in \mathbb{N}, \boldsymbol{p}_i \in P\}.$$

We call the hybrid linear sets constituting a semilinear set its *components*, and we denote by $\|M\|$ the maximum of 2 and the absolute values of all the numbers appearing in the generators. Analogously, by the Minkowski–Weyl theorem (see, e.g., [33, Thm. 2.8] or [40, Ch. 8]), rational convex polyhedra admit a generator representation $K(V, W) \subseteq \mathbb{R}^d$ as the sum of the convex hull of a finite set $V \subseteq \mathbb{Q}^d$ and a cone generated by another finite set $W \subseteq \mathbb{Q}^d$. The generator

representation of $\mathbb{R}$-semilinear sets are finite unions of copolyhedra, i.e., sets of the form $K(V,W) \setminus \big(K(V_1,W_1) \cup \cdots \cup K(V_n,W_n)\big)$, where all $K(V_i,W_i)$ are faces of $K(V,W)$. Since the components of $\mathbb{R}$-semilinear sets and semilinear sets are easily seen to be definable in LRA and LIA, respectively, it follows that they are effectively closed under projection along the coordinate axes and under all Boolean operations. Consequently, it is not difficult to see that ($\mathbb{R}$-)semilinear sets in generator representation can be employed in *geometric (generator-based) decision procedures* for LRA and LIA, respectively. Given a formula $\Phi(\boldsymbol{x}) \equiv \exists \boldsymbol{y}_1\, \forall \boldsymbol{y}_2 \cdots Q_n \boldsymbol{y}_n\, \Psi(\boldsymbol{x}, \boldsymbol{y}_1, \ldots \boldsymbol{y}_n)$, $Q_n \in \{\exists, \forall\}$, of LRA or LIA in prenex normal form, the idea is to transform Ψ into an ($\mathbb{R}$-)semilinear set and to then perform repeated complementation and projection steps to eliminate all $\boldsymbol{y}_i$ until a generator representation for the set of all $\boldsymbol{x}$ satisfying Φ is obtained.

Algorithms for Boolean operations on ($\mathbb{R}$-)semilinear sets given in generator representation have been investigated over the last 40 years. For the reals, generator-based decision procedures have seen early successes. E. Sontag [44] gave such a decision procedure for LRA with optimal complexity-theoretic upper bounds, in particular for a fixed number of quantifier alternations. Over the integers, however, the situation has been less satisfactory. D.T. Huynh [20, 21] was the first to use a geometric approach to show that the inclusion problem for explicitly given semilinear sets is in Π_2^{P} by establishing that the complement of a semilinear set, if non-empty, contains an element of polynomially bounded bit size. E. Kopczyński [25] generalised this result and furthermore showed that for (implicitly defined) semilinear sets $M, N \subseteq \mathbb{Z}^d$ in fixed dimension d, of n components each, only a subset of points of bit size $O(n \cdot \log(\|M\| + \|N\|))$ needs to be explored to decide the set inclusion $M \subseteq N$, which is hence in Π_2^{P} in this setting. Continuing this line of research, the first two authors of the present paper established that the maximum bit size of numbers in the generator representation of the complement of M can be bounded by $O(n \cdot d^4 \cdot \log\|M\|)$ [6]. Furthermore, S. Beier et al. [2] analysed the growth of numbers in S. Ginsburg and E.H. Spanier's seminal paper on the relationship between Presburger arithmetic and semilinear sets [14]. All the constructions and algorithms in this line of work so far lead to a non-elementary blow-up for repeated complementation of any given semilinear set. It has been a widely open problem whether there exists a complementation algorithm which, when interleaved with intersection and projection operations, results in an elementary procedure.

The first main contribution of this paper is to affirmatively settle this open problem in a general setting. We establish that a term in an algebra over semilinear sets consisting of Boolean operations and projection operations can be evaluated in triply exponential time. A consequence of this result is a generator-based decision procedure for Presburger arithmetic whose running time matches the triply exponential upper bounds of quantifier elimination and automata-based approaches [9, 32]. At the heart of our algorithm lies an algorithm for constructing a *splitter* for a semilinear set $M \subseteq \mathbb{Z}^d$. In a nutshell, this is a partition of $\mathbb{Z}^d$ into simple disjoint parts, such that inside each of them the set is easy to complement. These parts are all hybrid linear sets of the form $L(B,P)$. We control the number of periods P: for all of these parts combined, this number is upper bounded (in any fixed dimension d) by a polynomial of the same number for the original set M. Iteration of this bound leads to the aforementioned triply exponential bound.

Our second main contribution concerns the *Vapnik–Chervonenkis (VC) dimension* of Presburger arithmetic. The VC dimension is a core concept in computational learning theory and gives an upper bound on the sample complexity required to train a binary classifier, see e.g. [24]; we refer the reader to Section 6 for a formal definition. Y. Gurevich and P.H. Schmitt showed that every complete theory of ordered abelian groups, Presburger arithmetic being one, has finite VC dimension [16]. In the context of establishing bounds on the VC dimension of neural networks, M. Karpinski and A. Macintyre proposed a systematic study of concrete bounds on the VC dimension of various first-order theories [22, 23] and related concepts. This line of research has led to deep results in model theory, for instance, that every quasi-o-minimal structure has linear VC density [1]. Recently, D. Nguyen and I. Pak established polynomial upper bounds on the VC dimension of LIA with a fixed number of variables [30, Thm. 1.4], building upon a geometric approach for inferring properties of Boolean operations on semilinear sets [29]. The authors of [30] conjecture that it should be possible to establish a doubly exponential upper bound on the VC dimension of full LIA, but also remark that this is unlikely to be achieved by analysing quantifier elimination procedures because of known lower bounds on the growth of formula sizes in such procedures [45]. The second main contribution of our paper is to prove this conjecture, establishing singly and doubly exponential upper bounds on the VC dimension of LRA and LIA, respectively. The basis for these upper bounds are the bounds on the size and structure of ($\mathbb{R}$-)semilinear sets established in the first part of the paper.

2 PRELIMINARIES

Let $\mathbb{Z}$, $\mathbb{N}$, $\mathbb{Q}$, and $\mathbb{R}$ denote the set of integers, non-negative integers, rationals, and reals, respectively. We write $\mathbb{Q}_+$ and $\mathbb{R}_+$ to denote the non-negative part of $\mathbb{Q}$ and $\mathbb{R}$, respectively. Given $a, b \in \mathbb{Z}$, we define $[a,b] \coloneqq \{a, a+1, \ldots, b\}$. We denote by $\mathbf{0}$ and $\mathbf{1}$ the null vector and the vector with all components equal to 1, respectively, in any finite dimension.

For an arbitrary set S, we write $\#S$ for its cardinality. If S is infinite, then we write $\#S = \infty$. For sets of vectors S and T, we use the *Minkowski sum notation*: $S + T \coloneqq \{\boldsymbol{s} + \boldsymbol{t} : \boldsymbol{s} \in S, \boldsymbol{t} \in T\}$. We see sets of numbers as sets of one-dimensional vectors. We omit curly brackets when S (or alternatively T) is a singleton, and thus abbreviate $\{s\}+T$ to $s+T$. For a finite set of vectors $P = \{\boldsymbol{p}_1, \ldots, \boldsymbol{p}_n\}$ over a numerical domain, e.g. $P \subseteq \mathbb{R}^d$, we assume a lexicographic ordering on the elements of P and thus sometimes treat P as a matrix whose column vectors are its elements. Then, for instance, for $P \subseteq \mathbb{R}^d$ and $\boldsymbol{\lambda} \in \mathbb{R}^{\#P}$, the notation $P \cdot \boldsymbol{\lambda}$ denotes the product of the matrix P with $\boldsymbol{\lambda}$, and given a set $Q \subseteq \mathbb{R}^{\#P}$, $P \cdot Q \coloneqq \{P \cdot \boldsymbol{\lambda} : \boldsymbol{\lambda} \in Q\}$.

We write $\operatorname{rank} A$ for the rank of the matrix A, i.e., its maximal number of linearly independent columns (equiv., rows).

The binary logarithm function is denoted by $\log(\cdot)$.

Linear arithmetic theories. We assume basic familiarity with first-order logic. *Linear integer arithmetic (LIA)* and *linear real arithmetic (LRA)* are the first-order theories of the structures $\langle \mathbb{Z}, 0, 1, +, \leq \rangle$ and $\langle \mathbb{R}, 0, 1, +, \leq \rangle$, respectively. Formulae $\Phi, \Psi, \ldots$ from both theories

are formed by taking the closure of linear inequalities under binary Boolean connectives $\wedge, \vee$, negation $\neg$ and first-order quantification $\exists, \forall$. In a linear inequality $a_1 \cdot x_1 + \cdots + a_d \cdot x_d \leq b$, usually abbreviated as $\boldsymbol{a} \cdot \boldsymbol{x} \leq b$ where $\boldsymbol{a} = (a_1, \ldots, a_d)$ and $\boldsymbol{x} = (x_1, \ldots, x_d)$, all *coefficients* $a_1, \ldots, a_d$ and the *constant term* b are taken from $\mathbb{Z}$. In LIA, variables $\boldsymbol{x}$ are interpreted over $\mathbb{Z}$; in LRA they are interpreted over $\mathbb{R}$.

We write $[\![\Phi]\!]$ for the set of solutions of a formula Φ; it should always be clear from the context whether the interpretation $[\![.]\!]$ concerns LIA or LRA.

Linear algebra and geometry. The *linear span*, *cone*, *convex hull* and *affine hull* of a set $S \subseteq \mathbb{R}^d$ are defined as:

$$\operatorname{span} S := \left\{ T \cdot \boldsymbol{\lambda} \,:\, T \subseteq S,\ \#T \neq \infty,\ \boldsymbol{\lambda} \in \mathbb{R}^{\#T} \right\};$$

$$\operatorname{cone} S := \left\{ T \cdot \boldsymbol{\lambda} \,:\, T \subseteq S,\ \#T \neq \infty,\ \boldsymbol{\lambda} \in \mathbb{R}_+^{\#T} \right\};$$

$$\operatorname{conv} S := \left\{ T \cdot \boldsymbol{\lambda} \,:\, T \subseteq S,\ \#T \neq \infty,\ \boldsymbol{\lambda} \in \mathbb{R}_+^{\#T},\ \boldsymbol{\lambda} \cdot \mathbf{1} = 1 \right\};$$

$$\operatorname{aff} S := \left\{ T \cdot \boldsymbol{\lambda} \,:\, T \subseteq S,\ \#T \neq \infty,\ \boldsymbol{\lambda} \in \mathbb{R}^{\#T},\ \boldsymbol{\lambda} \cdot \mathbf{1} = 1 \right\}.$$

A nonempty subset of $\mathbb{R}^d$ is a *linear subspace* (alternatively a *vector subspace*) if it is closed under taking linear combinations of its elements. A subset of $\mathbb{R}^d$ is an *affine subspace* if it coincides with its affine hull; such sets have the form $\boldsymbol{v} + T$ where T is a linear subspace of $\mathbb{R}^d$. The *dimension* of an affine subspace A is the minimal number of vectors that spans it minus 1, i.e., the smallest k such that $A = \operatorname{aff} G$ and $\#G = k + 1$. The dimension does not exceed d. The dimension of an arbitrary non-empty set $S \subseteq \mathbb{R}^d$, written $\dim S$, is the dimension of its affine hull $\operatorname{aff} S$; and $\dim \emptyset := -1$. A *hyperplane* in $\mathbb{R}^d$ is an affine subspace of dimension $d - 1$.

We call sets of linearly independent vectors *proper*.

Polyhedral geometry. We refer the reader to [40, Ch. 7–8] and [33] for further background on the following concepts.

Let $S \subseteq \mathbb{R}^d$ be the set of solutions of a system of linear inequalities $\mathfrak{S}\colon A \cdot \boldsymbol{x} \leq \boldsymbol{c}$, $S \neq \emptyset$. Such sets are called *(closed) convex polyhedra*. A row $\boldsymbol{a} \cdot \boldsymbol{x} \leq c$ of $\mathfrak{S}$ is called an *implicit equality* of $\mathfrak{S}$ whenever $\boldsymbol{a} \cdot \boldsymbol{x} = c$ holds for every $x \in S$. Given $\boldsymbol{a} \neq \mathbf{0}$, the set of solutions in $\mathbb{R}^d$ of a single equation $\boldsymbol{a} \cdot \boldsymbol{x} = c$ is a hyperplane. The convex polyhedron $S \subseteq \mathbb{R}^d$ above is said to be *rational* whenever all entries of A and $\boldsymbol{c}$ are from $\mathbb{Q}$. Throughout the paper, we only consider convex polyhedra that are rational.

Given a nonzero vector $\boldsymbol{w} \in \mathbb{R}^d$ such that $\delta = \max\{\boldsymbol{w} \cdot \boldsymbol{x} : A \cdot \boldsymbol{x} \leq \boldsymbol{c}\}$ is finite, the hyperplane $\{\boldsymbol{x} : \boldsymbol{w} \cdot \boldsymbol{x} = \delta\}$ is called a *supporting hyperplane* of S. A set $F \subseteq \mathbb{R}^d$ is a *face* of S if $F = S$ or if F is the non-empty intersection of S with a supporting hyperplane of S. This means that $F \subseteq S$ is a face whenever there is some $\boldsymbol{w} \in \mathbb{R}^d$ for which F is the (non-empty) set of all points in S attaining $\max\{\boldsymbol{w} \cdot \boldsymbol{x} : \boldsymbol{x} \in S\}$, provided that this maximum is finite (possibly $\boldsymbol{w} = \mathbf{0}$). Alternatively, a face F of S is a nonempty subset of S such that $F = \{\boldsymbol{x} \in S : A' \cdot \boldsymbol{x} = \boldsymbol{c}'\}$ for some subsystem $A' \cdot \boldsymbol{x} \leq \boldsymbol{c}'$ of $\mathfrak{S}$.

Note that if $\mathfrak{S}$ has rational coefficients and right-hand sides then all vectors $\boldsymbol{w}$ in the previous paragraph lie in $\mathbb{Q}^d$.

A face F of S is said to be *minimal* whenever $F = \{\boldsymbol{x} \in \mathbb{R}^d : A' \cdot \boldsymbol{x} = \boldsymbol{c}'\}$ for some subsystem $A' \cdot \boldsymbol{x} \leq \boldsymbol{c}'$ of $\mathfrak{S}$. In fact, the minimal faces of S are exactly those faces of S that are affine subspaces.

