The Taming of the Semi-Linear Set

Dmitry Chistikov[1] and Christoph Haase[*2]

1 **Max Planck Institute for Software Systems (MPI-SWS), Germany,** `dch@mpi-sws.org`

2 **Laboratoire Spécification et Vérification (LSV), CNRS & ENS de Cachan, France,** `haase@lsv.ens-cachan.fr`

Abstract

Semi-linear sets, which are finitely generated subsets of the monoid $(\mathbb{Z}^d, +)$, have numerous applications in theoretical computer science. Although semi-linear sets are usually given implicitly, by formulas in Presburger arithmetic or by other means, the effect of Boolean operations on semi-linear sets in terms of the size of generators has primarily been studied for explicit representations. In this paper, we develop a framework suitable for implicitly presented semi-linear sets, in which the size of a semi-linear set is characterized by its norm—the maximal magnitude of a generator.

We put together a "toolbox" of operations and decompositions for semi-linear sets which give bounds in terms of the norm (as opposed to just the bit-size of the description), a unified presentation, and simplified proofs. This toolbox, in particular, provides exponentially better bounds for the complement and set-theoretic difference. We also obtain bounds on unambiguous decompositions and, as an application of the toolbox, settle the complexity of the equivalence problem for exponent-sensitive commutative grammars.

1998 ACM Subject Classification G.2 Discrete Mathematics

Keywords and phrases semi-linear sets, convex polyhedra, triangulations, integer linear programming, commutative grammars

Digital Object Identifier 10.4230/LIPIcs.xxx.yyy.p

1 Introduction

Semi-linear sets are a generalisation of ultimately periodic sets of natural numbers to any dimension d. By a classic result due to Ginsburg and Spanier [5], they coincide with the sets of integers[1] definable in Presburger arithmetic (the first-order theory of the integers with addition and order), and hence enjoy closure under all Boolean operations. Their nice properties make them a versatile tool in many application domains such as formal language theory, automata theory, and database theory.

More formally, semi-linear sets are finitely represented finite and infinite subsets of $\mathbb{Z}^d$. For $d \geq 1$, a *semi-linear set* M in dimension d is a finite union of *linear sets*. The latter are presented as a base vector $\boldsymbol{b} \in \mathbb{Z}^d$ and a finite set of period vectors $P = \{\boldsymbol{p}_1, \ldots, \boldsymbol{p}_n\} \subseteq \mathbb{Z}^d$ and have the form

$$L(\boldsymbol{b}, P) := \boldsymbol{b} + \{\lambda_1 \cdot \boldsymbol{p}_1 + \cdots + \lambda_n \cdot \boldsymbol{p}_n : \lambda_1, \ldots, \lambda_n \in \mathbb{N}\}. \tag{1}$$

* Supported by Labex Digicosme, Univ. Paris-Saclay, project VERICONISS.

[1] In the literature, semi-linear sets are often defined as subsets of $\mathbb{N}^d$ instead of $\mathbb{Z}^d$ as in this paper. All of our results do, however, carry over if one wishes to restrict semi-linear sets to $\mathbb{N}^d$.

Such representations are, in fact, only rarely encountered in applications, because in many contexts semi-linear sets are defined implicitly. A semi-linear set can, for instance, be succinctly encoded by a formula in Presburger arithmetic; or a set can be just *proved* to be semi-linear with an estimation of its *norm*, $\|M\|$. The norm is the absolute value of the largest number occurring in the smallest description of M as a union of sets of the form (1). Examples of implicitly presented semi-linear sets include languages of various types of commutative grammars [9, 18] and reachability sets of reversal-bounded counter automata [12, 8].

The effect of Boolean operations is, however, not easy to track in terms of the size of vectors $\boldsymbol{b}$ and $\boldsymbol{p}_i$ if semi-linear sets are only presented implicitly. As an example, consider the set of non-negative integer solutions to a system of linear inequalities $\mathfrak{S}\colon A \cdot \boldsymbol{x} \leq \boldsymbol{c}$, which is a semi-linear set $S \subseteq \mathbb{N}^d$ encoded by $\mathfrak{S}$ with exponential succinctness. Huynh [11, 10] shows that, in general, if the complement of a semi-linear set M is non-empty, then there is some $\boldsymbol{u} \in \mathbb{Z}^d \setminus M$ whose entries are bounded by an exponential in the explicit representation of M—which amounts to doubly exponential in the size of description of $\mathfrak{S}$. This upper bound is far from optimal: by Farkas' lemma, $\overline{M}$ contains an element $\boldsymbol{u}$ whose magnitude $\|\boldsymbol{u}\|$ is at most singly-exponential in the size of description of $\mathfrak{S}$.

Somewhat surprisingly, to the best of the authors' knowledge, there has been no unified framework for deriving bounds of this kind for implicitly presented semi-linear sets. Even if we take an explicitly given linear set as in (1) and describe it by an existential formula $\Psi(\boldsymbol{v})$ in Presburger arithmetic, the representation of the complement with a universally quantified formula $\neg\Psi(\boldsymbol{v})$ provides poor estimates on the magnitude of small elements: although upper bounds can be derived from an analysis of quantifier-elimination procedures, these bounds are only doubly exponential (see, e.g., [24]) and hence far from being optimal.

Our contribution

In this paper, we develop a framework suitable for implicitly presented semi-linear sets (explicitly presented sets are, of course, included as the simplest special case). In this framework the size of a semi-linear set $M \subseteq \mathbb{Z}^d$ is characterised by its norm, $\|M\|$, rather than the full bit-size of the description of M. We prove novel upper bounds in which, as a rule of thumb, the norm of the result of an operation is upper-bounded by $\|M\|^F$ where the quantity F behaves in a "controlled" way (say, $F = \mathsf{poly}(d)$), thus *taming* the effect of Boolean operations and decompositions. In more detail, our contributions are as follows:

- We put together a "toolbox" of operations and decompositions for semi-linear sets, with *tame* bounds, unified presentation, and simplified proofs. This toolbox includes improved bounds on the norm of the complement and, as a corollary, improved bounds on the norm of the set-theoretic difference. These bounds can give an exponential advantage over previously known techniques that upper-bound the bit-size of the result by n^F where n is the bit-size of the description of M—because n can be exponential in $\|M\|$.
- We derive from our toolbox an alternative proof of the Π_2^{P} upper bound for non-emptiness of semi-linear set inclusion, shown originally by Huynh [11, 10]. As an application, we settle the complexity of the equivalence problem for exponent-sensitive commutative grammars, which have recently been introduced by Mayr and Weihmann [18].
- We give a new proof of and provide an explicit upper bound on the unambiguous decomposition of semi-linear sets. It was first asked by Ginsburg [4] whether any semi-linear set is equivalent to a semi-linear set in which every element is generated in a unique way by exactly one linear set. This question was independently positively answered by

Eilenberg and Schützenberger [3] and by Ito [13]. However, to the best of our knowledge, no bounds on this decomposition have been established so far.

We now give a brief guide to the developed techniques and to the remainder of the paper. Our starting point is the fact that the set of non-negative solutions of a system of inequalities $\mathfrak{S}$ can be obtained as $L(B,P) := \bigcup_{\boldsymbol{b}\in B} L(\boldsymbol{b},P)$ for some finite sets $B,P \subseteq \mathbb{N}^d$. We call semi-linear sets of the form $L(B,P)$ *hybrid linear sets* and use them, instead of linear sets, as basic building blocks for general semi-linear sets. A hybrid linear set preserves more structural information about the "infinite behaviour" of the linear sets it contains; it is, in fact, a discrete analogue of the Minkowski-Weyl representation of a convex polyhedron as the sum of a polytope and a convex cone.

Since the effect of operations on linear sets is primarily dominated by the magnitude and number of period vectors, reasoning in terms of hybrid linear sets lets us treat a potentially exponential number of linear sets in a uniform way. This, in turn, enables us, for instance, to obtain bounds on the representation of the intersection of two hybrid linear sets of the form $L(B,P)$ where, as one would indeed expect, the magnitude of the generators of the result does not depend on the cardinality of B (Subsection 2.3).

Our path to the results on the complement and set-theoretic difference of semi-linear sets (Section 4) goes through another development, a *proper disjoint decomposition theorem*. It splits a hybrid linear set into a union $\bigcup_{i\in I} L(B_i,P_i)$ where each P_i is *proper* (i.e., consists of linearly independent vectors) and the *convex hulls* of $L(B_i,P_i)$ are disjoint (Section 3). For this result, we use the concept of a generalised simplex in order to construct triangulations of infinite polyhedra in $\mathbb{Q}^d$, and use the technique of half-open decompositions to ensure the disjointness of the aforementioned convex hulls.

Decomposing $\mathbb{Q}^d$ into convex polyhedra is by no means a new technique in the study of semi-linear sets. In particular, such decompositions were used by Huynh [11, 10] and recently by Kopczyński [14] in the context of semi-linear set inclusion. However, our decomposition theorem is different from theirs and gives stronger corollaries, in that we obtain a full semi-linear representation of the complement and, through intersection, of the set-theoretic difference. While the window theorem of Kopczyński in [14] gives an upper on the magnitude of the smallest vector in the set difference, our results upper-bound on the magnitude of the largest generator.

2 Preliminaries

2.1 Basic definitions

Let $\mathbb{Z}$, $\mathbb{N}$, $\mathbb{Q}$, and $\mathbb{Q}_{\geq 0}$ denote the set of integers, non-negative integers, rationals, and non-negative rationals, respectively. For $x \in \mathbb{Q}$, $\lfloor x \rfloor$ is the largest integer that does not exceed x. For subsets of numbers or vectors A and B, we use the Minkowski sum notation: $A + B := \{a + b : a \in A, b \in B\}$. In this and other contexts, we often omit the curly braces when referring to singletons. For sets of vectors $P = \{\boldsymbol{p}_1, \ldots, \boldsymbol{p}_n\}, Q \subseteq \mathbb{Z}^m$, we may assume some fixed ordering on their elements, e.g., a lexicographic ordering, and thus sometimes treat P as a matrix whose column vectors are $\boldsymbol{p}_1, \ldots, \boldsymbol{p}_n$. This leads to the notation $P \cdot \boldsymbol{\lambda}$ and $P \cdot Q$, for products of P with a vector $\boldsymbol{\lambda}$ and a matrix Q, respectively.

Linear, hybrid linear, and semi-linear sets

Suppose a natural $d \geq 1$ is fixed; we will call this d the *dimension.* A set $L \subseteq \mathbb{Z}^d$ is called *linear* if it is of the form

$$L = L(\boldsymbol{b}, P) := \{\boldsymbol{b} + \lambda_1 \boldsymbol{p}_1 + \cdots + \lambda_k \boldsymbol{p}_k : \lambda_1, \ldots, \lambda_k \in \mathbb{N}, \boldsymbol{p}_1, \ldots, \boldsymbol{p}_k \in P\} \tag{2}$$

where $\boldsymbol{b} \in \mathbb{Z}^d$ and $P \subseteq \mathbb{Z}^d$ is a finite set. We call the vector $\boldsymbol{b}$ the *base vector* and vectors $\boldsymbol{p} \in P$ the *period vectors* (or simply *base* and *periods*) of L. A set $S \subseteq \mathbb{Z}^d$ is called *semi-linear* if it is a finite union of linear sets. Semi-linear sets can be represented as

$$S = \bigcup_{i \in I} L(B_i, P_i) \quad \text{where} \tag{3}$$

$$L(B_i, P_i) := \bigcup_{\boldsymbol{b}_i \in B_i} L(\boldsymbol{b}_i, P_i) \tag{4}$$

and $L(\boldsymbol{b}_i, P_i)$ is as in (2); we call sets $L(B_i, P_i)$ in (4) *hybrid linear sets.* Every linear set is also a hybrid linear set, and every hybrid linear set is semi-linear, but the converse statements are not true in general.

A hybrid linear set $L(B_i, P_i)$ is *proper* if the vectors P_i are linearly independent. Moreover, a hybrid linear set $L(B, P)$, $\#P = r$, is called *unambiguous* if for every $\boldsymbol{x} \in L(B, P)$ there exist a unique $\boldsymbol{b} \in B$ and a unique $\boldsymbol{\lambda} \in \mathbb{N}^r$ such that $\boldsymbol{x} = \boldsymbol{b} + P \cdot \boldsymbol{\lambda}$. A representation $\bigcup_{i \in I} L(B_i, P_i)$ is an *unambiguous decomposition* if each hybrid linear set $L(B_i, P_i)$ is unambiguous and the union is disjoint.

From the computational perspective, it is standard to represent semi-linear sets of the form (3) by listing all vectors in the sets B_i, P_i for all $i \in I$; components of the vectors are written in binary. We use the following notation to refer to various size measures for this representation. For any set A, the number of elements of A is $\#A$. For any $\boldsymbol{v} = (v_1, \ldots, v_d) \in \mathbb{Z}^d$, $\|v\| := \max_{1 \leq i \leq d} |v_i|$; similarly, for any $A \subseteq \mathbb{Z}^d$ we denote $\|A\| := \max_{\boldsymbol{v} \in A} \|\boldsymbol{v}\|$; observe that $\#A \leq (\|A\| + 1)^d$. Finally, for the representation (3) of a semi-linear set S we write $\|S\| := \max(\max_{i \in I} \|B_i\|, \max_{i \in I} \|P_i\|)$, $\#_{\mathsf{b}} S := \max_{i \in I} \#B_i$, $\#_{\mathsf{p}} S := \max_{i \in I} \#P_i$, and $\#_{\mathsf{b+p}} S := \#_{\mathsf{b}} S + \#_{\mathsf{p}} S$.

Convex polyhedra

We now introduce some terminology and notation from convex geometry. For a system of vectors $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k \in \mathbb{Q}^d$, a linear combination $\lambda_1 \boldsymbol{v}_1 + \ldots + \lambda_k \boldsymbol{v}_k$ with $\lambda_1, \ldots, \lambda_k \in \mathbb{Q}$ is called: *non-negative*, or *conical*, if all $\lambda_i \geq 0$; *affine* if $\sum_{i=1}^{k} \lambda_i = 1$; and *convex* if it is non-negative and affine. For a possibly infinite set of vectors $A \subseteq \mathbb{Q}^d$, by $\operatorname{cone} A$, $\operatorname{aff} A$, and $\operatorname{conv} A$ we denote the *(rational) cone generated by* A, the *affine hull of* A, and the *convex hull of* A, respectively: they are the sets of all non-negative, affine, and convex combinations of finite subsets of A, respectively. We use the convention that $\mathbf{0} \in \operatorname{cone} A$ for any A; in particular, $\operatorname{cone} \emptyset = \{\mathbf{0}\}$. However, $\operatorname{conv} \emptyset = \emptyset$. Sets of the form $\boldsymbol{b} + \operatorname{cone} A$, for $\boldsymbol{b} \in \mathbb{Q}^d$, are *shifted cones*; we often refer to them simply as cones.

A set $X \subseteq \mathbb{Q}^d$ is said to *recede* in direction $\boldsymbol{y} \in \mathbb{Q}^d \setminus \{\mathbf{0}\}$ if $X + \lambda \boldsymbol{y} \subseteq X$ for all $\lambda \subseteq \mathbb{Q}_{\geq 0}$; the vector $\boldsymbol{y}$ is then a *direction of recession* for X. Note that shifted cones of the form $\boldsymbol{b} + \operatorname{cone} A$ recede in all directions from $\operatorname{cone} A \setminus \{\mathbf{0}\}$.

