The Identity Problem in virtually solvable matrix groups over algebraic numbers

Corentin Bodart
Mathematical Institute, University of Oxford
Oxford, United Kingdom
cobodart123@gmail.com

Ruiwen Dong
Magdalen College, University of Oxford
Oxford, United Kingdom
ruiwen.dong@magd.ox.ac.uk

***Abstract*—The *Tits alternative* states that a finitely generated matrix group either contains a nonabelian free subgroup F_2, or it is virtually solvable. This paper considers two decision problems in virtually solvable matrix groups: the *Identity Problem* (does a given finitely generated subsemigroup contain the identity matrix?), and the *Group Problem* (is a given finitely generated subsemigroup a group?). We show that both problems are decidable in virtually solvable matrix groups over the field of algebraic numbers $\overline{\mathbb{Q}}$. Our proof also extends the decidability result for nilpotent groups by Bodart, Ciobanu, Metcalfe and Shaffrir, and the decidability result for metabelian groups by Dong (STOC'24). Since the Identity Problem and the Group Problem are known to be undecidable in matrix groups containing $F_2 \times F_2$, our result significantly reduces the decidability gap for both decision problems.**

***Index Terms*—matrix semigroups, virtually solvable groups, rational semigroups, computational group theory, Identity Problem**

1. Introduction

A. Decision problems in matrix semigroups

The computational theory of matrix groups and semigroups is one of the oldest and most well-developed parts of computational algebra. In the seminal work of Markov from the 1940s [1], the *Semigroup Membership* problem was shown to be undecidable for integer matrices of dimension six. This marked the first undecidability results obtained outside of mathematical logic and the theory of computing. This area now plays an essential role in analysing system dynamics, and has numerous applications in automata theory, randomized algorithms, program analysis, and interactive proof systems [2], [3], [4], [5], [6]. In the 1950s, Mikhailova [7] similarly introduced the *Group Membership* problem. For both problems, we work in some fixed matrix group G. For effectiveness reasons[1], this paper focuses on the case where G is a subgroup of $\mathsf{GL}(d, \overline{\mathbb{Q}})$ for some $d \geq 1$ (the group of $d \times d$ invertible matrices over algebraic numbers). Given a set $X \subseteq G$, denote by $\langle X \rangle$ the semigroup generated by X, and by $\langle X \rangle_{\text{grp}}$ the group generated by X. Then the two decision problems are formulated as follows.

(i) *(Semigroup Membership)* given $A_1, \ldots, A_m, T \in G$, decide whether $T \in \langle A_1, \ldots, A_m \rangle$.

(ii) *(Group Membership)* given $A_1, \ldots, A_m, T \in G$, decide whether $T \in \langle A_1, \ldots, A_m \rangle_{\text{grp}}$.

In this paper, we consider two closely related problems introduced by Choffrut and Karhumäki in the 2000s [5]. Let I denote the identity matrix.

(iii) *(Identity Problem)* given $A_1, \ldots, A_m \in G$, decide whether $I \in \langle A_1, \ldots, A_m \rangle$.

(iv) *(Group Problem)* given $A_1, \ldots, A_m \in G$, decide whether $\langle A_1, \ldots, A_m \rangle$ is a group.

These decision problems concern the *structure* of a semigroup rather than its *membership*. See for example [9], [10], [11] for earlier developments on the Identity Problem and the Group Problem, and see [12], [13] for surveys on more recent progress. Note that decidability of the Group Problem subsumes decidability of the Identity Problem and the *Inverse Problem* (decide whether $A_1^{-1} \in \langle A_1, \ldots, A_m \rangle$) [14]: these are the essential special cases of Semigroup Membership.

All four algorithmic problems above are undecidable when G contains as a subgroup a direct product of two free groups $F_2 \times F_2$ [7], [9], for example when $G = \mathsf{SL}(4, \mathbb{Z})$ (the group of 4×4 integer matrices with determinant one). This motivates us to study groups on the other end of the spectrum: namely when G does not contain F_2 as a subgroup. By the celebrated *Tits alternative* [15], a finitely generated subgroup of $\mathsf{GL}(d, \overline{\mathbb{Q}})$ either contains F_2 as a subgroup, or it is *virtually solvable*. This paper will focus on the latter case.

B. Virtually solvable matrix groups over $\overline{\mathbb{Q}}$

We briefly recall the definitions of solvable, virtually solvable, metabelian, and nilpotent groups. Given a group G and its subgroup H, denote by $[G, H]$ the group generated by the elements $ghg^{-1}h^{-1}, g \in G, h \in H$. A group G is *solvable* if its *derived series* $G = G^{(0)} \geq G^{(1)} \geq \cdots$, defined by $G^{(i+1)} = [G^{(i)}, G^{(i)}]$, reaches the trivial group in a finite number of steps. A group is *virtually solvable* if it admits a finite index subgroup that is solvable. In particular, solvable groups are also virtually solvable. Metabelian groups and nilpotent groups are special cases of solvable groups. A group G is called *metabelian* if $G^{(2)}$ is trivial, or equivalently, if G admits an abelian normal subgroup A such that the quotient G/A is abelian. A group G is *nilpotent* if its *lower central series* $G = G_0 \geq G_1 \geq \cdots$, defined by $G_{i+1} = [G, G_i]$, reaches the trivial group in a finite number of steps.

[1]Elements of the field of algebraic numbers $\overline{\mathbb{Q}}$ can be effectively represented and computed [8].

A classic result of Kopytov [16] showed that Group Membership is decidable in virtually solvable matrix groups over $\overline{\mathbb{Q}}$. Semigroup Membership is proven to be undecidable for some instances of solvable matrix groups, such as large direct powers of the Heisenberg group $\mathsf{H}_3(\mathbb{Z})$ [17]. Conversely, it has been shown to be decidable for other instances, such as commutative matrix groups over $\overline{\mathbb{Q}}$ [18], the Heisenberg groups $\mathsf{H}_{2n+1}(\mathbb{Q})$ [19], the Baumslag-Solitar groups $\mathsf{BS}(1,q)$ [20], and the lamplighter groups $(\mathbb{Z}/n\mathbb{Z}) \wr \mathbb{Z}$ [21]. Decidability of the Identity Problem and the Group Problem was open for virtually solvable matrix groups over $\overline{\mathbb{Q}}$. Nevertheless, they were recently proven to be decidable in the case of nilpotent groups [22], [23] and in the case of metabelian groups [14]. In this paper, we completely answer this open problem by proving decidability of the Identity Problem and the Group Problem in all virtually solvable matrix groups over $\overline{\mathbb{Q}}$.

Note that in the definition of both problems, the input is a set of matrices $\{A_1, \dots, A_m\}$ in some virtually solvable group $G \leq \mathsf{GL}(d, \overline{\mathbb{Q}})$. It is not important whether G is given as a part of the input, as we can always suppose G to be the group generated by $\{A_1, \dots, A_m\}$. This does not change the fact that G is virtually solvable, since finitely generated subgroups of virtually solvable groups are still virtually solvable [24].

Theorem 1.1. *The Identity Problem and the Group Problem are decidable in virtually solvable subgroups of* $\mathsf{GL}(d, \overline{\mathbb{Q}})$. *That is, given matrices* $A_1, \dots, A_m \in \mathsf{GL}(d, \overline{\mathbb{Q}})$ *that generate a virtually solvable group*[2]*, it is decidable whether* $I \in \langle A_1, \dots, A_m \rangle$, *and whether* $\langle A_1, \dots, A_m \rangle$ *is a group.*

C. Related work and our contributions

Two significant results on the Identity Problem are its decidability in nilpotent groups, due to Shaffrir [23] (and independently by Bodart, Ciobanu, Metcalfe [22]), as well as its decidability in metabelian groups, due to Dong [14]. Our paper generalizes these two results, and then uses their generalization as crucial lemmas in our solution for virtually solvable matrix groups over $\overline{\mathbb{Q}}$. In particular:

(1) We extend a key theorem in [22] and [23] from *finitely generated* nilpotent groups to *infinitely generated* nilpotent groups of finite Prüfer rank (Theorem 3.4, proof in Section 5). This applies to groups of *unitriangular* matrices over an algebraic number field $\mathbb{K}$.

(2) We generalize the result in [14] from finitely generated subsemigroups of metabelian groups to their *rational subsemigroups* (Theorem 3.8, proof in Section 4). To this end, we combine automata theory with the concepts developed in [14], and introduce new techniques such as *$\mathcal{A}$-graphs* and *partial contractions*. We connect automata over metabelian groups to graphs over lattices, convex polytopes and algebraic geometry, and prove several theorems under this new context (Theorem 4.7, Lemma 4.12, Theorem 4.14).

(3) We then reduce the Group Problem in a virtually solvable matrix group G to deciding if a rational subsemigroup of a metabelian group is a group (Section 3). This reduction is done by constructing a metabelian quotient $T/[N,N]$ of a triangularizable subgroup T of G. The normal subgroup $[N,N] \trianglelefteq T$ is the commutator of an *infinitely* generated nilpotent group N, hence the extension in (1) is needed. By reducing from G to $T/[N,N]$, we inevitably pass from finitely generated subsemigroups of G to *rational* subsemigroups of $T/[N,N]$. Hence the generalization in (2) is needed.

Finally, in Section 6, we discuss possible future work and the limit of our results. In particular, our techniques cannot extend to matrix groups over effective fields larger than $\overline{\mathbb{Q}}$, such as $\mathbb{Q}(X)$, due to the failure of a key theorem (see Remark 5.8).

2. Preliminaries

A. Rational subsemigroups and automata over groups

Let S be a set of elements in G. The semigroup $\langle S \rangle$ generated by S is defined as the set of non-empty products of elements in S, that is, $\langle S \rangle := \{g_1 g_2 \cdots g_p \mid p \geq 1, g_1, g_2, \dots, g_p \in S\}$.

Lemma 2.1 ([14, Lemma 2.2])**.** *Let X be a finite set of elements in a group G. The semigroup $\langle X \rangle$ contains the neutral element I if and only if there is a non-empty subset $Y \subseteq X$ such that $\langle Y \rangle$ is a group. Hence, if the Group Problem is decidable in G, then the Identity Problem is also decidable by testing the Group Problem on all subsets of the input.*

In this paper, we will need the more general notion of *rational semigroups*, which are recognized by *automata over groups*. See [26] for a general reference on rational subsets of groups. Given a group G, an *automaton* over G is defined by a set of s *states* $q_1, \dots, q_s$, and a set of t *transitions* $\delta_1, \dots, \delta_t$. For each $\ell = 1, \dots, t$, the transition δ_ℓ has an *origin* state which we denote by $q_{\Omega(\ell)}$, a *destination* state which we denote by $q_{\Delta(\ell)}$, as well as an *evaluation* in G which we denote by $\mathrm{ev}(\delta_\ell) \in G$. We call q_1 both the *initial state* and the *accepting state*, that is, we only consider automata whose initial state is the same as the accepting state.

A *path* in $\mathcal{A}$ is a non-empty sequence of transitions $w = \delta_{i_1} \delta_{i_2} \cdots \delta_{i_m}$, such that $\Delta(i_1) = \Omega(i_2), \Delta(i_2) = \Omega(i_3), \dots, \Delta(i_{m-1}) = \Omega(i_m)$. The *evaluation* of such a path is defined as $\mathrm{ev}(w) := \mathrm{ev}(\delta_{i_1}) \mathrm{ev}(\delta_{i_2}) \cdots \mathrm{ev}(\delta_{i_m}) \in G$. A path is called an *accepting run* if additionally $\Omega(i_1) = \Delta(i_m) = 1$. Let $\mathrm{ev}(\mathcal{A}) := \{\mathrm{ev}(w) \mid w \text{ is an accepting run of } \mathcal{A}\}$, this is the set of elements of G recognized by accepting runs. Then $\mathrm{ev}(\mathcal{A})$ is a subsemigroup of G because, if w and w' are accepting runs of $\mathcal{A}$, then the concatenation ww' is also an accepting run, and $\mathrm{ev}(ww') = \mathrm{ev}(w)\,\mathrm{ev}(w')$. However, $\mathrm{ev}(\mathcal{A})$ does not necessarily contain the neutral element of G, since the empty sequence is not considered as an accepting run. We say that the automaton $\mathcal{A}$ *recognizes* the semigroup $\mathrm{ev}(\mathcal{A})$. A subset $S \subseteq G$ is called a *rational semigroup* if there is some automaton $\mathcal{A}$ over G that recognizes S.

An automaton $\mathcal{A}$ is called *trim* if every state is the origin of some transition and every transition appears in some accepting run. Every rational subsemigroup of G is recognized by a trim

[2]Note that given $A_1, \dots, A_m \in \mathsf{GL}(d, \overline{\mathbb{Q}})$, it is decidable whether $\langle A_1, \dots, A_m \rangle_{\mathrm{grp}}$ is virtually solvable [25].

automaton over G by removing states unreachable from q_1 and states from which q_1 is unreachable.

If $\mathcal{A}$ has only one state q_1, then all its transitions are loops, so $\mathrm{ev}(\mathcal{A})$ is the semigroup generated by $\mathrm{ev}(\delta_1), \dots, \mathrm{ev}(\delta_t)$, and we recover the definition of finitely generated semigroups.