For finite sets $V, W \in \mathbb{Q}^d$, define

$$K(V, W) := \operatorname{conv} V + \operatorname{cone} W\,.$$

The Minkowski–Weyl theorem (see, e.g., [33, Thm. 2.8] or [40, Ch. 8]) states that a set $S \subseteq \mathbb{R}^d$ is a rational convex polyhedron if and only if $S = K(V, W)$ for some $V, W \in \mathbb{Q}^d$. A set $C \subseteq \mathbb{R}^d$ is a *finitely generated shifted (rational) cone* whenever $C = K(\boldsymbol{v}, W)$ for some $\boldsymbol{v} \in \mathbb{Q}^d$ and finite $W \subseteq \mathbb{Q}^d$.

Given a system of inequalities $\mathfrak{S}$ with the set of its solutions S, we say that a set H of hyperplanes *carves out* S whenever for every row $\boldsymbol{a} \cdot \boldsymbol{x} \leq c$ of $\mathfrak{S}$ there is a hyperplane $h \in H$ with $h\colon \boldsymbol{a} \cdot \boldsymbol{x} = c$. Two comments are in order:

- S can be obtained by intersecting $\mathbb{R}^d$ with a subset of the half-spaces induced by H. Each $h\colon \boldsymbol{a} \cdot \boldsymbol{x} = c$ in H induces two half-spaces: $\boldsymbol{a} \cdot \boldsymbol{x} \geq c$ and $\boldsymbol{a} \cdot \boldsymbol{x} \leq c$;
- $\operatorname{aff} S$ can be obtained by intersecting $\mathbb{R}^d$ with a subset of the hyperplanes in H. This follows since $\operatorname{aff} S$ is the set of vectors satisfying all implicit equalities in $\mathfrak{S}$, see [40, Ch. 8].

We postulate that $H = \emptyset$ carves out $\mathbb{R}^d$.

Semilinear sets and $\mathbb{R}$-semilinear sets. Fix a natural number $d \geq 1$. A set $S \subseteq \mathbb{Z}^d$ is a (d-dimensional) *linear set* if it is of the form $S = L(\boldsymbol{b}, P) := \boldsymbol{b} + P \cdot \mathbb{N}^{\#P}$ for some *base* $\boldsymbol{b} \in \mathbb{Z}^d$ and a finite set of *periods* $P \subseteq \mathbb{Z}^d$. The set S is *hybrid linear* if it is of the form $S = L(B, P) := B + P \cdot \mathbb{N}^{\#P}$, where $B, P \subseteq \mathbb{Z}^d$ are finite sets. Notice that $L(B, P) = \bigcup_{\boldsymbol{b} \in B} L(\boldsymbol{b}, P)$, and thus every hybrid linear set is a union of finitely many linear sets sharing the same periods P. A *semilinear set* is a finite union of linear sets, i.e., represented as $\bigcup_{i \in I} L(B_i, P_i)$, where I is a finite set of indices.

Notice that every semilinear set $\bigcup_{i \in I} L(B_i, P_i) \subseteq \mathbb{Z}^d$ is equal to the set $[\![\Phi]\!]$, where

$$\Phi(\boldsymbol{x}) := \bigvee_{i \in I} \bigvee_{\boldsymbol{b} \in B_i} \exists \boldsymbol{y}_i : \boldsymbol{x} = \boldsymbol{b} + P_i \cdot \boldsymbol{y}_i \wedge \boldsymbol{y}_i \geq \mathbf{0}\,,$$

$\boldsymbol{x}$ is a vector of d variables and every $\boldsymbol{y}_i$ is a vector of $\#P_i$ fresh variables. Here, Φ is an LIA formula. Conversely, whenever Φ is an LIA formula, $[\![\Phi]\!]$ is a semilinear set [15].

A set $S \subseteq \mathbb{R}^d$ is an *$\mathbb{R}$-semilinear set* whenever it is of the form

$$S = \bigcup_{i \in I} \Big(K(V_i, W_i) \setminus \bigcup_{j \in J_i} K(V_j, W_j) \Big),$$

where I and J_i (for all $i \in I$) are finite sets and, for all $i \in I$ and $j \in J_i$, the polyhedron $K(V_j, W_j)$ is a face of $K(V_i, W_i)$. By the Minkowski–Weyl theorem and the definition of face of a polyhedron, each component $K(V_i, W_i) \setminus \bigcup_{j \in J_i} K(V_j, W_j)$ is the set of solutions of a system $A \cdot \boldsymbol{x} \leq \boldsymbol{c} \wedge B \cdot \boldsymbol{x} < \boldsymbol{d}$.

For every LRA formula Φ, the set $[\![\Phi]\!]$ is $\mathbb{R}$-semilinear. This is a consequence of, e.g., [44].

We remark that representing a convex polyhedron $K(V, W)$ by reference to V and W is standard and sometimes called "V-representation" (V stands for "vertex"), in contrast with the dual "H-representation" (H for "half-space") as a conjunction of linear inequalities. To capture LRA and LIA one must extend the V-representation to ($\mathbb{R}$-)semilinear sets. In the absence of a useful dual, we choose to use a different term, *generator representation*, to refer to the representation of ($\mathbb{R}$-)semilinear sets by explicit lists

of all members of generator sets B_i, P_i ($i \in I$) and V_i, W_i, V_j, W_j ($j \in J_i, i \in I$), respectively.

Magnitude and encoding of numbers. In this paper, the *(infinity) norm* of a vector $\boldsymbol{v} = (v_1, \ldots, v_d) \in \mathbb{R}^d$ is defined as $\|\boldsymbol{v}\| := \max\{2, |v_i| : i \in [1,d]\}$. This non-standard definition is for technical and presentational convenience only as it, e.g., prevents multiplication by 0 or 1 and ensures that $\|\boldsymbol{v}\|^n \geq 2^n$ for all $\boldsymbol{v}$ and $n \in \mathbb{N}$, when deriving bounds on the size of objects. For a matrix A, $\|A\|$ is the maximum norm of its columns. Similarly, for a finite set $W \subseteq \mathbb{R}^d$, we define $\|W\| := \max\{\|\boldsymbol{v}\| : \boldsymbol{v} \in W\}$.

For finite representations of infinite sets, we extend the notation $\|\cdot\|$ to refer to the maximum infinity norm of all numbers appearing in the representation of that set. For instance, given a semilinear set $M = \bigcup_{i \in I} L(B_i, P_i)$, we write $\|M\| := \max\{\|B_i\|, \|P_i\| : i \in I\}$.

Following [40, Sec. 3.2], given a rational number $\frac{p}{q}$ where p and $q \geq 1$ are relatively prime integers, we write

$$\langle \tfrac{p}{q} \rangle := 1 + \lceil \log_2(|p|+1) \rceil + \lceil \log_2(|q|+1) \rceil.$$

Intuitively, $\frac{p}{q}$ can be encoded in binary using $O(\langle \frac{p}{q} \rangle)$ bits. We extend this notation to rational matrices and finite sets of rational matrices. Given a matrix $A \in \mathbb{Q}^{n \times d}$, we denote $\langle A \rangle := \max\{\langle A[i,j] \rangle : i \in [1,n], j \in [1,d]\}$, where $A[i,j]$ is the rational number at the intersection of the i-th row and j-th column of A. Notice that the number of bits required to encode A is $O(n \cdot d \cdot \langle A \rangle)$. Similarly, for a finite set $W \subseteq \mathbb{Q}^d$ of rational vectors, $\langle W \rangle := \max_{\boldsymbol{v} \in W} \langle \boldsymbol{v} \rangle$. Our convention for the infinity norm for finite representations of infinite sets extends to the notation $\langle \cdot \rangle$. For instance, given a set $S = K(V, W) \subseteq \mathbb{R}^d$ with $V, W \subseteq \mathbb{Q}^d$, we write $\langle S \rangle := \max\{\langle V \rangle, \langle W \rangle\}$.

Given a formula Φ of LIA or LRA, we write $\langle \Phi \rangle$ for the maximal $\langle c \rangle$ for a coefficient or constant c appearing in a linear inequality of Φ. The *length* of a formula is the number of symbols required to write it down, assuming binary encoding of numbers.

3 OPERATIONS ON POLYHEDRA AND THEIR REPRESENTATION

In this section, we identify a set of technical tools from polyhedral geometry that we use for establishing our main results. We mostly recall such results and provide bounds on algorithms and descriptional complexity when necessary.

Change of representation over $\mathbb{R}$. We need to move between the representations of polyhedra as solutions to systems of (in)equalities and as sets of the form $K(V, W)$.

Proposition 3.1. *Let $S = K(V, W)$, with $V, W \subseteq \mathbb{Q}^d$ finite sets. There is a system of linear inequalities $\mathfrak{S}\colon A \cdot \boldsymbol{x} \leq \boldsymbol{c}$ whose set of solutions is S and such that*

- *$A \in \mathbb{Q}^{n \times d}$ with $n \leq (\#V + \#W)^d + 2d$;*
- *$\langle A \rangle, \langle \boldsymbol{c} \rangle \leq O(d^2) \cdot \langle S \rangle$.*

The system $\mathfrak{S}$ can be computed in time $(\#V + \#W)^d \cdot \mathrm{poly}(d, \langle S \rangle)$.

We also rely on further results of this kind, omitted here for brevity. These are all underpinned by the fact that Gaussian elimination over $\mathbb{Q}$ in dimension d can be carried out in time polynomial in the size of the matrix and bit size of its entries; see, e.g., [40, Sec. 3.3].

Membership and representation results over $\mathbb{Z}$ *and* $\mathbb{N}$. The following lemma gives an algorithm to decide membership in a semilinear set.

Lemma 3.2. *Let $\boldsymbol{v} \in \mathbb{Z}^d$ and $M = L(B, P) \subseteq \mathbb{Z}^d$. Deciding $\boldsymbol{v} \in M$ can be done in time $\mathrm{poly}(d^d, \langle \boldsymbol{v} \rangle, (\|B\| + \#P \cdot \|P\|)^d)$.*

We recall a discrete version of Carathéodory's theorem.

Proposition 3.3 ([6, Prop. 5]). *Let $S = L(B, P) \subseteq \mathbb{Z}^d$ be a hybrid linear set. Then $S = \bigcup_{i \in I} L(C_i, Q_i)$ where*

- *$\#I \leq (\#P)^d$; $\max_{i \in I} \|C_i\| \leq \|B\| + (\#P \cdot \|P\|)^{O(d)}$; and*
- *for all $i \in I$, $Q_i \subseteq P$ and Q_i is proper.*

The family $\{(C_i, Q_i)\}_{i \in I}$ can be computed in time

$$O(\#B \cdot (d \cdot \#P \cdot \|P\|)^{d+1}).$$

The following lemma shows that, when represented as a hybrid linear set, the set of non-negative solutions of a homogeneous system of linear equations has few periods. Its proof relies on a characterisation of such sets of solutions due to E. Domenjoud [8].

Lemma 3.4. *Let $S \subseteq \mathbb{N}^d$ be the set of all non-negative integer solutions of $\mathfrak{S}\colon A \cdot \boldsymbol{x} = 0$, with $A \in \mathbb{Z}^{n \times d}$. Then $S = L(B, P)$ such that $\langle B \rangle, \langle P \rangle \leq O(n \cdot d^3) \cdot \langle A \rangle$, $\#P \leq d^{k+1}$, where $k = \operatorname{rank} A$; and B and P can be computed in time $\mathrm{poly}(d^{k+1}, \|A\|^{n \cdot k^3})$.*

An equivalence relation induced by hyperplanes. Consider a set of rational hyperplanes $H = \{h_1, \ldots, h_n\}$ given by n equations $h_i : \boldsymbol{a}_i \cdot \boldsymbol{x} = c_i$ in d variables. Let $\sim_H \subseteq \mathbb{R}^d \times \mathbb{R}^d$ be the equivalence relation defined as

$$\boldsymbol{x}_1 \sim_H \boldsymbol{x}_2 \text{ iff, for all } i \in [1,n], \operatorname{sgn}(\boldsymbol{a}_i \cdot \boldsymbol{x}_1 - c_i) = \operatorname{sgn}(\boldsymbol{a}_i \cdot \boldsymbol{x}_2 - c_i),$$

where $\operatorname{sgn}\colon \mathbb{R} \to \{-1, 0, 1\}$ is the *sign function*: $\operatorname{sgn}(0) := 0$, $\operatorname{sgn}(r) := -1$ for $r < 0$, and $\operatorname{sgn}(r) := 1$ for $r > 0$.

We recall a folklore result on the number of regions induced by H on $\mathbb{R}^d$ (cf. [28, Ch. 6]).

Proposition 3.5. *For every set H of n hyperplanes in $\mathbb{R}^d$, the relation $\sim_H$ has at most $(2n)^d + 1$ many equivalence classes.*

Polyhedral complexes and triangulations. A *polyhedral complex* is a finite set $\mathcal{R}$ of convex polyhedra that satisfies the following two properties:

- for every face R' of every $R \in \mathcal{R}$, $R' \in \mathcal{R}$;
- for every $R_1, R_2 \in \mathcal{R}$, either $R_1 \cap R_2 = \emptyset$ or $R_1 \cap R_2$ is a face of both R_1 and R_2.

The following definitions and statements about generalised simplices, triangulations and half-openings are only required for our construction of $\mathbb{Z}$-splitters (Sec. 4.3) and can be skipped at the first reading.

A *generalised m-dimensional simplex* is a set $T = K(V, W)$ where $V, W \subseteq \mathbb{Q}^d$ are such that $\#V + \#W = m + 1$ and $\dim(\mathrm{aff}\, T) = m$. For example, two-dimensional generalised simplices are triangles, closed half-infinite strips, and closed infinite sectors [38, Sec. 17].

A *triangulation* is a polyhedral complex $\mathcal{T}$ where every $T \in \mathcal{T}$ is a generalised simplex and all $T \in \mathcal{T}$ that are not a face of any $T' \in \mathcal{T} \setminus \{T\}$ have the same dimension m. The latter T are called the maxima of $\mathcal{T}$, and we write $\dim \mathcal{T} = m$. Given $S \subseteq \mathbb{R}^d$, we say that $\mathcal{T}$ is a *triangulation of S* whenever $S = \bigcup_{T \in \mathcal{T}} T$.