For any non-empty set $X \subseteq \mathbb{Q}^d$ its affine hull satisfies $X = X_0 + \boldsymbol{v}$ for some vector $\boldsymbol{v} \in \mathbb{Q}^d$ and a uniquely determined subspace of $\mathbb{Q}^d$ denoted X_0. The *dimension* of X, written as $\dim X$, is the dimension of the subspace X_0.

A *(rational) convex polyhedron* in $\mathbb{Q}^d$ is a set of the form $\{\boldsymbol{x} \in \mathbb{Q}^d : A \cdot \boldsymbol{x} \leq \boldsymbol{b}\}$ where $A \in \mathbb{Z}^{m \times d}$ and $\boldsymbol{b} \in \mathbb{Z}^m$ for some m. A *face* of a convex polyhedron $W \subseteq \mathbb{Q}^d$ is a set of points where some linear function $\eta\colon \mathbb{Q}^d \to \mathbb{Q}$ achieves its maximum η^* over W; the hyperplane $h = \{\boldsymbol{x} \in \mathbb{Q}^d : \eta(\boldsymbol{x}) = \eta^*\}$ is a *supporting hyperplane* of W. A face of a convex polyhedron is always a convex polyhedron itself. Faces of dimension 0, 1, and $\dim W - 1$ are *vertices*, *edges*, and *facets* respectively. All faces of W form a partial order with respect to set inclusion, the largest element being the set W itself (it is always a face by convention).

For a hybrid linear set $L(B, P)$, we denote $K(B, P) := \operatorname{conv} L(B, P) = \operatorname{conv} B + \operatorname{cone} P$. Note that if B is a singleton, i.e., if $L(B, P)$ is a linear set, then $K(B, P)$ is a rational cone; in general, though, $K(B, P)$ is a convex polyhedron.

Given a set S, we call its representation (3) a *proper disjoint decomposition* if each hybrid linear set $L(B_i, P_i)$ is proper and $K(B_i, P_i) \cap K(B_j, P_j) = \emptyset$ for $i \neq j$.

2.2 Auxiliary tools: Systems of linear inequalities

Let $A \in \mathbb{Z}^{m \times n}$ be an integer $m \times n$-matrix and $\boldsymbol{c} \in \mathbb{Z}^m$. We call $\mathfrak{S}\colon A \cdot \boldsymbol{x} \leq \boldsymbol{c}$ a *system of linear inequalities* and $\mathfrak{T}\colon A \cdot \boldsymbol{x} = \boldsymbol{c}$ a *system of linear equations*. By $[\![\mathfrak{S}]\!], [\![\mathfrak{T}]\!] \subseteq \mathbb{Z}^n$ we denote the *solution set* of $\mathfrak{S}$ and $\mathfrak{T}$, i.e, the set of all $\boldsymbol{v} \in \mathbb{Z}^n$ such that $A \cdot \boldsymbol{v} \leq \boldsymbol{b}$ and $A \cdot \boldsymbol{v} = \boldsymbol{b}$, respectively, where $\leq$ is interpreted component-wise. We use $[\![\mathfrak{T}]\!]_{\geq 0}$ as a shorthand for $[\![\mathfrak{T}]\!] \cap \mathbb{N}^n$, and write $(\!|\mathfrak{S}|\!)$ for the set of rational solutions from $\mathbb{Q}^n$ of $\mathfrak{S}$. Moreover, we define $\|\mathfrak{S}\|, \|\mathfrak{T}\| := \max\{\|A\|, \|\boldsymbol{c}\|\}$. We first recall a result of von zur Gathen and Sieveking on the sets of solutions of systems of linear inequalities [23].

▶ **Proposition 1.** *Let $\mathfrak{S}\colon A \cdot \boldsymbol{x} \leq \boldsymbol{c}$ be a system of inequalities such that $A \in \mathbb{Z}^{m \times n}$. Then $[\![\mathfrak{S}]\!] = \bigcup_{i \in I} L(B_i, P_i)$ such that*
- *$K(B_i, P_i) \cap K(B_j, P_j) = \emptyset$ for all $i \neq j$,*
- *$\max_{i \in I} \|B_i\|, \max \|P_i\| \leq 2^{n^2+n} \cdot (\|A\| + \|\boldsymbol{c}\|)$,*
- *$\#I \leq 2^n$.*

Next, we additionally recall a result on the sets of solutions of linear equalities that follows from results of Domenjoud [2] and Pottier [20].

▶ **Proposition 2.** *Let $\mathfrak{S}_0\colon A \cdot \boldsymbol{x} = \boldsymbol{0}$ and $\mathfrak{S}\colon A \cdot \boldsymbol{x} = \boldsymbol{c}$ be systems of linear Diophantine equations, where $A \in \mathbb{Z}^{d \times n}$. Then $[\![\mathfrak{S}_0]\!]_{\geq 0} = L(\boldsymbol{0}, P)$ and $[\![\mathfrak{S}]\!]_{\geq 0} = L(B, P)$ such that*
- *$\|B\| \leq ((n+1) \cdot \|A\| + \|\boldsymbol{c}\| + 1)^d$, $\|P\| \leq (n \cdot \|A\| + 1)^d$,*
- *$\#B \leq (n+1)^d$, and $\#P \leq n^d$.*

The following two propositions let us switch between representations of rational convex polyhedra in $\mathbb{Q}^d$.

▶ **Proposition 3** ([19])**.** *Let $\mathfrak{S}\colon A \cdot \boldsymbol{x} \leq \boldsymbol{c}$ be a convex polyhedron in $\mathbb{Q}^n$. Then there are $B \subseteq \mathbb{Q}^n$ and $P \subseteq \mathbb{Z}^n$ such that $(\!|\mathfrak{S}|\!) = \operatorname{conv} B + \operatorname{cone} P$, $\|P\| \leq 2^{O(n^3)} \cdot \|\mathfrak{S}\|^n$, and all numerators and denominators in B are bounded by $2^{O(n^2)} \cdot \|\mathfrak{S}\|$.*

Proof. It is shown in [19, Prop. 5.12] that there are $C, Q \subseteq \mathbb{Q}^n$ such that $[\![\mathfrak{S}]\!] = \operatorname{conv} C + \operatorname{conv} Q$ and $\|C\|, \|Q\| \leq 2^{O(n^2)} \cdot \|\mathfrak{S}\|$. In order to obtain the desired set of integer vectors P, the numbers in each element $\boldsymbol{v} \in Q$ can be multiplied through by the least common multiple of the denominators of its entries, yielding the set P with the desired properties. ◀

▶ **Proposition 4** ([19])**.** *Let $M = L(\boldsymbol{b}, P) \subseteq \mathbb{Z}^d$ be a proper linear set. There exists a system of linear inequalities $\mathfrak{S}\colon A \cdot \boldsymbol{x} \leq \boldsymbol{c}$ such that*
- *A is a $2d \times d$-matrix that does not depend on $\boldsymbol{b}$,*
- *$\|A\|, \|\boldsymbol{c}\| \leq 2^{O(d^3)} \cdot (\max(\|\boldsymbol{b}\|, \|P\|))^d$, and*

- $\operatorname{conv} L(\boldsymbol{b}, P) = (\!|\mathfrak{S}|\!)$.

Proof. Since M is proper, $\operatorname{conv} L(\boldsymbol{b}, P)$ has at most d facets, resulting in at most $2 \cdot d$ inequalities in $\mathfrak{S}$. By [19, Prop. 5.12], A and $\boldsymbol{c}$ are rational matrices whose entries are bounded by $2^{O(d^2)} \cdot \max(\|\boldsymbol{b}\|, \|P\|)$. Multiplying each row through by the least common multiple of its denominators, we obtain the desired bounds on A and $\boldsymbol{c}$. ◀

Finally, we will need a discrete version of Carathéodory's theorem:

▶ **Proposition 5.** *Let $M = \bigcup_{j \in J} L(C, Q)$ be a hybrid linear set. Then $M = \bigcup_{i \in I} L(B_i, P_i)$ such that*
- $\max_{i \in I} \|B_i\| \leq \|C\| + (\#Q \cdot \|Q\|)^{O(d)}$,
- $\max_{i \in I} \#P_i \leq d$, *$P_i \subseteq P$ and each P_i is linearly independent, and*
- $\#I \leq (\#Q)^d$.

The proof can be found in the appendix and is essentially a combination of Lemmas 2.7 and 2.8 in [9], which do however not establish any concrete bounds. In our proof, we use the result on the intersection of hybrid linear sets from the following subsection 2.3.

2.3 Intersection of semi-linear sets

▶ **Theorem 6.** *Let M and N be semi-linear sets with representations $M = \bigcup_{j \in J} L(C_j, Q_j)$, $N = \bigcup_{k \in K} L(D_k, R_k)$. Then the set $L := M \cap N$ is a semi-linear set with representation $L = \bigcup_{i \in I} L(B_i, P_i)$ such that $I = J \times K$,*
- $\max_{i \in I} \|B_i\|, \max_{i \in I} \|P_i\| \leq ((\#_{\mathsf{p}} M + \#_{\mathsf{p}} N) \cdot \max(\|M\|, \|N\|))^{O(d)}$,
- $\max_{i \in I} \#B_i \leq (\#_{\mathsf{b}} M + \#_{\mathsf{b}} N) \cdot (\#_{\mathsf{p}} M + \#_{\mathsf{p}} N)^{O(d)}$,
- $\max_{i \in I} \#P_i \leq (\#_{\mathsf{p}} M + \#_{\mathsf{p}} N)^d$, *and*
- $\#I \leq \#J \cdot \#K$.

Moreover, if $Q_j \subseteq R_k$ and $i = (j, k)$ then $P_i = Q_j$.

Proof (sketch). We have $M \cap N = \bigcup_{j \in J} L(C_j, Q_j) \cap \bigcup_{k \in K} L(D_k, R_k) = \bigcup_{j \in J, k \in K} L(C_j, Q_j) \cap L(D_k, R_k)$. Hence it suffices to show that every $L(C_j, Q_j) \cap L(D_k, R_k)$ is some $L(B_{j,k}, P_{j,k})$ with the desired properties. To this end, one can obtain the set of elements in the intersection as the set of solutions to a suitable system of linear equations and then apply the bounds from Proposition 2. Finally, the fact that if $Q_j \subseteq R_k$ then $P_i = Q_j$ follows from Theorem 5.6.1 in [4, p. 180]. ◀

3 Hybrid linear sets

In the sequel, we develop a close connection between hybrid linear sets and convex polyhedra viewed as generalized convex hulls. Convex polyhedra in $\mathbb{Q}^d$ are sets of the form $\operatorname{conv} C + \operatorname{cone} Q$ for $C, Q \subseteq \mathbb{Q}^d$; they can be viewed as a convex hulls of a set of points C and *directions* Q. Suppose $C = \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_r\}$ and $Q = \{\boldsymbol{p}_1, \ldots, \boldsymbol{p}_m\}$. The connection builds upon on the similarity of the following sets:

$$\operatorname{conv} C + \operatorname{cone} Q = \left\{ \sum_{i=1}^{r} \lambda_i \boldsymbol{b}_i + \sum_{j=1}^{m} \mu_j \boldsymbol{p}_j : \lambda_i \in \mathbb{Q}_{\geq 0},\ \sum_{i=1}^{r} \lambda_i = 1,\ \mu_j \in \mathbb{Q}_{\geq 0} \right\} \text{ and}$$

$$L(C, Q) = \left\{ \sum_{i=1}^{r} \lambda_i \boldsymbol{b}_i + \sum_{j=1}^{m} \mu_j \boldsymbol{p}_j : \lambda_i \in \mathbb{N},\ \sum_{i=1}^{i} \lambda_i = 1,\ \mu_j \in \mathbb{N} \right\}.$$

As mentioned above, $\operatorname{conv} L(C, Q) = K(C, Q) = \operatorname{conv} C + \operatorname{cone} Q$.

3.1 Proper disjoint decompositions (PDD)

Recall that $S = \bigcup_{i \in I} L(B_i, P_i)$ is a proper disjoint decomposition if vectors in each P_i are linearly independent and the convex hulls $K(B_i, P_i) = \operatorname{conv} L(B_i, P_i)$ are pairwise disjoint.

▶ **Theorem 7** (PDD for hybrid linear sets). *Every hybrid linear set $M = L(C, Q)$ has a proper disjoint decomposition $\bigcup_{i \in I} L(B_i, P_i)$ where each P_i is a subset of Q and the following inequalities hold:*
- $\|B_i\| \le (\#Q + \|C\| + \|Q\| + d)^{O(d)} \le \|M\|^{O(d^2)}$,
- $\#B_i \le ((\|C\| + \|Q\| + d)^{O(d)} + \#C) \cdot (d + \#Q)^{O(d)} \le \|M\|^{O(d^2)}$,
- $\#I \le (\#Q)^{d+1}$.

The idea of the proof of Theorem 7 is to rely on the connection between hybrid linear sets and convex polyhedra. We will use the observation that each set of the form $\operatorname{conv} C + \operatorname{cone} Q$ has a triangulation. While this term usually refers to the basic construction that splits a convex polygon in a plane into a number of non-overlapping triangles, we will use a construction that extends this concept in two ways: first, instead of $\mathbb{Q}^2$ the sets are in $\mathbb{Q}^d$, so triangles become simplices; second, the sets can be infinite, i.e., with $Q \neq \emptyset$.

The strategy of the proof of Theorem 7 is depicted in the following diagram:

$$\begin{array}{ccl} L(C,Q) & \xrightarrow{\;3\;} & \Pi, \text{ a proper disjoint decomposition of } L(C,Q) \\ \big\downarrow{\scriptstyle 1} & & \big\uparrow{\scriptstyle 3} \\ K(C,Q) & \xrightarrow{\;2\;} & \mathcal{T}, \text{ a triangulation of } K(C,Q) \end{array}$$

Step 1 is just taking the convex hull as above, step 2 is the triangulation in $\mathbb{Q}^d$, and step 3 constructs a proper disjoint decomposition given the original set $L(C, Q)$ and the triangulation of $K(C, Q)$.

A *generalized δ-dimensional simplex* T is a set of the form $T = \operatorname{conv} V + \operatorname{cone} D \subseteq \mathbb{Q}^d$ where $\#V + \#D = \delta + 1$, $V \neq \emptyset$, and the dimension of the affine hull of T is exactly δ. Elements of V are ordinary vertices of T, and elements of D are vertices at infinity and can be understood as directions. (The set D is, in fact, the set of extreme directions of the set T, see [21, p. 162].) Faces of generalized simplices $\operatorname{conv} V + \operatorname{cone} D$ are also generalized simplices and have the form $\operatorname{conv} V' + \operatorname{cone} D'$ where $V' \subseteq V$ and $D' \subseteq D$.

A *triangulation* of a set $W \subseteq Z^d$ is a collection $\mathcal{T}$ of generalized simplices that satisfies the following properties:
1. $\bigcup_{F \in \mathcal{T}} F = W$;
2. for every $F \in \mathcal{T}$ and every face F' of F, it holds that $F' \in \mathcal{T}$;
3. the intersection of any two $F_1, F_2 \in \mathcal{T}$ is either empty or is a face of both F_1 and F_2;
4. all (generalized) simplices in the set of maxima of $\mathcal{T}$, denoted $\operatorname{Max} \mathcal{T} := \{F' \in \mathcal{T} : \nexists F \in \mathcal{T}.\ F' \text{ is a face of } F \text{ and } F \neq F'\}$, have the same dimension δ, denoted $\dim \mathcal{T}$.