B. Triangular matrix groups

Let $\mathbb{K}$ be a field. Denote respectively by $\mathsf{T}(d, \mathbb{K})$ and $\mathsf{UT}(d, \mathbb{K})$ the group of $d \times d$ upper-triangular invertible matrices over $\mathbb{K}$ and the group of $d \times d$ upper-unitriangular matrices over $\mathbb{K}$:

$$\mathsf{T}(d, \mathbb{K}) \coloneqq \left\{ \begin{pmatrix} a_1 & * & \cdots & * \\ 0 & a_2 & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_d \end{pmatrix}, \ a_1 a_2 \cdots a_d \neq 0 \right\},$$

$$\mathsf{UT}(d, \mathbb{K}) \coloneqq \left\{ \begin{pmatrix} 1 & * & \cdots & * \\ 0 & 1 & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} \right\},$$

where a_i and $*$ denote arbitrary entries in $\mathbb{K}$. The group $\mathsf{T}(d, \mathbb{K})$ and its subgroups are solvable; the group $\mathsf{UT}(d, \mathbb{K})$ and its subgroups are nilpotent [24]. If T is any subgroup of $\mathsf{T}(d, \mathbb{K})$, then $N \coloneqq T \cap \mathsf{UT}(d, \mathbb{K})$ is a normal subgroup of T, and the quotient T/N is abelian.

Let G be a finitely generated subgroup of $\mathsf{GL}(d, \overline{\mathbb{Q}})$. By a classic result of Mal'cev [27], G is virtually solvable if and only if it contains a finite index normal subgroup T that is conjugate to a subgroup of $\mathsf{T}(d, \overline{\mathbb{Q}})$. This gave rise to algorithms that decide whether a given finitely generated matrix group over $\overline{\mathbb{Q}}$ is virtually solvable:

Theorem 2.2 ([25, Theorem 1.1], [28, Section 2.8])**.** *There is an algorithm that, given a finite number of generators for a group $G \leq \mathsf{GL}(d, \overline{\mathbb{Q}})$, decides whether G is virtually solvable. Furthermore, when G is virtually solvable, the algorithm computes the generators[3] for a finite index normal subgroup $T \trianglelefteq G$, as well as a matrix $g \in \mathsf{GL}(d, \overline{\mathbb{Q}})$, such that $gTg^{-1} \leq \mathsf{T}(n, \overline{\mathbb{Q}})$.*

C. Polynomial rings, modules and semidirect products

Let R be a commutative ring or semiring (such as $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{N}$ or $\mathbb{R}_{\geq 0}$). Denote by $R[X_1^{\pm}, \dots, X_n^{\pm}]$ the Laurent polynomial ring or semiring over R with n variables: this is the set of polynomials of variables $X_1, X_1^{-1}, \dots, X_n, X_n^{-1}$, with coefficients in R. We have $X_i X_i^{-1} = 1$. When n is fixed, we denote $R[\overline{X}^{\pm}] \coloneqq R[X_1^{\pm}, \dots, X_n^{\pm}]$. For a vector $a = (a_1, \dots, a_n) \in \mathbb{Z}^n$, denote by $\overline{X}^a$ the monomial $X_1^{a_1} X_2^{a_2} \cdots X_n^{a_n}$.

When R is a commutative ring, an $R[\overline{X}^{\pm}]$-module is defined as an abelian group $(M, +)$ along with an operation $\cdot : R[\overline{X}^{\pm}] \times M \to M$ satisfying $f \cdot (m + m') = f \cdot m + f \cdot m'$, $(f + g) \cdot m = f \cdot m + g \cdot m$, $fg \cdot m = f \cdot (g \cdot m)$ and $1 \cdot m = m$. For example, for any $d \in \mathbb{N}$, $R[\overline{X}^{\pm}]^d$ is an $R[\overline{X}^{\pm}]$-module by $f \cdot (g_1, \dots, g_d) = (fg_1, \dots, fg_d)$. Throughout this paper, we use the bold symbol $\boldsymbol{f}$ to denote a vector $(f_1, \dots, f_d) \in R[\overline{X}^{\pm}]^d$.

Given vectors $\boldsymbol{h}_1, \dots, \boldsymbol{h}_k \in R[\overline{X}^{\pm}]^d$, we say that they *generate* the $R[\overline{X}^{\pm}]$-module

$$\sum_{i=1}^{k} R[\overline{X}^{\pm}] \cdot \boldsymbol{h}_i \coloneqq \left\{ \sum_{i=1}^{k} p_i \cdot \boldsymbol{h}_i \;\middle|\; p_1, \dots, p_k \in R[\overline{X}^{\pm}] \right\}.$$

Given submodules M, N of $R[\overline{X}^{\pm}]^d$ such that $M \supseteq N$, we define the quotient $M/N \coloneqq \{\overline{m} \mid m \in M\}$ where $\overline{m_1} = \overline{m_2}$ if and only if $m_1 - m_2 \in N$. This quotient is also an $R[\overline{X}^{\pm}]$-module. We say that an $R[\overline{X}^{\pm}]$-module $\mathcal{Y}$ is *finitely presented* if it can be written as a quotient M/N for two submodules M, N of $R[\overline{X}^{\pm}]^d$ for some $d \in \mathbb{N}$, where both M and N are generated by finitely many elements. We call a *finite presentation* of $\mathcal{Y}$ the respective generators of such M, N. Given a finitely presented $\mathbb{Z}[X_1^{\pm}, \dots, X_n^{\pm}]$-module $\mathcal{Y}$, we can define a metabelian group using *semidirect product*:

$$\mathcal{Y} \rtimes \mathbb{Z}^n \coloneqq \{(y, a) \mid y \in \mathcal{Y}, a \in \mathbb{Z}^n\}; \tag{1}$$

multiplication and inversion in this group are defined by

$$(y, a)(y', a') = \left(y + \overline{X}^a \cdot y', a + a'\right), (y, a)^{-1} = \left(-\overline{X}^{-a} \cdot y, -a\right). \tag{2}$$

The neutral element of $\mathcal{Y} \rtimes \mathbb{Z}^n$ is $(0, 0)$. Intuitively, the element (y, a) can be seen as a 2×2 matrix $\begin{pmatrix} \overline{X}^a & y \\ 0 & 1 \end{pmatrix}$, where group multiplication is represented by matrix multiplication. Note that $\mathcal{Y} \rtimes \mathbb{Z}^n$ naturally contains the subgroups $\mathbb{Z}^n \cong \{(0, a) \mid a \in \mathbb{Z}^n\}$ and $\mathcal{Y} \cong \{(y, 0^n) \mid y \in \mathcal{Y}\}$.

3. Decidability in virtually solvable matrix groups: proof overview

Omitted proofs can be found in Appendix A. In this section we prove our main result:

Theorem 1.1. *The Identity Problem and the Group Problem are decidable in virtually solvable subgroups of $\mathsf{GL}(d, \overline{\mathbb{Q}})$. That is, given matrices $A_1, \dots, A_m \in \mathsf{GL}(d, \overline{\mathbb{Q}})$ that generate a virtually solvable group, it is decidable whether $I \in \langle A_1, \dots, A_m \rangle$, and whether $\langle A_1, \dots, A_m \rangle$ is a group.*

By Lemma 2.1, it suffices to show decidability of the Group Problem. Given $A_1, \dots, A_m \in \mathsf{GL}(d, \overline{\mathbb{Q}})$ such that $G \coloneqq \langle A_1, \dots, A_m \rangle_{\mathrm{grp}}$ is virtually solvable, our goal is to decide whether $\langle A_1, \dots, A_m \rangle$ is a group.

By Theorem 2.2, G admits a finite index normal subgroup T such that $gTg^{-1} \leq \mathsf{T}(d, \overline{\mathbb{Q}})$ for an effectively computable element $g \in \mathsf{GL}(d, \overline{\mathbb{Q}})$. We can replace G with gGg^{-1} (that is, replace the generators $A_1, \dots, A_m$ by their conjugates $gA_1g^{-1}, \dots, gA_mg^{-1}$), and thus without loss of generality suppose $T \leq \mathsf{T}(d, \overline{\mathbb{Q}})$. Furthermore, a finite set of generators for T is also given by Theorem 2.2. After the replacement, let $\mathbb{K}$ denote the field generated by all the entries of $A_1, \dots, A_m$. Then, G and T are respectively subgroups of $\mathsf{GL}(d, \mathbb{K})$ and $\mathsf{T}(d, \mathbb{K})$.

[3] Note that when G is finitely generated, its finite index subgroups are also finitely generated [24, Lemma 7.86].

Deciding whether $\langle A_1, \ldots, A_m \rangle$ is a group is done through a series of reductions. First, we reduce it to a deciding whether the rational semigroup $S \coloneqq \langle A_1, \ldots, A_m \rangle \cap T$ is a group:

Lemma 3.1. *Let $T \leq \mathsf{T}(d, \mathbb{K})$ be a finite index normal subgroup of $G = \langle A_1, \ldots, A_m \rangle_{\text{grp}}$, given by a finite set of generators. Then, $\langle A_1, \ldots, A_m \rangle$ is a group if and only if $S \coloneqq \langle A_1, \ldots, A_m \rangle \cap T$ is a group. Furthermore, S is a rational subsemigroup of T, whose automaton can be effectively computed from $A_1, \ldots, A_m$ and the generators of T.*

Example 3.2. This will be the running example of this section. Consider the following elements in the virtually solvable group $\mathsf{T}(3, \mathbb{Q}) \times (\mathbb{Z}/2\mathbb{Z})$:

$$A_1 = \left(\begin{pmatrix} 2 & 7 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, 1 \right), \; A_2 = \left(\begin{pmatrix} 1 & -1 & 1 \\ 0 & 2 & 5 \\ 0 & 0 & 1 \end{pmatrix}, 0 \right),$$
$$A_3 = \left(\begin{pmatrix} 1/2 & 1 & 3 \\ 0 & 1/2 & -1 \\ 0 & 0 & 1 \end{pmatrix}, 0 \right).$$

Let $G = \langle A_1, A_2, A_3 \rangle_{\text{grp}}$ and let T be its index-two subgroup $T \coloneqq \{(B, z) \in G \mid z = 0\}$. One can for brevity discard the entry $z = 0$, and simply write T as a group of upper triangular matrices $\{B \in \mathsf{T}(3, \mathbb{Q}) \mid (B, 0) \in G\}$. Then, the semigroup $S \coloneqq \langle A_1, A_2, A_3 \rangle \cap T$ consists of those products of A_1, A_2, A_3 where A_1 is used an even number of times. Therefore, S is recognized by automaton $\mathcal{A}$ over T in Figure 1. Here, T can be directly computed as:

$$T = \left\{ \begin{pmatrix} 2^a & x & z \\ 0 & 2^b & y \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; a, b \in \mathbb{Z}, x, y, z \in \mathbb{Z}[1/2] \right\}, \quad (3)$$

where $\mathbb{Z}[1/2] \coloneqq \left\{ \frac{a}{2^p} \;\middle|\; a \in \mathbb{Z}, p \in \mathbb{N} \right\}$. □

The following lemma further shows we can without loss of generality suppose $\langle S \rangle_{\text{grp}} = T$:

Lemma 3.3. *Let S be a rational subsemigroup of T, then $\langle S \rangle_{\text{grp}}$ is finitely generated. Furthermore, given an automaton over T that recognizes S, one can compute an automaton over $\langle S \rangle_{\text{grp}}$ that recognizes S, as well as compute a set of generators for $\langle S \rangle_{\text{grp}}$.*

Lemma 3.1 and 3.3 are proven using only classic ideas and techniques from automata theory. In particular, Lemma 3.1 shows that $\langle A_1, \ldots, A_m \rangle$ is a group if and only if S is a group. Lemma 3.3 shows that we can suppose S to be given by an automaton over $\langle S \rangle_{\text{grp}}$ instead of T. In other words, we can replace T by its subgroup $\langle S \rangle_{\text{grp}}$, and suppose without loss of generality $\langle S \rangle_{\text{grp}} = T$. We proceed to decide whether S is a group.