Proposition 3.6. *Every convex polyhedron $K(V,W) \subseteq \mathbb{R}^d$ has a triangulation $\mathcal{T}$ such that for every $T \in \mathcal{T}$, $T = K(V',W')$ for some $V' \subseteq V$ and $W' \subseteq W$. The triangulation $\mathcal{T}$ can computed in time $(\#V + \#W)^{O(d)} \cdot \mathrm{poly}(d, \langle V\rangle + \langle W\rangle)$.*

Let $S \subseteq \mathbb{R}^d$ be a rational polyhedron given as the set of solutions of a system $\mathfrak{S}\colon A \cdot \boldsymbol{x} \leq \boldsymbol{b}$. A *half-opening* of S is a set of the form $S^{\mathrm{op}} = \{\boldsymbol{x} \in S : A' \cdot \boldsymbol{x} < \boldsymbol{b}'\}$ for some subsystem $A' \cdot \boldsymbol{x} \leq \boldsymbol{b}'$ of $\mathfrak{S}$.

The following proposition is a version of [6, Lem. 10], slightly strengthened to accommodate the case of non-integer vectors in the set of base vectors V.

Proposition 3.7. *Let $S = K(V,W)$ where $V \subseteq \mathbb{Q}^d$, $W \subseteq \mathbb{Z}^d$, $\#V + \#W \leq d+1$ and W is proper. Then $S^{\mathrm{op}} \cap \mathbb{Z}^d = L(B,W)$ for any half-opening S^{op} of S, and $\|B\| \leq \|V\| + 2d \cdot \|W\|$. The set B can be computed in time $(\|V\| + \|W\|)^{O(d)}$.*

Let $\mathcal{T}$ be a triangulation of some polyhedron $P \subseteq \mathbb{R}^d$. We define the *maximal half-opening* $\mathcal{T}^{\mathrm{op}}$ of $\mathcal{T}$ as the smallest set containing all finite $T \in \mathcal{T}$ and for every infinite $T \in \mathcal{T}$ given by $\mathfrak{T}\colon A \cdot \boldsymbol{x} \leq \boldsymbol{c}$ the half-opening given by $\mathfrak{T}'\colon A \cdot \boldsymbol{x} < \boldsymbol{c}$.

Intuitively, if P is a generalised simplex itself, then $\mathcal{T}^{\mathrm{op}}$ contains, for each face F of P, the relative interior of that face (i.e., the set difference of F and all its proper sub-faces). This extends to the general case, enumerating all $F \in \mathcal{T}$. We remark that in the definition above, since each $T \in \mathcal{T}$ is a generalised simplex, it cannot contain any line (affine subspace of dimension 1), so T is finite if and only if T is a minimal face of $\mathcal{T}$.

Proposition 3.8. *Let $\mathcal{T}$ be a triangulation and $\mathcal{T}^{\mathrm{op}}$ its maximal half-opening. Then $\bigcup_{T^{\mathrm{op}} \in \mathcal{T}^{\mathrm{op}}} T^{\mathrm{op}} = \bigcup_{T \in \mathcal{T}} T$ and, for all distinct $T_1^{\mathrm{op}}, T_2^{\mathrm{op}} \in \mathcal{T}^{\mathrm{op}}$, $T_1^{\mathrm{op}} \cap T_2^{\mathrm{op}} = \emptyset$.*

4 SPLITTERS

In this section we present geometric constructions that are at the core of our main results. We start with the setting of $\mathbb{R}$-semilinear sets and later move to the integer case.

Splitters in $\mathbb{R}^d$. Let us first fix $M = \bigcup_{i\in I} K(V_i, W_i) \subseteq \mathbb{R}^d$. Our overall goal here is to characterise the complement $\overline{M}$ of the set M as a union of polyhedra. To do this, we construct a partition of $\mathbb{R}^d$ induced by M, in the sense captured by the following definition, and study the descriptional and computational complexity of this construction.

Given a family $\mathcal{P}$ of polyhedra in $\mathbb{R}^d$, a *splitter* for $\mathcal{P}$ is any polyhedral complex $\mathcal{R} = \{R_1, \ldots, R_m\}$ that satisfies the following two properties:

(S1) for all $R \in \mathcal{R}$ and all $P \in \mathcal{P}$, the set $R \cap P$ is either empty or equal to a face of R; and
(S2) $R_1 \cup \cdots \cup R_m = \mathbb{R}^d$.

We remark that, as every polyhedron is a face of itself, condition (S1) is satisfied if in particular $R \subseteq P$. Abusing notation slightly, we will talk about splitters for a *union* of convex polyhedra (making the *family* of polyhedra implicit).

In the theorem below, recall that $\langle M\rangle := \max_{i\in I}\langle K(V_i,W_i)\rangle$.

Theorem 4.1 (splitters for unions of polyhedra). *Given any $\mathbb{R}$-semilinear set $M = \bigcup_{i\in I} K(V_i,W_i) \subseteq \mathbb{R}^d$, there exists a splitter $\mathcal{R} = \{R_1, \ldots, R_m\}$ for M that has the following properties:*

(i) for each $j \in J := [1,m]$ we have $R_j = K(C_j, Q_j)$ where $C_j, Q_j \subseteq \mathbb{Q}^d$ and $\langle C_j\rangle, \langle Q_j\rangle \leq O(d^5) \cdot \langle M\rangle$; and
(ii) $m, \#(\bigcup_{j\in J} C_j), \#(\bigcup_{j\in J} Q_j) \leq (\#I \cdot \max_{i\in I}(\#V_i + \#W_i) + d)^{O(d^2)}$.

The family $\{(C_j, Q_j)\}_{j\in J}$ can be computed from M in time

$$(\#I \cdot \max_{i\in I}(\#V_i + \#W_i + 1))^{O(d^2)} \cdot \mathrm{poly}(\langle M\rangle).$$

We describe the proof idea for Theorem 4.1 in Section 4.1.

While Theorem 4.1 will be useful to us when we deal with operations on $\mathbb{R}$-semilinear sets, it is not sufficient as it is to support our constructions for sets inside $\mathbb{Z}^d$. Intuitively, the reason for this is that, in the presence of polyhedra $K(V_i, W_i)$ with large $\#V_i$, the splitter for the union M will have to "respect" many hyperplanes that pass through various subsets of V_i. These hyperplanes will be irrelevant if we view the set $M = \bigcup_{i\in I} K(V_i,W_i)$ as an overapproximation of the semilinear set $\bigcup_{i\in I} L(V_i,W_i)$: the latter is simply the union of many sets of the form $L(\boldsymbol{v}, W_i)$, and, roughly speaking, there is no "interaction" between different elements of the same set V_i. This motivates the following refinement of Theorem 4.1.

Theorem 4.2 (splitters for unions of cones). *Given any $\mathbb{R}$-semilinear set of the form $N = \bigcup_{i\in I}\bigcup_{\boldsymbol{v}\in V_i} K(\boldsymbol{v}, W_i) \subseteq \mathbb{R}^d$, there is a splitter $\mathcal{R}' = \{R'_1, \ldots, R'_t\}$ for N that has the following properties:*

(i) for each $j \in J := [1,t]$, $R'_j = K(E_j, F_j)$ where $E_j \subseteq \mathbb{Q}^d$, $F_j \subseteq \mathbb{Z}^d$, $\langle E_j\rangle \leq O(d^5) \cdot \langle N\rangle$, $\langle F_j\rangle \leq O(d^6) \cdot \max_{i\in I}\langle W_i\rangle$;
(ii) $\#(\bigcup_{j\in J} F_j) \leq (\#I \cdot \max_{i\in I} \#W_i + d)^{O(d^2)}$; and
(iii) $t, \#(\bigcup_{j\in J} E_j) \leq (\#I \cdot \max_{i\in I} \#V_i \cdot \max_{i\in I}(1 + \#W_i) + d)^{O(d^2)}$.

The family $\{(E_j, F_j)\}_{j\in J}$ can be computed from N in time

$$(\#I \cdot \max_{i\in I}(\#V_i + \#W_i + 1))^{O(d^2)} \cdot \mathrm{poly}(\langle N\rangle).$$

While some of the bounds of Theorem 4.2 follow directly from the previous theorem, there are several differences, of which we highlight one. The upper bound on $\#(\bigcup_{j\in[1,t]} F_j)$ is independent of the cardinality and norms of sets V_i; controlling the number of cone generators is crucial for the triply exponential running time bound of our decision procedure for Presburger arithmetic.

Splitters in $\mathbb{Z}^d$. Moving from $\mathbb{R}$ to $\mathbb{Z}$, let us fix a semilinear set $M = \bigcup_{i\in I} L(B_i, P_i) \subseteq \mathbb{Z}^d$. We will need an integer analogue of splitters, partitioning $\mathbb{Z}^d$ into disjoint regions that are in some sense induced by M.

Given a family $\mathcal{M} = \{L(B_i,P_i)\}_{i\in I}$ of hybrid linear sets in $\mathbb{Z}^d$, a *$\mathbb{Z}$-splitter* for $\mathcal{M}$ is any family of sets $\mathcal{Z} = \{Z_1, \ldots, Z_m\}$ that satisfies the following four properties for all $j \in [1,m]$:

(Z1) $Z_j = L(C_j, Q_j)$ for some $C_j, Q_j \subseteq \mathbb{Z}^d$ with Q_j proper;
(Z2) $Z_j \subseteq K(\boldsymbol{b}, P_i)$ or $Z_j \cap K(\boldsymbol{b}, P_i) = \emptyset$, for all $i \in I$, $\boldsymbol{b} \in B_i$;
(Z3) for all $i \in I$, $\boldsymbol{b} \in B_i$, if $Z_j \subseteq K(\boldsymbol{b}, P_i)$ then $Q_j \subseteq L(\boldsymbol{0}, P_i)$;
(Z4) $Z_1 \cup \cdots \cup Z_m = \mathbb{Z}^d$, where the union is disjoint.

As above, we will abuse notation and talk about $\mathbb{Z}$-splitters for a semilinear set M, implying the family of hybrid linear sets to be the set of components of M in a given representation. We show the following theorem:

Theorem 4.3 (splitters for semilinear sets). *Given any semilinear set $M = \bigcup_{i\in I} L(B_i, P_i) \subseteq \mathbb{Z}^d$, there exists a $\mathbb{Z}$-splitter $\mathcal{Z} = \{Z_1, \ldots, Z_m\}$ for M that has the following properties:*

(i) for all $j \in J := [1, m]$ and $Z_j = L(C_j, Q_j)$, we have $\|C_j\| \le \|M\|^{O(d^{10})\cdot \#I}$ and $\|Q_j\| \le \max_{i\in I} \|P_i\|^{O(d^{10})\cdot \#I}$;

(ii) $\#(\bigcup_{j\in J} Q_j) \le (\#I \cdot \max_{i\in I} \#P_i + d)^{O(d^2)}$; and

(iii) $m \le (\#I \cdot \max_{i\in I} \#B_i \cdot (1 + \max_{i\in I} \#P_i))^{O(d^3)}$.

The family $\{(C_j, Q_j)\}_{j\in J}$ can be computed from M in time

$$(\max_{i\in I}(\#B_i + \#P_i) + \|M\|)^{O(d^{11})\cdot \#I}.$$

Observe that, while $\|Q_j\|$ may be exponential in $\#I$, the number of different vectors across all Q_j is comparably small and bounded, in any fixed dimension d, by a polynomial in $\#I \cdot \max_{i\in I} \#P_i$. The proof of Theorem 4.3 invokes the construction of splitter for a union of cones (Theorem 4.2), decomposes each atomic polyhedron (see Sec. 4.1) further and intersects parts of the decomposition with $\mathbb{Z}^d$.

Importantly, Theorem 4.3 benefits from the refined bounds of Theorem 4.2 to control the cardinality of $\bigcup_{j\in J} Q_j$. This turns out to be possible even though the dependency of $\|Q_j\|$ on $\#I$ is exponential, roughly speaking because (Z3) effectively forces an intersection of up to $\#I$ hybrid linear sets. As mentioned previously, our upper bound on the total number of periods (coming from the splitters) is the key to an elementary decision procedure.

4.1 Splitters for unions of polyhedra: sketch

We sketch the proof of Theorem 4.1. Let $i \in I$. We start by considering a set of hyperplanes $\mathcal{H}(V_i, W_i)$ that carves out $K(V_i, W_i)$, of which we characterise the descriptional complexity. By Proposition 3.1, there exists such a set of hyperplanes $\mathcal{H}(V_i, W_i)$, respecting the following bounds:

$$\begin{aligned} \#\mathcal{H}(V_i, W_i) &\le (\#V_i + \#W_i)^d + 2d\,; \\ \langle \mathcal{H}(V_i, W_i)\rangle &\le O(d^2)\cdot \langle K(V_i, W_i)\rangle\,. \end{aligned} \tag{$*$}$$

The left-hand side of the second equation in ($*$) refers to the maximum $\langle\cdot\rangle$ measure of numbers appearing in the linear equations defining these hyperplanes. The set of hyperplanes in $\mathcal{H}(M) := \bigcup_{i\in I} \mathcal{H}(V_i, W_i)$ divides $\mathbb{R}^d$ into regions that we call *atomic polyhedra*. More precisely, for $\mathcal{H}(M) = \{h_1, \ldots, h_k\}$ with $h_i : \boldsymbol{a_i}\cdot\boldsymbol{x} = c_i$, an atomic polyhedron R induced by $\mathcal{H}(M)$ associates to every h_i a set H_i that is the set of solutions to $\boldsymbol{a_i}\cdot\boldsymbol{x} \sim c_i$ for some $\sim \in \{\le, =, \ge\}$ such that R is the intersection $R = \bigcap_{1\le i\le m} H_i$. Let $R_1, \ldots, R_m$ be the family of all atomic polyhedra induced by $\mathcal{H}(M)$.

We first show that polyhedra $R_1, \ldots, R_m$ form a polyhedral complex. Indeed, by our definition of atomic polyhedra, $\{R_1, \ldots, R_m\}$ is closed under taking faces of polyhedra. This is due to the characterisation of faces using systems of equations, recalled in Sec. 2. To see the closure under intersection, whenever for some $j, k \in [1, m]$ the set $R_j \cap R_k$ is non-empty and different from R_j, we note that $R_j \cap R_k$ can be obtained as the intersection of R_j with some hyperplanes specified by equations of the form $\boldsymbol{a_i}\cdot\boldsymbol{x} = \boldsymbol{c_i}$, and thus forms a face of R_j. Thus, $\{R_1, \ldots, R_m\}$ is a polyhedral complex.