In other words, a triangulation of W is a pure polyhedral complex that consists of generalized simplices and covers exactly W.

To simplify notation, we write $\mathcal{T} = (T_1, \ldots, T_m)$ whenever $\operatorname{Max} \mathcal{T} = \{T_1, \ldots, T_m\}$; of course, the set $\{T_1, \ldots, T_m\}$ is a subset of the set $\mathcal{T}$. It is straightforward that $W = T_1 \cup \ldots \cup T_m$ if $\mathcal{T} = (T_1, \ldots, T_m)$ is a triangulation of W. Conversely, if $T_1, \ldots, T_m$ are (generalized) simplices of equal dimension such that the collection $\mathcal{T}$ of all their faces satisfies Condition 3 in the definition of triangulation, then this collection $\mathcal{T}$ is a triangulation of $T_1 \cup \ldots \cup T_m$. Lemma 8 triangulates possibly unbounded convex polyhedra (for non-empty Q, it treats its elements as vertices at infinity) without introducing new vertices or directions.

▶ **Lemma 8.** *Every polyhedron of the form $W = \operatorname{conv} C + \operatorname{cone} Q \subseteq \mathbb{Q}^d$ has a triangulation $\mathcal{T} = (T_1, \ldots, T_m)$ where $m \le (\#C + \#Q)^{d+1}$ and $T_i = \operatorname{conv} C_i + \operatorname{cone} Q_i$ with $C_i \subseteq C$ and $Q_i \subseteq Q$ for all i.*

Note that adjacent simplices T_i and T_j in a triangulation can share points in common lower-dimensional faces and so, for our purposes, should be transformed into disjoint sets. Suppose U is a polyhedron of the form $X = \{\boldsymbol{x} \in \mathbb{Q}^d : \boldsymbol{a}_i \cdot \boldsymbol{x} \le b_i, 1 \le i \le m\}$ where $\boldsymbol{a}_i \in \mathbb{Z}^d$ and $b_i \in \mathbb{Z}$ for all i. For any $A \subseteq \{1, \ldots, m\}$, we call the set

$$X_A = \{\boldsymbol{x} \in \mathbb{Q}^d : \boldsymbol{a}_i \cdot \boldsymbol{x} < b_i, i \in A, \text{ and } \boldsymbol{a}_i \cdot \boldsymbol{x} \le b_i, i \in \{1, \ldots, m\} \setminus A\}$$

a *half-opening* of U obtained by cutting off the hyperplanes $\boldsymbol{a}_i \cdot \boldsymbol{x} = b_i$, $i \in A$.

▶ **Lemma 9.** *Let W be a δ-dimensional polyhedron in $\mathbb{Q}^d$. For each triangulation $\mathcal{T} = (T_1, \ldots, T_m)$ of W there exists a collection of sets $\mathcal{T}^0 = (T_1^0, \ldots, T_m^0) \subseteq \mathbb{Q}^d$ that satisfies the following conditions:*

1. *$T_1^0 \cup \ldots \cup T_m^0 = W$;*
2. *for every i, T_i^0 is a half-opening of T_i;*
3. *T_i and T_j are disjoint for $i \ne j$.*

Lemma 9 is the *half-open decomposition*, originally from [1] and [15]. Our formulation is a direct corollary of Theorem 3 in the latter paper; see also [6, Section 3.2].

▶ **Lemma 10.** *Suppose $T = \operatorname{conv} V + \operatorname{cone} D$ is a generalized δ-dimensional simplex in $\mathbb{Q}^d$ where $V, D \subseteq \mathbb{Z}^d$ and $\#V + \#D = \delta + 1$. Then for any half-opening T^0 of T it holds that $T^0 \cap \mathbb{Z}^d = L(E, D)$ where $\|E\| \le \|V\| + (d+1) \cdot \|D\|$ and $\#E \le (\|V\| + (d+1) \cdot \|D\| + 1)^d$.*

Proof of Theorem 7 (sketch). Take a triangulation of $W = K(C, Q) = \operatorname{conv} C + \operatorname{cone} Q$, which exists by Lemma 8, and apply Lemma 9 to this triangulation. The result is a collection $\mathcal{T}^0 = (T_1^0, \ldots, T_m^0)$ where each T_i^0 is a half-opening of some generalized simplex $\operatorname{conv} C_i + \operatorname{cone} Q_i$ such that $C_i \subseteq C$ and $Q_i \subseteq Q$. By Lemma 10, $T_i^0 \cap \mathbb{Z}^d = L(D_i, Q_i)$. We now apply Theorem 6: since $Q_i \subseteq Q$, we have $L(D_i, Q_i) \cap L(C, Q) = L(B_i, P_i)$ where $P_i = Q_i$. Vectors in each set $P_i = Q_i$ are, in fact, linearly independent, because $\operatorname{conv} C_i + \operatorname{cone} Q_i$ is a generalized simplex. Moreover, $K(B_i, P_i) \subseteq \operatorname{conv} L(D_i, Q_i) \subseteq T_i^0$ for each i; since the sets $T_1^0, \ldots, T_m^0$ are pairwise disjoint, so are the sets $K(B_i, P_i)$. Finally,

$$\begin{aligned} \bigcup_{i=1}^{m} L(B_i, P_i) &= \bigcup_{i=1}^{m} T_i^0 \cap \mathbb{Z}^d \cap L(C, Q) = L(C, Q) \cap \bigcup_{i=1}^{m} T_i^0 \\ &= L(C, Q) \cap W = L(C, Q) \cap \operatorname{conv} L(C, Q) = L(C, Q). \end{aligned}$$ ◀

3.2 Unambiguous decompositions (UD)

The main results of this subsection are the following theorems:

▶ **Theorem 11** (UD for proper hybrid linear sets). *Every proper hybrid linear set $M = L(C, Q)$ has an unambiguous decomposition $\bigcup_{i \in I} L(B_i, P_i)$ where each P_i is a subset of Q and the following conditions are satisfied:*

- *$\|B_i\| \le \|C\|$, and*
- *$\#I \le (2 \cdot \#C)^{\#Q}$.*

▶ **Theorem 12** (UD for hybrid linear sets). *Every hybrid linear set $M = L(C, Q)$ has an unambiguous decomposition $\bigcup_{i \in I} L(B_i, P_i)$ where each P_i is a subset of Q and the following inequalities hold:*

- $\|B_i\| \le (\#Q + \|C\| + \|Q\| + d)^{O(d)} \le \|M\|^{O(d^2)}$, *and*
- $\#I \le ((\|C\| + \|Q\| + d)^{O(d)} + \#C)^d \cdot (d + \#Q)^{O(d^2)} \le \|M\|^{O(d^3)}$.

We now show how to prove Theorem 11. The idea is to reduce the disambiguation of a proper hybrid linear set to disambiguation of an ideal in a finitely generated commutative monoid, captured by the following lemma. Here and below, by $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_r$ we denote coordinate vectors in $\mathbb{N}^r$.

▶ **Lemma 13.** *Every set of the form $U = F + \mathbb{N}^r$ with a finite $F \subseteq \mathbb{N}^r$ has a representation $U = \bigcup_{k \in K} L(G_k, E_k)$ such that the following conditions are satisfied:*
- *each set $L(G_k, E_k)$ is unambiguous,*
- *the polyhedra $\operatorname{conv} L(G_k, E_k)$ and $\operatorname{conv} L(G_{k'}, E_{k'})$ are disjoint for $k \ne k'$,*
- $\|G_k\| \le \|F\|$,
- *$E_k \subseteq \{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_r\}$, and*
- $\#K \le (\#F + 1)^r$.

Proof (sketch). The condition that a vector $\boldsymbol{x}$ belongs to $F + \mathbb{N}^r$ can be specified by a logical formula Φ over predicates of the form $x_j \ge c$. These predicates break up $\mathbb{N}^r$ into at most $(m + 1)^r$ disjoint regions, and each region is described by a unambiguous hybrid linear set in a straightforward way. ◀

Proof of Theorem 11 (sketch). Take $M = L(C, Q) \subseteq \mathbb{Z}^d$ where $Q = \{\boldsymbol{q}_1, \ldots, \boldsymbol{q}_r\} \subseteq \mathbb{Z}^d$ and vectors in Q are linearly independent, $r \le d$. Consider the *point lattice* $\mathcal{L} = Q \cdot \mathbb{Z}^r = \{Q \cdot \boldsymbol{\lambda} : \lambda \in \mathbb{Z}^r\}$; see, e.g., [17, Chapter 2]. Vectors $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{Z}^r$ are congruent modulo $\mathcal{L}$, $\boldsymbol{x} \equiv \boldsymbol{y} \pmod{\mathcal{L}}$ if and only if $\boldsymbol{x} - \boldsymbol{y} \in \mathcal{L}$. This congruence splits the set C into a disjoint union $C = C_1 \cup \ldots \cup C_s$ where $\boldsymbol{x} \in C_i$ and $\boldsymbol{y} \in C_j$ are congruent if and only if $i = j$. It is easy to see that $M = \bigcup_{1 \le j \le s} L(C_j, Q)$ is a disjoint union, and disambiguating each $L(C_j, Q)$ separately will disambiguate M.

Suppose $C_1 = \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m\} \subseteq \boldsymbol{x}_1 + \mathcal{L}$. Since the vectors in $Q = \{\boldsymbol{q}_1, \ldots, \boldsymbol{q}_r\}$ are linearly independent, each vector from the set $\boldsymbol{x}_1 + \mathcal{L}$ has a unique expansion of the form $\boldsymbol{x}_1 + \sum_{j=1}^r a_j \boldsymbol{q}_j$. Consider the mapping $\psi \colon \boldsymbol{x}_1 + \mathcal{L} \to \mathbb{Z}^r$ taking each vector $\boldsymbol{x}_1 + \sum_{j=1}^r a_j \boldsymbol{q}_j$ to the vector $(a_1, \ldots, a_r) \in \mathbb{Z}^r$. For each j, let a_j^0 be the smallest of the numbers $\psi(\boldsymbol{x}_t)[j]$ over $1 \le t \le m$; here $[j]$ refers to the jth component of an r-dimensional vector. Denote $\boldsymbol{a}^0 = (a_1^0, \ldots, a_r^0)$ and let $\psi' : \boldsymbol{x}_1 + \mathcal{L} \to \mathbb{Z}^r$ be given by $\psi'(\boldsymbol{x}) = \psi(\boldsymbol{x}) - \boldsymbol{a}^0$. Observe that the mapping ψ' is injective and maps C_1 to some finite set $F \subseteq \mathbb{N}^r$; in fact, $\psi'(L(C_1, Q_1)) = F + \mathbb{N}^r$. After this, it remains to apply Lemma 13. ◀

4 Semi-linear sets

4.1 Geometric ingredients: Splitting into atomic polyhedra

Consider a semi-linear set given by $M = \bigcup_{j \in J} L(C_j, Q_j)$. Take the proper disjoint decomposition of each $L(C_j, Q_j)$ according to Theorem 7; this decomposes M as

$$M = \bigcup_{j \in J} \bigcup_{t \in T_j} L(C_{jt}, Q_{jt}), \tag{5}$$

where hybrid linear sets $L(C_{jt}, Q_{jt})$ are proper and, moreover, for any fixed j the polyhedra $K(C_{jt}, Q_{jt})$ are pairwise disjoint.

Denote by $\mathcal{H}$ the collection of principal supporting hyperplanes for shifted cones $K(\boldsymbol{b}, Q_{jt})$, $\boldsymbol{b} \in C_{jt}$, $t \in T_j$, and $j \in J$: for each cone, take its d principal supporting hyperplanes, i.e., those hyperplanes obtained in Proposition 4, each of the form $h\colon \boldsymbol{a}\cdot\boldsymbol{x} = c$ (with fixed $\boldsymbol{a}\in\mathbb{Z}^d$ and $c\in\mathbb{Z}$), and put them into $\mathcal{H}$. Note that each hyperplane h' is associated with half-spaces $h^-\colon \boldsymbol{a}\cdot\boldsymbol{x}\le c$ and $h^+\colon \boldsymbol{a}\cdot\boldsymbol{x}\ge c+1$; moreover, we can pick the signs so that $K(\boldsymbol{b},Q_{jt})\subseteq h^-$. An *atomic polyhedron* with respect to $\mathcal{H}$ is a non-empty set of the form

$$A(H) = \bigcap_{h\in H} h^- \cap \bigcap_{h\in\mathcal{H}\setminus H} h^+,$$

where $H\subseteq\mathcal{H}$. Clearly, $\mathbb{Z}^d\subseteq\bigcup_{H\subseteq\mathcal{H}} A(H)$.

▶ **Lemma 14.** *For every $L(\boldsymbol{b},Q_{jt})$ with $\boldsymbol{b}\in C_{jt}$ and every $A = A(H)$, either $A\subseteq \operatorname{conv} L(\boldsymbol{b},Q_{jt})$ or $A\cap\operatorname{conv} L(\boldsymbol{b},Q_{jt}) = \emptyset$.*

Take a hybrid linear set $L(C_{jt},Q_{jt})$ and let $\boldsymbol{b}\in C_{jt}$. We say that the linear set $L(\boldsymbol{b},Q_{jt})$ *shares* an atomic polyhedron A iff $A\subseteq\operatorname{conv} L(\boldsymbol{b},Q_{jt})$; otherwise we say that it *avoids* A.

▶ **Lemma 15.** *Every atomic polyhedron $A(H)$ is the set of rational solutions to a system of at most $O(d\cdot\sum_{j\in J}(\#Q_j)^{d+1})$ linear inequalities with entries bounded by $2^{O(d^3)}\cdot(\#Q + \|C\|+\|Q\|+d)^{O(d^2)}$.*

▶ **Lemma 16.** *The number of atomic polyhedra is at most $\left(d\cdot\sum_{j\in J}\#C_j\cdot(\#Q_j)^{d+1}\right)^{d+1}$.*

Consider an atomic polyhedron A; in everything that follows, we assume that A is shared by at least one linear set. Even though the total number of sets of the form $L(\boldsymbol{b},Q_{jt})$ that share A can be large, the following property holds.

▶ **Lemma 17.** *If linear sets $L(\boldsymbol{b},Q_{jt})$ and $L(\boldsymbol{b}',Q_{jt'})$ share A, then $t=t'$. In particular, the number of pairs (j,t) such that some linear set $L(\boldsymbol{b},Q_{jt})$ shares A does not exceed $\#J$.*

▶ **Lemma 18.** *For every A there exist finite sets $E\subseteq\mathbb{Q}^d$ and $G\subseteq\mathbb{Z}^d$ that satisfy the following conditions:*

1. *$A = \operatorname{conv} E + \operatorname{cone} G$,*
2. *for every linear set $L(\boldsymbol{b},Q_{jt})$ that shares A, the set G is a subset of $L(\boldsymbol{0},Q_{jt})$,*
3. *numerators and denominators of all entries in all $\boldsymbol{e}\in E$ are bounded by $\|M\|^{O(d^4)}$,*
4. *$\|G\|\le\|M\|^{\#J\cdot O(d^4)}$.*

It is worth mentioning that the upper bound on $\|G\|$ in Lemma 18 relies on the fact that, for every $j\in J$, our decomposition (5) ensures disjointness of $K(C_{jt},Q_{jt})$ among $t\in T_j$; the proof of Lemma 18 uses this property via Lemma 17.

4.2 Decompositions, complement, and difference

We first state the results on decompositions of semi-linear sets and on the semi-linear representation of the complement.