Let $N \coloneqq T \cap \mathsf{UT}(d, \mathbb{K})$, then N is a nilpotent normal subgroup of T. Consider the normal subgroup $[N, N]$ of N, we obtain a descending sequence of subgroups

$$T \trianglerighteq N \trianglerighteq [N, N],$$

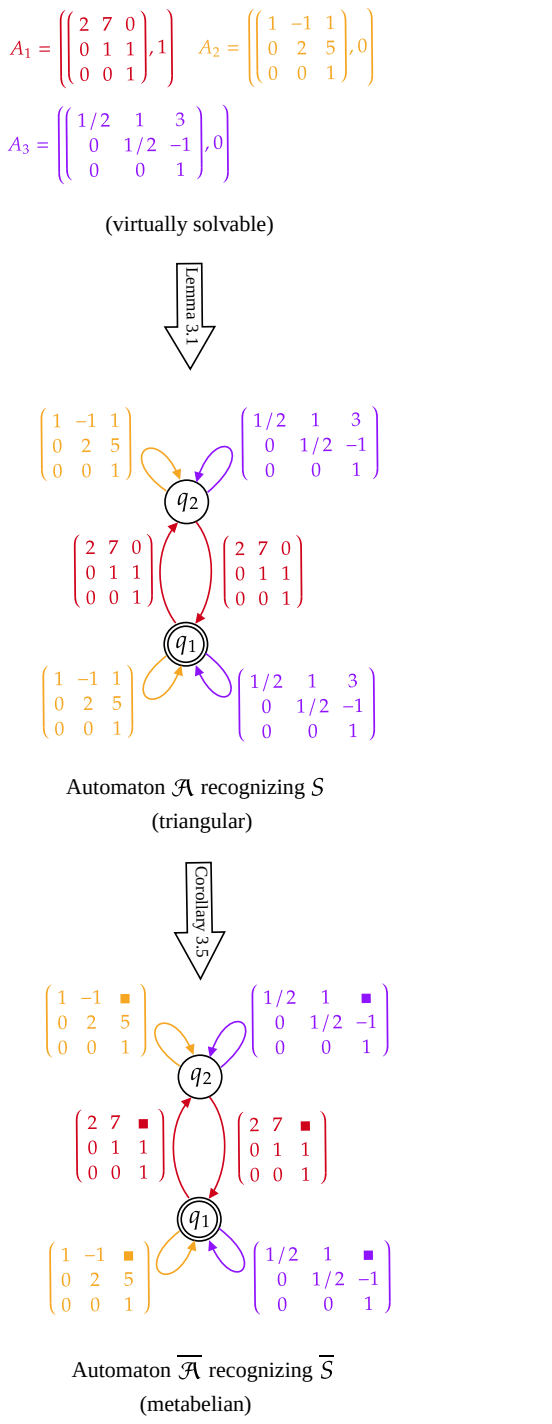

Fig. 1. Illustration of Example 3.2: reduction from the virtually solvable group $G \supseteq \langle A_1, A_2, A_3 \rangle$, to the triangular matrix group $T \supseteq S$, then to the metabelian group $T/[N, N] \supseteq \overline{S}$.

where T/N is finitely generated abelian, and $N/[N, N]$ is abelian.

The group $[N, N]$ is also a normal subgroup of T because, for all $t \in T, n, m \in N$, we have $t(nmn^{-1}m^{-1})t^{-1} = (tnt^{-1})(tmt^{-1})(tnt^{-1})^{-1}(tmt^{-1})^{-1} \in [N, N]$. Therefore,

the quotient $T/[N,N]$ is a finitely generated metabelian group.

Example 3.2 (continued)**.** Recall T from Equation (3). Directly computing $N \coloneqq T \cap \mathsf{UT}(3,\mathbb{Q})$, we have

$$N = \left\{ \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; x,y,z \in \mathbb{Z}[1/2] \right\},$$

and hence

$$[N,N] = \left\{ \begin{pmatrix} 1 & 0 & z \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; z \in \mathbb{Z}[1/2] \right\}.$$

Note that N and $[N,N]$ are not finitely generated, even though T is finitely generated. □

Our next step is to show that $S \subseteq T$ is a group if and only if its image $\overline{S}$ under the quotient map $T \to T/[N,N]$ is a group. In other words, we will simplify T by "modulo" $[N,N]$, and show that this (remarkably) does not change whether S is a group.

Our first main technical theorem is a weak version of the above simplification:

Theorem 3.4. *Let $\mathbb{K}$ be an algebraic number field and N be a subgroup of $\mathsf{UT}(d,\mathbb{K})$. Let M be a subsemigroup of N and denote by $\overline{M}$ its image under the quotient map $N \to N/[N,N]$. If $\overline{M} = N/[N,N]$ (equivalently, if $M[N,N] = N$), then $M = N$.*

Theorem 3.4 is a deep generalization of [23, Corollary 1] (see also [22, Proposition 19]), which proved the case when N is finitely generated. Theorem 3.4 relaxes this constraint, the key idea being that for an algebraic number field $\mathbb{K}$, subgroups of $\mathsf{UT}(d,\mathbb{K})$ have finite *Prüfer rank*. The proof of Theorem 3.4 is given in Section 5. We now strengthen Theorem 3.4 from N to T:

Corollary 3.5. *Let S be a subsemigroup of T such that $\langle S \rangle_{\mathrm{grp}} = T$. Then S is a group (i.e. $S = T$) if and only if its image $\overline{S}$ under the quotient map $T \to T/[N,N]$ is a group (i.e. $\overline{S} = T/[N,N]$).*

Proof. If $S = T$ then obviously $\overline{S} = T/[N,N]$. In the other direction, if $\overline{S} = T/[N,N]$ (which yields $S[N,N] = T$), then $(S \cap N)[N,N] = N$. Using Theorem 3.4 we deduce that the semigroup $M = S \cap N$ is actually equal to N, and therefore $S \supseteq N \supseteq [N,N]$. It follows that $S = S[N,N] = T$. □

Example 3.2 (continued)**.** We continue Example 3.2 to give an intuition about the group $T/[N,N]$. Since $T = \left\{ \begin{pmatrix} 2^a & x & z \\ 0 & 2^b & y \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; a,b \in \mathbb{Z}, x,y,z \in \mathbb{Z}[1/2] \right\}$ and $[N,N] = \left\{ \begin{pmatrix} 1 & 0 & z \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; z \in \mathbb{Z}[1/2] \right\}$, elements of $T/[N,N]$ can be seen as matrices of the form $\begin{pmatrix} 2^a & x & \blacksquare \\ 0 & 2^b & y \\ 0 & 0 & 1 \end{pmatrix}$, $a,b \in \mathbb{Z}$, $x,y \in \mathbb{Z}[1/2]$, where $\blacksquare$ is an extra symbol. The group operation in $T/[N,N]$ is like matrix multiplication in T but ignoring the upper-right entry $\blacksquare$. Therefore, the image $\overline{S}$ of the semigroup S under the quotient map $T \to T/[N,N]$ is recognized by the automaton $\overline{\mathcal{A}}$ at the bottom of Figure 1. Intuitively, the quotient by $[N,N]$ simplifies S by "ignoring" all the upper-right entries, and Corollary 3.5 shows that such a simplification does not change whether S is a group. This allows us to reduce from the subsemigroup S of the *triangular* matrix group T to the subsemigroup $\overline{S}$ of the *metabelian* group $T/[N,N]$.

By Corollary 3.5, deciding whether $S \subseteq T$ is a group boils down to deciding whether $\overline{S} \subseteq T/[N,N]$ is a group: this will be our new task. From an automaton $\mathcal{A}$ over T that recognizes S, we can construct an automaton $\overline{\mathcal{A}}$ over $T/[N,N]$ that recognizes $\overline{S}$ by projecting the transition evaluations under $T \to T/[N,N]$. Next, we switch from the matrix representation of $T/[N,N]$ to the following more standard way of representing metabelian groups.

Lemma 3.6 (Composition of [29, Lemma 2] and [14, Lemma B.3])**.** *Let $\mathbb{K}$ be an algebraic number field. Suppose we are given a finitely generated subgroup T of $\mathsf{T}(d,\mathbb{K})$, let $N \coloneqq T \cap \mathsf{UT}(d,\mathbb{K})$. One can compute an embedding $\varphi\colon T/[N,N] \hookrightarrow (\mathcal{Y} \rtimes \mathbb{Z}^n)/H$, where*

(i) *$n \in \mathbb{N}$ and $\mathcal{Y}$ is a finitely presented $\mathbb{Z}[X_1^{\pm},\dots,X_n^{\pm}]$-module.*

(ii) *H is a subgroup of $\mathbb{Z}^n \leq \mathcal{Y} \rtimes \mathbb{Z}^n$, and elements of H commute with all elements in $\mathcal{Y} \rtimes \mathbb{Z}^n$.*

In particular, given any $g \in T$, one can compute $(y,z) \in \mathcal{Y} \rtimes \mathbb{Z}^n$ such that $\varphi(g[N,N]) = (y,z)H$.

Since φ is an embedding, the semigroup $\overline{S} \subseteq T/[N,N]$ is a group if and only if its image $\varphi(\overline{S}) \subseteq (\mathcal{Y} \rtimes \mathbb{Z}^n)/H$ is a group. In turn $\varphi(\overline{S})$ is a group if and only if $\varphi(\overline{S})H \subseteq \mathcal{Y} \rtimes \mathbb{Z}^n$ is a group. We went from "abstract" semigroups inside $T/[N,N]$ to "concrete" semigroups inside $\mathcal{Y} \rtimes \mathbb{Z}^n$.

Lemma 3.7. *Let $\varphi(\overline{S})$ be a rational subsemigroup of $(\mathcal{Y} \rtimes \mathbb{Z}^n)/H$ recognized by a given automaton. Then one can compute an automaton over $\mathcal{Y} \rtimes \mathbb{Z}^n$ that recognizes the subsemigroup $\varphi(\overline{S})H$.*

The idea behind Lemma 3.7 is as follows: from an automaton that recognizes $\varphi(\overline{S})$, one can construct an automaton that recognizes $\varphi(\overline{S})H$ by attaching loops at q_1, whose evaluations generate H as a semigroup. Now, deciding whether a rational semigroup $\overline{S} \subseteq T/[N,N]$ is a group boils down to deciding whether the rational semigroup $\varphi(\overline{S})H \subseteq \mathcal{Y} \rtimes \mathbb{Z}^n$ is a group.

Theorem 3.8. *Given as input a finitely presented $\mathbb{Z}[X_1^{\pm},\dots,X_n^{\pm}]$-module $\mathcal{Y}$ and an automaton $\mathcal{A}$ over $\mathcal{Y} \rtimes \mathbb{Z}^n$, it is decidable whether $\mathrm{ev}(\mathcal{A})$ is a group.*

Theorem 3.8 is highly non-trivial and is our second main technical contribution. Its proof is given in Section 4. Theorem 3.8 can be seen a generalization of [14, Theorem 1.1], which proves the decidability result for *finitely generated* subsemigroups of $\mathcal{Y} \rtimes \mathbb{Z}^n$.

Summarizing all the above results, we obtain a proof of Theorem 1.1:

Proof of Theorem 1.1. By Lemma 2.1, it suffices to decide the Group Problem. Conjugating $A_1, \dots, A_m$ by the element g computed in Theorem 2.2, we can suppose $G := \langle A_1, \dots, A_m \rangle_{\mathrm{grp}}$ admits a finite index normal subgroup $T \leq \mathrm{T}(d, \mathbb{K})$ for some algebraic number field $\mathbb{K}$. Then, Lemma 3.1 shows that $\langle A_1, \dots, A_m \rangle$ is a group if and only if the rational semigroup $S = \langle A_1, \dots, A_m \rangle \cap T$ is a group, and Lemma 3.3 shows that we can replace T with its subgroup $\langle S \rangle_{\mathrm{grp}}$. Then, by Corollary 3.5, Lemma 3.6 and Lemma 3.7, the rational semigroup S is a group if and only if $\varphi(\overline{S})H$ is a group. Furthermore, one can construct an automaton $\mathcal{A}$ over $\mathcal{Y} \rtimes \mathbb{Z}^n$ that recognizes $\varphi(\overline{S})H$. It is then decidable by Theorem 3.8 whether $\varphi(\overline{S})H$ is a group. □

4. Rational subsemigroups of metabelian groups

In this section we prove Theorem 3.8. Our proof extends a number of ideas from [14]. We present here a self-contained proof of Theorem 3.8, but whenever a definition or theorem comes from generalizing [14], we will give a comparison to the original work and include a reference, often as footnote.

Suppose the automaton $\mathcal{A}$ over $\mathcal{Y} \rtimes \mathbb{Z}^n$ has states $q_1, \dots, q_s$ and transitions $\delta_1, \dots, \delta_t$. Without loss of generality we can suppose $\mathcal{A}$ to be trim. For each transition $\delta_\ell, \ell = 1, \dots, t$, denote its evaluation by $(y_\ell, a_\ell) \in \mathcal{Y} \rtimes \mathbb{Z}^n$. Our first step of deciding whether $\mathrm{ev}(\mathcal{A})$ is a group is to reduce it to finding an *Identity Traversal* of a *primitive automaton*.

Given an automaton $\mathcal{A}$ over $\mathcal{Y} \rtimes \mathbb{Z}^n$, we define a new automaton $\mathcal{A}^{\pm}$ as follows: the states of $\mathcal{A}^{\pm}$ are the same as $\mathcal{A}$, and the transitions of $\mathcal{A}^{\pm}$ are $\delta_1, \dots, \delta_t, \delta_1^-, \dots, \delta_t^-$. Here, δ_ℓ^- is a transition from the destination of δ_ℓ to the origin of δ_ℓ, with evaluation $\mathrm{ev}(\delta_\ell^-) := (y_\ell, a_\ell)^{-1}$. We say that $\mathcal{A}$ is *primitive*, if the image of $\mathrm{ev}(\mathcal{A}^{\pm})$ under the projection $\mathcal{Y} \rtimes \mathbb{Z}^n \to \mathbb{Z}^n$ is $\mathbb{Z}^n$.