We next show that this family is a splitter for $\{K(V_i, W_i)\}_{i\in I}$. Property (S2), i.e., the equality $R_1 \cup \cdots \cup R_m = \mathbb{R}^d$, is immediate. Property (S1) follows from the definition of atomic polyhedra and the definition of $\mathcal{H}(M)$. Indeed, take some R_j and $P_i = K(V_i, W_i)$. Suppose $R_j \cap P_i$ is nonempty and different from R_j; we show that it must be a face of R_j. We know that, for each $h \in \mathcal{H}(M)$, all points of R_j lie on the same side of h, in the non-strict sense; or possibly even on h itself. Recall that $P_i = K(V_i, W_i)$ is a convex polyhedron and, as such, is the set of solutions to a conjunction of affine inequalities, all represented by constraints of the form $\boldsymbol{a_i}\cdot\boldsymbol{x} \sim c_i$, for $\sim \in \{\le, =, \ge\}$ and some $h_i : \boldsymbol{a_i}\cdot\boldsymbol{x} = c_i$ with $h_i \in \mathcal{H}(M)$. Hence, each of these inequalities either is valid for all points of the set R_j, or is violated at all these points, or restricts R_j to some non-empty face. Since an intersection of faces is itself a face, we conclude that $R_j \cap P_i$ is a face of R_j.

Towards checking the satisfaction of the two properties required by Theorem 4.1, note that from Proposition 3.5 together with Eqs. ($*$) we conclude that the number m of atomic polyhedra is bounded by $(\#I \cdot \max_{i\in I}(\#V_i + \#W_i))^{O(d^2)}$, as required by Property (ii). What is left is to study the descriptional complexity of atomic polyhedra: prove that they satisfy Property (i) and show that the sets of bases and periods required to describe all atomic polyhedra satisfy the bound in Property (ii). We leave this part out for space reasons.

4.2 Splitters for unions of cones: idea

The proof of Theorem 4.2 is left out for space reasons. Our construction refines the analysis of Theorem 4.1 for the case of sets N, where polyhedra are cones, but big groups of these cones share periods. This analysis is possible because, intuitively, supporting hyperplanes for cones from a union $\bigcup_{\boldsymbol{v}\in V_i} K(\boldsymbol{v}, W_i)$ are translates of one another.

4.3 Splitters for semilinear sets: sketch

We sketch the proof of Theorem 4.3. We start with a semilinear set $M = \bigcup_{i\in I} L(B_i, P_i)$. We first apply Theorem 4.2 to obtain a splitter for the union of cones $\bigcup_{i\in I}\bigcup_{\boldsymbol{b}\in B_i} K(\boldsymbol{b}, P_i)$. Let the obtained splitter be $\mathcal{A} = \{R_1, \ldots, R_t\}$ with $R_j = K(E_j, F_j)$. We further split these polyhedra to obtain a $\mathbb{Z}$-splitter. Define $F := \bigcup_{j\in[1,t]} F_j$, recalling that $F \subseteq \mathbb{Z}^d$ by Property (i) in Theorem 4.2. The set F enjoys the bound from Property (ii) in the same theorem.

In order to satisfy the property (Z3) in the definition of $\mathbb{Z}$-splitter, we scale each vector in F using the lemma below.

Lemma 4.4. *For each $\boldsymbol{p} \in F$ there is an integer $\lambda \ge 0$ such that $\langle\lambda\rangle \le \#I \cdot O(d^{10}) \cdot \max_{i\in I}\langle P_i\rangle$ and, for all $i \in I$, if $\boldsymbol{p} \in \operatorname{cone} P_i$ then $\lambda\cdot\boldsymbol{p} \in L(\boldsymbol{0}, P_i)$. This λ can be computed in time*

$$((\#I)^2 + \sum_{i\in I} (\#P_i)^{d+1}) \cdot \operatorname{poly}(d, \max_{i\in I}\langle P_i\rangle, \langle\boldsymbol{p}\rangle).$$

Below, we write $\widehat{F}$ for the set $\{\lambda_{\boldsymbol{p}}\cdot\boldsymbol{p} : \boldsymbol{p} \in F\}$, where $\lambda_{\boldsymbol{p}}$ is the integer obtained from Lemma 4.4 for the vector $\boldsymbol{p}$. The following lemma partitions $\mathbb{Z}^d$ into hybrid linear sets with periods from $\widehat{F}$. Taking the splitter $\mathcal{A}$ computed above, we let $\mathcal{A}_k = \{A \in \mathcal{A} : \dim A \le k\}$ and notice that $\mathcal{A} = \mathcal{A}_d$.

Lemma 4.5. *For every $k \in [0, d]$ there is a finite collection C_k of subsets of $\mathbb{R}^d$ such that*

(i) all sets in C_k are pairwise disjoint;

(ii) $\#C_k \le \#\mathcal{A}_k \cdot (\#I \cdot \max_{i\in I} \#B_i \cdot (1 + \max_{i\in I} \#P_i) + d)^{O(d^3)}$;

(iii) $\bigcup_{A\in\mathcal{A}_k} A = \bigcup_{C\in C_k} C$;
(iv) for every $C \in C_k$, *we have* $C \cap \mathbb{Z}^d = L(D, Q)$ *where* $\|D\| \le \|M\|^{O(d^{10})\cdot \#I}$, $Q \subseteq \widehat{F}$, *and* Q *is proper; and*
(v) for every $C \in C_k$ *there is* $A \in \mathcal{A}_k$ *such that* $C \subseteq A$.

Overall, all the sets D *and* Q *required to represent* $C_0, \ldots, C_d$ *can be computed in time* $(\max_{i\in I}(\#B_i + \#P_i) + \|M\|)^{O(d^{11})\cdot \#I}$.

Proof (sketch). We use induction on $k \le d$. In the induction base case $k = 0$, we set $C_0 = \mathcal{A}_0$, the latter being a finite set of points. For the induction step, C_{k+1} contains C_k and is further populated as follows. For every $A \in \mathcal{A}_{k+1} \setminus \mathcal{A}_k$, let $\mathcal{T}$ be a triangulation of A, and let $\mathcal{T}^{\mathrm{op}}$ be the maximal half-opening of $\mathcal{T}$. We add to C_{k+1} every $T^{\mathrm{op}} \in \mathcal{T}^{\mathrm{op}}$ that is not fully contained in some $A' \in \mathcal{A}_k$.

We show that the resulting set has Property (iv), skipping the other properties for space reasons. Recall that every polyhedron $A \in \mathcal{A}$ has a representation $K(E_j, F_j)$, where $F_j \subseteq F \subseteq \mathbb{Z}^d$, and $E_j \subseteq \mathbb{Q}^d$ is such that $\langle E_j\rangle \le O(d^5)\cdot\langle M\rangle$. By definition of $\widehat{F}$ and following Lemma 4.4, there is $F'_j \subseteq \widehat{F} \subseteq \mathbb{Z}^d$ such that $\#F'_j = \#F_j$, $\langle F'_j\rangle \le \#I\cdot O(d^{10})\cdot\max_{i\in I}\langle P_i\rangle$ and $A = K(E_j, F'_j)$. Then Property (iv) follows by computing the triangulation of $K(E_j, F'_j)$ with Proposition 3.6 and by applying Proposition 3.7. An observation: when applying Proposition 3.7, we consider the infinity norm of bases and period, instead of their bit length. The relation between bit length and infinity norm is simple: for every rational number $\frac{p}{q}$ with p and $q \ge 1$ relatively prime integers, if $\langle\frac{p}{q}\rangle \le \alpha$ then $\|\frac{p}{q}\| \le 2^{O(\alpha)}$, as $\|\frac{p}{q}\| \le \|p\| \le 2^{O(\langle p\rangle)}$ and $\langle p\rangle \le \langle\frac{p}{q}\rangle$. □

Once Lemma 4.5 is in place, in order to show Theorem 4.3 it suffices to pick $\mathcal{Z} = \{C \cap \mathbb{Z}^d : C \in C_d\}$.

5 SEMILINEAR AND $\mathbb{R}$-SEMILINEAR EXPRESSIONS

In this section, we define an algebra of ($\mathbb{R}$-)semilinear sets comprising all Boolean operations with projections along the coordinate axes and show that expressions in this algebra can be evaluated in doubly and triply exponential time over the reals and integers, respectively. To this end, consider the grammar

$$s ::= a \mid \pi_D(s) \mid \overline{s} \mid s \cap s \mid s \cup s,$$

where a are *atoms* to be defined below, and D can be any finite subset of positive integers.

A *semilinear expression* is an expression from the above grammar where atoms are hybrid linear sets. Whenever possible, we endow a semilinear expression s with a *dimension* $d \in \mathbb{N}$, written below as "$s : d$" and given by the typing rules

$$\frac{L(B,P) \subseteq \mathbb{Z}^d}{L(B,P) : d} \qquad \frac{s : d \quad D \subseteq [1,d]}{\pi_D(s) : d - \#D} \qquad \frac{s : d}{\overline{s} : d} \qquad \frac{s_1 : d \quad s_2 : d}{s_1 \oplus s_2 : d}$$

where $\oplus \in \{\cap, \cup\}$. Expressions that comply with the type assertions above are *well-formed*, and we restrict ourselves subsequently to well-formed expressions.

A well-formed semilinear expression $s : d$ evaluates to a subset $[\![s]\!] \subseteq \mathbb{Z}^d$ following the standard semantics where the symbols $\cup$, $\cap$ and $\bar{\cdot}$ denote the Boolean operations union, intersection and complement, respectively, and $\pi_D(\cdot)$ is the function projecting away the coordinates indexed by all $i \in D$. By convention, the coordinates in $\mathbb{Z}^d$ are indexed 1 through d.

Analogously, we define $\mathbb{R}$-*semilinear expressions* in which atoms are rational closed convex polyhedra given as $K(V, W)$.

For an ($\mathbb{R}$-)semilinear expression s, we write

- $d(s)$ for the *maximal dimension* of atoms in s;
- $h(s)$ for the *height* of s, i.e., the maximum nesting depth of operations appearing in s; and
- $\langle s\rangle$ for the maximal $\langle a\rangle$ of an atom a appearing in s.

When s is a semilinear expression, $n_{\mathrm{p}}(s)$ (*number of periods*) denotes the maximal cardinality of P of a hybrid linear set $L(B, P)$ appearing as an atom of s. When s is an $\mathbb{R}$-semilinear expression, $n_{\mathrm{g}}(s)$ (*number of generators*) denotes the maximal cardinality of $V \cup W$ for a convex polyhedron $K(V, W)$ appearing as an atom of s.

Theorem 5.1. *There is an algorithm that, given a well-formed semilinear expression* s, *computes a family* $\{(B_i, P_i)\}_{i\in I}$ *such that* $[\![s]\!] = \bigcup_{i\in I} L(B_i, P_i)$. *Let* $n = n_{\mathrm{p}}(s)$, $d = d(s)$ *and* $h = h(s)$. *Assume* $d, n \ge 2$; *the algorithm ensures*

$$\#I \le n^{d^{O(h)}}; \quad \langle B_i\rangle, \langle P_i\rangle \le (\langle s\rangle + n)^{d^{O(h)}}; \quad P_i \text{ proper.}$$

The algorithm runs in time $\exp((\langle s\rangle + n)^{d^{O(h)}})$.

As a consequence, we obtain a triply exponential geometric decision procedure for Presburger arithmetic, matching the optimal running time of quantifier elimination and automata-based decision procedures [9, 32]. Below, given a formula Φ of LIA or LRA, we write $d(\Phi)$ for the maximum number of free variables appearing in a subformula of Φ, and $h(\Phi)$ for the maximum nesting depth of binary Boolean connectives, negations and quantifications appearing in Φ.

Corollary 5.2. *There is an algorithm that, given a formula* Φ *of LIA, computes a family* $\{(B_i, P_i)\}_{i\in I}$ *such that* $[\![\Phi]\!] = \bigcup_{i\in I} L(B_i, P_i)$. *Let* $d = d(\Phi)$ *and* $h = h(\Phi)$. *Assume* $d \ge 2$; *the algorithm ensures*

$$\#I \le 2^{d^{O(h)}}; \quad \langle B_i\rangle, \langle P_i\rangle \le (\langle\Phi\rangle + 2)^{d^{O(h)}}; \quad P_i \text{ proper.}$$

The algorithm runs in time $\exp((\langle\Phi\rangle + 2)^{d^{O(h)}})$.

We establish analogous results for $\mathbb{R}$-semilinear expressions and formulae of LRA where the running time and bounds on the constants is one exponential lower.

Theorem 5.3. *There is an algorithm that, given a well-formed* $\mathbb{R}$-*semilinear expression* s, *computes a family of triples* $\{(U_k, Y_k, \{(U_\ell, Y_\ell)\}_{\ell\in L_k})\}_{k\in K}$ *such that* $[\![s]\!] = \bigcup_{k\in K}\big(K(U_k, Y_k) \setminus \bigcup_{\ell\in L_k} K(U_\ell, Y_\ell)\big)$. *Let* $d = d(s)$, $h = h(s)$ *and* $n = n_{\mathrm{g}}(s)$. *Assume* $d, n, \langle s\rangle \ge 2$; *the algorithm ensures*

$$\#K, \#L_k, \#U_k, \#Y_k, \#U_\ell, \#Y_\ell \le n^{d^{O(h)}}; \quad \langle U_k\rangle, \langle Y_k\rangle \le d^{O(h)}\langle s\rangle.$$

The algorithm runs in time $\langle s\rangle^{O(d)}\cdot n^{d^{O(h)}}$.

Interestingly enough, the bound on the number $\#K$ of components of $[\![s]\!]$ derived in Theorem 5.3 is doubly exponential, exactly as in the case of LIA. While this may on the first sight seem surprising, it turns out that there is a matching lower bound. It is known from [26, Lecture 23, p. 146] that there is a formula I_n of size linear in $n \in \mathbb{N}$ that defines the set of integers in the interval $[0, 2^{2^n} - 1]$. The only way to represent this formula as an $\mathbb{R}$-semilinear set

is $\bigcup_{i\in[0,2^{2^n}-1]} K(\{i\},\emptyset)$. Theorem 5.3 yields a doubly exponential procedure for deciding LRA.

Corollary 5.4. *There is an algorithm that, given a formula Φ of LRA, computes a family of triples $\{(U_k, Y_k, \{(U_\ell, Y_\ell)\}_{\ell\in L_k})\}_{k\in K}$ such that $[\![\Phi]\!] = \bigcup_{k\in K}\big(K(U_k,Y_k)\setminus\bigcup_{\ell\in L_k} K(U_\ell,Y_\ell)\big)$. Let $d = d(\Phi)$ and $h = h(\Phi)$. Assume $d, \langle\Phi\rangle \geq 2$; the algorithm ensures*

$$\#K, \#L_k, \#U_k, \#Y_k, \#U_\ell, \#Y_\ell \leq 2^{d^{O(h)}}; \quad \langle U_k\rangle, \langle Y_k\rangle \leq d^{O(h)}\langle\Phi\rangle.$$

The algorithm runs in time $\langle\Phi\rangle^{O(d)}\cdot 2^{d^{O(h)}}$.