▶ **Theorem 19** (PDD for semi-linear sets)**.** *Every semi-linear set $M=\bigcup_{j\in J} L(C_j,Q_j)$ has a proper disjoint decomposition $\bigcup_{i\in I} L(B_i,P_i)$ where*
- $\|B_i\|\le\|M\|^{\#J\cdot O(d^7\cdot\log d)}$,
- $\|P_i\|\le\|M\|^{\#J\cdot O(d^7)}$, *and*
- $\#I\le\|M\|^{\#J\cdot O(d^7)}$.

▶ **Corollary 20** (UD for semi-linear sets)**.** *Every semi-linear set $M=\bigcup_{j\in J} L(C_j,Q_j)$ has an unambiguous decomposition $\bigcup_{i\in I} L(B_i,P_i)$ where*

- $\|B_i\| \le \|M\|^{\#J \cdot O(d^7 \log d)}$, *and*
- $\|P_i\| \le \|M\|^{\#J \cdot O(d^7)}$.

▶ **Theorem 21** (complement of semi-linear sets)**.** *The complement of every semi-linear set $M = \bigcup_{j \in J} L(C_j, Q_j)$ has a representation of the form $\bigcup_{i \in I} L(B_i, P_i)$, where*
- $\|B_i\| \le \|M\|^{\#J \cdot O(d^7 \cdot \log d)}$, *and*
- $\|P_i\| \le \|M\|^{\#J \cdot O(d^7)}$.

We state the results on set difference at the end of this subsection. Most of the material below is devoted to the proofs of Theorems 19 and 21; Corollary 20 follows from Theorem 19 and Theorem 11.

Recall that in Subsection 4.1 we decomposed the space into disjoint atomic polyhedra A. Each $A = \operatorname{conv} E + \operatorname{cone} G$ by Lemma 18, with $E \subseteq \mathbb{Q}^d$ and $G \subseteq \mathbb{Z}^d$. By Carathéodory's theorem, every vector $\boldsymbol{x} \in A$ has an expansion of the form

$$\boldsymbol{x} = \sum_{\boldsymbol{e} \in E} \nu_{\boldsymbol{e}} \cdot \boldsymbol{e} + \sum_{\boldsymbol{g} \in G'} \mu_{\boldsymbol{g}} \cdot \boldsymbol{g} = \tau(\boldsymbol{x}) + \pi(\boldsymbol{x}), \tag{6}$$

where $\tau(\boldsymbol{x}) = \sum_{\boldsymbol{e} \in E} \nu_{\boldsymbol{e}} \cdot \boldsymbol{e} + \sum_{\boldsymbol{g} \in G'} (\mu_{\boldsymbol{g}} - \lfloor \mu_{\boldsymbol{g}} \rfloor) \cdot \boldsymbol{g}$ denotes the *truncation* of $\boldsymbol{x}$, $\pi(\boldsymbol{x}) = \sum_{\boldsymbol{g} \in G'} \lfloor \mu_{\boldsymbol{g}} \rfloor \cdot \boldsymbol{g}$ denotes the *periodic part* of $\boldsymbol{x}$, and $G' \subseteq G$ is some subset of linearly independent vectors in G. We will consider sets $X = A \cap \mathbb{Z}^d \setminus M$ and $Y = A \cap \mathbb{Z}^d \cap M = A \cap M$.

It is not difficult to show that $\|\tau(X)\|$ and $\|\tau(Y)\|$ are bounded from above by $\|M\|^{\#J \cdot \mathsf{poly}(d)}$; these estimations are relevant as we prove that the equalities $X = L(\tau(X), G)$ and $Y = L(\tau(Y), G)$ hold. While the latter equality requires no sophisticated arguments, a proof of the former turns out to be somewhat delicate. As an auxiliary statement, we show that $\tau(X) \subseteq X$; with this fact at hand, the proof of the inclusion $L(\tau(X), G) \subseteq X$ goes via the following checkpoints. Suppose there exists a vector $\boldsymbol{z} \in L(\tau(X), G) \cap M$, say with $\boldsymbol{z} \in L(\boldsymbol{b}, Q_{jt})$ such that $L(\boldsymbol{b}, Q_{jt})$ shares A. This implies the existence of another vector $\boldsymbol{x} \in X$ with $\tau(\boldsymbol{x}) \in \boldsymbol{b} + Q_{jt} \cdot \mathbb{Z}^\delta$ where δ is the cardinality of Q_{jt}. At the same time, this $\tau(\boldsymbol{x})$ also belongs to X and thus to A and to the cone $K(\boldsymbol{b}, Q_{jt})$. Since the vectors in Q_{jt} are linearly independent (recall that sets Q_{jt} come from a *proper* disjoint decomposition of $L(C_j, Q_j)$), it follows that $\tau(\boldsymbol{x}) \in L(\boldsymbol{b}, Q_{jt})$, which contradicts the fact that $\tau(X) \subseteq X$, because X excludes all linear sets from M.

As seen from this sketch, our ability to construct the hybrid linear representation of X (which corresponds to the complement of M) relies on the fact that our decomposition of M in (5) only uses linear sets with linearly independent periods.

Proofs of Theorems 19 and 21 (sketch). Use equalities

$$M = \bigcup_{H \subseteq \mathcal{H}} A(H) \cap M \qquad \text{and} \qquad \mathbb{Z}^d \setminus M = \bigcup_{H \subseteq \mathcal{H}} A(H) \cap \mathbb{Z}^d \setminus M$$

where it suffices to consider only (non-empty) atomic polyhedra $A = A(H)$. Whenever all linear sets $L(\boldsymbol{b}, Q_{jt})$, $\boldsymbol{b} \in C_{jt}$ (see (5)) avoid a polyhedron A, we have $Y = A \cap M = \emptyset$ and $X = A \cap \mathbb{Z}^d \setminus M = A \cap \mathbb{Z}^d$. The first case is trivial, and the second sends us to Proposition 1. Otherwise, if at least one linear set shares A, we use the representations $X = L(\tau(X), G)$ and $Y = L(\tau(Y), G)$ as discussed above. For the purposes of proper disjoint decomposition (Theorem 19), we need to invoke Theorem 7 on $L(\tau(Y), G)$. Upper bounds on $\|B_i\|$, $\|P_i\|$, and $\#I$ follow from Lemmas 18 and 16 and from Theorem 7. ◀

▶ **Corollary 22** (difference of semi-linear sets). *The set-theoretic difference $M \setminus N$ of semi-linear sets $M = \bigcup_{j \in J} L(C_j, Q_j)$ and $N = \bigcup_{k \in K} L(D_k, R_k)$ has a representation of the form $L = \bigcup_{i \in I} L(B_i, P_i)$, where*

- $\max_{i \in I} \|B_i\|, \max_{i \in I} \|P_i\| \leq \#_{\mathsf{p}} M \cdot \|M\| \cdot \|N\|^{\#K \cdot O(d^8)}$.

▶ **Corollary 23** (small vector in set difference). *Let M, N be semi-linear sets such that $\|M\|, \|N\| \leq n$ and $M \setminus N \neq \emptyset$. Then there is $\boldsymbol{v} \in M \setminus N$ such that $\|\boldsymbol{v}\| \leq 2^{n^{O(d^2)}}$.*

5 An application: Exponent-sensitive commutative grammars

In this section, we show that our bounds on the difference of semi-linear sets yield a novel tight upper bound for the equivalence problem for a certain class of commutative grammars.

Let $\Sigma = \{a_1, \ldots, a_m\}$ be a finite alphabet. The free commutative monoid generated by Σ is denoted by $\Sigma^\odot$, and we treat elements of $\Sigma^\odot$ as vectors in $\mathbb{N}^d$ where $d = |\Sigma|$. By $\Sigma^\oplus := \Sigma^\odot \setminus \mathbf{0}$ we denote the free commutative semi-group generated by Σ. An *exponent-sensitive commutative grammar* (ESCG) is a tuple $G = (N, \Sigma, S, \Pi)$, where

- N is a finite set of non-terminal symbols;
- Σ is a finite alphabet, the set of terminal symbols, such that $N \cap \Sigma = \emptyset$;
- $S \in N$ is the axiom; and
- $\Pi \subseteq (\bigcup_{U \in N} \{U\}^\oplus) \times (N \cup \Sigma)^\odot$ is a finite set of productions.

The size $|G|$ of G is the number of symbols required write it down; in particular we assume that commutative words from $\Sigma^\odot$ are encoded in *binary*. Subsequently, we write $V \to W$ whenever $(V, W) \in \Pi$. Let $D, E \in (N \cup \Sigma)^\odot$, we say D directly generates E, written $D \Rightarrow_G E$, iff there are $F \in (N \cup \Sigma)^\odot$ and $\pi \in \Pi$ such that $\pi = V \to W$, $D = V + F$ and $E = F + W$. We write $U \Rightarrow_G^* W$ for the reflexive transitive closure of $\Rightarrow_G$ and say that U generates W in this case. If G is clear from the context, we omit the subscript G. For $U \in N^\oplus$, the reachability set $\mathcal{R}(G, U)$ and the language $\mathcal{L}(G, U)$ generated by G starting at U are defined as

$$\mathcal{R}(G, U) := \{W \in (N \cup \Sigma)^\odot : U \Rightarrow^* W\}, \text{ and } \qquad \mathcal{L}(G, U) := \mathcal{R}(G, U) \cap \Sigma^\odot.$$

The reachability set $\mathcal{R}(G)$ and the language $\mathcal{L}(G)$ of G are then defined as $\mathcal{R}(G) := \mathcal{R}(G, S)$ and $\mathcal{L}(G) := \mathcal{L}(G, S)$. Given ESCG G, H and $w \in \Sigma^\odot$, the word problem is to decide whether $w \in \mathcal{L}(G)$, and equivalence is to decide whether $\mathcal{L}(G) = \mathcal{L}(H)$. The word problem is PSPACE-complete; the equivalence problem was shown PSPACE-hard and decidable in 2-EXPSPACE by Mayr and Weihmann [18]. The latter result has recently been improved to coNEXP-hardness and membership in co-2NEXP in [7]. An application of Corollary 23 enables us to settle the complexity of the equivalence problem for ESCG.

▶ **Theorem 24.** *Equivalence for ESCG is* coNEXP*-complete.*

Proof (sketch). Let G, H be ESCG such that $\mathcal{L}(G) \neq \mathcal{L}(H)$, and with no loss of generality assume that there is some $w \in \mathcal{L}(G) \setminus \mathcal{L}(H)$. It is shown in [18] that $M = \mathcal{L}(G)$ and $N = \mathcal{L}(H)$ are semi-linear with $\|M\|, \|N\| \leq 2^{p(|G|+|H|)}$ for some fixed polynomial p. Consequently, by Corollary 23 we may assume that $\|w\| \leq 2^{2^{q(|G|+|H|)}}$ for some fixed polynomial q, and hence the representation size n of w is bounded by $2^{q(|G|+|H|)}$. Thus, for the coNEXP-upper bound it only remains to show that $w \in \mathcal{L}(G)$ and $w \notin \mathcal{L}(H)$ can be checked in time polynomial in the n. This is not completely obvious since the word problem for ESCG is PSPACE-complete. In the appendix, we show how this obstacle can be avoided, bringing in a strategy that was used by Huynh [9] in order to show a coNEXP-upper bound for the equivalence problem for context-free commutative grammars. ◀

References

1 Matthias Beck and Frank Sottile. Irrational proofs for three theorems of Stanley. *Eur. J. Comb.*, 28(1):403–409, 2007.
2 Eric Domenjoud. Solving systems of linear Diophantine equations: An algebraic approach. In *Mathematical Foundations of Computer Science, MFCS*, pages 141–150, 1991.
3 Samuel Eilenberg and M.P Schützenberger. Rational sets in commutative monoids. *Journal of Algebra*, 13(2):173 – 191, 1969.
4 Seymour Ginsburg. *The mathematical theory of context free languages.* McGraw-Hill, 1966.
5 Seymour Ginsburg and Edwin H. Spanier. Bounded ALGOL-like languages. *Transactions of the American Mathematical Society*, pages 333–368, 1964.
6 Christian Haase, Benjamin Nill, and Andreas Paffenholz. Lecture notes on lattice polytopes. Preliminary version of December 7, 2012, available at `http://polymake.org/polytopes/paffenholz/data/preprints/ln_lattice_polytopes.pdf`.
7 Christoph Haase and Piotr Hofman. Tightening the complexity of equivalence problems for commutative grammars. In *Symposium on Theoretical Aspects of Computer Science, STACS*, Leibniz International Proceedings in Informatics (LIPIcs), pages 41:1–41:14. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2016.
8 Matthew Hague and Anthony Widjaja Lin. Model checking recursive programs with numeric data types. In *Computer Aided Verification, CAV*, volume 6806 of *Lecture Notes in Computer Science*, pages 743–759. Springer, 2011.
9 Dung T. Huynh. The complexity of equivalence problems for commutative grammars. *Information and Control*, 66(1–2):103–121, 1985.
10 Dung T. Huynh. A simple proof for the Σ_2^p upper bound of the inequivalence problem for semilinear sets. *Elektronische Informationsverarbeitung und Kybernetik*, 22(4):147–156, 1986.
11 Thiet-Dung Huynh. The complexity of semilinear sets. *Elektronische Informationsverarbeitung und Kybernetik*, 18(6):291–338, 1982.
12 Oscar H. Ibarra. Reversal-bounded multicounter machines and their decision problems. *J. ACM*, 25(1):116–133, 1978.
13 Ryuichi Ito. Every semilinear set is a finite union of disjoint linear sets. *J. Comput. Syst. Sci.*, 3(2):221–231, 1969.
14 Eryk Kopczyński. Complexity of problems of commutative grammars. *Logical Methods in Computer Science*, 11(1), 2015.
15 Matthias Köppe and Sven Verdoolaege. Computing parametric rational generating functions with a primal Barvinok algorithm. *Electr. J. Comb.*, 15(1), 2008.
16 Jesús A. Loera, Jörg Rambau, and Francisco Santos. *Triangulations: Structures for Algorithms and Applications.* Springer Berlin Heidelberg, Berlin, Heidelberg, 2010.
17 Jiři Matoušek. *Lectures on discrete geometry.* Graduate texts in mathematics. Springer, New York, Berlin, Paris, 2002.
18 Ernst W. Mayr and Jeremias Weihmann. Completeness results for generalized communication-free Petri nets with arbitrary edge multiplicities. In *Reachability Problems, RP*, volume 8169 of *Lecture Notes in Computer Science*, pages 209–221. Springer, 2013.
19 Andreas Paffenholz. Polyhedral geometry and linear optimization. Preliminary version of July, 2010, available at `http://www.mathematik.tu-darmstadt.de/~paffenholz/daten/preprints/ln.pdf`.
20 Loïc Pottier. Minimal solutions of linear Diophantine systems: Bounds and algorithms. In *Rewriting Techniques and Applications, RTA*, volume 488 of *Lecture Notes in Computer Science*, pages 162–173. Springer, 1991.
21 R. Tyrell Rockafellar. *Convex Analysis.* Princeton University Press, 1970.

22 Alexander Schrijver. *Theory of linear and integer programming*. John Wiley & Sons, 1998.

23 Joachim von zur Gathen and Malte Sieveking. A bound on solutions of linear integer equalities and inequalities. *Proceedings of the American Mathematical Society*, 72(1):155–158, 1978.

24 Volker Weispfenning. The complexity of almost linear Diophantine problems. *Journal of Symbolic Computation*, 10(5):395–403, 1990.