Lemma 4.1. *Suppose we are given a trim automaton $\mathcal{A}$ over $\mathcal{Y} \rtimes \mathbb{Z}^n$. One can compute $\widetilde{n} \in \mathbb{N}$, a finitely presented $\mathbb{Z}[\widetilde{X_1}^{\pm}, \dots, \widetilde{X_{\widetilde{n}}}^{\pm}]$-module $\widetilde{\mathcal{Y}}$, and a primitive trim automaton $\widetilde{\mathcal{A}}$ over $\widetilde{\mathcal{Y}} \rtimes \mathbb{Z}^{\widetilde{n}}$, such that $\mathrm{ev}(\mathcal{A})$ is a group if and only if $\mathrm{ev}(\widetilde{\mathcal{A}})$ is a group.*

By Lemma 4.1, throughout this section we can without loss of generality suppose $\mathcal{A}$ to be trim and primitive by replacing it with $\widetilde{\mathcal{A}}$. We define an *accepting traversal* of $\mathcal{A}$ to be an accepting run that uses every transition at least once. We define an *Identity Traversal* of $\mathcal{A}$ to be an accepting traversal whose evaluation is the neutral element $(0, 0^n) \in \mathcal{Y} \rtimes \mathbb{Z}^n$.

Proposition 4.2. *The semigroup $\mathrm{ev}(\mathcal{A})$ is a group if and only if $\mathcal{A}$ admits an Identity Traversal.*

A. From Identity Traversals to $\mathcal{A}$-graphs

We define the notion of an *$\mathcal{A}$-graph*[4]. For each state q_i of $\mathcal{A}$, we assign to it a lattice $\Lambda_i \cong \mathbb{Z}^n$. We consider the disjoint union $\Lambda := \Lambda_1 \sqcup \cdots \sqcup \Lambda_s$ as a subset of a larger lattice $\mathbb{Z}^{s+n}$ in the following way. Let $(b_1, 0^n), \dots, (b_s, 0^n), (0^s, d_1), \dots, (0^s, d_n)$ be the natural basis of $\mathbb{Z}^{s+n}$. Here, $b_i \in \mathbb{Z}^s$ is the vector with 1 on the i-th coordinate and 0 elsewhere, and $d_j \in \mathbb{Z}^n$ is the vector with 1 on the j-th coordinate and 0 elsewhere. For $i = 1, \dots, s$, we identify Λ_i with $\{b_i\} \times \mathbb{Z}^n$ by the map $z \mapsto (b_i, z)$. See Figure 2 for an illustration. Thus, a vertex v in $\Lambda \subset \mathbb{Z}^{s+n}$ is always denoted by a pair $(b_i, z) \in \{b_1, \dots, b_s\} \times \mathbb{Z}^n$, where the index i signifies that v is in the lattice Λ_i, and z is the coordinate of v within $\Lambda_i \cong \mathbb{Z}^n$.

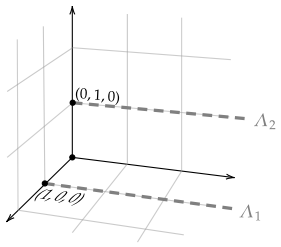

Fig. 2. The disjoint union $\Lambda = \Lambda_1 \sqcup \Lambda_2$ as a subset of $\mathbb{Z}^{s+n}$, where $s = 2, n = 1$.

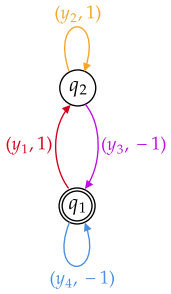

Fig. 3. An automaton $\mathcal{A}$, where $a_1 = 1, a_2 = 1, a_3 = -1, a_4 = -1$.

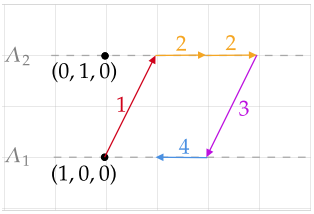

Fig. 4. The $\mathcal{A}$-graph $\Gamma(w)$ associated to the accepting run $w = \delta_1\delta_2\delta_2\delta_3\delta_4$.

Definition 4.3 ($\mathcal{A}$-graphs)**.** An *$\mathcal{A}$-graph* is a directed multigraph Γ, whose set of vertices is a finite subset of Λ. The

[4] $\mathcal{A}$-graphs are a generalization of the *$\mathcal{G}$-graphs* defined in [14], which are exactly $\mathcal{A}$-graphs with $s = 1$. In other words, $\mathcal{A}$-graphs can be considered as a collection of $\mathcal{G}$-graphs with edges between them.

edges of Γ are each labeled with an index in $\{1, \dots, t\}$. Furthermore, each edge with label ℓ connects from some vertex $(b_{\Omega(\ell)}, z), z \in \mathbb{Z}^n$ to the vertex $(b_{\Delta(\ell)}, z+a_\ell)$. Recall that $\Omega(\ell)$ and $\Delta(\ell)$ are the indices of the origin and destination states of the transition δ_ℓ, and $a_\ell \in \mathbb{Z}^n$ is such that $\mathrm{ev}(\delta_\ell) = (y_\ell, a_\ell)$. In other words, an edge with label ℓ connects from $\Lambda_{\Omega(\ell)}$ to $\Lambda_{\Delta(\ell)}$, the $\mathbb{Z}^n$-coordinates of the target and source of the edge differ by a_ℓ.

For an $\mathcal{A}$-graph Γ, denote by $V(\Gamma)$ its set of vertices, and by $E(\Gamma)$ its set of edges. For an edge $e \in E(\Gamma)$, we denote its source vertex by $\sigma(e)$ and its target vertex by $\tau(e)$.

For an accepting run w of $\mathcal{A}$, we associate to it a unique $\mathcal{A}$-graph $\Gamma(w)$, defined as follows. Write $w = \delta_{\ell_1} \cdots \delta_{\ell_m}$. For each $j = 1, \dots, m$, we add an edge starting at the vertex $(b_{\Omega(\ell_j)}, a_{\ell_1} + \cdots + a_{\ell_{j-1}})$, ending at the vertex $(b_{\Delta(\ell_j)}, a_{\ell_1} + \cdots + a_{\ell_j})$, with the label ℓ_j. For $j = 1$, the edge starts at $(b_1, 0^n)$. See Figure 3 and 4 for an illustration.

Definition 4.4 (Element represented by an $\mathcal{A}$-graph)**.** For an edge e in an $\mathcal{A}$-graph Γ, denote by $\lambda(e)$ its label. Let $\pi_{\mathbb{Z}^n} \colon \mathbb{Z}^{s+n} \to \mathbb{Z}^n$ denote the projection $(b, z) \mapsto z$. The element in $\mathcal{Y}$ *represented* by an edge e is defined as $\overline{X}^{\pi_{\mathbb{Z}^n}(\sigma(e))} \cdot y_{\lambda(e)}$. (For example in Figure 4, the edge with label 4 represents the element $X_1^2 \cdot y_4 \in \mathcal{Y}$.) The element *represented* by an $\mathcal{A}$-graph is defined as $\sum_{e \in E(\Gamma)} \overline{X}^{\pi_{\mathbb{Z}^n}(\sigma(e))} y_{\lambda(e)}$, the sum of all the elements represented by its edges. By direct computation, if w is an accepting run of $\mathcal{A}$ with evaluation $(y, z) \in \mathcal{Y} \rtimes \mathbb{Z}^n$, then y is the element represented by the associated graph $\Gamma(w)$, and z is the sum $\sum_{e \in E(\Gamma)} a_{\lambda(e)}$.

Given an $\mathcal{A}$-graph Γ and a vector $z \in \mathbb{Z}^n$, we define the translation $\Gamma + (0^s, z)$ to be a copy of Γ where each vertex and edge is moved by the vector $(0^s, z)$. Note that if Γ represents $y \in \mathcal{Y}$, then $\Gamma + (0^s, z)$ represents $\overline{X}^z \cdot y$. We call an $\mathcal{A}$-graph *full-image* if it contains at least one edge of label ℓ for each $\ell \in \{1, \dots, t\}$. Let Γ be a full-image Eulerian $\mathcal{A}$-graph, then it has a translation $\Gamma + (0^s, z)$ that contains the vertex $(b_1, 0^n)$. By reading the labels on its Eulerian circuit starting from $(b_1, 0^n)$, we obtain an accepting run w of $\mathcal{A}$ such that $\Gamma(w) = \Gamma + (0^s, z)$. We can then show:

Lemma 4.5. *There exists an Identity Traversal of $\mathcal{A}$ if and only if there exists a full-image Eulerian $\mathcal{A}$-graph that represents* 0.

Our next step is to replace the Eulerian property in Lemma 4.5 by a more "local" property. For this, we need the notion of *face-accessibility*[5]. Let C be a (closed) convex polytope. A *face* F of C is the intersection of C with any closed halfspace whose boundary is disjoint from the interior of C. A *strict face* is a face of C that is not the empty set or C itself. For example, if C is of dimension two, then the strict faces of C are its edges and its vertices.

[5]When $s = 1$, face-accessibility of an $\mathcal{A}$-graph is equivalent to face-accessibility of a $\mathcal{G}$-graph defined in [14].

Definition 4.6 (face-accessibility of an $\mathcal{A}$-graph)**.** Let Γ be an $\mathcal{A}$-graph. Denote by $C \subsetneq \mathbb{R}^{s+n}$ the convex hull of $V(\Gamma)$. A strict face F of C is called *accessible* if there is an edge $e \in E(\Gamma)$ such that $\sigma(e) \in F$ and $\tau(e) \in C \setminus F$. The $\mathcal{A}$-graph Γ is called *face-accessible* if every strict face of C is accessible. See Figures 5, 6 and 7 for examples.

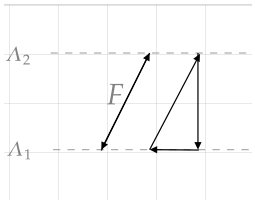

Fig. 5. Example of a non face-accessible graph: the strict face F not accessible.

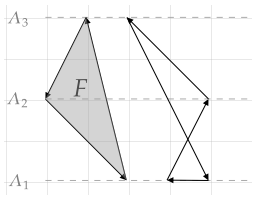

Fig. 6. A non face-accessible graph: F is not accessible. Note that $\Lambda_1, \Lambda_2, \Lambda_3$ are not in the same plane, despite appearing so in the figure.

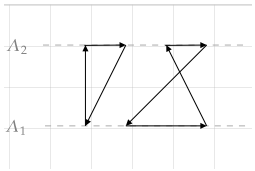

Fig. 7. A face-accessible graph Γ that is not Eulerian due to disconnectivity.

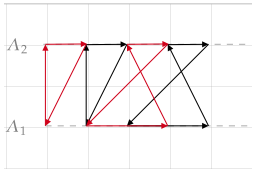

Fig. 8. The union $\widehat{\Gamma}$ of two translations of Γ drawn respectively in black and red.

Recall that a directed graph Γ is called *symmetric* if the in-degree is equal to the out-degree at every vertex. An Eulerian graph is symmetric and face-accessible. While symmetric face-accessible graphs are not necessarily Eulerian, we show that they can be used to construct Eulerian graphs:

Theorem 4.7. *Suppose $\mathcal{A}$ is trim and primitive. Let Γ be a full-image, symmetric and face-accessible $\mathcal{A}$-graph. Then there exist $z_1, \dots, z_m \in \mathbb{Z}^n$, such that the union of translations $\widehat{\Gamma} := \bigcup_{i=1}^m \Gamma + (0^s, z_i)$ is an Eulerian graph.*[6]

See Figure 8 for an illustration of Theorem 4.7. The proof is given in Appendix B. Note that the face-accessibility condition

[6]Theorem 4.7 is a generalization of [14, Theorem 3.3], which covers the case of $s = 1$. Proving the general statement with $s \geq 2$ is highly non-trivial. It is crucial that Γ is an $\mathcal{A}$-graph (with vertices in Λ) instead of an arbitrary graph over $\mathbb{Z}^{s+n}$: the theorem is false for arbitrary graphs over $\mathbb{Z}^{s+n}$.

is necessary: one can verify that taking a union of horizontal translations of the graphs in Figure 5 or 6 cannot produce a connected graph. Lemma 4.5 and Theorem 4.7 lead to:

Proposition 4.8. *A trim primitive automaton $\mathcal{A}$ admits an Identity Traversal if and only if there exists a full-image symmetric face-accessible $\mathcal{A}$-graph that represents 0.*

B. From $\mathcal{A}$-graphs to position polynomials

We now describe $\mathcal{A}$-graphs using their *position polynomials*. The difficulty here is the characterization of face-accessibility when $s \geq 2$. We overcome this by introducing the notion of *partial contractions*. This can be intuitively understood as "contracting" the collection of lattices $\Lambda_1, \ldots, \Lambda_s$ into a single lattice, and reducing to the case $s = 1$, which has been completely understood in [14].