5.1 Evaluating semilinear expressions

We now provide an analysis of the operations required to evaluate a semilinear expression, which in turn enables us to prove Theorem 5.1. Thanks to the notion of $\mathbb{Z}$-splitters and the bounds derived in Theorem 4.3, we can design a complementation procedure for semilinear sets that, when combined with further algorithms for other Boolean operations and projection, enables evaluating a semilinear expression in triply exponential time. Below, we give a complementation procedure for semilinear sets with proper sets of periods, which has to be combined with Proposition 3.3 to apply to arbitrary semilinear sets.

Lemma 5.5. *There is an algorithm that, given a semilinear set $M = \bigcup_{i\in I} L(B_i,P_i) \subseteq \mathbb{Z}^d$, where each P_i is proper, computes a family of pairs $\{(D_j,Q_j)\}_{j\in J}$ such that $\overline{M} = \bigcup_{j\in J} L(D_j,Q_j)$, and*

- *$\#J \leq ((\#I+1)\cdot d)^{O(d^3)}$ and each Q_j is proper; and*
- *$\langle D_j\rangle, \langle Q_j\rangle \leq \#I\cdot O(d^{10})\cdot\langle M\rangle$.*

The algorithm runs in time $(\max_{i\in I}(\#B_i+\#P_i)+\|M\|)^{O(d^{11})\cdot\#I}$.

The algorithm is simple to state:

1: $\mathcal{Z} = \{Z_1,\dots,Z_m\} \leftarrow \mathbb{Z}$-splitter for $\{L(B_i,P_i)\}_{i\in I}$, where $Z_j = L(C_j,Q_j)$
2: **for** $j\in J := [1,m]$ **do**
3: $\quad E_j \leftarrow C_j \setminus M$
4: **for** each distinct $Q \in \{Q_j : j\in J\}$ **do**
5: $\quad D_Q \leftarrow \bigcup_j E_j : j\in J$ is such that $Q_j = Q$
6: $\quad$ **output** (D_Q, Q)

In Line 1 of the algorithm, the $\mathbb{Z}$-splitter is computed according to Theorem 4.3. The set E_j in Line 3 can be computed by deciding membership in M of all $\boldsymbol{v}\in C_j$ using Lemma 3.2 and discarding such $\boldsymbol{v}$ accordingly. The running time of the overall algorithm is easily seen to have the same order of magnitude as that for the $\mathbb{Z}$-splitter.

The algorithm returns the set of all pairs (D_Q, Q), so

$$\bigcup_{j\in J} L(E_j,Q_j) = \bigcup_{Q} L(D_Q,Q),$$

where the union on the right-hand side enumerates all distinct sets among $Q_1,\dots,Q_m$. The difference between the two expressions on the left-hand side and on the right-hand side is that the latter groups together base points from hybrid linear sets sharing the same set of periods, i.e., if on the left-hand side we have $L(E_1,Q)\cup L(E_2,Q)$, then on the right-hand side we have $L(E_1\cup E_2,Q)$.

For every $j\in J$, let $F_j := C_j\cap M$. So,

$$\mathbb{Z}^d = \bigcup_{j\in J} L(C_j,Q_j) = \Big(\bigcup_{j\in J} L(E_j,Q_j)\Big)\cup\Big(\bigcup_{j\in J} L(F_j,Q_j)\Big).$$

To establish the correctness of the algorithm, it suffices to show that $\overline{M} = \bigcup_{j\in J} L(E_j,Q_j)$. This is done by relying on the conditions (Z2) and (Z3) from the definition of $\mathbb{Z}$-splitters in order to show that, given $j\in J$, both $L(E_j,Q_j)\cap M = \emptyset$ and $L(F_j,Q_j)\subseteq M$ hold.

We now turn towards the proof of Theorem 5.1, for which the complementation procedure established in Lemma 5.5 is the key. Informally, the algorithm to construct $[\![s]\!]$ as a semilinear set starting from a semilinear expression s works bottom up, beginning from the atoms of s. When considering an expression $s = s_1\cup s_2$, $s = s_1\cap s_2$, $s = \overline{s_1}$ or $s = \pi_D(s_1)$, the algorithm first computes semilinear sets $[\![s_1]\!]$ and $[\![s_2]\!]$, and then computes $[\![s]\!]$ according to the type of the operator. Whenever needed, e.g., before a complementation step, the algorithm uses Proposition 3.3 to make all period sets of the semilinear sets $[\![s_1]\!]$ and $[\![s_2]\!]$ proper. To compute the complement $[\![\overline{s_1}]\!]$, the algorithm invokes Lemma 5.5.

For the intersection of $[\![s_1]\!] = \bigcup_{j\in J} L(C_j,Q_j)$ and $[\![s_2]\!] = \bigcup_{k\in K} L(D_k,R_k)$, the algorithm first distributes the intersection over the unions, obtaining $[\![s_1\cap s_2]\!] = \bigcup_{(j,k)\in J\times K}(L(C_j,Q_j)\cap L(D_k,R_k))$, and then computes a hybrid linear set equivalent to each $L(C_j,Q_j)\cap L(D_k,R_k)$ following the lemma below, which makes the construction of [6, Thm. 6] effective.

Lemma 5.6. *Let $M = L(C,Q)\subseteq\mathbb{Z}^d$ and $N = L(D,R)\subseteq\mathbb{Z}^d$. Then $M\cap N = L(B,P)$ where*

- *$\langle B\rangle, \langle P\rangle \leq O(d\cdot(\#Q+\#R)^3)\cdot\max\{\langle M\rangle,\langle N\rangle\}^2$; and*
- *$\#P \leq (\#Q+\#R)^{(d+1)}$.*

The sets $B,P\subseteq\mathbb{Z}^d$ can be computed in time

$$(\#Q+\#R)^{O(d)}\cdot\max(\|M\|,\|N\|)^{O(d^4)}.$$

The cases for union and projection are not difficult, and only recalled in the lemma below for completeness.

Lemma 5.7. *Let $M_k = \bigcup_{i\in I_k} L(B_i,P_i)\subseteq\mathbb{Z}^d$, with $k\in\{1,2\}$ and $I_1\cap I_2 = \emptyset$, and let $D\subseteq[1,d]$. We have:*

- *$M_1\cup M_2 = \bigcup_{i\in I_1\cup I_2} L(B_i,P_i)$;*
- *$\pi_D(M_1) = \bigcup_{i\in I_1} L(\pi_D(B_i),\pi_D(P_i))$.*

Such a representation of $M_1\cup M_2$ (resp. $\pi_D(M_1)$) can be computed in time $O(\max_{k\in\{1,2\}}(\sum_{i\in I_k}\#(B_i\cup P_i)\cdot\langle M_k\rangle))$ (resp. with $k=1$).

The bounds and running time in Theorem 5.1 are established with an induction on the height of the input semilinear expression, together with the bounds and running times of the operations established in Lemmas 5.5, 5.6 and 5.7. We rely on Proposition 3.3 to make period sets proper whenever needed, for instance before complementing a semilinear set.

In a nutshell, notice that complementation is the most expensive of the operations. For a sequence of h nested complementation operations (possibly interleaved with projections), first estimate the number of hybrid linear sets in the output, $\#J$. Assuming $\#I\geq 2$, this will be

$$(((\#I)^e)^e\dots)^e, \qquad \text{where } e = O(d^3\log d)$$

and there are h exponentiations in total. Therefore, $\#J \leq (\#I)^{d^{O(h)}}$. Other bounds on the description size and running time then rely on this key estimate. As Lemma 5.5 relies on each input $L(B_i,P_i)$ having linear independent P_i, we can use Proposition 3.3 so that we initially have $\#I\leq(n_{\mathrm{p}}(s))^d$.

Finally, to establish Corollary 5.2, given a formula of Presburger arithmetic, we first translate it into a semilinear expression: disjunctions, conjunctions and negations become unions, intersections and complements, respectively; a sequence of quantifiers $\exists x_1 \cdots \exists x_k$ is translated into a projection $\pi_D(\cdot)$ where D contains k indices for the variables $x_1, \ldots, x_k$ (assuming an enumeration across all variables in the formula). To handle $\forall x_1 \cdots \forall x_k$, we first rewrite it into $\neg\exists x_1 \cdots \exists x_k \neg$. Each inequality $\boldsymbol{a} \cdot \boldsymbol{x} \leq c$ is translated into a hybrid linear set thanks to the following lemma.

Lemma 5.8. *Let $S \subseteq \mathbb{Z}^d$ be the set of integer solutions of a linear inequality $\boldsymbol{a} \cdot \boldsymbol{x} \leq c$, $\boldsymbol{a} \in \mathbb{Z}^{1\times d}$ and $c \in \mathbb{Z}$. Then $S = L(B, P)$ such that $\#P \leq 2d - 1$ and $\langle B\rangle, \langle P\rangle \leq O(d^4) \cdot (\langle \boldsymbol{a}\rangle + \langle c\rangle)$. Moreover, B and P can be computed in time $(\|\boldsymbol{a}\| + |c|)^{\mathrm{poly}(d)}$.*

Corollary 5.2 then follows by an application of Theorem 5.1.

5.2 Evaluating $\mathbb{R}$-semilinear expressions

Analogously to the previous section, the algorithm for evaluating $\mathbb{R}$-semilinear expressions required by Theorem 5.3 can be obtained from algorithms for Boolean operations and projections on $\mathbb{R}$-semilinear sets. Due to space constraints, we only provide the relevant statements. It is worth mentioning that due to $\mathbb{R}$-semilinear sets being constituted by copolyhedra, projection is not a trivial operation as it is in the case of semilinear sets.

Lemma 5.9. *There is an algorithm that, given an $\mathbb{R}$-semilinear set $M = \bigcup_{i\in I} \big(K(V_i, W_i) \setminus \bigcup_{j\in J_i} K(V_j, W_j)\big) \subseteq \mathbb{R}^d$, computes a family of triples $\{(U_k, Y_k, \{(U_\ell, Y_\ell)\}_{\ell\in L_k})\}_{k\in K}$ such that*

$$\overline{M} = \bigcup_{k\in K} \Big(K(U_k, Y_k) \setminus \bigcup_{\ell\in L_k} K(U_\ell, Y_\ell)\Big).$$

The algorithm ensures, for every $k \in K$ and $\ell \in K_\ell$,

- $\#U_k, \#Y_k, \#U_\ell, \#Y_\ell \leq (\#I \cdot \max_{i\in I}(\#V_i + \#W_i) + d)^{O(d^2)}$;
- $\langle U_k\rangle, \langle Y_k\rangle, \langle U_\ell\rangle, \langle Y_\ell\rangle \leq O(d^5) \cdot \langle M\rangle$; *and*
- $\#K, \#L_k \leq (\#I \cdot \max_{i\in I}(\#V_i + \#W_i) + d)^{O(d^2)}$.

The algorithm runs in time

$$\mathrm{poly}(\#I, \max_{i\in I} \#J_i, (\max_{i\in I}(\#V_i + \#W_i) + d)^{d^3}, \langle M\rangle).$$

Lemma 5.10. *Let $M_k = \bigcup_{i\in I_k} \big(K(V_i, W_i) \setminus \bigcup_{j\in J_i} K(V_j, W_j)\big)$, with $k \in \{1, 2\}$ and $I_1 \cap I_2 = \emptyset$. We have*

$$M_1 \cap M_2 = \bigcup_{k\in K} \Big(K(U_k, Y_k) \setminus \bigcup_{\ell\in L_k} K(U_\ell, Y_\ell)\Big)$$

where, given $\#\mathcal{P} \coloneqq \max_{i\in I_1\cup I_2,\, j\in J_i}(\#V_i, \#W_i, \#V_j, \#W_j)$,

- $\#K \leq \#I_1 \cdot \#I_2$ *and* $\#L_k \leq 2 \cdot \max_{i\in I_1\cup I_2} \#J_i$;
- $\#U_k, \#Y_k, \#U_\ell, \#Y_\ell \leq (\#\mathcal{P} + d)^{O(d^2)}$; *and*
- $\langle U_k\rangle, \langle Y_k\rangle, \langle U_\ell\rangle, \langle Y_\ell\rangle \leq O(d^4) \cdot \max_{k\in\{1,2\}} \langle M_k\rangle$.

The family of triples $\{(U_k, Y_k, \{(U_\ell, Y_\ell)\}_{\ell\in L_k})\}_{k\in K}$ can be computed in time $\mathrm{poly}(\#I_1, \#I_2, \max_{i\in I_1\cup I_2} \#J_i, \max_{k\in\{1,2\}} \langle M_k\rangle, (\#\mathcal{P} + d)^{d^2})$.

Lemma 5.11. *Let $M = \bigcup_{i\in I} \big(K(V_i, W_i) \setminus \bigcup_{j\in J_i} K(V_j, W_j)\big)$ be an $\mathbb{R}$-semilinear set, and let $D \subseteq [1, d]$. Then*

$$\pi_D(M) = \bigcup_{i\in I} \Big(K(\pi_D(V_i), \pi_D(W_i)) \setminus \bigcup_{\ell\in L_i} K(U_\ell, Y_\ell)\Big)$$

is a $\mathbb{R}$-semilinear set where, for every $i \in I$ and $\ell \in L_i$,

- $\#L_i \leq (\#V_i + \#W_i + 2d)^{d^2}$;
- $\#U_\ell, \#Y_\ell \leq 2(\#V_i + \#W_i + 2d)^{d^2}$; *and*
- $\langle U_\ell\rangle, \langle Y_\ell\rangle \leq O(d^4) \cdot \max_{i\in I}(\langle V_i\rangle, \langle W_i\rangle)$.

Such a representation of $\pi_D(M)$ can be computed in time

$$\mathrm{poly}(\#I, \max_{i\in I}(\#J_i + 1), \langle M\rangle, (\#\mathcal{P} + d)^{d^2}),$$

where $\#\mathcal{P} \coloneqq \max_{i\in I,\, j\in J_i}(\#V_i, \#W_i, \#V_j, \#W_j)$.

Lemma 5.12. *Let $M_k = \bigcup_{i\in I_k} \big(K(V_i, W_i) \setminus \bigcup_{j\in J_i} K(V_j, W_j)\big)$, with $k \in \{1, 2\}$ and $I_1 \cap I_2 = \emptyset$. We have*

$$M_1 \cup M_2 = \bigcup_{i\in I_1\cup I_2} \Big(K(V_i, W_i) \setminus \bigcup_{j\in J_i} K(V_j, W_j)\Big),$$

which can be computed in time $\max_{k\in\{1,2\}} O(\#I_k \cdot \#\mathcal{P}) \cdot \langle M_k\rangle$, where $\#\mathcal{P} \coloneqq \max_{i\in I_1\cup I_2,\, j\in J_i}(\#V_i, \#W_i, \#V_j, \#W_j)$.