A Proofs for Section 2

▶ **Proposition 1.** *Let $\mathfrak{S}\colon A \cdot \boldsymbol{x} \le \boldsymbol{c}$ be a system of inequalities such that $A \in \mathbb{Z}^{m \times n}$. Then $[\![\mathfrak{S}]\!] = \bigcup_{i \in I} L(B_i, P_i)$ such that*

- $K(B_i, P_i) \cap K(B_j, P_j) = \emptyset$ *for all* $i \ne j$,
- $\max_{i \in I} \|B_i\|, \max \|P_i\| \le 2^{n^2+n} \cdot (\|A\| + \|\boldsymbol{c}\|)$,
- $\#I \le 2^n$.

Proof. An orthant matrix is a diagonal matrix whose elements are all either -1 or $+1$. Let $\mathcal{O}_n$ denote the set of all $n \times n$ orthant matrices. For $O \in \mathcal{O}$, let

$$\mathfrak{S}_O\colon \begin{pmatrix} A \\ O \end{pmatrix} \cdot \boldsymbol{x} \le \begin{pmatrix} \boldsymbol{c} \\ \boldsymbol{d}_O \end{pmatrix},$$

where for $1 \le i \le n$, $(\boldsymbol{d}_O)_i := -1$ if the i-th diagonal element of O is positive, and $(\boldsymbol{d}_O)_i := 0$ otherwise.

Clearly, $[\![\mathfrak{S}]\!] = \bigcup_{O \in \mathcal{O}} [\![\mathfrak{S}_O]\!]$, and the constraint matrix of each $\mathfrak{S}_O$ has full column rank. It then follows from [23, Thm.] that $\mathfrak{S}_O = L(B, P)$ such that

$$\|B\|, \|P\| \le (n+1) \cdot 2^{n^2} \cdot (\|A\| + \|\boldsymbol{c}\|) \le 2^{n^2+n} \cdot (\|A\| + \|\boldsymbol{c}\|).$$

Moreover, the choice of the $\boldsymbol{d}_O$ ensures that the $K(B_i, P_i)$ are pairwise disjoint. ◀

▶ **Proposition 2.** *Let $\mathfrak{S}_0\colon A \cdot \boldsymbol{x} = \boldsymbol{0}$ and $\mathfrak{S}\colon A \cdot \boldsymbol{x} = \boldsymbol{c}$ be systems of linear Diophantine equations, where $A \in \mathbb{Z}^{d \times n}$. Then $[\![\mathfrak{S}_0]\!]_{\ge 0} = L(\boldsymbol{0}, P)$ and $[\![\mathfrak{S}]\!]_{\ge 0} = L(B, P)$ such that*

- $\|B\| \le ((n+1) \cdot \|A\| + \|\boldsymbol{c}\| + 1)^d$, $\|P\| \le (n \cdot \|A\| + 1)^d$,
- $\#B \le (n+1)^d$, *and* $\#P \le n^d$.

Proof. It is shown in [20, Thm. 1] that $[\![\mathfrak{S}_0]\!]_{\ge 0} = L(\boldsymbol{0}, P)$ such that $\|P\| \le (n \cdot \|A\| + 1)^d$. Moreover, it follows from [2, Thm. 5] that $\#P \le \binom{n}{d} \le n^d$. Let $\mathfrak{S}'\colon \left(A \mid -\boldsymbol{c} \right) \cdot \boldsymbol{x}' = \boldsymbol{0}$, observe that B is the set of minimal solutions of $\mathfrak{S}'$ whose last component is equal to one; thus the estimations for $\mathfrak{S}$ reduce to the homogenous case. ◀

▶ **Theorem 6.** *Let M and N be semi-linear sets with representations $M = \bigcup_{j \in J} L(C_j, Q_j)$, $N = \bigcup_{k \in K} L(D_k, R_k)$. Then the set $L := M \cap N$ is a semi-linear set with representation $L = \bigcup_{i \in I} L(B_i, P_i)$ such that $I = J \times K$,*

- $\max_{i \in I} \|B_i\|, \max_{i \in I} \|P_i\| \le ((\#_{\mathsf{p}} M + \#_{\mathsf{p}} N) \cdot \max(\|M\|, \|N\|))^{O(d)}$,
- $\max_{i \in I} \#B_i \le (\#_{\mathsf{b}} M + \#_{\mathsf{b}} N) \cdot (\#_{\mathsf{p}} M + \#_{\mathsf{p}} N)^{O(d)}$,
- $\max_{i \in I} \#P_i \le (\#_{\mathsf{p}} M + \#_{\mathsf{p}} N)^d$, *and*
- $\#I \le \#J \cdot \#K$.

Moreover, if $Q_j \subseteq R_k$ and $i = (j, k)$ then $P_i = Q_j$.

Proof. We have $M \cap N = \bigcup_{j \in J} L(C_j, Q_j) \cap \bigcup_{k \in K} L(D_k, R_k) = \bigcup_{j \in J, k \in K} L(C_j, Q_j) \cap L(D_k, R_k)$. Hence it suffices to show that every $L(C_j, Q_j) \cap L(D_k, R_k)$ is some $L(B_{j,k}, P_{j,k})$ with the desired properties. For the sake of readability, we drop indices and let $L(C, Q)$ and $L(D, R)$ be hybrid linear sets of M and N, respectively. Let $\boldsymbol{c} \in C$, $\boldsymbol{d} \in D$ and consider the following system of linear Diophantine inequalities:

$$\mathfrak{S}\colon \boldsymbol{c} + Q \cdot \boldsymbol{\gamma} = \boldsymbol{d} + R \cdot \boldsymbol{\theta}.$$

By Lemma 2 we have $[\![\mathfrak{S}]\!]_{\geq 0}|_{\boldsymbol{\gamma}} = L(E,S) \subseteq \mathbb{N}^q$; in particular S is independent of $\boldsymbol{c}$ and $\boldsymbol{d}$. Now

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

Denote by $E(\boldsymbol{c},\boldsymbol{d})$ the set E as above for a particular choice of $\boldsymbol{c} \in C$ and $\boldsymbol{d} \in D$, we then have

$$L(C,D) \cap L(D,R) = \bigcup_{\boldsymbol{c}\in C, \boldsymbol{d}\in D} L(\boldsymbol{c},Q) \cap L(\boldsymbol{d},R) = \bigcup_{\boldsymbol{c}\in C, \boldsymbol{d}\in D} L(\boldsymbol{c} + Q \cdot E(\boldsymbol{c},\boldsymbol{d}), Q \cdot S).$$

Set $B := \{\boldsymbol{c} + Q \cdot E(\boldsymbol{c},\boldsymbol{d}) : \boldsymbol{c} \in C, \boldsymbol{d} \in D\}$ and $P := Q \cdot S$. The descriptive complexity of B and P can now be estimated as follows using the bounds provided in Lemma 2:

$$\begin{aligned}
\|E(\boldsymbol{c},\boldsymbol{d})\|, \|S\| &\leq ((\#Q + \#R) \cdot \max(\|Q\|, \|R\|) + \|C\| + \|D\| + 1)^d \\
&\leq ((\#_{\mathsf{p}} M + \#_{\mathsf{p}} N) \cdot \max(\|M\|, \|N\|))^{O(d)}.
\end{aligned}$$

Set $E = \bigcup_{\boldsymbol{c}\in C, \boldsymbol{d}\in D} E(\boldsymbol{c},\boldsymbol{d})$, we have

$$\|P\| \leq \|B\| = \|C + Q \cdot E\| \leq ((\#_{\mathsf{p}} M + \#_{\mathsf{p}} N) \cdot \max(\|M\|, \|N\|))^{O(d)}.$$

The cardinality of each $E(\boldsymbol{c},\boldsymbol{d})$ and S can also be estimated using Lemma 2:

$$\#E(\boldsymbol{c},\boldsymbol{d}), \leq (\#Q + \#R + 1)^d \qquad\qquad \#S \leq (\#Q + \#R)^d.$$

Hence, the cardinalities of B and P are obtained as follows:

$$\#B \leq \#C \cdot \#D \cdot (\#Q + \#R)^{O(d)}, \qquad\qquad \#P \leq (\#Q + \#R)^d.$$

Note that whenever $Q \subseteq R$, then by Theorem 5.6.1 in [4, p. 180], we actually have $L(C,Q) \cap L(D,R) = L(B,Q)$. ◀

▶ **Proposition 5.** *Let $M = \bigcup_{j\in J} L(C,Q)$ be a hybrid linear set. Then $M = \bigcup_{i\in I} L(B_i,P_i)$ such that*

- $\max_{i\in I} \|B_i\| \leq \|C\| + (\#Q \cdot \|Q\|)^{O(d)}$,
- $\max_{i\in I} \#P_i \leq d$, *$P_i \subseteq P$ and each P_i is linearly independent, and*
- $\#I \leq (\#Q)^d$.

Proof. Let $I(Q)$ be the set of all linearly independent subsets of Q of maximal cardinality. We clearly have $\#I(Q) \leq \binom{\#Q}{d} \leq (\#Q)^d$. Carathéodory's theorem, see e.g. [22, p. 94], states that

$$\operatorname{cone}(Q) = \bigcup_{Q' \in I(Q)} \operatorname{cone}(Q'). \tag{7}$$

Moreover, for any $Q' = \{\boldsymbol{q}_1, \ldots, \boldsymbol{q}_j\} \in I(Q)$ and $\boldsymbol{u} \in \mathbb{N}^m$, we have

$$\begin{aligned}
&\boldsymbol{u} = \lambda_1 \cdot \boldsymbol{q}_1 + \cdots + \lambda_j \cdot \boldsymbol{q}_j,\ \lambda_i \in \mathbb{Q}_{\geq 0} \\
\iff &\boldsymbol{u} = (\lambda_1 - \lfloor \lambda_1 \rfloor) \cdot \boldsymbol{q}_1 + \cdots + (\lambda_j - \lfloor \lambda_j \rfloor) \cdot \boldsymbol{q}_j + \lfloor \lambda_1 \rfloor \cdot \boldsymbol{q}_1 + \cdots + \lfloor \lambda_j \rfloor \cdot \boldsymbol{q}_j,\ \lambda_i \in \mathbb{Q}_{\geq 0} \\
\iff &\boldsymbol{u} \in L(E_{Q'}, Q'),
\end{aligned} \tag{8}$$

where $E_{Q'} := \{\lambda_1 \cdot \boldsymbol{q}_1 + \cdots + \lambda_j \cdot \boldsymbol{q}_j \in \mathbb{N}^m : \boldsymbol{q}_i \in Q', \lambda_i \in \mathbb{Q}, 0 \leq \lambda_i < 1\}$. Hence $\operatorname{cone}(Q') \cap \mathbb{N}^m = L(E_{Q'}, Q')$, and since $\#Q' \leq d$, it is easily checked that $\|E_{Q'}\| \leq d \cdot \|Q\|$.

Now $L(C, Q)$ can be decomposed as:

$$\begin{aligned}
& C + L(\mathbf{0}, Q) \\
&= C + (L(\mathbf{0}, Q) \cap \bigcup_{Q' \in I(Q)} \operatorname{cone}(Q') \cap \mathbb{Z}^d) && \text{(by (7))} \\
&= C + \bigcup_{Q' \in I(Q)} L(E_{Q'}, Q') \cap L(\mathbf{0}, Q) && \text{(by distributivity and (8))} \\
&= C + \bigcup_{Q' \in I(Q)} L(B_{Q'}, Q') && \text{(by Theorem 6)} \\
&= \bigcup_{Q' \in I(Q)} L(C + B_{Q'}, Q')
\end{aligned}$$

Here, $B_{Q'}$ is such that $L(B_{Q'}, Q') = L(E_{Q'}, Q') \cap L(\mathbf{0}, Q)$, and by our estimation on $\|E_{Q'}\|$ and Theorem 6 we have

$$\|B_{Q'}\| \leq (d + \#Q) \cdot \|Q\|^{O(d)} \leq (\#Q \cdot \|M\|)^{O(d)}. \qquad \blacktriangleleft$$

B Proofs for Section 3

B.1 Triangulations and Proof of Lemma 8

We first introduce several auxiliary definitions. For $s = 0, 1$, define injective mappings $\varphi_s \colon \mathbb{Q}^d \to \mathbb{Q}^{d+1}$ by the rule $\varphi_s(\boldsymbol{x}) = (s, \boldsymbol{x})$. The mapping φ_0 treats $\boldsymbol{x}$ as a direction in $\mathbb{Q}^d$ and maps this direction to its representation in $\mathbb{Q}^{d+1}$; we will never apply it to $\mathbf{0} \in \mathbb{Q}^d$. The mapping φ_1 treats $\boldsymbol{x}$ simply as a point in $\mathbb{Q}^d$ and maps this point to its representation in $\mathbb{Q}^{d+1}$.

For any $V \subseteq \mathbb{Q}^d$ and $D \subseteq \mathbb{Q}^d \setminus \{\mathbf{0}\}$ denote $\varphi(V, D) = \operatorname{cone}(\varphi_1(V) \cup \varphi_0(D))$.

▶ Claim 25. $\varphi_1^{-1}(\varphi(V, D)) = \operatorname{conv} V + \operatorname{cone} D$.

▶ Claim 26. The set $\operatorname{conv} V + \operatorname{cone} D$ with $\#V + \#D = \delta + 1$ and $V \neq \emptyset$ is a generalized δ-dimensional simplex iff $\delta + 1$ points in $\varphi_1(V) \cup \varphi_0(D)$ are linearly independent in $\mathbb{Q}^{d+1}$.

The condition of Claim 26 implies, for example, that $\mathbf{0} \notin D$.

Claims 25 and 26 follow the presentation of directions and generalized simplices in [21, pp. 153–155 and 60–61].

Proof of Claim 25. Note that $(1, \boldsymbol{w}) \in \varphi(V, D)$ iff there exist vectors $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k \in V$, $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_r \in D$, and rational numbers $\lambda_1, \ldots, \lambda_k \in \mathbb{Q}_{\geq 0}$ and $\mu_1, \ldots, \mu_k \in \mathbb{Q}_{\geq 0}$ such that

$$(1, \boldsymbol{w}) = \sum_{i=1}^{k} \lambda_i (1, \boldsymbol{v}_i) + \sum_{j=1}^{r} \mu_j (0, \boldsymbol{u}_j). \tag{9}$$

This is, of course, only possible with $\sum_{i=1}^{k} \lambda_i = 1$. As a result, vectors $\boldsymbol{v}_i \in V$, $\boldsymbol{u}_j \in D$, and numbers $\lambda_i, \mu_j \in \mathbb{Q}_{\geq 0}$ satisfying (9) exist if and only if there exist two vectors $\boldsymbol{v} \in \operatorname{conv} V$ and $\boldsymbol{u} \in \operatorname{cone} D$ such that $\boldsymbol{w} = \boldsymbol{v} + \boldsymbol{u}$. That is, each $(1, \boldsymbol{w}) \in \varphi(V, D)$ has a corresponding pair $\boldsymbol{v}, \boldsymbol{u}$ with $\boldsymbol{w} = \boldsymbol{v} + \boldsymbol{u}$, $\boldsymbol{v} \in \operatorname{conv} V$, and $\boldsymbol{u} \in \operatorname{cone} D$; vice versa, each pair of $\boldsymbol{v} \in \operatorname{conv} V$ and $\boldsymbol{u} \in \operatorname{cone} D$ gives rise to $(1, \boldsymbol{w}) \in \varphi(V, D)$. By the definition of φ_1, this concludes the proof. ◀

While we expect the result of Lemma 8 to be known, we are aware of no reference.