The *position polynomials* of an $\mathcal{A}$-graph is a tuple $\boldsymbol{f} = (f_1, \ldots, f_t) \in \mathbb{N}[\overline{X}^{\pm}]^t$, where

$$f_\ell := \sum_{e \in E(\Gamma), \lambda(e) = \ell} \overline{X}^{\pi_{\mathbb{Z}^n}(\sigma(e))}, \quad \ell = 1, \ldots, t.$$

That is, f_ℓ is the sum of monomials $\overline{X}^z$, where z ranges over the $\mathbb{Z}^n$-coordinate of the source vertex of all edges of label ℓ. These polynomials have only non-negative coefficients, hence are in $\mathbb{N}[\overline{X}^{\pm}]$. For example, for the $\mathcal{A}$-graph Γ drawn in Figure 4, the position polynomials will be the four-tuple (f_1, f_2, f_3, f_4), where $f_1 = 1, f_2 = X_1 + X_1^2, f_3 = X_1^3, f_4 = X_1^2$.

Conversely, given any tuple of polynomials $\boldsymbol{f} = (f_1, \ldots, f_t) \in \mathbb{N}[\overline{X}^{\pm}]^t$, one can construct a $\mathcal{G}$-graph Γ such that $\boldsymbol{f}$ is exactly its tuple of position polynomials. Indeed, for each monomial $c\overline{X}^z$ appearing in f_ℓ, we can draw $c \geq 1$ edges of label ℓ starting at vertex $(b_{\Omega(\ell)}, z)$.

In the wake of Proposition 4.8, we will characterize the following four properties of an $\mathcal{A}$-graph Γ using its position polynomials: (i) whether Γ is full-image, (ii) whether Γ is symmetric, (iii) whether Γ represents $0 \in \mathcal{Y}$, (iv) whether Γ is face-accessible. Properties (i)-(iii) are easy to characterize:

Lemma 4.9. *Let Γ be an $\mathcal{A}$-graph with position polynomials $\boldsymbol{f} = (f_1, \ldots, f_t) \in \mathbb{N}[\overline{X}^{\pm}]^t$.*

(i) *Γ is full-image if and only if $f_\ell \in \mathbb{N}[\overline{X}^{\pm}]^* := \mathbb{N}[\overline{X}^{\pm}] \setminus \{0\}$, for $\ell = 1, \ldots, t$.*

(ii) *Γ is symmetric if and only if for each $i = 1, \ldots, s$, we have $\sum_{\ell:\, \Omega(\ell) = i} f_\ell = \sum_{\ell:\, \Delta(\ell) = i} f_\ell \cdot \overline{X}^{a_\ell}$.*

(iii) *Γ represents 0 if and only if $\sum_{\ell=1}^{t} f_\ell \cdot y_\ell = 0$.*

To characterize the face-accessibility of Γ, we will use the *weighted degree* of a "contracted" version of position polynomials. Let $\cdot$ denote the dot product in $\mathbb{R}^n$. Given a polynomial $f = \sum_{a \in \mathbb{Z}^n} c_a \overline{X}^a \in \mathbb{R}[\overline{X}^{\pm}]^*$ and a vector $v \in (\mathbb{R}^n)^* := \mathbb{R}^n \setminus \{0\}$, the *weighted degree* of f at direction v is defined as $\deg_v(f) := \max\{v \cdot a \mid a \in \mathbb{Z}^n, c_a \neq 0\}$. Define additionally $\deg_v(0) = -\infty$. We now introduce the notion of *partial contractions* of an automaton $\mathcal{A}$:

Definition 4.10 (Partial contraction)**.** A *partial contraction* of $\mathcal{A}$ is a tuple $(S, \mathcal{T}, \rho)$, where

(i) S is a non-empty subset of $\{1, \ldots, s\}$.

(ii) $\mathcal{T}$ is a subset of $\{1, \ldots, t\}$, such that the transitions $\{\delta_\ell \mid \ell \in \mathcal{T}\}$ form a spanning tree of the state set $\{q_i \mid i \in S\}$ in the underlying *undirected* graph. In particular, $|\mathcal{T}| = |S| - 1$.

(iii) ρ is an element of S; the state q_ρ will be seen as the "root" of the undirected spanning tree.

Then in the automaton $\mathcal{A}^{\pm}$ (recall its definition before Lemma 4.1), for every index $i \in S$, there exists a unique path consisting of transitions in $\{\delta_\ell \mid \ell \in \mathcal{T}\} \cup \{\delta_\ell^- \mid \ell \in \mathcal{T}\}$, that connects from q_i to q_ρ. See the automaton in Figure 9 for an illustration.

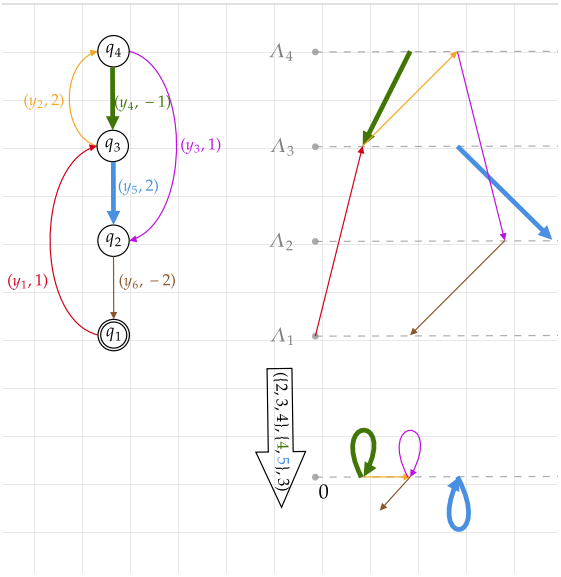

Fig. 9. Partial contraction with $S = \{2, 3, 4\}$, $\mathcal{T} = \{4, 5\}$, $\rho = 3$. The contracted transitions (δ_4 and δ_5) are marked with thick arrows, and $\Omega^{-1}(S) = \{2, 3, 4, 5, 6\}$.

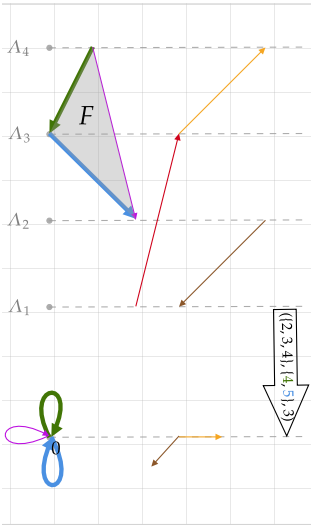

Fig. 10. Non-accessible face F becomes three petals after contraction.

Let $\boldsymbol{f} = (f_1, \ldots, f_t) \in \mathbb{N}[\overline{X}^{\pm}]^t$ be the position polynomials of Γ. For a set $S \subseteq \{1, \ldots, s\}$, denote $\Omega^{-1}(S) := \{\ell \mid \Omega(\ell) \in$

$S\}$. Given a partial contraction $(S, \mathcal{T}, \rho)$ and a tuple of position polynomials $\boldsymbol{f} = (f_1, \ldots, f_t) \in \mathbb{N}[\overline{X}^{\pm}]^t$, define the tuple of *contracted position polynomials*

$$\boldsymbol{f}^{(S,\mathcal{T},\rho)} \coloneqq \left(f_\ell^{(S,\mathcal{T},\rho)}\right)_{\ell\in\Omega^{-1}(S)} \in \mathbb{N}[\overline{X}^{\pm}]^{|\Omega^{-1}(S)|},$$

where the polynomial $f_\ell^{(S,\mathcal{T},\rho)} \in \mathbb{N}[\overline{X}^{\pm}], \ell \in \Omega^{-1}(S)$, is defined as follows: there is a unique path $P_{\Omega(\ell)}$ in $\mathcal{A}^{\pm}$, consisting of transitions in $\{\delta_\ell \mid \ell \in \mathcal{T}\} \cup \{\delta_\ell^- \mid \ell \in \mathcal{T}\}$, that connects from $q_{\Omega(\ell)}$ to q_ρ. Write its evaluation $\mathrm{ev}(P_{\Omega(\ell)})$ as $(y_{P_{\Omega(\ell)}}, z_{P_{\Omega(\ell)}})$. We define $f_\ell^{(S,\mathcal{T},\rho)} \coloneqq f_\ell \cdot \overline{X}^{z_{P_{\Omega(\ell)}}}$.

Similarly, if $\Delta(\ell) \in S$, we denote by $P_{\Delta(\ell)}$ the path in $\mathcal{A}^{\pm}$ from $q_{\Delta(\ell)}$ to q_ρ, consisting of transitions in $\{\delta_\ell \mid \ell \in \mathcal{T}\} \cup \{\delta_\ell^- \mid \ell \in \mathcal{T}\}$. The path $P_{\Delta(\ell)}$ evaluates to an element $(y_{P_{\Delta(\ell)}}, z_{P_{\Delta(\ell)}})$ for some $z_{P_{\Delta(\ell)}} \in \mathbb{Z}^n$. Define the *contracted edge vectors* in $\mathbb{Z}^n$:

$$a_\ell^{(S,\mathcal{T},\rho)} \coloneqq \begin{cases} a_\ell + z_{P_{\Delta(\ell)}} - z_{P_{\Omega(\ell)}}, & \ell \in \Omega^{-1}(S) \cap \Delta^{-1}(S), \\ 0^n & \ell \in \Omega^{-1}(S) \setminus \Delta^{-1}(S). \end{cases}$$

Example 4.11. Let us compute the contracted position polynomials for the example in Figure 9. As shown in the figure, let $f_1 = 1$, $f_2 = X_1$, $f_3 = X_1^3$, $f_4 = X_1^2$, $f_5 = X_1^3$ and $f_6 = X_1^4$. The partial contraction we use is $S = \{2, 3, 4\}$, $\mathcal{T} = \{4, 5\}$, $\rho = 3$, so $\Omega^{-1}(S) = \{2, 3, 4, 5, 6\}$. The path P_4 from q_4 to q_3 evaluates to $(y_4, -1)$, so $z_{P_4} = -1$. We have $\Omega(2) = \Omega(3) = 4$, therefore $f_3^{(S,\mathcal{T},\rho)} = f_3 \cdot X_1^{-1} = X_1^2$ and $f_4^{(S,\mathcal{T},\rho)} = f_4 \cdot X_1^{-1} = X_1$. Similarly, the path P_2 from q_2 to q_3 evaluates to $(y_5, 2)^{-1} = (-X_1^{-2} y_5, -2)$, so $z_{P_2} = -2$. We have $\Omega(6) = 2$, therefore $f_6^{(S,\mathcal{T},\rho)} = f_6 \cdot X_1^{-2} = X_1^2$. Finally, we have $\Omega(2) = \Omega(5) = 3$, therefore $f_2^{(S,\mathcal{T},\rho)} = f_2 = X_1$ and $f_5^{(S,\mathcal{T},\rho)} = f_5 = X_1^3$. The contracted position polynomials are therefore $(f_2^{(S,\mathcal{T},\rho)}, f_3^{(S,\mathcal{T},\rho)}, f_4^{(S,\mathcal{T},\rho)}, f_5^{(S,\mathcal{T},\rho)}, f_6^{(S,\mathcal{T},\rho)}) = (X_1, X_1^2, X_1, X_1^3, X_1^2)$. The contracted edge vectors are $(a_2^{(S,\mathcal{T},\rho)}, a_3^{(S,\mathcal{T},\rho)}, a_4^{(S,\mathcal{T},\rho)}, a_5^{(S,\mathcal{T},\rho)}, a_6^{(S,\mathcal{T},\rho)}) = (1, 0, 0, 0, 0)$. □

The contracted position polynomials can be seen as "position polynomials" of a graph $\Gamma^{(S,\mathcal{T},\rho)}$ over $\mathbb{Z}^n$, which is obtained from Γ by contracting the lattices $\Lambda_i, i \in S$ into a single lattice $\mathbb{Z}^n$, and discarding the other lattices $\Lambda_i, i \notin S$. See Figure 9 for an illustration. During the contraction, each lattice $\Lambda_i = \{b_i\} \times \mathbb{Z}^n, i \in S$, is translated by the vector $(-b_i, z_{P_i})$, where z_{P_i} is the sum of the $\mathbb{Z}^n$-coordinates along the unique path (in the subgraph of $\mathcal{A}^{\pm}$ defined by $\mathcal{T}$) from q_i to q_ρ. In particular, if two lattices $\Lambda_i, \Lambda_j, i, j \in S$, are connected by some edge e with label $\ell \in \mathcal{T}$, then the edge e will become a loop after the contraction (e.g. the green and blue edges in Figure 9). Similarly, the contracted edge vector $a_\ell^{(S,\mathcal{T},\rho)}$ corresponds to the edge vector of label ℓ after the contraction. The edges in the contracted graph $\Gamma^{(S,\mathcal{T},\rho)}$ have labels in $\Omega^{-1}(S)$. Edges going to a discarded lattice $\Lambda_i, i \notin S$ (e.g. the brown edge) can be seen as "dangling": these are edges with labels in $\Omega^{-1}(S) \cap \Delta^{-1}(S)^{\complement}$, where $\Delta^{-1}(S)^{\complement} \coloneqq \{1, \ldots, t\} \setminus \Delta^{-1}(S)$. Note that when S is a singleton $\{\rho\}$, the set $\mathcal{T}$ is empty, and the tuple $\boldsymbol{f}^{(\{\rho\},\emptyset,\rho)}$ is simply $(f_\ell)_{\ell\in\Omega^{-1}(\rho)}$.