6 THE VC DIMENSION OF LRA AND LIA

We recall the notion of VC dimension [24, Ch. 3]. Let $(X, \mathcal{F})$ be a *set system* consisting of a set X and a family $\mathcal{F}$ of subsets of X. We say that $\mathcal{F}$ *shatters* a set $A \subseteq X$ if for every $A' \subseteq A$ there is $S \in \mathcal{F}$ such that $S \cap A = A'$. The largest cardinality k of some $A \subseteq X$ shattered by $\mathcal{F}$ is the *Vapnik–Chervonenkis (VC) dimension* of $\mathcal{F}$, written as $\mathrm{VC}(\mathcal{F}) = k$, which may be infinite. The VC dimension is a fundamental measure in computational learning theory: if $\mathrm{VC}(\mathcal{F}) = k$ holds for a family $\mathcal{F}$ then the sample complexity of $\mathcal{F}$, i.e., the number of samples needed to PAC learn $\mathcal{F}$, is linear in k [10, 18].

As a simple example, consider the family of all closed intervals $\mathcal{I} \coloneqq \{[p, q] : p, q \in \mathbb{R}\}$. This family has a VC dimension of 2. Indeed, $\mathrm{VC}(\mathcal{I}) \geq 2$, since $\mathcal{I}$ shatters the set $\{0, 1\}$. To show that $\mathrm{VC}(\mathcal{I}) \leq 2$, it suffices to pick any set $\{a, b, c\}$ with $a < b < c$ and notice that no interval $I \in \mathcal{I}$ is such that $\{a, b, c\} \cap I = \{a, c\}$.

The notion of VC dimension can be applied to formulae of any first-order theory [1]. Consider a *partitioned* first-order formula $\Phi(\boldsymbol{x}; \boldsymbol{y})$, in the structure $\mathcal{M}$ with universe M, whose $n + m$ free variables are separated into two groups of $n \geq 1$ *object variables* $\boldsymbol{x}$ and $m \geq 1$ *parameter variables* $\boldsymbol{y}$. Given a *parameter* $\boldsymbol{w} \in M^m$, i.e., a particular choice of the m parameter variables, we define $\mathcal{S}_{\boldsymbol{w}} \coloneqq \{\boldsymbol{v} \in M^n : \mathcal{M} \models \Phi(\boldsymbol{v}, \boldsymbol{w})\}$ and we associate to $\Phi(\boldsymbol{x}; \boldsymbol{y})$ the family $\mathcal{S}_\Phi \coloneqq \{\mathcal{S}_{\boldsymbol{w}} : \boldsymbol{w} \in M^m\}$. The VC dimension of Φ, written $\mathrm{VC}(\Phi)$, is defined as $\mathrm{VC}(\mathcal{S}_\Phi)$. For example, for the formula $\Phi(x, y_1, y_2) \coloneqq y_1 \leq x \wedge x \leq y_2$ with object variable x and parameter variables y_1 and y_2, we have $\mathrm{VC}(\Phi) = 2$ since $\mathcal{S}_\Phi = \mathcal{I}$ for the family of intervals $\mathcal{I}$ defined above.

In model theory, finiteness of $\mathrm{VC}(\Phi)$ is equivalent to Φ *not having the independence property* (Φ *is NIP*, for short) in the sense of S. Shelah [42]; see also [1, Sec. 1.3] for a modern account on NIP theories. A structure $\mathcal{M}$ is NIP if every partitioned first-order formula in $\mathcal{M}$ is NIP. While insufficient to deduce precise bounds on the VC dimension, the results of Y. Gurevich and P.H. Schmitt [16, Thm. 3.1], relying on [35, Thm. 7] of B. Poizat, imply that both LRA and LIA are NIP, and thus all formulae from these theories have finite VC dimension.

The goal of this section is to establish precise upper bounds on the VC dimension for both LRA and LIA.

Theorem 6.1. *Every formula Φ of LRA has VC dimension that is at most exponential in the length of Φ.*

Theorem 6.2. *Every formula Φ of LIA has VC dimension that is at most doubly exponential in the length of Φ.*

These upper bounds have simple matching lower bounds. For LRA, it is known from [26, Lec. 23] that there is a formula $\mathrm{div}_n(x, y)$, of length polynomial in $n \in \mathbb{N}$, that is satisfied whenever $x, y \in \mathbb{N}$ with $0 \le x \le y < 2^{2^n}$, and x divides y. With x as an object variable and y as a parameter variables, $\mathrm{div}_{(n+1)}(x, y)$ shatters the set $\mathbb{P}_{2^n}$ of prime numbers below 2^n. By the prime number theorem [19], $\#\mathbb{P}_{2^n}$ is $\Theta(2^{n-\log n})$, i.e., it is exponential in the length of $\mathrm{div}_{(n+1)}(x, y)$, and the product of the primes in $\mathbb{P}_{2^n}$ is less than $2^{2^{n+1}}$. Then each subset $\{p_1, \ldots, p_k\} \subseteq \mathbb{P}_{2^n}$ is obtained by setting $y = \prod_{i=1}^{k} p_i$. Similarly, for LIA, [26, Lec. 24] defines another formula $\mathrm{div}_n(x, y)$, of length polynomial in $n \in \mathbb{N}$, that is satisfied whenever x divides y and $0 \le x \le y \le \ell_n$, where ℓ_n is the product of all primes below 2^{2^n}; thus $\ell_n \le 2^{c2^{2^n}}$ for some constant $c > 0$. With x as an object variable and y as a parameter variable, this formula shatters the set of all primes below 2^{2^n}.

6.1 The VC dimension of linear real arithmetic

To derive an upper bound on the VC dimension of LRA, we consider the analogous problem of bounding the VC dimension of an $\mathbb{R}$-semilinear set. Similarly to the definition of VC dimension for a first-order theory, given a set $M \subseteq \mathbb{R}^{n+m}$, where the first $n \ge 1$ coordinates are called *object coordinates* and the last $m \ge 1$ are called *parameter coordinates*, we define sets $\mathcal{S}_{\boldsymbol{w}} := \{\boldsymbol{v} \in \mathbb{R}^n : (\boldsymbol{v}, \boldsymbol{w}) \in M\}$ for each choice $\boldsymbol{w} \in \mathbb{R}^m$ of the parameters, and consider the family $\mathcal{S}_M := \{\mathcal{S}_{\boldsymbol{w}} : \boldsymbol{w} \in \mathbb{R}^m\}$. Define $\mathrm{VC}(M) := \mathrm{VC}(\mathcal{S}_M)$.

Whenever M is an $\mathbb{R}$-semilinear set, we show that its VC dimension is polynomial in the dimension $n + m$ and (only) logarithmic in the number of its components and the maximum cardinality of its generator sets. There is no dependence on $\|M\|$, i.e., on the magnitude of numbers in the presentation.

Theorem 6.3. *Let $M = \bigcup_{i \in I} \left(K(V_i, W_i) \setminus \bigcup_{j \in J_i} K(V_j, W_j)\right)$ be an $\mathbb{R}$-semilinear set of dimension $d = n + m$, with coordinates partitioned into $n \ge 1$ object coordinates and $m \ge 1$ parameter coordinates. Then $\mathrm{VC}(M) \le 6 \cdot (d+1)^2 \cdot \log\left(\#I \cdot d \cdot \max_{i \in I}(\#V_i + \#W_i + 1)\right)$.*

Thanks to Corollary 5.4, Theorem 6.3 suffices to prove the upper bound on the VC dimension of LRA in Theorem 6.1.

The key insight that leads to this result is depicted in Figure 1. Pick a set V of objects, in the figure $V = \{v_1, v_2\}$. Each object corresponds to a hyperplane h that, when intersected with M, generates an $\mathbb{R}$-semilinear set. We project all these intersections (cross-sections) coming from the different objects in V on the parameter space $\mathbb{R}^m$, and build a set $\mathcal{H}$ of hyperplanes that carves out all the convex polyhedra appearing in the $\mathbb{R}$-semilinear set resulting from this projection. The hyperplanes in $\mathcal{H}$ divide the parameter space into regions with a fundamental property: every two parameters $\boldsymbol{w}_1$ and $\boldsymbol{w}_2$ belonging to the same region satisfy $\mathcal{S}_{\boldsymbol{w}_1} \cap V = \mathcal{S}_{\boldsymbol{w}_2} \cap V$. This implies that, if M shatters V, the set $\mathcal{H}$ divides $\mathbb{R}^m$ into at least $2^{\#V}$ regions. By relying on Proposition 3.5, we show that the number of these regions is at most $\#V^d \cdot \alpha$, where α is a quantity that depends on the descriptional complexity of M. As $f(n) = 2^n$ grows faster than $g(n) = c \cdot n^d$, this allows us to derive an upper bound on the maximum cardinality of sets V that $\mathcal{S}_M$ shatters.

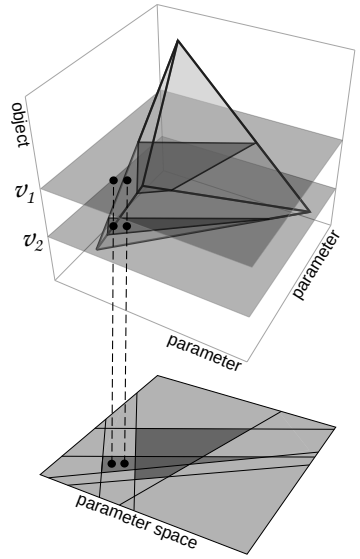

Figure 1: Above: two cross-sections of a tetrahedron, associated with two objects v_1 and v_2. Below: supporting hyperplanes (lines) of these cross-sections, splitting the parameter space into regions. Every two parameters $\boldsymbol{w}_1$ and $\boldsymbol{w}_2$ belonging to the same region satisfy $\mathcal{S}_{\boldsymbol{w}_1} \cap \{v_1, v_2\} = \mathcal{S}_{\boldsymbol{w}_2} \cap \{v_1, v_2\}$.

Let us now formalise this idea. Consider the set $\mathcal{H}(M) := \bigcup_{i \in I} \mathcal{H}(V_i, W_i)$, where $\mathcal{H}(V_i, W_i)$ is a set of hyperplanes in $\mathbb{R}^{n+m}$ carving out $K(V_i, W_i)$. In M, for each $i \in I$ and $j \in J_i$, the polyhedron $K(V_j, W_j)$ is a face of $K(V_i, W_i)$, so $\mathcal{H}(M)$ also carves out $K(V_j, W_j)$. By Proposition 3.1, $\#\mathcal{H}(M) \le \#I \cdot (2d + \max_{i \in I}(\#V_i + \#W_i)^d)$.

Assume that $\mathcal{S}_M$ shatters a set $V = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k\} \subseteq \mathbb{R}^n$ of $k \ge 1$ objects. We derive an upper bound on k. For each $\boldsymbol{v} \in V$, we define the m-dimensional affine subspace $A_{\boldsymbol{v}} := \{(\boldsymbol{v}, \boldsymbol{y}) : \boldsymbol{y} \in \mathbb{R}^m\}$. In the top part of Figure 1, these affine subspaces are the two hyperplanes in light grey.

We construct a set $\mathcal{H}_{\boldsymbol{v}}$ of non-trivial intersections between $A_{\boldsymbol{v}}$ and hyperplanes in $\mathcal{H}(M)$. First, observe that for every $h \in \mathcal{H}(M)$ one of the following holds:

- $\emptyset \ne (A_{\boldsymbol{v}} \cap h) \ne A_{\boldsymbol{v}}$: in this case, $\dim(A_{\boldsymbol{v}} \cap h) = m - 1$;
- $A_{\boldsymbol{v}} \subseteq h$: in this case, $\dim(A_{\boldsymbol{v}} \cap h) = \dim(A_{\boldsymbol{v}}) = m$; or
- $A_{\boldsymbol{v}} \cap h = \emptyset$: in this case, $\dim(A_{\boldsymbol{v}} \cap h) = -1$.

The dimension of the set $A_{\boldsymbol{v}} \cap h$ can be calculated trivially in the second and third cases. In the first case, pick $\boldsymbol{s} \in A_{\boldsymbol{v}} \cap h$ and $\boldsymbol{t} \in A_{\boldsymbol{v}} \setminus h$. Consider the sets $A_{\boldsymbol{v}} - \boldsymbol{s} := A_{\boldsymbol{v}} + \{-\boldsymbol{s}\}$ and $h - \boldsymbol{s}$, which are both subspaces of $\mathbb{R}^d$. We will apply to $A_{\boldsymbol{v}} - \boldsymbol{s}$ and $h - \boldsymbol{s}$ Grassmann's formula

$$\dim(U \cap W) = \dim U + \dim W - \dim(U + W),$$

valid for any two subspaces U and W. Notice that $h - \boldsymbol{s}$ has dimension $d - 1$ and does not contain the vector $\boldsymbol{t} - \boldsymbol{s}$. Since this vector belongs to $A_{\boldsymbol{v}} - \boldsymbol{s}$, we conclude that $(A_{\boldsymbol{v}} - \boldsymbol{s}) + (h - \boldsymbol{s}) = \mathbb{R}^d$, and so $\dim(A_{\boldsymbol{v}} \cap h) = \dim((A_{\boldsymbol{v}} - \boldsymbol{s}) \cap (h - \boldsymbol{s})) = m + (d - 1) - d = m - 1$.

Define $\mathcal{H}_{\boldsymbol{v}} := \{A_{\boldsymbol{v}} \cap h : \dim(A_{\boldsymbol{v}} \cap h) = m - 1, h \in \mathcal{H}(M)\}$. Notice that each $A_{\boldsymbol{v}} \cap h$ in $\mathcal{H}_{\boldsymbol{v}}$ is a hyperplane when considered

relative to the affine subspace $A_{\boldsymbol{v}}$ and that all points in $A_{\boldsymbol{v}} \cap h$ are of the form $(\boldsymbol{v}, \boldsymbol{w}) \in \mathbb{R}^{n+m}$, for some $\boldsymbol{w} \in \mathbb{R}^m$.