Proof of Lemma 8. It is known that the desired triangulation exists when W is a finitely generated convex cone (see, e.g., [16, Section 2.5]); we show how to use this fact to obtain triangulations of polyhedra.

Denote $F = \varphi_1(C) \cup \varphi_0(Q) = \{f_1, \ldots, f_l\} \subseteq \mathbb{Q}^{d+1}$ and consider the cone $\varphi(C, Q) = \operatorname{cone} F$. As a convex cone in $\mathbb{Q}^{d+1}$, it has a triangulation $\mathcal{T}(F) = (G_1, \ldots, G_m)$ with $G_i = \operatorname{cone} F_i$ for $F_i \subseteq F$ and $\#F_i = \delta + 1$ where $\delta + 1$ is the dimension of each cone G_i. We claim that $\mathcal{T} = (T_1, \ldots, T_m)$ with $T_i = \varphi_1^{-1}(G_i)$ is a triangulation of W that satisfies the conditions of the lemma.

Indeed,assume without loss of generality that $F_i = \{\varphi_1(\boldsymbol{v}_1), \ldots, \varphi_1(\boldsymbol{v}_t), \varphi_0(\boldsymbol{u}_1), \ldots, \varphi_0(\boldsymbol{u}_s)\}$ where $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_t \in C$, $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_s \in Q$, and $t + s = \delta + 1$. By Claim 25, $T_i = \varphi_1^{-1}(\operatorname{cone} F_i) = \operatorname{conv} C_i + \operatorname{cone} Q_i$ where $C_i = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_t\} \subseteq C$ and $Q_i = \{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_s\} \subseteq Q$, so it remains to show that $\mathcal{T}$ is a triangulation of W. (Notice that $m \le \binom{\#C + \#Q}{d+1} \le (\#C + \#Q)^{d+1}$.)

First of all, note that each T_i is a generalized δ-dimensional simplex in $\mathbb{Q}^d$ by Claim 26, since F_i consists of $\delta + 1$ linearly independent vectors of $\mathbb{Q}^{d+1}$. Now recall that for any function f and any sets X and Y the equalities $f^{-1}(X \cup Y) = f^{-1}(X) \cup f^{-1}(Y)$ and $f^{-1}(X \cap Y) = f^{-1}(X) \cap f^{-1}(Y)$ hold; we will need these equalities in what follows. So, observe that

$$\begin{aligned} T_1 \cup \ldots \cup T_m &= \varphi_1^{-1}(G_1) \cup \ldots \cup \varphi_1^{-1}(G_m) \\ &= \varphi_1^{-1}(G_1 \cup \ldots \cup G_m) = \varphi_1^{-1}(\varphi(C, Q)) = \operatorname{conv} C + \operatorname{cone} D, \end{aligned}$$

where the last two equalities are by definition of a triangulation and by Claim 25. Similarly, suppose T_i' and T_j' are faces of T_i and T_j with $1 \le i, j \le m$; then

$$T_i' = \operatorname{conv} C_i' + \operatorname{cone} Q_i' = \varphi_1^{-1}(G_i')$$

where $C_i' \subseteq C_i$, $Q_i' \subseteq Q_i$, and $G_i' := \operatorname{cone} F_i'$ with $F_i' := \varphi_1(C_i') \cup \varphi_0(Q_i') \subseteq F_i$. Hence, $G_i' = \operatorname{cone} F_i'$ is a face of $G_i = \operatorname{cone} F_i$; similarly, $G_j' = \operatorname{cone} F_j'$ is a face of $G_j = \operatorname{cone} F_j$. As $\mathcal{T}(F)$ is a triangulation of $\operatorname{cone} F$, it follows that $G_i' \cap G_j'$ is either empty or a face of both G_i' and G_j'. Now note that

$$T_i' \cap T_j' = \varphi_1^{-1}(G_i') \cap \varphi_1^{-1}(G_j') = \varphi_1^{-1}(G_i' \cap G_j').$$

By definition, the function φ_1 is injective, maps polyhedra into polyhedra, and preserves dimensions and the face-of relation, so $\varphi_1^{-1}(G_i' \cap G_j')$ is either empty or a face of both $\varphi_1^{-1}(G_i')$ and $\varphi_1^{-1}(G_j')$. This concludes the proof. ◀

B.2 Proof of Lemma 10

Suppose $V = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k\}$ and $D = \{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_r\}$ with $k + r = \delta + 1$. First note that a vector $\boldsymbol{x} \in \mathbb{Z}^d$ belongs to T iff there exist numbers $\lambda_1, \ldots, \lambda_k \in \mathbb{Q}_{\ge 0}$ and $\mu_1, \ldots, \mu_r \in \mathbb{Q}_{\ge 0}$ with $\sum_{i=1}^k \lambda_i = 1$ such that

$$\boldsymbol{x} = \sum_{i=1}^k \lambda_i \boldsymbol{v}_i + \sum_{j=1}^r \mu_j \boldsymbol{u}_j = \left(\sum_{i=1}^k \lambda_i \boldsymbol{v}_i + \sum_{j=1}^r (\mu_j - \lfloor \mu_j \rfloor) \boldsymbol{u}_j \right) + \sum_{j=1}^r \lfloor \mu_j \rfloor \boldsymbol{u}_j.$$

Define

$$A = \mathbb{Z}^d \cap \left\{ \sum_{i=1}^{k} \lambda_i \boldsymbol{v}_i + \sum_{j=1}^{r} (\rho_j + \mu_j - \lfloor \mu_j \rfloor)\, \boldsymbol{u}_j : \right.$$

$$\left. \lambda_1, \ldots, \lambda_k \in \mathbb{Q}_{\geq 0}, \sum_{i=1}^{k} \lambda_i = 1, \rho_1, \ldots, \rho_r \in \{0,1\}, \mu_1, \ldots, \mu_r \in \mathbb{Q}_{\geq 0} \right\}$$

and observe that $T \cap \mathbb{Z}^d = L(A, D)$. Now let T^0 be the half-opening of T obtained by cutting off some ℓ supporting hyperplanes, i.e., hyperplanes that contain faces of T: every such hyperplane contains at least one point of T, and the rest of T lies to one side of the hyperplane. Suppose these ℓ hyperplanes are of the form $\boldsymbol{a}_s \cdot \boldsymbol{x} = b_s$, $1 \leq s \leq \ell$.

We now claim that $T^0 \cap \mathbb{Z}^d = L(E, D)$ where $E = A \cap \{\boldsymbol{x} \in \mathbb{Q}^d : \boldsymbol{a}_s \cdot \boldsymbol{x} < b_s, 1 \leq s \leq \ell\}$. Indeed, first note that $L(E, D) \subseteq T^0 \cap \mathbb{Z}^d$. This inclusion holds because all directions $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_r \in D$ satisfy $\boldsymbol{a}_s \cdot \boldsymbol{u}_j \leq 0$, $1 \leq s \leq \ell$, and all vectors $\boldsymbol{v} \in E$ satisfy $\boldsymbol{a}_s \cdot \boldsymbol{v} < b_s$. Next, observe that, conversely, $T^0 \cap \mathbb{Z}^d \subseteq L(E, D)$. Indeed, take any vector $\boldsymbol{x} \in T^0 \cap \mathbb{Z}^d$; since $T^0 \subseteq T$, it can be written as $\boldsymbol{x} = \boldsymbol{y} + \boldsymbol{z}$ where $\boldsymbol{y}, \boldsymbol{z} \in \mathbb{Z}^d$,

$$\boldsymbol{y} = \sum_{i=1}^{k} \lambda_i \boldsymbol{v}_i + \sum_{j=1}^{r} (\mu_j - \lfloor \mu_j \rfloor) \boldsymbol{u}_j \qquad \text{and} \qquad \boldsymbol{z} = \sum_{j=1}^{r} \lfloor \mu_j \rfloor \boldsymbol{u}_j$$

for some $\lambda_1, \ldots, \lambda_k \in \mathbb{Q}_{\geq 0}$, $\sum_{i=1}^{k} \lambda_i = 1$, and $\mu_1, \ldots, \mu_r \in \mathbb{Q}_{\geq 0}$. If $\boldsymbol{y} \in E$, then $\boldsymbol{x} \in L(E, D)$, so assume otherwise. Note that $\boldsymbol{y} \in A$ with $\rho_1 = \ldots = \rho_r = 0$ and $A \subseteq T$. Assume that $\boldsymbol{a}_s \cdot \boldsymbol{y} = b_s$, $1 \leq s \leq t$, and $\boldsymbol{a}_s \cdot \boldsymbol{y} < b_s$, $t < s \leq t$. Then for each $s = 1, \ldots, s$, since $\boldsymbol{y} + \boldsymbol{z} \in T^0$ and so $\boldsymbol{a}_s \cdot \boldsymbol{y} < b_s$, there exists a $\boldsymbol{u}_j \in D$ such that $\boldsymbol{a}_s \cdot \boldsymbol{u}_j < 0$ and $\lfloor \mu_j \rfloor \geq 1$. Therefore, decreasing μ_j by 1 and setting $\rho_j = 1$ instead, we make sure that the newly obtained vector $\boldsymbol{y}'$ satisfies $\boldsymbol{a}_s \cdot \boldsymbol{y}' < b_s$. Repeating this procedure at most once for each direction $\boldsymbol{u}_j$, we obtain a new representation $\boldsymbol{x} = \boldsymbol{y}' + \boldsymbol{z}'$ where $\boldsymbol{y}' \in A$ and $z' \in L(\boldsymbol{0}, D)$. Therefore, we conclude that $T^0 \cap \mathbb{Z}^d = L(E, D)$, and the upper bound on the magnitude of elements holds by our choice of C.

B.3 Proof of Theorem 7

Take a triangulation of $W = K(C, Q) = \operatorname{conv} C + \operatorname{cone} Q$, which exists by Lemma 8, and apply Lemma 9 to this triangulation. The result is a collection $\mathcal{T}^0 = (T_1^0, \ldots, T_m^0)$ where each T_i^0 is a half-opening of some generalized simplex $\operatorname{conv} C_i + \operatorname{cone} Q_i$ such that $C_i \subseteq C$ and $Q_i \subseteq Q$. By Lemma 10, $T_i^0 \cap \mathbb{Z}^d = L(D_i, Q_i)$ with $\|D_i\| \leq \|C\| + (d+1)\,\|Q\|$.

We now apply Theorem 6: since $Q_i \subseteq Q$, we have $L(D_i, Q_i) \cap L(C, Q) = L(B_i, P_i)$ where $P_i = Q_i$ and

$$\begin{aligned}
\|B_i\| &\leq ((\#Q_i + \#Q) \cdot \|D_i\|)^{O(d)} \\
&\leq ((\#Q + d) \cdot (\|C\| + (d+1)\,\|Q\|))^{O(d)} \\
&= (\#Q + \|C\| + \|Q\| + d)^{O(d)}, \\
\#B_i &\leq (\#D_i + \#C) \cdot (\#P_i + \#Q)^{O(d)} \\
&\leq ((\|C_i\| + (d+1) \cdot \|Q_i\| + 1)^d + \#C) \cdot (d + \#Q)^{O(d)} \\
&= ((\|C\| + \|Q\| + d)^{O(d)} + \#C) \cdot (d + \#Q)^{O(d)}.
\end{aligned}$$

Note that we can now, by merging hybrid linear sets with identical P_is, make sure that subsets $P_i \subseteq Q$ are all different, so $\#I \leq \min(m, \binom{\#Q}{d+1}) \leq (\#Q)^{d+1}$.

Notice that vectors in each set $P_i = Q_i$ are linearly independent, because $\operatorname{conv} C_i + \operatorname{cone} Q_i$ is a generalized simplex. Moreover, $K(B_i, P_i) \subseteq \operatorname{conv} L(D_i, Q_i) \subseteq T_i^0$ for each i; since the sets $T_1^0, \ldots, T_m^0$ are pairwise disjoint, so are the sets $K(B_i, P_i)$. Finally,

$$\begin{aligned}\bigcup_{i=1}^{m} L(B_i, P_i) &= \bigcup_{i=1}^{m} T_i^0 \cap \mathbb{Z}^d \cap L(C, Q) = L(C, Q) \cap \bigcup_{i=1}^{m} T_i^0 \\ &= L(C, Q) \cap W = L(C, Q) \cap \operatorname{conv} L(C, Q) = L(C, Q).\end{aligned}$$

B.4 Unambiguous decompositions: Proofs for Subsection 3.2

Proof of Lemma 13. Consider any $\boldsymbol{x} \in \mathbb{N}^r$. This vector $\boldsymbol{x}$ belongs to $F + \mathbb{N}^r$ if and only if $\boldsymbol{x} \geq \boldsymbol{f}$ for some $\boldsymbol{f} \in F$; this condition can be specified by a logical formula Φ over predicates of the form $x_j \geq c$ where $c \in \mathbb{Z}$ and x_j is the jth component of $\boldsymbol{x}$, $1 \leq j \leq r$. Note that whenever, for some j, the numbers $c_1, \ldots, c_m$ are the jth components of $F = \{\boldsymbol{f}_1, \ldots, \boldsymbol{f}_m\}$, these predicates break a copy of $\mathbb{N}$ associated with x_j into at most $m + 1$ nonempty intervals: $[0, c_{(1)} - 1]$, $[c_{(1)}, c_{(2)} - 1]$, $\ldots$, $[c_{(m-1)} - 1, c_{(m)}]$, and $[c_{(m)}, +\infty)$ where $\{c_{(1)}, \ldots, c_{(m)}\} = \{c_1, \ldots, c_m\}$ and $c_{(l)} \leq c_{(l+1)}$ for all l.

Bring the formula Φ into a sum-of-products form where any two products disagree on the interval of at least one variable x_j; this is an analogue of the canonical disjunctive normal form (CDNF), although, in fact, we do not need to require that each product contain a predicate for each variable. Each product is of the form $\bigwedge(x_j \in I_j)$, for j ranging over some subset of $\{1, \ldots, r\}$, and there are at most $(m + 1)^r$ products. (Note that we can assume without loss of generality that vectors in the set F are pairwise incomparable with respect to the product order, otherwise F can be shrunk without any effect on the set $F + \mathbb{N}^r$.) This product defines a hybrid linear set $L(G, E)$ that has period $\boldsymbol{e}_j$ if and only if I_j is an infinite interval, and the base vectors are determined as follows. We pick $G = G_1 \times \ldots \times G_r$ where G_j is:

- $\{c\}$ if $I_j = [c, +\infty)$,
- $[a, b]$ if $I_j = [a, b]$, and
- $\{\boldsymbol{0}\}$ if the product does not contain a predicate referring to x_j.

Now $L(G, E) = \bigcup_{\boldsymbol{g} \in G} L(\boldsymbol{g}, E)$, where sets on the right-hand side are pairwise disjoint. This completes the proof. ◀

Proof of Theorem 11. Take $M = L(C, Q) \subseteq \mathbb{Z}^d$ where $Q = \{\boldsymbol{q}_1, \ldots, \boldsymbol{q}_r\} \subseteq \mathbb{Z}^d$ and vectors in Q are linearly independent, $r \leq d$. Consider the *point lattice* $\mathcal{L} = Q \cdot \mathbb{Z}^r = \{Q \cdot \boldsymbol{\lambda} : \lambda \in \mathbb{Z}^r\}$; see, e.g., [17, Chapter 2]. Vectors $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{Z}^r$ are congruent modulo $\mathcal{L}$, $\boldsymbol{x} \equiv \boldsymbol{y} \pmod{\mathcal{L}}$ if and only if $\boldsymbol{x} - \boldsymbol{y} \in \mathcal{L}$. This congruence splits the set C into a disjoint union $C = C_1 \cup \ldots \cup C_s$ where $\boldsymbol{x} \in C_i$ and $\boldsymbol{y} \in C_j$ are congruent if and only if $i = j$. It is easy to see that $M = \bigcup_{1 \leq j \leq s} L(C_j, Q)$ is a disjoint union, and disambiguating each $L(C_j, Q)$ separately will disambiguate M.