Given a partial contraction $(S, \mathcal{T}, \rho)$ and a vector $v \in (\mathbb{R}^n)^*$, define

$$M_v((S,\mathcal{T},\rho), \boldsymbol{f}) \coloneqq \left\{ \ell \in \Omega^{-1}(S) \;\middle|\; \deg_v\left(f_\ell^{(S,\mathcal{T},\rho)}\right) = \max_{\ell'\in\Omega^{-1}(S)} \left\{\deg_v\left(f_{\ell'}^{(S,\mathcal{T},\rho)}\right)\right\} \right\}.$$

This is the set of labels $\ell \in \Omega^{-1}(S)$ such that $\deg_v\left(f_\ell^{(S,\mathcal{T},\rho)}\right)$ is maximal. In the contracted graph $\Gamma^{(S,\mathcal{T},\rho)}$, the source coordinate of edges with labels in $M_v((S, \mathcal{T}, \rho), \boldsymbol{f})$ have the largest inner product with v. Define additionally

$$O_v(S, \mathcal{T}, \rho) \coloneqq \left\{ \ell \in \Omega^{-1}(S) \;\middle|\; a_\ell^{(S,\mathcal{T},\rho)} \not\perp v \right\}.$$

This is the set of labels whose contracted edge vectors $a_\ell^{(S,\mathcal{T},\rho)}$ are not orthogonal to v.

Example 4.11 (continued)**.** We now compute the sets $M_v((S, \mathcal{T}, \rho), \boldsymbol{f})$ and $O_v(S, \mathcal{T}, \rho)$ for Example 4.11. Since we are working in dimension $n = 1$, the vector v is a real number in $\mathbb{R}^*$. If $v < 0$, then $M_v((S, \mathcal{T}, \rho), \boldsymbol{f}) = \{2, 4\}$, because $f_2^{(S,\mathcal{T},\rho)}$ and $f_4^{(S,\mathcal{T},\rho)}$ have the lowest degree (that is, *highest* degree at direction $v = -1$) in the tuple $\boldsymbol{f}^{(S,\mathcal{T},\rho)}$. If $v > 0$, then $M_v((S, \mathcal{T}, \rho), \boldsymbol{f}) = \{5\}$, because $f_5^{(S,\mathcal{T},\rho)}$ has the highest degree in the tuple $\boldsymbol{f}^{(S,\mathcal{T},\rho)}$. Correspondingly in the contracted graph $\Gamma^{(S,\mathcal{T},\rho)}$, at the left extremity we have the sources of edges with label in $\{2, 4\}$; and at the right extremity we have the sources of edges with label in $\{5\}$. See Figure 9.

As for the set $O_v(S, \mathcal{T}, \rho)$, for all $v \in \mathbb{R}^*$ we have $O_v((S, \mathcal{T}, \rho), \boldsymbol{f}) = \{2\}$, because $a_2^{(S,\mathcal{T},\rho)}$ is the only non-zero vector among $a_\ell^{(S,\mathcal{T},\rho)}, \ell \in \Omega^{-1}(S)$. Correspondingly in the contracted graph $\Gamma^{(S,\mathcal{T},\rho)}$, only the edge with label 2 is not a loop or a dangling edge. □

Using the contracted position polynomials and the contracted edge vectors, we can characterize face-accessibility of Γ. The following lemma is a formal way of expressing "Γ is face-accessible if and only if all its partial contractions $\Gamma^{(S,\mathcal{T},\rho)}$ are face-accessible" (in particular, faces containing sources of "dangling" edges are considered accessible).

Lemma 4.12. *Let Γ be a symmetric $\mathcal{A}$-graph with position polynomials $\boldsymbol{f} = (f_1, \ldots, f_t) \in \mathbb{N}[\overline{X}^{\pm}]^t$. Then Γ is face-accessible if and only if for every partial contraction $(S, \mathcal{T}, \rho)$, we have*

$$\left(O_v(S, \mathcal{T}, \rho) \cup \Delta^{-1}(S)^{\complement}\right) \cap M_v((S, \mathcal{T}, \rho), \boldsymbol{f}) \neq \emptyset \qquad (4)$$

for every $v \in (\mathbb{R}^n)^*$.

Sketch of proof. See Appendix A for a full proof. We show the contrapositive: the convex hull C of $V(\Gamma)$ has a non-accessible face if and only if $\exists (S, \mathcal{T}, \rho), \exists v \in (\mathbb{R}^n)^*$, such that

$$\left(O_v(S, \mathcal{T}, \rho) \cup \Delta^{-1}(S)^{\complement}\right) \cap M_v((S, \mathcal{T}, \rho), \boldsymbol{f}) = \emptyset.$$

If F is a non-accessible face of C, then consider all the edges whose source is in F (their target will also be in F).

Let $\widetilde{\mathcal{T}}$ be the set of labels of these edges, and let $\widetilde{S}$ be the index set of origin and destination states of all transitions with label in $\widetilde{\mathcal{T}}$. Consider the subautomaton $\mathcal{A}'$ of $\mathcal{A}$ whose states are $q_i, i \in \widetilde{S}$, and whose transitions are $\delta_t, t \in \widetilde{\mathcal{T}}$ (we do not specify the initial or accepting state of $\mathcal{A}'$). Let $S \subseteq \widetilde{S}$ be such that $\{q_i \mid i \in S\}$ is a weakly connected component of $\mathcal{A}'$, let $\mathcal{T} \subseteq \widetilde{\mathcal{T}}$ be such that $\{\delta_t \mid t \in \mathcal{T}\}$ is an undirected spanning tree of this weakly connected component. Let ρ be any element of S. We contract Γ according to $(S, \mathcal{T}, \rho)$ (see Figure 10 for an illustration). Since F is non-accessible, it will still be non-accessible after the contraction. After contraction, F will be the extremal face at some direction $v \in (\mathbb{R}^n)^*$ (e.g. in Figure 10, v would be (-1), a vector pointing to the left). This means that among the position polynomials $f_\ell^{(S,\mathcal{T},\rho)}, \ell \in \Omega^{-1}(S)$, of $\Gamma^{(S,\mathcal{T},\rho)}$, the index of those with the highest $\deg_v(\cdot)$ correspond to the labels of contracted edges that are orthogonal to v (e.g. the three loops in the leftmost position in the contracted graph of Figure 10). This is because F is orthogonal to v after contraction. In terms of description by $\deg_v(\cdot)$, the indices of these polynomials are exactly $M_v((S, \mathcal{T}, \rho), \boldsymbol{f})$. Whereas the labels ℓ whose corresponding contracted edges that are *not* orthogonal to v are either in $O_v(S, \mathcal{T}, \rho)$ (if the contracted edge is not dangling), or in $\Delta^{-1}(S)^{\complement}$ (if the contracted edge is dangling). Therefore $\left(O_v(S, \mathcal{T}, \rho) \cup \Delta^{-1}(S)^{\complement}\right) \cap M_v((S, \mathcal{T}, \rho), \boldsymbol{f}) = \emptyset$.

The other implication direction can be proved similarly. □

The definition of $\boldsymbol{f}^{(S,\mathcal{T},\rho)}$ can be naturally extended to the case where $\boldsymbol{f} \in \mathbb{Z}[\overline{X}^{\pm}]^t$ instead of $\mathbb{N}[\overline{X}^{\pm}]^t$: write $\boldsymbol{f} = \boldsymbol{f}^+ - \boldsymbol{f}^-$ where $\boldsymbol{f}^+, \boldsymbol{f}^- \in \mathbb{N}[\overline{X}^{\pm}]^t$, and define $\boldsymbol{f}^{(S,\mathcal{T},\rho)} \coloneqq \left(\boldsymbol{f}^+\right)^{(S,\mathcal{T},\rho)} - \left(\boldsymbol{f}^-\right)^{(S,\mathcal{T},\rho)}$.

Define

$$\mathcal{M}_{\mathbb{Z}} \coloneqq \left\{ \boldsymbol{f} = (f_1, \dots, f_t) \in \mathbb{Z}[\overline{X}^{\pm}]^t \;\middle|\; \text{for } i = 1, \dots, s, \right.$$
$$\left. \sum_{\ell:\, \Omega(\ell)=i} f_\ell = \sum_{\ell:\, \Delta(\ell)=i} f_\ell \cdot \overline{X}^{a_\ell};\ \sum_{\ell=1}^{K} f_\ell \cdot y_\ell = 0 \right\}. \quad (5)$$

This is the $\mathbb{Z}[\overline{X}^{\pm}]$-module consisting of all $\boldsymbol{f} \in \mathbb{Z}[\overline{X}^{\pm}]^t$ satisfying the conditions in Lemma 4.9 (ii) and (iii). A finite set of generators for $\mathcal{M}_{\mathbb{Z}}$ can be effectively computed [30], for example using Gröbner basis [31].

We then want to include the condition in Lemma 4.12. For this, we will replace the information of $\boldsymbol{f}$ by all its contracted position polynomials. Denote by $\mathcal{PC}$ the set of all partial contractions of $\mathcal{A}$, denote $K \coloneqq \sum_{(S,\mathcal{T},\rho)\in\mathcal{PC}} |\Omega^{-1}(S)|$, and define the $\mathbb{Z}[\overline{X}^{\pm}]$-module

$$\widetilde{\mathcal{M}_{\mathbb{Z}}} \coloneqq \left\{ \widetilde{\boldsymbol{f}} \coloneqq \left(f_\ell^{(S,\mathcal{T},\rho)}\right)_{(S,\mathcal{T},\rho)\in\mathcal{PC}, \ell\in\Omega^{-1}(S)} \in \mathbb{Z}[\overline{X}^{\pm}]^K \right.$$
$$\left. \;\middle|\; \boldsymbol{f} \in \mathcal{M}_{\mathbb{Z}} \right\}. \quad (6)$$

Note that each entry $f_\ell^{(S,\mathcal{T},\rho)}$ in $\widetilde{\boldsymbol{f}}$ is obtained by multiplying f_ℓ by a fixed monomial, independant of $\boldsymbol{f}$. Therefore, if $\{\boldsymbol{f}_i \mid i \in I\}$ is a generating set of $\mathcal{M}_{\mathbb{Z}}$, then $\{\widetilde{\boldsymbol{f}}_i \mid i \in I\}$ is a generating set of $\widetilde{\mathcal{M}_{\mathbb{Z}}}$. Note that we can recover $\boldsymbol{f}$ as a sub-tuple of $\widetilde{\boldsymbol{f}}$: for $\rho \in \{1, \dots, s\}$, the sub-tuple $\boldsymbol{f}^{(\{\rho\},\emptyset,\rho)}$ of $\widetilde{\boldsymbol{f}}$ is simply $(f_\ell)_{\ell\in\Omega^{-1}(\rho)}$, and therefore $\widetilde{\boldsymbol{f}}$ contains as a sub-tuple $(f_\ell)_{\ell\in\bigcup_{\rho=1}^{s}\Omega^{-1}(\rho)} = (f_\ell)_{\ell\in\{1,\dots,t\}}$.

Using Lemma 4.12, we now characterize the face-accessibility of Γ by its contracted position polynomials $\widetilde{\boldsymbol{f}}$. For simplicity, rename the indices of $\widetilde{\boldsymbol{f}}$ by writing $\widetilde{\boldsymbol{f}} = (\widetilde{f}_1, \dots, \widetilde{f}_K)$, where $\widetilde{f}_i = f_{\ell_i}^{(S_i,\mathcal{T}_i,\rho_i)}, i = 1, \dots, K$. Similarly, define $\widetilde{a}_i = a_{\ell_i}^{(S_i,\mathcal{T}_i,\rho_i)}, i = 1, \dots, K$. For a partial contraction $(S, \mathcal{T}, \rho)$, define the sets

$$I_{(S,\mathcal{T},\rho)} \coloneqq \{i \in \{1, \dots, K\} \mid (S_i, \mathcal{T}_i, \rho_i) = (S, \mathcal{T}, \rho)\},$$
$$J_{(S,\mathcal{T},\rho)} \coloneqq \left\{ i \in I_{(S,\mathcal{T},\rho)} \;\middle|\; \ell_i \in \Delta^{-1}(S)^{\complement} \right\}.$$

For a set $I \subseteq \{1, \dots, K\}$, define

$$M_v\left(I, \widetilde{\boldsymbol{f}}\right) \coloneqq \left\{ i \in I \;\middle|\; \deg_v\left(\widetilde{f}_i\right) = \max_{i'\in I} \left\{ \deg_v\left(\widetilde{f}_{i'}\right) \right\} \right\},$$

and define

$$O_v \coloneqq \{i \in \{1, \dots, K\} \mid \widetilde{a}_i \not\perp v\}.$$

One can see that $\boldsymbol{f} \in \left(\mathbb{N}[\overline{X}^{\pm}]^*\right)^t$ if and only if $\widetilde{\boldsymbol{f}} \in \left(\mathbb{N}[\overline{X}^{\pm}]^*\right)^K$, because $\widetilde{\boldsymbol{f}}$ contains $\boldsymbol{f}$ as a sub-tuple. Summarizing the definition of $\widetilde{\mathcal{M}_{\mathbb{Z}}}$ as well as Lemma 4.9 and 4.12, we obtain:

Proposition 4.13. *There exists a full-image symmetric face-accessible $\mathcal{A}$-graph Γ, if and only if there exists $\widetilde{\boldsymbol{f}} \in \widetilde{\mathcal{M}_{\mathbb{Z}}} \cap \left(\mathbb{N}[\overline{X}^{\pm}]^*\right)^K$, satisfying*

$$\left(O_v \cup J_{(S,\mathcal{T},\rho)}\right) \cap M_v\left(I_{(S,\mathcal{T},\rho)}, \widetilde{\boldsymbol{f}}\right) \neq \emptyset, \quad (7)$$

for every $v \in (\mathbb{R}^n)^*$, $(S, \mathcal{T}, \rho) \in \mathcal{PC}$.