We define an equivalence relation $\sim_{\mathcal{H}} \subseteq \mathbb{R}^m \times \mathbb{R}^m$ of finite index, such that $\boldsymbol{w}_1 \sim_{\mathcal{H}} \boldsymbol{w}_2$ implies $\mathcal{S}_{\boldsymbol{w}_1} \cap V = \mathcal{S}_{\boldsymbol{w}_2} \cap V$. Intuitively, $\sim_{\mathcal{H}}$ splits the parameter space $\mathbb{R}^m$ as shown in the bottom-most part of Figure 1. We first build analogous relations with respect to a single $\boldsymbol{v} \in V$. Let $\boldsymbol{v} = (v_1, \ldots, v_n)$ and $\mathcal{H}_{\boldsymbol{v}} = \{A_{\boldsymbol{v}} \cap h_1, \ldots, A_{\boldsymbol{v}} \cap h_r\}$, where each hyperplane h_i is the set of solutions to the equation $\mathfrak{h}_i \colon \boldsymbol{a}_i \cdot (\boldsymbol{x}, \boldsymbol{y}) = c_i$. Let $\sim_{\mathcal{H}_{\boldsymbol{v}}}$ be the equivalence relation on $\mathbb{R}^m$ given by:

$\boldsymbol{w}_1 \sim_{\mathcal{H}_{\boldsymbol{v}}} \boldsymbol{w}_2$ iff, for every $i \in [1, r]$,

$$\operatorname{sgn}(\boldsymbol{a}_i \cdot (\boldsymbol{v}, \boldsymbol{w}_1) - c_i) = \operatorname{sgn}(\boldsymbol{a}_i \cdot (\boldsymbol{v}, \boldsymbol{w}_2) - c_i).$$

Lemma 6.4. *Consider $\boldsymbol{w}_1$ and $\boldsymbol{w}_2$ in $\mathbb{R}^m$ such that $\boldsymbol{w}_1 \sim_{\mathcal{H}_{\boldsymbol{v}}} \boldsymbol{w}_2$. Then $(\boldsymbol{v}, \boldsymbol{w}_1) \in M$ if and only if $(\boldsymbol{v}, \boldsymbol{w}_2) \in M$.*

This lemma follows from the definition of $A_{\boldsymbol{v}}$ and $\mathcal{H}(M)$.

We define $\sim_{\mathcal{H}} \coloneqq \bigcap_{\boldsymbol{v} \in V} \sim_{\mathcal{H}_{\boldsymbol{v}}}$, which enjoys three properties listed in the following lemma. These are proved by appealing to Lemma 6.4, Proposition 3.5, plus the fact that $\mathcal{H}(M)$ carves out each polyhedron $K(V_i, W_i)$ in M.

Lemma 6.5. *Let $V \subseteq \mathbb{R}^n$ be a set of $k \geq 1$ objects. Consider an $\mathbb{R}$-semilinear set $M = \bigcup_{i \in I} M_i \subseteq \mathbb{R}^{n+m}$, where $M_i = K(V_i, W_i) \setminus \bigcup_{j \in J_i} K(V_j, W_j)$, having $d = n + m$ dimensions, $n \geq 1$ object coordinates and $m \geq 1$ parameter coordinates. The equivalence relation $\sim_{\mathcal{H}}$ has the following properties:*

(i) given $i \in I$, $\boldsymbol{w}_1, \boldsymbol{w}_2 \in \mathbb{R}^m$ and $\boldsymbol{v} \in V$, if $\boldsymbol{w}_1 \sim_{\mathcal{H}} \boldsymbol{w}_2$, then $(\boldsymbol{v}, \boldsymbol{w}_1) \in M_i$ if and only if $(\boldsymbol{v}, \boldsymbol{w}_2) \in M_i$;

(ii) given $i \in I$, $\boldsymbol{w}_1, \boldsymbol{w}_2 \in \mathbb{R}^m$ and $\boldsymbol{v} \in V$, if $\boldsymbol{w}_1 \sim_{\mathcal{H}} \boldsymbol{w}_2$, then $(\boldsymbol{v}, \boldsymbol{w}_1) \in \operatorname{aff} M_i$ if and only if $(\boldsymbol{v}, \boldsymbol{w}_2) \in \operatorname{aff} M_i$;

(iii) the number of equivalence classes of $\sim_{\mathcal{H}}$ is bounded by $k^d \cdot 2^d \cdot \#I^d \cdot \left(2d + \max_{i \in I}(\#V_i + \#W_i)^d\right)^d + 1$.

By definition, Property (i) of Lemma 6.5 implies that, for every two parameters $\boldsymbol{w}_1 \sim_{\mathcal{H}} \boldsymbol{w}_2$, we have $\mathcal{S}_{\boldsymbol{w}_1} \cap V = \mathcal{S}_{\boldsymbol{w}_2} \cap V$. Then, Property (iii) implies that $\#\{\mathcal{S}_{\boldsymbol{w}} \cap V : \boldsymbol{w} \in \mathbb{R}^m\}$ is bounded from above by $k^d \cdot 2^d \cdot \#I^d \cdot \left(2d + \max_{i \in I}(\#V_i + \#W_i)^d\right)^d + 1$. Since we are assuming that $\mathcal{S}_M$ shatters V, it follows that

$$2^k \leq k^d \cdot 2^d \cdot \#I^d \cdot \left(2d + \max_{i \in I}(\#V_i + \#W_i)^d\right)^d + 1. \qquad (\dagger)$$

It remains to analyse this inequality.

Lemma 6.6. *Consider any $k, d, \alpha \in \mathbb{R}$ satisfying*

$$k^d \cdot \alpha \geq 2^k, \quad d \geq 1, \quad \alpha \geq 2, \quad k \geq 1.$$

Then $k \leq 2 \cdot (\log \alpha + d \log(2d))$.

Plugging Equation (†) in Lemma 6.6 yields the following bound on k, which implies Theorem 6.3.

Lemma 6.7. *Consider k from Equation (†). We have*

$$k \leq 6(d+1)^2 \cdot \log\left(\#I \cdot d \cdot \max_{i \in I}(\#V_i + \#W_i + 1)\right).$$

6.2 The VC dimension of Presburger arithmetic

We now move to Presburger arithmetic, and adapt the proof technique used for Theorem 6.1 in order to establish Theorem 6.2, as well as upper bounds on the VC dimension of semilinear sets. Throughout this section, given a set $M \subseteq \mathbb{Z}^{n+m}$ of dimension $n+m$, where the first $n \geq 1$ coordinates are called *object coordinates* and the last $m \geq 1$ are called *parameter coordinates*, we define sets $\mathcal{S}_{\boldsymbol{w}} \coloneqq \{\boldsymbol{v} \in \mathbb{Z}^n : (\boldsymbol{v}, \boldsymbol{w}) \in M\}$ for each choice $\boldsymbol{w} \in \mathbb{Z}^m$ of the parameters, and associate with M the family $\mathcal{S}_M = \{\mathcal{S}_{\boldsymbol{w}} : \boldsymbol{w} \in \mathbb{Z}^m\}$. Then $\mathrm{VC}(M) \coloneqq \mathrm{VC}(\mathcal{S}_M)$.

We establish an upper bound on the VC dimension of a semilinear set $M \subseteq \mathbb{Z}^d$: it is exponential, but only in d.

Theorem 6.8. *Let $M = \bigcup_{i \in I} L(B_i, P_i)$ be a semilinear set in dimension $d = n + m$, with $n \geq 1$ object coordinates and $m \geq 1$ parameter coordinates. Then $\mathrm{VC}(M) \leq \alpha \log \alpha$ with α in*

$$O(\#I \cdot (\max_{i \in I} \#P_i + 1)^{d+1} (d+1)^6 \log(\max_{i \in I} \|B_i\| \cdot \max_{i \in I} \|P_i\|^2)).$$

In the proof of Theorem 6.8, the main difficulty lies in handling the discrete behaviour of the various hybrid linear sets. Here, we employ a simple yet effective approach that consists of establishing an upper bound, firstly, on the VC dimension of a hybrid linear set with a proper period set, and then on the VC dimension of a semilinear set with the help of Proposition 3.3 together with the following proposition by Sauer and Shelah [39, 43] (see also [30, Proof of Thm. 4]).

Proposition 6.9. *Let $S_1, \ldots, S_t \subseteq \mathbb{Z}^{n+m}$ be any t sets with $\mathrm{VC}(\mathcal{S}_{S_i}) = k_i$. If T is any Boolean combination of $S_1, \ldots, S_t$, then $\mathrm{VC}(T) = O((\sum_{i=1}^t k_i) \cdot \log(\sum_{i=1}^t k_i))$.*

We start by deriving an upper bound on the VC dimension of a hybrid linear set with a proper set of periods.

A set $S \subseteq \mathbb{Z}^d$ is an *(integer) lattice* whenever it is of the form $S = \Lambda(P) \coloneqq P \cdot \mathbb{Z}^{\#P}$ with $P \subseteq \mathbb{Z}^d$ proper. Notice that for our purposes we do not require $\dim S$ to be d.

Below, let us fix a hybrid linear set $L = L(B, P) \subseteq \mathbb{Z}^{n+m}$ having a *proper* period set P and $d = n + m$ dimensions partitioned into $n \geq 1$ object coordinates and $m \geq 1$ parameter coordinates. Let us assume that $\mathcal{S}_L$ shatters a set $V = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k\} \subseteq \mathbb{Z}^n$ of size $k \geq 1$. Following the lemma below, the strategy to bound k becomes clear: it is sufficient to add to the strategy employed in Section 6.1 an analysis of how the VC dimension increases in the presence of the integer lattice $\Lambda(P)$.

Lemma 6.10. *For P proper, $L(\boldsymbol{b}, P) = K(\boldsymbol{b}, P) \cap (\boldsymbol{b} + \Lambda(P))$.*

Proof. As P is proper, every $\boldsymbol{v} \in \mathbb{R}^d$ has at most one $\boldsymbol{\lambda} \in \mathbb{R}^{\#P}$ s.t. $\boldsymbol{v} = \boldsymbol{b} + P \cdot \lambda$. Then the lemma follows as $\mathbb{N} = \mathbb{R}_+ \cap \mathbb{Z}$. □

We consider the $\mathbb{R}$-semilinear set $\bigcup_{\boldsymbol{b} \in B} K(\boldsymbol{b}, P)$ and, by Lemma 6.5, construct an equivalence relation $\sim_{\mathcal{H}}$ such that:

1) given $\boldsymbol{b} \in B$, $\boldsymbol{v} \in V$ and $\boldsymbol{w}_1, \boldsymbol{w}_2 \in \mathbb{R}^m$ such that $\boldsymbol{w}_1 \sim_{\mathcal{H}} \boldsymbol{w}_2$, we have $(\boldsymbol{v}, \boldsymbol{w}_1) \in K(\boldsymbol{b}, P)$ if and only if $(\boldsymbol{v}, \boldsymbol{w}_2) \in K(\boldsymbol{b}, P)$;
2) given $\boldsymbol{b} \in B$, $\boldsymbol{v} \in V$ and $\boldsymbol{w}_1, \boldsymbol{w}_2 \in \mathbb{R}^m$ such that $\boldsymbol{w}_1 \sim_{\mathcal{H}} \boldsymbol{w}_2$, we have $(\boldsymbol{v}, \boldsymbol{w}_1) \in \operatorname{aff} K(\boldsymbol{b}, P)$ if and only if $(\boldsymbol{v}, \boldsymbol{w}_2) \in \operatorname{aff} K(\boldsymbol{b}, P)$;
3) the number of equivalence classes of the relation $\sim_{\mathcal{H}}$ is bounded by $k^d \cdot 2^{2d} \cdot \#B^d \cdot (d+1)^{d^2} + 1$ (given that $\#P \leq d$).

Given two parameters $\boldsymbol{w}_1, \boldsymbol{w}_2 \in \mathbb{Z}^m$, we write $\boldsymbol{w}_1 \sim_{\Lambda} \boldsymbol{w}_2$ whenever $(\boldsymbol{0}, \boldsymbol{w}_1) - (\boldsymbol{0}, \boldsymbol{w}_2) \in \Lambda(P)$, with $\boldsymbol{0} \in \mathbb{Z}^n$. It is easy to see that $\sim_{\Lambda}$ is an equivalence relation. The following two lemmas show how to refine $\sim_{\mathcal{H}}$ to account for the lattice $\Lambda(P)$.

Lemma 6.11. *Let $\boldsymbol{w}_1, \boldsymbol{w}_2 \in \mathbb{Z}^n$ such that $\boldsymbol{w}_1 \, (\sim_{\mathcal{H}} \cap \sim_{\Lambda}) \, \boldsymbol{w}_2$, and let $\boldsymbol{v} \in V$. Then $(\boldsymbol{v}, \boldsymbol{w}_1) \in L$ if and only if $(\boldsymbol{v}, w_2) \in L$.*

Proof. We only show the left to right direction. Suppose $(\boldsymbol{v}, \boldsymbol{w}_1) \in L$, and thus $(\boldsymbol{v}, \boldsymbol{w}_1) \in L(\boldsymbol{b}, P)$ for some $\boldsymbol{b} \in B$. Since P is proper, by Lemma 6.10, $(\boldsymbol{v}, \boldsymbol{w}_1) \in K(\boldsymbol{b}, P)$ and $(\boldsymbol{v}, \boldsymbol{w}_1) \in \boldsymbol{b} + \Lambda(P)$; and to conclude the proof it suffices to show that $(\boldsymbol{v}, \boldsymbol{w}_2) \in K(\boldsymbol{b}, P)$ and $(\boldsymbol{v}, \boldsymbol{w}_2) \in \boldsymbol{b} + \Lambda(P)$. The former, i.e., $(\boldsymbol{v}, \boldsymbol{w}_2) \in K(\boldsymbol{b}, P)$, follows directly from $\boldsymbol{w}_1 \sim_{\mathcal{H}} \boldsymbol{w}_2$. We also have $(\boldsymbol{v}, \boldsymbol{w}_2) - (\boldsymbol{v}, \boldsymbol{w}_1) = P \cdot \boldsymbol{\lambda}$ for some $\boldsymbol{\lambda} \in \mathbb{Z}^d$, and by $(\boldsymbol{v}, \boldsymbol{w}_1) \in \boldsymbol{b} + \Lambda(P)$ there is $\boldsymbol{\mu} \in \mathbb{Z}^d$ such that $(\boldsymbol{v}, \boldsymbol{w}_1) = \boldsymbol{b} + P \cdot \boldsymbol{\mu}$. So, $(\boldsymbol{v}, \boldsymbol{w}_2) = \boldsymbol{b} + P \cdot (\boldsymbol{\lambda} + \boldsymbol{\mu}) \in \boldsymbol{b} + \Lambda(P)$. □

Lemma 6.12. *Let E be an equivalence class of $\sim_{\mathcal{H}}$. Either*

- *for every $\boldsymbol{w} \in E$, $\mathcal{S}_{\boldsymbol{w}} \cap V = \emptyset$; or*
- *the relation $\sim_\Lambda$ partitions $E \cap \mathbb{Z}^m$ into at most $(2d \cdot \|P\|)^d$ equivalence classes.*

Assuming $\dim \operatorname{span}(P) = d$, this lemma follows from the fact that the number of equivalence classes in $\sim_\Lambda$ is $|\det P|$ [27, Lem. 2.3.14]. A proof not requiring $\dim \operatorname{span}(P) = d$ can be established by relying on Property 2 of $\sim_{\mathcal{H}}$.