Suppose $C_1 = \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m\} \subseteq \boldsymbol{x}_1 + \mathcal{L}$. Since the vectors in $Q = \{\boldsymbol{q}_1, \ldots, \boldsymbol{q}_r\}$ are linearly independent, each vector from the set $\boldsymbol{x}_1 + \mathcal{L}$ has a unique expansion of the form $\boldsymbol{x}_1 + \sum_{j=1}^{r} a_j \boldsymbol{q}_j$. Consider the mapping $\psi \colon \boldsymbol{x}_1 + \mathcal{L} \to \mathbb{Z}^r$ taking each vector $\boldsymbol{x}_1 + \sum_{j=1}^{r} a_j \boldsymbol{q}_j$ to the vector $(a_1, \ldots, a_r) \in \mathbb{Z}^r$. For each j, let a_j^0 be the smallest of the numbers $\psi(\boldsymbol{x}_t)[j]$ over $1 \leq t \leq m$; here $[j]$ refers to the jth component of an r-dimensional vector. Denote $\boldsymbol{a}^0 = (a_1^0, \ldots, a_r^0)$ and let $\psi' \colon \boldsymbol{x}_1 + \mathcal{L} \to \mathbb{Z}^r$ be given by $\psi'(\boldsymbol{x}) = \psi(\boldsymbol{x}) - \boldsymbol{a}^0$. Observe that the mapping ψ' is injective and maps C_1 to some finite set $F \subseteq \mathbb{N}^r$; in fact, $\psi'(L(C_1, Q_1)) = F + \mathbb{N}^r$. Lemma 13 decomposes this ideal $F + \mathbb{N}^r \subseteq \mathbb{N}^r$ into a disjoint union of at most $(\#F + 1)^r$ hybrid linear sets, all unambiguous. Taking the inverse image under ψ' then produces a disjoint union of at most $\sum_{j=1}^{s}(\#C_j+1)^r \le (2\#C)^r$ unambiguous sets $L(B_i, P_i)$ with $P_i \subseteq Q$ and $\|B_i\| \le \|B\|$. ◀

Proof of Theorem 12. The statement follows from Theorems 7 and 11. ◀

C Proofs for Section 4

C.1 Geometric ingredients: Subsection 4.1

Proof of Lemma 14. Consider each principal supporting hyperplane h of the cone $K := \operatorname{conv} L(\boldsymbol{b}, Q_{jt}) = K(\boldsymbol{b}, Q_{jt})$; this cone K lies either completely inside the half-space h^-. If at least one of the supporting hyperplanes h does not belong to H, then $A \subseteq h^+$ and so $A \cap K \subseteq h^+ \cap K = \emptyset$. Now assume that all these hyperplanes h are in H; then A is a subset of the intersection of the corresponding half-spaces h^-, and thus into A. ◀

Proof of Lemma 15. By definition, the polyhedron $A(H)$ is defined by a system of inequalities, one per each $h \in \mathcal{H}$. The cardinality of $\mathcal{H}$ can be comparatively big; we note, however, that principal supporting hyperplanes of any two rational cones of the form $K(\boldsymbol{b}, Q_{jt})$ and $K(\boldsymbol{b}', Q_{jt})$ are parallel to each other; in other words, they are of the form $\boldsymbol{a} \cdot \boldsymbol{x} = c$ and $\boldsymbol{a} \cdot \boldsymbol{x} = c'$ for some fixed $\boldsymbol{a} \in \mathbb{Z}^d$ and potentially different numbers $c, c' \in \mathbb{Z}$ (cf. Proposition 4). Hence, each hybrid linear set $L(C_{jt}, Q_{jt})$ defines d families of hyperplanes in $\mathbb{Q}^d$: each family contains at most $\#C_{jt}$ hyperplanes, and all hyperplanes in each family are parallel to each other. Any intersection of half-spaces associated to hyperplanes of a single family is, unless empty, defined by one or two inequalities: $\boldsymbol{a} \cdot \boldsymbol{x} \le c_1$, or $\boldsymbol{a} \cdot \boldsymbol{x} \ge c_2$, or $c_3 \le \boldsymbol{a} \cdot \boldsymbol{x} \ge c_4$. Hence, each the number of inequalities defining $A(H)$ is at most $2d \cdot \sum_{j \in J} \#T_j$. But $\#T_j \le (\#Q_j)^{d+1}$ by Theorem 7. It remains to note that the bound on the magnitude of the entries follows from combining Theorem 7 and Proposition 4. This completes the proof. ◀

Proof of Lemma 16. Apply the basic fact that n hyperplanes in $\mathbb{Q}^d$ define at most $\sum_{i=0}^{d}\binom{n}{d} = O(n^{d+1})$ regions (see, e.g., [17, Proposition 6.1.1]). The number of hyperplanes n for our case was essentially already estimated in the proof of the previous Lemma 15: as $L(C_{jt}, Q_{jt})$ defines at most $d \cdot \#C_j$ hyperplanes, it follows that $n \le d \cdot \sum_{j \in J} \#C_j(\#Q_j)^{d+1}$. ◀

Proof of Lemma 17. Note that $K(\boldsymbol{b}, Q_{jt}) \subseteq K(C_{jt}, Q_{jt})$ and $K(\boldsymbol{b}', Q_{jt'}) \subseteq K(C_{jt'}, Q_{jt'})$. The sets on the right-hand sides of these inclusions are disjoint, by the definition of a proper disjoint decomposition for $L(C_j, Q_j)$. Therefore, the sets on the left-hand sides are also disjoint, and so $L(\boldsymbol{b}, Q_{jt})$ and $L(\boldsymbol{b}', Q_{jt'})$ cannot share an atomic polyhedron—recall that A is non-empty by our definition. This proves the first statement of the lemma; the second statement follows from the first. ◀

Proof of Lemma 18. By Lemma 15, every A is defined by a system of $O(d \cdot \sum_{i \in I}(\#P_i)^{d+1})$ inequalities with entries bounded by $2^{O(d^3)} \cdot (\#Q + \|C\| + \|Q\| + d)^{O(d^2)}$. By Proposition 3, $A = \operatorname{conv} E + \operatorname{cone} G'$ for finite sets $E \subseteq \mathbb{Q}^d$, $G' \subseteq \mathbb{Z}^d$ where absolute values of numerators and denominators of all entries in E, as well as $\|G\|$, are bounded by

$$2^{O(d^3)} \cdot \left(2^{O(d^3)} \cdot (\#Q + \|C\| + \|Q\| + d)^{O(d^2)}\right)^d = 2^{O(d^4)} \cdot (\#Q + \|C\| + \|Q\| + d)^{O(d^3)} \le \|M\|^{O(d^4)}.$$

Let us now show how to satisfy condition 2 of the lemma.

First, recall that by Lemma 17 the polyhedron A can only be shared by linear sets of the form $L(\boldsymbol{b}, Q_{jt})$ where the number of different sets Q_{jt} is at most $\#J$. Denote these sets by $R_1, \ldots, R_s$, $s \leq \#J$; each R_i consists of (at most d) linearly independent vectors from $\mathbb{Q}^d$.

Second, note that $G' \subseteq \operatorname{cone} R_i$ for all i. Indeed, the polyhedron A recedes in all directions in G', and $A \subseteq \operatorname{conv} L(\boldsymbol{b}, R_i)$ for some linear set $L(\boldsymbol{b}, R_i) = L(\boldsymbol{b}, Q_{jt}$ sharing A, which means that, whenever A recedes in a direction $\boldsymbol{u} \in \mathbb{Q}^d \subseteq \{\mathbf{0}\}$, the shifted cone $K(\boldsymbol{b}, Q_{jt})$ also recedes in the direction $\boldsymbol{u}$, i.e., $\boldsymbol{u} \in \operatorname{cone} Q_{jt} = \operatorname{cone} R_i$.

We now claim that we can rescale each vector $\boldsymbol{u} \in G' \subseteq \mathbb{Q}^d$, finding an appropriate $\mu_{\boldsymbol{u}} \in \mathbb{N}$, so that the set $G = \{\mu_{\boldsymbol{u}} \boldsymbol{u} : \boldsymbol{u} \in G'\}$ satisfies condition 2 of the lemma.

We consider each vector $\boldsymbol{u} \in G'$ separately. Fix $\boldsymbol{u} \in G'$ and observe that elements of R_i are linearly independent, so there exists a unique rational solution $\boldsymbol{\lambda} \in \mathbb{Q}^{\ell_i}_{\geq 0}$, $\ell_i = \#R_i$, to the equation $R_i \cdot \boldsymbol{\lambda} = \boldsymbol{u}$. By Cramer's rule, numerators and denominators of $\boldsymbol{\lambda}$ are bounded by

$$\begin{aligned} 2^{O(d^2)} \cdot \|R_i\| \cdot \|\boldsymbol{u}\| &\leq 2^{O(d^2)} \cdot \|Q\| \cdot 2^{O(d^4)} \cdot (\#Q + \|C\| + \|Q\| + d)^{O(d^3)} \\ &\leq 2^{O(d^4)} \cdot (\#Q + \|C\| + \|Q\| + d)^{O(d^3)}. \end{aligned}$$

Let $\mu_i \in \mathbb{N}$ be the least common multiple of the (at most d) denominators; then

$$\mu_i \leq 2^{O(d^5)} \cdot (\#Q + \|C\| + \|Q\| + d)^{O(d^4)}.$$

This number μ_i is such that $\mu_i \cdot \boldsymbol{u} \in L(\mathbf{0}, R_i)$. Therefore, we pick $\mu_{\boldsymbol{u}} = \operatorname{lcm}(\mu_1, \ldots, \mu_s)$; then the vector $\mu_{\boldsymbol{u}} \cdot \boldsymbol{u}$ indeed belongs to all linear sets $L(\mathbf{0}, R_i)$, $1 \leq i \leq s$. This completes the description of our choice of G; we now have $A = \operatorname{conv} E + \operatorname{cone} G$, as well as

$$\begin{aligned} \|\mu_{\boldsymbol{u}} \cdot \boldsymbol{u}\| &\leq (\max \mu_i)^s \, \|G'\| \\ &\leq \left(2^{O(d^5)} \cdot (\#Q + \|C\| + \|Q\| + d)^{O(d^4)}\right)^{\#J} \cdot 2^{O(d^4)} \cdot (\#Q + \|C\| + \|Q\| + d)^{O(d^3)} \\ &\leq \left(2^{O(d^5)} \cdot (\#Q + \|C\| + \|Q\| + d)^{O(d^4)}\right)^{\#J}. \end{aligned}$$

and

$$\|G\| = \max_{\boldsymbol{u} \in G'} \|\mu_{\boldsymbol{u}} \cdot \boldsymbol{u}\| \leq \left(2^{O(d^5)} \cdot (\#Q + \|C\| + \|Q\| + d)^{O(d^4)}\right)^{\#J} \leq \|M\|^{\#J \cdot O(d^5)}.$$

◀

C.2 Decompositions, complement, and difference: Subsection 4.2

▶ **Lemma 27.** $\|\tau(X)\|, \|\tau(Y)\| \leq \|M\|^{\#J \cdot O(d^5 \log d)}$.

Proof of Lemma 27. Since

$$\|\tau(X)\| \leq \|E\| + d \cdot \|G\| \leq \|M\|^{\#J \cdot O(d^5 \log d)}.$$ ◀

▶ **Lemma 28.** $Y = L(\tau(Y), G)$.

Proof of Lemma 28. The inclusion $Y \subseteq L(\tau(Y), G)$ is by the expansion (6), so we focus on the backwards direction. Take some $\boldsymbol{y} \in L(\tau(Y), G)$: $\boldsymbol{y} = \boldsymbol{u} + \boldsymbol{z}$, where $\boldsymbol{u} \in \tau(Y)$ and $\boldsymbol{z} \in G$. This $\boldsymbol{y}$ is integral, because all vectors in $\tau(Y) \subseteq \tau(A)$ are integral by our choice of τ and π; it is also in A because $\tau(Y) \subseteq A$ and the polyhedron A recedes in all directions in G. It now remains to prove that $\boldsymbol{y} \in M$. Since $\boldsymbol{u} \in M$, we have $\boldsymbol{u} \in L(\boldsymbol{b}, Q_{jt})$, $\boldsymbol{b} \in C_{jt}$, where the linear set $L(\boldsymbol{b}, Q_{jt})$ shares the atomic polyhedron A—otherwise the set $L(\boldsymbol{b}, Q_{jt}) \cap A$ would be empty and so could not contain $\boldsymbol{u}$ (recall that $\boldsymbol{u} \in \tau(Y) \subseteq A$ by our choice of $\boldsymbol{y}$, τ, and π). From $\boldsymbol{u} \in L(\boldsymbol{b}, Q_{jt})$, $\boldsymbol{z} \in G$, and from Lemma 18 we conclude that $\boldsymbol{y} = \boldsymbol{u} + \boldsymbol{z} \in L(\boldsymbol{b}, Q_{jt}) \subseteq M$. This completes the proof. ◀

▶ **Lemma 29.** $\tau(X) \subseteq X$.

Proof of Lemma 29. For any $\boldsymbol{x} \in X$, $\tau(\boldsymbol{x}) \in A$ and $\tau(\boldsymbol{x}) \in \mathbb{Z}^d$ by our choice of τ; recall that $G \subseteq \mathbb{Z}^d$. If $\tau(\boldsymbol{x}) \in M$ for some $\boldsymbol{x}$, then $\tau(\boldsymbol{x}) + G \subseteq M$ by Lemma 18 (condition 2). But $\boldsymbol{x} \in \tau(\boldsymbol{x}) + G$ by the expansion (5), so $\boldsymbol{x} \in M$, which contradicts the definition of X. This concludes the proof. ◀

▶ **Lemma 30.** $X = L(\tau(X), G)$.

Proof of Lemma 30. If $\boldsymbol{x} \in X$, then $\boldsymbol{x} \in L(\tau(X), G)$ by the expansion (6).

Conversely, take some $\boldsymbol{z} \in L(\tau(X), G)$. This $\boldsymbol{z}$ is integral, because all vectors in $\tau(X) \subseteq A$ are integral by our choice of τ and π; it is also in A because $\tau(X) \subseteq A$ and the polyhedron A recedes in all directions in G. It now remains to prove that $\boldsymbol{z} \notin M$. Suppose $\boldsymbol{z} \in M$; then $\boldsymbol{z} \in L(\boldsymbol{b}, Q_{jt})$ for some $\boldsymbol{b} \in C_{jt}$, so $\boldsymbol{z} = \boldsymbol{b} + Q_{jt} \cdot \boldsymbol{\lambda}$ with $\boldsymbol{\lambda} \in \mathbb{N}^\delta$ where $\delta = \# Q_{jt}$. Note that this linear set $L(\boldsymbol{b}, Q_{jt})$ shares the atomic polyhedron A, because the set $L(\boldsymbol{b}, Q_{jt}) \cap A$ contains $\boldsymbol{z}$ and so cannot be empty.