C. Decidability for position polynomials

Following Proposition 4.13, the last ingredient needed to finish this section is the following extension of [14, Theorem 3.9].

Theorem 4.14. *Denote $\mathbb{A} \coloneqq \mathbb{R}[\overline{X}^{\pm}], \mathbb{A}^+ \coloneqq \mathbb{R}_{\geq 0}[\overline{X}^{\pm}]^*$. Fix $n \in \mathbb{N}$ and let Ξ be a finite set of indices. Suppose we are given as input a set of generators $\boldsymbol{g}_1, \dots, \boldsymbol{g}_m \in \mathbb{A}^K$ with integer coefficients, the vectors $\widetilde{a}_1, \dots, \widetilde{a}_K \in \mathbb{Z}^n$, as well as subsets $I_\xi, J_\xi \subseteq \{1, \dots, K\}$ for each $\xi \in \Xi$. Denote by $\mathcal{M}$ be the $\mathbb{A}$-submodule of $\mathbb{A}^K$ generated by $\boldsymbol{g}_1, \dots, \boldsymbol{g}_m$. It is decidable whether there exists $\boldsymbol{f} \in \mathcal{M} \cap (\mathbb{A}^+)^K$ satisfying*

$$(O_v \cup J_\xi) \cap M_v(I_\xi, \boldsymbol{f}) \neq \emptyset, \quad \text{for every } v \in (\mathbb{R}^n)^*, \xi \in \Xi. \quad (8)$$

Here, if $n = 0$ then $\mathbb{A}$ is understood as $\mathbb{R}$, and Property (8) is considered trivially true.

When the index set Ξ has cardinality one, Theorem 4.14 is exactly [14, Theorem 3.9]. Our proof of Theorem 4.14 essentially involves adding the quantifier "for every $\xi \in \Xi$" in all appropriate places in the proof of [14, Theorem 3.9], and thus does not present new conceptual difficulties. The full

proof of Theorem 4.14 as well as a comparison with [14, Theorem 3.9] is provided in Appendix C.

We now finish the proof of Theorem 3.8. In the wake of Proposition 4.13, we need to decide whether there exists $\widetilde{\boldsymbol{f}} \in \widetilde{\mathcal{M}_{\mathbb{Z}}} \cap \left(\mathbb{N}[\overline{X}^{\pm}]^*\right)^K$ that satisfies condition (7). Our goal is to apply Theorem 4.14 with the index set $\Xi = \mathcal{PC}$. However, $\widetilde{\mathcal{M}_{\mathbb{Z}}}$ is a $\mathbb{Z}[\overline{X}^{\pm}]$-module, and in order to apply Theorem 4.14 we need an $\mathbb{R}[\overline{X}^{\pm}]$-module $\mathcal{M}$. Let $\boldsymbol{g}_1, \dots, \boldsymbol{g}_m$ be the generators of the $\mathbb{Z}[\overline{X}^{\pm}]$-module $\widetilde{\mathcal{M}_{\mathbb{Z}}}$, define

$$\mathcal{M} \coloneqq \left\{ h_1 \cdot \boldsymbol{g}_1 + \cdots + h_m \cdot \boldsymbol{g}_m \;\middle|\; h_1, \dots, h_m \in \mathbb{R}[\overline{X}^{\pm}] \right\}.$$

Lemma 4.15. *There exists an element $\widetilde{\boldsymbol{f}} \in \widetilde{\mathcal{M}_{\mathbb{Z}}} \cap \left(\mathbb{N}[\overline{X}^{\pm}]^*\right)^K$ satisfying Property (7), if and only if there exists $\boldsymbol{f} \in \mathcal{M} \cap \left(\mathbb{R}_{\geq 0}[\overline{X}^{\pm}]^*\right)^K$ satisfying Property (7).*

Therefore, by Lemma 4.15 we can apply Theorem 4.14 with $\Xi = \mathcal{PC}$ to the $\mathbb{R}[\overline{X}^{\pm}]$-module $\mathcal{M}$ instead of the $\mathbb{Z}[\overline{X}^{\pm}]$-module $\widetilde{\mathcal{M}_{\mathbb{Z}}}$. Summarizing Proposition 4.2, 4.8, 4.13, Lemma 4.15 and Theorem 4.14, we obtain a proof of Theorem 3.8, the main goal of this section:

Theorem 3.8. *Given as input a finitely presented $\mathbb{Z}[X_1^{\pm}, \dots, X_n^{\pm}]$-module $\mathcal{Y}$ and an automaton $\mathcal{A}$ over $\mathcal{Y} \rtimes \mathbb{Z}^n$, it is decidable whether $\mathrm{ev}(\mathcal{A})$ is a group.*

Proof. Without loss of generality suppose $\mathcal{A}$ is trim. By Lemma 4.1 we can suppose $\mathcal{A}$ to be primitive. By the series of reductions Proposition 4.2, 4.8 and 4.13, $\mathrm{ev}(\mathcal{A})$ is a group if and only if there exists $\widetilde{\boldsymbol{f}} \in \widetilde{\mathcal{M}_{\mathbb{Z}}} \cap \left(\mathbb{N}[\overline{X}^{\pm}]^*\right)^K$ that satisfies condition (7). By Lemma 4.15, this is equivalent to the existence of $\boldsymbol{f} \in \mathcal{M} \cap \left(\mathbb{R}_{\geq 0}[\overline{X}^{\pm}]^*\right)^K$ that satisfies condition (7). Note that $\mathcal{M}_{\mathbb{Z}}$ is defined as the solution set of a system of linear equations over $\mathbb{Z}[\overline{X}^{\pm}]$, therefore its generating set (and even Gröbner basis) can be effectively computed [30], [31]. We then extend the generating set of $\mathcal{M}_{\mathbb{Z}}$ to the generating set of $\widetilde{\mathcal{M}_{\mathbb{Z}}}$ and $\mathcal{M}$. Applying Theorem 4.14 with Ξ being the set of partial contractions $\mathcal{PC}$, we conclude that it is decidable whether there exists $\boldsymbol{f} \in \mathcal{M} \cap \left(\mathbb{R}_{\geq 0}[\overline{X}^{\pm}]^*\right)^K$ satisfying condition (7). □

It is worth noting that – similar to Lemma 2.1 – we can define a procedure that decides whether a rational semigroup $\mathrm{ev}(\mathcal{A})$ contains the neutral element from any algorithm deciding whether such semigroups are groups. This may be of independent interest:

Lemma 4.16. *Let G be a group and $\mathcal{A}$ a trim automaton over G (with q_1 as the only starting and accepting state). Then $\mathrm{ev}(\mathcal{A})$ contains the neutral element if and only if $\mathcal{A}$ admits a trim* sub-automaton *$\mathcal{A}'$, such that $\mathrm{ev}(\mathcal{A}')$ is a group. Here, a sub-automaton of $\mathcal{A}$ is defined as an automaton whose state set and transition set are subsets of the state set and transition set of $\mathcal{A}$.*

Proof. Let e denote the neutral element of G. If $e \in \mathrm{ev}(\mathcal{A})$, then $\mathcal{A}$ admits some accepting run w with $\mathrm{ev}(w) = e$. Let $\mathcal{A}'$ be the trim sub-automaton of $\mathcal{A}$ whose states and transitions are exactly those used in w. Then w is an Identity Traversal of $\mathcal{A}'$, so $\mathrm{ev}(\mathcal{A}')$ is a group by Proposition 4.2. If $\mathcal{A}$ admits a sub-automaton $\mathcal{A}'$ such that $\mathrm{ev}(\mathcal{A}')$ is a group, take any Identity Traversal w of $\mathcal{A}'$, then w is an accepting run of $\mathcal{A}$ with $\mathrm{ev}(w) = e$. So $\mathrm{ev}(\mathcal{A})$ contains the neutral element.

Therefore, to decide whether $\mathrm{ev}(\mathcal{A})$ contains the neutral element, it suffices to enumerate all trim sub-automata $\mathcal{A}'$ of $\mathcal{A}$, and decide whether any of them satisfies the condition "$\mathrm{ev}(\mathcal{A}')$ is a group". □

Therefore, Theorem 3.8 and Lemma 4.16 show that it is decidable whether a rational semigroup $\mathrm{ev}(\mathcal{A})$ of $\mathcal{Y} \rtimes \mathbb{Z}^n$ contains the neutral element, by enumerating all sub-automaton of the trim automaton $\mathcal{A}$. Furthermore, recall that Section 3 showed for a given automaton $\mathcal{A}$ over $\mathsf{T}(d, \mathbb{K})$, where $\mathbb{K}$ is an algebraic number field, it is decidable whether $\mathrm{ev}(\mathcal{A})$ is a group. Therefore, by Lemma 4.16, it is also decidable whether $\mathrm{ev}(\mathcal{A}) \subseteq \mathsf{T}(d, \mathbb{K})$ contains the neutral element.

5. Nilpotent groups of finite Prüfer rank

In this section we prove Theorem 3.4:

Theorem 3.4. *Let $\mathbb{K}$ be an algebraic number field and N be a subgroup of $\mathsf{UT}(d, \mathbb{K})$. Let M be a subsemigroup of N and denote by $\overline{M}$ its image under the quotient map $N \to N/[N,N]$. If $\overline{M} = N/[N,N]$ (equivalently, if $M[N,N] = N$), then $M = N$.*

The idea is to extend a weaker version of the theorem due to Shafrir, and independently, to Bodart, Ciobanu and Metcalfe:

Theorem 5.1 ([23, Corollary 1], see also [22, Proposition 19])**.** *Let N be a finitely generated nilpotent group and M be a subsemigroup of N. If $M[N,N] = N$, then $M = N$. More generally, if $M[N,N]$ is a finite-index subgroup of N, then M is a finite-index subgroup of N.*

This result should also be compared to the following:

Theorem 5.2 (Folklore, see [32, Theorem 2.2.3])**.** *Let G be a nilpotent group and H a subgroup. Suppose that $H[G,G] = G[G,G]$, then $H = G$.*

We will extend Theorem 5.1 from finitely generated nilpotent groups to infinitely generated subgroups of $\mathsf{UT}(d, \mathbb{K})$. It should be noted that Theorem 5.1 does not extend to general nilpotent groups contrary to Theorem 5.2. Recall the classic notions of *isolators* and *Prüfer rank*.

Definition 5.3. The *isolator* of a subset $X \subseteq G$ is the subset

$$I(X) \coloneqq \{g \in G \mid \exists m \in \mathbb{Z}_{>0},\ g^m \in X\}.$$

Lemma 5.4 ([32, Theorem 2.5.8])**.** *If G is nilpotent and H a subgroup, then $I(H)$ is a subgroup.*

Definition 5.5 (Prüfer rank)**.** The *Prüfer rank* of a group G, denoted $\mathrm{rk}(G)$, is the maximum number of generators needed to generate a finitely generated subgroup $H \leq G$.

For instance, every finitely generated subgroup of $(\mathbb{Q},+)$ is cyclic, therefore $\mathrm{rk}(\mathbb{Q})=1$.

Lemma 5.6 (Folklore, see [33, p.85, 3.]). *Let G be a group*
(i) *If $H \leq G$, then* $\mathrm{rk}(H) \leq \mathrm{rk}(G)$.
(ii) *If $N \trianglelefteq G$, then* $\mathrm{rk}(G) \leq \mathrm{rk}(N) + \mathrm{rk}(G/N)$.

Theorem 5.7 ([34, Theorem 2.5]). *If G is nilpotent and has finite Prüfer rank, then there exists a finite set $B \subset G$ such that $I(\langle B\rangle_{\mathrm{grp}}) = G$.*

We are ready to prove Theorem 3.4. Recall $[x,y]$ denotes the element $xyx^{-1}y^{-1}$, called the *commutator* of x and y.