Below, let $\mathcal{S}_{\boldsymbol{w}} := \{\boldsymbol{v} \in \mathbb{Z}^n : (\boldsymbol{v}, \boldsymbol{w}) \in L(B, P)\}$. Lemmas 6.11 and 6.12 allow us to derive a bound on the number of distinct intersections $\mathcal{S}_{\boldsymbol{w}} \cap V$ across all parameters $\boldsymbol{w} \in \mathbb{Z}^m$.

Lemma 6.13. *Consider $L(B, P) \subseteq \mathbb{Z}^d$ with P proper, $d = n + m$ dimensions, $n \geq 1$ object coordinates and $m \geq 1$ parameter coordinates. Then the cardinality of the set $\{\mathcal{S}_{\boldsymbol{w}} \cap V : \boldsymbol{w} \in \mathbb{Z}^m\}$ does not exceed $k^d \cdot 2^{2d+2} \cdot (d+1)^{d^2+1} \cdot (\#B \cdot \|P\|)^d$.*

Since we are assuming that $\mathcal{S}_L$ shatters V, Lemma 6.13 yields an upper bound on the VC dimension of L by Lemma 6.6.

Lemma 6.14. *The VC dimension of a set $L(B, P) \subseteq \mathbb{Z}^d$ with P proper is at most $6 \cdot (d+1)^4 \log\big((d+1) \cdot \#B \cdot \|P\|\big)$.*

Finally, we apply Proposition 6.9 to extend Lemma 6.14 to semilinear sets with proper period sets.

Lemma 6.15. *The VC dimension of a set $\bigcup_{i \in I} L(B_i, P_i)$ where each P_i is proper does not exceed $\alpha \log \alpha$ where*

$$\alpha := 6 \cdot \#I \cdot (d+1)^4 \log\big((d+1) \cdot \#B \cdot \|P\|\big).$$

Theorem 6.8 follows from Lemma 6.15 and Proposition 3.3. Together with Theorem 5.1, this result show a doubly exponential upper bound on the VC dimension of semilinear expressions. Theorem 6.2 follows from Lemma 6.15 and Corollary 5.2.

7 CONCLUSIONS

We have presented geometric decision procedures for linear integer arithmetic (LIA) and linear real arithmetic (LRA) running in triply and doubly exponential time, respectively. The existence of such a procedure for LIA has been a long-standing problem. Whilst the focus of this work has been on *unrestricted* LIA and LRA, our results also deliver meaningful bounds for restricted fragments too. Corollary 5.4, for example, recovers a polynomial-time algorithm for the *short* fragment of LRA, i.e., for formulae in which both the number of variables and the number of occurrences of all linear inequalities are bounded from above by a fixed constant, independent of the given formula (cf. [31] for hardness results for short LIA). This result is not new, however, as even the nonlinear theory in fixed dimension is known to be polynomial-time decidable [37]. It would be interesting to see if the bounds of Sec. 5 that involve h, i.e., the maximum nesting depth of Boolean connectives and quantifications, could be strengthened to refer to the alternation depth instead, expanding the reach of the geometric approach.

It is no surprise that the decision problem for linear arithmetic theories is linked with standard computational geometry tasks such as enumerating faces and triangulating convex polyhedra in $\mathbb{R}^d$. However, before the present paper no elementary bound on the running time of geometric decision procedures for LIA was known, unlike for procedures based on automata and quantifier elimination. With Corollaries 5.2 and 5.4 offering such guarantees, we expect it possible to take advantage of established computational geometry algorithms and heuristics for these tasks (see, e.g., [13]), leading to competitive software implementations. By the results of L. Berman [3], the doubly and triply exponential running time and description size bounds from Sec. 5 cannot in the worst case be reduced to, e.g., single and double exponential, respectively. This barrier, however, need not hold for individual inputs arising from practice. Our results indicate the properties that *guarantee* that time and memory usage of our decision procedures (algorithms) stays within the stated bounds. These bounds, however, are conservative and are blind to savings that could be made on specific inputs.

Geometry can also be a strong tool to obtain decision procedures for logical theories with more powerful signatures, for instance, to show decidability of LIA enriched with a Kleene star operator [11, 17, 34]. However, it is currently open whether this extension of LIA admits an elementary decision procedure, even though all sets definable in this theory are still semilinear. The results of this paper leave open the possibility of a decision procedure for LIA enriched with a Kleene star operator with elementary running time.

Another direction for future work worth exploring is to investigate whether a geometric approach can lead to a decision procedure with elementary running time for the extension of LIA with a unary counting quantifier [7, 41].

Finally, while initial work on characterising the geometry of linear mixed integer and real arithmetic (LIRA) exists [46], to the best of our knowledge a full geometric characterisation has not been obtained. Furthermore, bounds on the VC dimension of LIRA are not known. We are confident that the approach taken in this paper can be used to address these open problems.

REFERENCES

[1] Matthias Aschenbrenner, Alf Dolich, Deirdre Haskell, Dugald Macpherson, and Sergei Starchenko. 2016. Vapnik-Chervonenkis density in some theories without the independence property, I. *Trans. Amer. Math. Soc.* 368, 8 (2016), 5889–5949. https://doi.org/10.1090/tran/6659

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

[3] Leonard Berman. 1980. The Complexity of Logical Theories. *Theor. Comput. Sci.* 11 (1980), 71–77. https://doi.org/10.1016/0304-3975(80)90037-7

[4] Bernard Boigelot, Sébastien Jodogne, and Pierre Wolper. 2005. An effective decision procedure for linear arithmetic over the integers and reals. *ACM Trans. Comput. Log.* 6, 3 (2005), 614–633. https://doi.org/10.1145/1071596.1071601

[5] J. Richard Büchi. 1960. Weak Second-Order Arithmetic and Finite Automata. *Math. Logic Quart.* 6, 1-6 (1960), 66–92. https://doi.org/10.1002/malq.19600060105

[6] Dmitry Chistikov and Christoph Haase. 2016. The Taming of the Semi-Linear Set. In *Proc. International Colloquium on Automata, Languages, and Programming, ICALP (LIPIcs, Vol. 55)*. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 128:1–128:13. https://doi.org/10.4230/LIPIcs.ICALP.2016.128

[7] Dmitry Chistikov, Christoph Haase, and Alessio Mansutti. 2022. Quantifier elimination for counting extensions of Presburger arithmetic. In *Proc. Foundations of Software Science and Computation Structures, FOSSACS (Lecture Notes in Computer*

Science, Vol. 13242). Springer, 225–243. https://doi.org/10.1007/978-3-030-99253-8_12

[8] Eric Domenjoud. 1991. Solving Systems of Linear Diophantine Equations: An Algebraic Approach. In *Proc. Mathematical Foundations of Computer Science, MFCS (Lecture Notes in Computer Science, Vol. 520)*. Springer, 141–150. https://doi.org/10.1007/3-540-54345-7_57

[9] Antoine Durand-Gasselin and Peter Habermehl. 2012. Ehrenfeucht-Fraïssé goes elementarily automatic for structures of bounded degree. In *Proc. International Symposium on Theoretical Aspects of Computer Science, STACS (LIPIcs, Vol. 14)*. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 242–253. https://doi.org/10.4230/LIPIcs.STACS.2012.242

[10] Andrzej Ehrenfeucht, David Haussler, Michael Kearns, and Leslie Valiant. 1989. A general lower bound on the number of examples needed for learning. *Inform. Comput.* 82, 3 (1989), 247–261. https://doi.org/10.1016/0890-5401(89)90002-3

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

[12] 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. https://doi.org/10.1137/0204006

[13] Komei Fukuda and Alain Prodon. 1996. Double Description Method Revisited. In *Proc. Combinatorics and Computer Science, CCS'95, Franco-Japanese and Franco-Chinese Conference (Lecture Notes in Computer Science, Vol. 1120)*. Springer, 91–111. https://doi.org/10.1007/3-540-61576-8_77

[14] Seymour Ginsburg and Edwin H. Spanier. 1964. Bounded ALGOL-like languages. *Trans. Amer. Math. Soc.* (1964), 333–368. https://doi.org/10.2307/1994067

[15] Seymour Ginsburg and Edwin H. Spanier. 1966. Semigroups, Presburger formulas, and languages. *Pacific J. Math.* 16, 2 (1966), 285–296. http://projecteuclid.org/euclid.pjm/1102994974

[16] Yuri Gurevich and Peter H. Schmitt. 1984. The Theory of Ordered Abelian Groups does not have the Independence Property. *Trans. Amer. Math. Soc.* 284, 1 (1984), 171–182. https://doi.org/10.2307/1999281

[17] Christoph Haase and Georg Zetzsche. 2019. Presburger arithmetic with stars, rational subsets of graph groups, and nested zero tests. In *Proc. Logic in Computer Science, LICS*. IEEE, 1–14. https://doi.org/10.1109/LICS.2019.8785850

[18] Steve Hanneke. 2016. The Optimal Sample Complexity of PAC Learning. *J. Mach. Learn. Res.* 17, 38 (2016), 1–15. http://jmlr.org/papers/v17/15-389.html

[19] Godfrey H. Hardy and Edward M. Wright. 2008. *An Introduction to the Theory of Numbers*. Oxford University Press.

[20] 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.

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

[22] Marek Karpinski and Angus Macintyre. 1997. Approximating volumes and integrals in o-minimal and p-minimal theories. *Connections between model theory and algebraic and analytic geometry* 6 (1997), 149–177.

[23] Marek Karpinski and Angus Macintyre. 1997. Polynomial Bounds for VC Dimension of Sigmoidal and General Pfaffian Neural Networks. *J. Comput. Syst. Sci.* 54, 1 (1997), 169–176. https://doi.org/10.1006/jcss.1997.1477

[24] Michael J Kearns and Umesh Vazirani. 1994. *An introduction to computational learning theory*. MIT Press.

[25] Eryk Kopczyński. 2015. Complexity of Problems of Commutative Grammars. *Log. Methods Comput. Sci.* 11, 1 (2015). https://doi.org/10.2168/LMCS-11(1:9)2015

[26] Dexter Kozen. 2006. *Theory of Computation*. Springer.

[27] Jesús A. De Loera, Raymond Hemmecke, and Matthias Köppe. 2013. *Algebraic and Geometric Ideas in the Theory of Discrete Optimization*. MOS-SIAM series on optimization, Vol. MO14. SIAM and MOS. https://doi.org/10.1137/1.9781611972443

[28] Jiří Matoušek. 2002. *Lectures on discrete geometry*. Graduate texts in mathematics, Vol. 212. Springer.

[29] Danny Nguyen and Igor Pak. 2018. Enumerating Projections of Integer Points in Unbounded Polyhedra. *SIAM J. Discret. Math.* 32, 2 (2018), 986–1002. https://doi.org/10.1137/17M1118907

[30] Danny Nguyen and Igor Pak. 2019. VC-Dimensions of Short Presburger Formulas. *Combinatorica* 39, 4 (2019), 923–932. https://doi.org/10.1007/s00493-018-4004-x

[31] Danny Nguyen and Igor Pak. 2022. Short Presburger Arithmetic Is Hard. *SIAM J. Comput.* 51, 2 (2022), STOC17–1–STOC17–30. https://doi.org/10.1137/17M1151146

[32] 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. https://doi.org/10.1016/0022-0000(78)90021-1

[33] Andreas Paffenholz. 2013. Polyhedral Geometry and Linear Optimization (Summer Semester 2010). Available at http://www.mathematik.tu-darmstadt.de/~paffenholz/daten/preprints/ln.pdf.

[34] Ruzica Piskac and Viktor Kuncak. 2008. Linear Arithmetic with Stars. In *Proc. Computer Aided Verification, CAV (Lecture Notes in Computer Science, Vol. 5123)*. Springer, 268–280. https://doi.org/10.1007/978-3-540-70545-1_25

[35] Bruno Poizat. 1981. Théories Instables. *J. Symbolic Logic* 46, 3 (1981), 513–522. https://doi.org/10.2307/2273753

[36] 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.

[37] James Renegar. 1992. On the Computational Complexity and Geometry of the First-Order Theory of the Reals, Part II: The General Decision Problem. Preliminaries for Quantifier Elimination. *J. Symb. Comput.* 13, 3 (1992), 301–328. https://doi.org/10.1016/S0747-7171(10)80004-5

[38] R. Tyrrell Rockafellar. 1970. *Convex Analysis*. Princeton University Press.

[39] Norbert Sauer. 1972. On the density of families of sets. *J. Comb. Theory A* 13, 1 (1972), 145–147. https://doi.org/10.1016/0097-3165(72)90019-2

[40] Alexander Schrijver. 1999. *Theory of linear and integer programming*. Wiley.

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

[42] Saharon Shelah. 1971. Stability, the f.c.p., and superstability; model theoretic properties of formulas in first order theory. *Ann. Math. Logic* 3, 3 (1971), 271–362. https://doi.org/10.1016/0003-4843(71)90015-5

[43] Saharon Shelah. 1972. A combinatorial problem; stability and order for models and theories in infinitary languages. *Pacific J. Math.* 41, 1 (1972), 247–261. http://projecteuclid.org/euclid.pjm/1102968432

[44] Eduardo D. Sontag. 1985. Real Addition and the Polynomial Hierarchy. *Inform. Process. Lett.* 20, 3 (1985), 115–120. https://doi.org/10.1016/0020-0190(85)90076-6

[45] Volker Weispfenning. 1997. Complexity and Uniformity of Elimination in Presburger Arithmetic. In *Proc. International Symposium on Symbolic and Algebraic Computation, ISSAC*. ACM, 48–53. https://doi.org/10.1145/258726.258746

[46] Volker Weispfenning. 1999. Mixed Real-Integer Linear Quantifier Elimination. In *Proc. International Symposium on Symbolic and Algebraic Computation, ISSAC*. ACM, 129–136. https://doi.org/10.1145/309831.309888

[47] Pierre Wolper and Bernard Boigelot. 2000. On the Construction of Automata from Linear Arithmetic Constraints. In *Proc. Tools and Algorithms for the Construction and Analysis of Systems, TACAS (Lecture Notes in Computer Science, Vol. 1785)*. Springer, 1–19. https://doi.org/10.1007/3-540-46419-0_1