Let us show that our assumption leads to a contradiction. Since we originally picked $\boldsymbol{z}$ from $L(\tau(X), G)$, we have $\boldsymbol{z} = \tau(\boldsymbol{x}) + \boldsymbol{y}$ for some $\boldsymbol{x} \in X$ and $\boldsymbol{y} \in L(\boldsymbol{0}, G) \subseteq L(\boldsymbol{0}, Q_{jt})$; the last inclusion holds by Lemma 18. Rewrite this $\boldsymbol{y}$ as $\boldsymbol{y} = Q_{jt} \cdot \boldsymbol{\mu}$ with $\boldsymbol{\mu} \in \mathbb{N}^\delta$. We now have two representations of the same vector: $\boldsymbol{z} = \boldsymbol{b} + Q_{jt} \cdot \boldsymbol{\lambda} = \tau(\boldsymbol{x}) + Q_{jt} \cdot \boldsymbol{\mu}$, so

$$\tau(\boldsymbol{x}) = \boldsymbol{b} + Q_{jt} \cdot (\boldsymbol{\lambda} - \boldsymbol{\mu}), \qquad \text{where } \boldsymbol{\lambda}, \boldsymbol{\mu} \in \mathbb{Z}^\delta. \tag{10}$$

Also observe that $\tau(\boldsymbol{x}) \in \tau(X) \subseteq X \subseteq A \subseteq K(\boldsymbol{b}, Q_{jt})$, where the second inclusion is Lemma 29, the third holds by the definition of A, and the last one is the fact that the linear set $L(\boldsymbol{b}, Q_{jt})$ shares the atomic polyhedron A. From this chain of inclusions we conclude that

$$\tau(\boldsymbol{x}) = \boldsymbol{b} + Q_{jt} \cdot \boldsymbol{\rho}, \qquad \text{where } \boldsymbol{\rho} \in \mathbb{Q}^\delta_{\geq 0}. \tag{11}$$

Since the vectors in Q_{jt} are linearly independent (by definition of the *proper* disjoint decomposition), from equations (10) and (11) it follows that

$$\boldsymbol{\lambda} - \boldsymbol{\mu} = \boldsymbol{\rho} \in \mathbb{Z}^\delta \cap \mathbb{Q}^\delta_{\geq 0} = \mathbb{N}^\delta,$$

which means that $\tau(\boldsymbol{x}) \in L(\boldsymbol{b}, Q_{jt}) \subseteq M$. This, however, is a contradiction with Lemma 29, as it implies $\tau(\boldsymbol{x}) \in \tau(X) \subseteq X = A \cap Z^d \setminus M$. This completes the proof. ◀

Proof of Theorem 19. Note that $M = M \cap \bigcup_{H \subseteq \mathcal{H}} A(H) = \bigcup_{H \subseteq \mathcal{H}} M \cap A(H)$ and, in fact, it suffices to consider only (non-empty) atomic polyhedra $A = A(H)$. Whenever in (5) all linear sets $L(\boldsymbol{b}, Q_{jt})$ avoid a polyhedron A, we have $M \cap A = \emptyset$, so this case is trivial. In the opposite case we denoted $M \cap A = Y$, and this set is equal to $L(\tau(Y), G)$ by Lemma 28. Therefore, M is the union of all sets of the form $L(\tau(Y), G)$ over all atomic polyhedra $A = A(H)$, where, in fact, $G = G(A)$ and $Y = Y(A)$. After that we subject each $L(\tau(Y), G)$ to the proper disjoint decomposition (Theorem 7); all resulting hybrid linear sets are proper, and it is straightforward that their convex hulls are disjoint (inside each A, this follows from Theorem 7, and sets corresponding to different A cannot intersect because atomic polyhedra are pairwise disjoint). This completes the proof; upper bounds on $\|B_i\|$, $\|P_i\|$ and $\#I$ follow from Lemmas 27, 18 and 16, and from Theorem 7. ◀

Proof of Theorem 21. In a similar way to the proof of Theorem 19, note that $\mathbb{Z}^d \setminus M = \bigcup_{H \subseteq \mathcal{H}} A(H) \cap \mathbb{Z}^d \setminus M$ and, in fact, it suffices to consider only (non-empty) atomic polyhedra

$A = A(H)$. Whenever in (5) all linear sets $L(\boldsymbol{b}, Q_{jt})$ avoid a polyhedron A, we have $A \cap \mathbb{Z}^d \setminus M = A \cap \mathbb{Z}^d$. By Proposition 1, this is a disjoint union of at most 2^d hybrid linear set of the form $L(B_i, P_i)$ with

$$\begin{aligned}\|B\|_i, \|P\|_i &\leq 2^{O(d^3)} \cdot \left(2^{O(d^3)} \cdot (\#Q + \|C\| + \|Q\| + d)^{O(d^2)}\right)^d \\ &= \|M\|^{O(d^4)}.\end{aligned}$$

In the opposite case we denoted $M \cap A = Y$, and this set is equal to $L(\tau(Y), G)$ by Lemma 28. Therefore, M is the union of all sets of the form $L(\tau(Y), G)$ over all atomic polyhedra $A = A(H)$, where, in fact, $G = G(A)$ and $Y = Y(A)$. After that we subject each $L(\tau(Y), G)$ to the proper disjoint decomposition (Theorem 7); all resulting hybrid linear sets are proper, and it is straightforward that their convex hulls are disjoint (inside each A, this follows from Theorem 7, and sets corresponding to different A cannot intersect because atomic polyhedra are pairwise disjoint). This completes the proof; upper bounds on $\|B_i\|$, $\|P_i\|$ follow from Lemmas 27 and 18. ◀

Proof of Corollary 20. The statement follows from Theorems 19 and 11. ◀

▶ **Corollary 22** (difference of semi-linear sets)**.** *The set-theoretic difference $M \setminus N$ of semi-linear sets $M = \bigcup_{j \in J} L(C_j, Q_j)$ and $N = \bigcup_{k \in K} L(D_k, R_k)$ has a representation of the form $L = \bigcup_{i \in I} L(B_i, P_i)$, where*

- $\max_{i \in I} \|B_i\|, \max_{i \in I} \|P_i\| \leq \#_{\mathsf{p}} M \cdot \|M\| \cdot \|N\|^{\#K \cdot O(d^8)}$.

Proof. By Theorem 21, $\overline{N} := \mathbb{Z}^d \setminus N$ has a semi-linear representation $\overline{N} = \bigcup_{\ell in L} (E_\ell, S_\ell)$ such that

- $\max_{\ell \in L} \|E_\ell\| \leq \|N\|^{\#K \cdot O(d^7 \cdot \log d)}$ and
- $\max_{\ell \in L} \|S_\ell\| \leq \|N\|^{\#K \cdot O(d^7)}$.

The trivial bound on $\#_{\mathsf{p}} \overline{N}$ gives $\#_{\mathsf{p}} \overline{N} \leq \|\overline{N}\|^d \leq \|N\|^{\#K \cdot O(d^8)}$. Consequently, by Theorem 6 we get $M \cap \overline{N} = \bigcup_{i \in I} L(B_i, P_i))$ such that

$$\begin{aligned}\max_{i \in I} \|B_i\|, \max_{i \in I} \|P_i\| &\leq (\#_{\mathsf{p}} M + \|N\|^{\#K \cdot O(d^8)}) \cdot \max(\|M\|, \|N\|^{\#K \cdot O(d^7 \cdot \log d)}) \\ &\leq (\#_{\mathsf{p}} M \cdot \|M\| \cdot \|N\|^{\#K \cdot O(d^8)}).\end{aligned}$$ ◀

▶ **Corollary 23** (small vector in set difference)**.** *Let M, N be semi-linear sets such that $\|M\|, \|N\| \leq n$ and $M \setminus N \neq \emptyset$. Then there is $\boldsymbol{v} \in M \setminus N$ such that $\|\boldsymbol{v}\| \leq 2^{n^{O(d^2)}}$.*

Proof. Let $M = \bigcup_{j \in J} L(C_j, Q_j)$ and $N = \bigcup_{k \in K} L(D_k, R_k)$. The trivial bound on $\#_{\mathsf{p}} M$ and $\#_{\mathsf{p}} N$ induced by n is $\#_{\mathsf{p}} M, \#_{\mathsf{p}} N \leq n^d$. By the discrete version of Carathéodory's theorem, Proposition 5, there are $M' = \bigcup_{j \in J'} L(C'_j, Q'_j)$ and $N' = \bigcup_{k \in K'} L(D'_k, R'_k)$ such that

- $\max_{j \in J'} \|C'_j\| \leq \|M\| + (\#_{\mathsf{p}} M \cdot \|M\|)^{O(d)} \leq n^{O(d^2)}$,
- $\max_{j \in J'} \|D'_j\| \leq \|N\| + (\#_{\mathsf{p}} N \cdot \|N\|)^{O(d)} \leq n^{O(d^2)}$,
- $\#_{\mathsf{p}} M', \#_{\mathsf{p}} N' \leq d$, and
- each $Q'_j \subseteq Q_j$ and each $R'_k \subseteq R_k$.

Consequently, $\#J', \#K' \leq \binom{n^d}{d} \leq n^{d^2}$. But then by Corollary 22, $M' \setminus N'$ contains an element $\boldsymbol{v}$ whose norm is bounded by

$$\|\boldsymbol{v}\| \leq \#_{\mathsf{p}} M' \cdot \|M'\| \cdot \|N'\|^{\#K' \cdot O(d^8)} \leq n^d \cdot n^{O(d^2)} \cdot n^{O(d^2)^{(n^{d^2} \cdot O(d^8))}} \leq 2^{n^{O(d^2)}}.$$ ◀

D Proof of Theorem 24

Here, we give a proof of Theorem 24.

▶ **Theorem 24.** *Equivalence for ESCG is* coNEXP*-complete.*

First, we introduce some additional notation. We write $D \overset{\pi}{\Rightarrow}_G E$ whenever $D \Rightarrow_G E$ by an application of the production π, and for a sequence of productions $\xi = \pi_1 \cdots \pi_n \in \Pi^*$, we write $U \overset{\xi}{\Rightarrow}_G V$ whenever there are $D_0, \dots, D_n$ such that $D_i \overset{\pi_i}{\Rightarrow}_G D_{i+1}$ for all $0 \le i < n$, $U = D_0$ and $V = D_n$. The effect of a production $\pi = V \to W$ is $\Delta(p) := W - V$, and the effect of a sequence of productions $\xi = \pi_1 \cdots \pi_n \in \Pi^*$ is $\Delta(\xi) := \sum_{1 \le i \le n} \Delta(\pi_i)$.

Call a linear set $L(\boldsymbol{b}, P) \subseteq \mathbb{N}^{(N \cup \Sigma)}$ with $P = \{\boldsymbol{p}_1, \dots, \boldsymbol{p}_k\}$ a *linear path scheme* whenever there are $\alpha_1, \dots, \alpha_{k+1} \in \Pi^*$ and $\tau_1, \dots, \tau_k \in \Pi^*$ such that

- $\boldsymbol{b}_i = \sum_{1 \le j \le k+1} \Delta(\alpha_i)$;
- $\boldsymbol{p}_j = \Delta(\tau_j)$ for every $1 \le j \le k$; and
- there are $W_1, W_1', \dots, W_k, W_k', W_{k+1}$ such that $S \overset{\pi_j}{\Rightarrow} W_j$ and $S \overset{\pi_j'}{\Rightarrow} W_j'$, where $\pi_j = \alpha_1 \cdots \alpha_j$ and $\pi_j' = \alpha_1 \cdots \alpha_j \tau_j$.

Observe that since the word problem for ESCG is in PSPACE, deciding whether a given linear set is a linear path scheme is also in PSPACE. We call a semi-linear set representation $\bigcup_{i \in I} L(\boldsymbol{b}_i, P_i)$ a *semi-linear path scheme* if every linear set it contains is a linear path scheme. In [18, Lem. 7], it is shown that reachability sets of ESCG can be obtained from semi-linear path schemes and bounds on the norm of their representation are provided as well.

▶ **Proposition 31** ([18]). *There exists a fixed polynomial p such that for every ESCG G, $\mathcal{R}(G) = \bigcup_{i \in I} L(\boldsymbol{b}_i, P_i)$, $\mathcal{R}(G)$ is a semi-linear path scheme, and $\|\mathcal{R}(G)\| \le 2^{p(|G|)}$.*

As an immediate consequence, we obtain the following corollary.

▶ **Corollary 32.** *There exists a fixed polynomial p such that for every ESCG G, $\mathcal{R}(G) = \bigcup_{j \in J} L(\boldsymbol{c}_i, Q_i)$ is a proper semi-linear set and a semi-linear path scheme with $\|\mathcal{R}(G)\| \le 2^{p(|G|)}$. In particular, the semi-linear representation of $\mathcal{R}(G)$ is computable in* $\mathsf{DTIME}(2^{\mathsf{poly}(|G|)})$.

Proof. By Theorem 5, every $L(\boldsymbol{b}_i, P_i)$ from Proposition 31 can be decomposed into a proper semi-linear set $M = \bigcup_{k \in K} L(\boldsymbol{c}_k, Q_k)$ such that $\|M\| \le 2^{p(|G|)}$ for some polynomial p. Since M is proper, $\#Q_k$ is bounded by $\#(N \cup \Sigma)$ and we can enumerate all proper linear sets $N = L(\boldsymbol{c}, Q)$ such that $\|N\| \le 2^{p(|G|)}$ in $\mathsf{DTIME}(2^{\mathsf{poly}(|G|)})$. Moreover, for every such N we can check in $\mathsf{PSPACE} \subseteq \mathsf{DTIME}(2^{\mathsf{poly}(|G|)})$ whether it is a linear path scheme. Hence the semi-linear representation of $\mathcal{R}(G)$ with the required properties can be constructed in $\mathsf{DTIME}(2^{\mathsf{poly}(|G|)})$. ◀

We can now show the coNEXP-upper bound for Theorem 24. Let G, H be ESCG such that $\mathcal{L}(G) \neq \mathcal{L}(H)$, and with no loss of generality assume that there is some $w \in \mathcal{L}(G) \setminus \mathcal{L}(H)$. By Corollary 23, we have $\|w\| \le 2^{2^{q(|G|+|H|)}}$ for some fixed polynomial q, hence the representation size n of w is bounded by $2^{q(|G|+|H|)}$. Thus, for the coNEXP-upper bound it only remains to be shown that $w \in \mathcal{L}(G)$ and $w \notin \mathcal{L}(H)$ can be checked in time polynomial in n. Thanks to Corollary 32, we can compute in $\mathsf{DTIME}(2^{\mathsf{poly}(|G|)}) = \mathsf{DTIME}(\mathsf{poly}(n))$ the proper semi-linear representations of $\mathcal{R}(G)$ and $\mathcal{R}(H)$. In particular, checking $w \in L(\boldsymbol{c}_j, Q_j)$ for proper linear sets $L(\boldsymbol{c}_j, Q_j)$ from $\mathcal{R}(G)$ or $\mathcal{R}(H)$ can be decided in polynomial time since Q_j is linearly independent, and hence deciding $w \in \mathcal{L}(G)$ and $w \notin \mathcal{L}(H)$ can be decided in $\mathsf{DTIME}(2^{\mathsf{poly}(|G|+|H|)})$. This in turn yields the coNEXP-upper bound for the equivalence problem for ESCG.