Proof of Theorem 3.4. We prove the result under a slightly weaker condition: $[N,N]$ has finite Prüfer rank. First observe this condition is indeed satisfied if $N \leq \mathsf{UT}(d,\mathbb{K})$. Indeed,

$$\mathrm{rk}[N,N] \leq \mathrm{rk}(N) \leq \mathrm{rk}(\mathsf{UT}(d,\mathbb{K})) \leq \dim_{\mathbb{Q}}(\mathbb{K}) \cdot \binom{d}{2} < \infty$$

using Lemma 5.6 (i) twice, then part (ii) iteratively on the lower central series of $\mathsf{UT}(d,\mathbb{K})$.

From now on, we only suppose that $\mathrm{rk}[N,N] < \infty$. Using Theorem 5.7, there exists a finite set $B \subset [N,N]$ such that $I(\langle B\rangle_{\mathrm{grp}}) = [N,N]$. Each element of $[N,N]$ (hence each element of B) can be written as a product of commutators, so we can in turn find a finite set $A \subset N$ such that

$$I\big(\big\langle \{[a,a'] \mid a,a' \in A\}\big\rangle_{\mathrm{grp}}\big) \supseteq [N,N].$$

As $M[N,N]=N$, we find a finite set $X \subset M$ such that, for each $a \in A$ there exists $x,y \in X$ such that $x = a$ and $y = a^{-1} \pmod{[N,N]}$. Fix $g \in M$. We take $h \in M$ such that $h = g^{-1} \pmod{[N,N]}$. Let $\tilde{N} = \langle g,h,A,X\rangle_{\mathrm{grp}}$ and $\tilde{M} = M \cap \tilde{N}$. By construction, we have

$$\begin{aligned}\tilde{M} \cdot I([\tilde{N},\tilde{N}]) \supseteq \tilde{M} \cdot [N,N] \supseteq \langle g,h,X\rangle \cdot [N,N] \\ = \tilde{N} \cdot [N,N] \supseteq \tilde{N}\end{aligned}$$

hence $\tilde{M} \cdot I_{\tilde{N}}([\tilde{N},\tilde{N}]) = \tilde{N}$ (where $I_{\tilde{N}}(X) := \{g \in \tilde{N} : \exists m > 0,\ x^m \in X\} = I(X) \cap \tilde{N}$).

As $\tilde{N}$ is finitely generated, this implies that $\tilde{M}[\tilde{N},\tilde{N}]$ is a finite-index subgroup of $\tilde{N}$. Theorem 5.1 gives that $\tilde{M}$ is a subgroup of $\tilde{N}$. In particular g admits an inverse in $\tilde{M}$, hence in M. We conclude that M is a subgroup, hence $M = N$ using Theorem 5.2. □

Remark 5.8. Theorem 3.4 doesn't hold for more general nilpotent groups. For example, it does not hold when N is a subgroup of $\mathsf{UT}(3,\mathbb{Q}(X))$, where $\mathbb{Q}(X)$ denotes the field of rational functions over $\mathbb{Q}$. Indeed, let N be the group generated by the following elements:

$$A_i = \begin{pmatrix}1 & X^i & X^{2i+1}\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix},\ B_i = \begin{pmatrix}1 & -X^i & X^{2i+1}\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix},$$

$$C_i = \begin{pmatrix}1 & 0 & X^{2i+1}\\ 0 & 1 & X^i\\ 0 & 0 & 1\end{pmatrix},\ D_i = \begin{pmatrix}1 & 0 & X^{2i+1}\\ 0 & 1 & -X^i\\ 0 & 0 & 1\end{pmatrix},$$

for $i = 0,1,2,\ldots$, that is, $N = \langle \{A_i,B_i,C_i,D_i \mid i \in \mathbb{N}\}\rangle_{\mathrm{grp}}$. Then

$$N = \left\{ \begin{pmatrix}1 & g & f\\ 0 & 1 & h\\ 0 & 0 & 1\end{pmatrix} \;\middle|\; f,g,h \in \mathbb{Z}[X] \right\},$$

$$[N,N] = \left\{ \begin{pmatrix}1 & 0 & f\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix} \;\middle|\; f \in \mathbb{Z}[X] \right\}.$$

The latter equality is justified by the fact that $[N,N]$ contains the elements

$$A_iC_0A_i^{-1}C_0^{-1} = \begin{pmatrix}1 & 0 & X^i\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix},\ i = 0,1,2,\ldots.$$

Let M be the semigroup $\langle \{A_i,B_i,C_i,D_i \mid i \in \mathbb{N}\}\rangle$, then $M[N,N] = N$. However, we have $M \neq N$ because $I \notin M$. Indeed, let $P = \begin{pmatrix}1 & g & f\\ 0 & 1 & h\\ 0 & 0 & 1\end{pmatrix}$ any non-empty product of $A_i,B_i,C_i,D_i, i \in \mathbb{N}$, where $m \geq 0$ is the largest index used. Then $\deg(g) \leq m, \deg(h) \leq m$. Furthermore, $\deg(f) = 2m+1$, and the coefficient of the term X^{2m+1} in f is positive. So $f \neq 0$, and $P \neq I$.

6. Conclusion and Outlook

In this paper we proved decidability of the Identity Problem and the Group Problem in virtually solvable subgroups of $\mathsf{GL}(d,\overline{\mathbb{Q}})$. An immediate open question is whether our decidability result still holds when the field $\overline{\mathbb{Q}}$ is replaced by other effectively computable fields such as $\mathbb{Q}(X)$ or $\mathbb{F}_p(X)$ (where $\mathbb{F}_p$ denotes the finite field of cardinality p). A number of interesting solvable groups are not embeddable in $\mathsf{GL}(d,\overline{\mathbb{Q}})$, such as the *wreath product* $\mathbb{Z} \wr \mathbb{Z} := \mathbb{Z}[X^{\pm}] \rtimes \mathbb{Z}$ (which is embeddable in $\mathsf{GL}(2,\mathbb{Q}(X))$) and the lamplighter group $(\mathbb{Z}/2\mathbb{Z}) \wr \mathbb{Z} := \mathbb{F}_2[X^{\pm}] \rtimes \mathbb{Z}$ (which is embeddable in $\mathsf{GL}(2,\mathbb{F}_2(X))$). Many such groups still have decidable Identity Problem and Group Problem (direct consequence of Theorem 3.8, also [14]), and the lamplighter group $\mathbb{Z}_2 \wr \mathbb{Z}$ even has decidable Semigroup Membership [21]. Therefore, one might expect the Identity Problem and the Group Problem to be decidable for virtually solvable matrix groups over some well-behaved fields other than $\overline{\mathbb{Q}}$. On the other hand, a celebrated result of Kharlampovich [35] shows that general solvable groups are highly intractable: there exists a 3-step solvable group (a group G such that $G^{(3)}$ is trivial), where the *Word Problem* is undecidable. Moreover, there exists center-by-metabelian groups with decidable Word Problem and undecidable Torsion Problem (hence undecidable Identity Problem) [36, Proposition 3.2]. Therefore, one might expect the Identity Problem and the Group Problem to be undecidable for solvable matrix groups over more complicated fields.

As demonstrated in Remark 5.8, one of our key theorems (Theorem 3.4) no longer holds for the group $\mathsf{UT}(3,\mathbb{Q}(X))$. Therefore, our proof of decidability for the Group Problem does not apply to solvable subgroups of $\mathsf{GL}(3,\mathbb{Q}(X))$.

References

[1] A. Markov, "On certain insoluble problems concerning matrices," *Doklady Akad. Nauk SSSR*, vol. 57, no. 6, pp. 539–542, 1947.

[2] L. Babai, "Trading group theory for randomness," in *Proceedings of the seventeenth annual ACM symposium on Theory of computing*, 1985, pp. 421–429.

[3] R. Beals and L. Babai, "Las vegas algorithms for matrix groups," in *Proceedings of 1993 IEEE 34th Annual Foundations of Computer Science*. IEEE, 1993, pp. 427–436.

[4] V. D. Blondel, E. Jeandel, P. Koiran, and N. Portier, "Decidable and undecidable problems about quantum automata," *SIAM Journal on Computing*, vol. 34, no. 6, pp. 1464–1473, 2005.

[5] C. Choffrut and J. Karhumäki, "Some decision problems on integer matrices," *RAIRO-Theoretical Informatics and Applications-Informatique Théorique et Applications*, vol. 39, no. 1, pp. 125–131, 2005.

[6] E. Hrushovski, J. Ouaknine, A. Pouly, and J. Worrell, "Polynomial invariants for affine programs," in *Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science*, 2018, pp. 530–539.

[7] K. A. Mikhailova, "The occurrence problem for direct products of groups," *Doklady Akad. Nauk SSSR*, vol. 119, no. 6, p. 1103–1105, 1958.

[8] H. Cohen, *A course in computational algebraic number theory*. Springer Science & Business Media, 2013, vol. 138.

[9] P. C. Bell and I. Potapov, "On the undecidability of the identity correspondence problem and its applications for word and matrix semigroups," *International Journal of Foundations of Computer Science*, vol. 21, no. 06, pp. 963–978, 2010.

[10] P. C. Bell, M. Hirvensalo, and I. Potapov, "The Identity Problem for matrix semigroups in $SL_2(\mathbb{Z})$ is NP-complete," in *Proceedings of the Twenty-Eighth Annual ACM-SIAM Symposium on Discrete Algorithms*. SIAM, 2017, pp. 187–206.

[11] S. Ko, R. Niskanen, and I. Potapov, "On the identity problem for the special linear group and the Heisenberg group," in *45th International Colloquium on Automata, Languages, and Programming, ICALP 2018*, ser. LIPIcs, vol. 107, 2018, pp. 132:1–132:15.

[12] R. Dong, "Recent advances in algorithmic problems for semigroups," *ACM SIGLOG News*, vol. 10, no. 4, pp. 3–23, 2023.

[13] M. Lohrey, "Membership problems in infinite groups," in *Conference on Computability in Europe*. Springer, 2024, pp. 44–59.

[14] R. Dong, "Semigroup algorithmic problems in metabelian groups," in *Proceedings of the 56th Annual ACM Symposium on Theory of Computing*, 2024, pp. 884–891, full version: arxiv.org/abs/2304.12893.

[15] J. Tits, "Free subgroups in linear groups," *Journal of Algebra*, vol. 20, no. 2, pp. 250–270, 1972.

[16] V. M. Kopytov, "Solvability of the problem of occurrence in finitely generated soluble groups of matrices over the field of algebraic numbers," *Algebra i Logika*, vol. 7, no. 6, pp. 388–393, 1968.

[17] V. Roman'kov, "Undecidability of the submonoid membership problem for a sufficiently large finite direct power of the Heisenberg group," *arXiv preprint arXiv:2209.14786*, 2022.

[18] L. Babai, R. Beals, J.-y. Cai, G. Ivanyos, and E. M. Luks, "Multiplicative equations over commuting matrices," in *Proceedings of the Seventh Annual ACM-SIAM Symposium on Discrete Algorithms*, 1996, pp. 498–507.

[19] T. Colcombet, J. Ouaknine, P. Semukhin, and J. Worrell, "On reachability problems for low-dimensional matrix semigroups," in *46th International Colloquium on Automata, Languages, and Programming, ICALP 2019*, ser. LIPIcs, vol. 132, 2019, pp. 44:1–44:15.

[20] M. Cadilhac, D. Chistikov, and G. Zetzsche, "Rational subsets of Baumslag-Solitar groups," in *47th International Colloquium on Automata, Languages, and Programming, ICALP 2020*, ser. LIPIcs, vol. 168, 2020, pp. 116:1–116:16.

[21] M. Lohrey, B. Steinberg, and G. Zetzsche, "Rational subsets and submonoids of wreath products," *Information and Computation*, vol. 243, pp. 191–204, 2015.

[22] C. Bodart, L. Ciobanu, and G. Metcalfe, "Ordering groups and the identity problem," *arXiv preprint arXiv:2411.15639*, 2024.

[23] D. Shafrir, "A saturation theorem for submonoids of nilpotent groups and the Identity Problem," *arXiv preprint arXiv:2402.07337*, 2024.

[24] C. Druţu and M. Kapovich, *Geometric group theory*. American Mathematical Soc., 2018, vol. 63.

[25] R. Beals, "Algorithms for matrix groups and the Tits alternative," *Journal of computer and system sciences*, vol. 58, no. 2, pp. 260–279, 1999.

[26] M. Lohrey, "The rational subset membership problem for groups: a survey," in *Groups St Andrews*, vol. 422. Cambridge University Press, 2013, pp. 368–389.

[27] A. I. Mal'tsev, "On some classes of infinite soluble groups," *Matematicheskii Sbornik*, vol. 70, no. 3, pp. 567–588, 1951.

[28] G. Ostheimer, "Practical algorithms for polycyclic matrix groups," *Journal of Symbolic Computation*, vol. 28, no. 3, pp. 361–379, 1999.

[29] V. M. Kopytov, "Solvability of the occurrence problem in finitely generated solvable matrix groups over a numbered field," *Algebra i Logika*, vol. 10, no. 2, p. 169–182, 1971.

[30] F.-O. Schreyer, "Die Berechnung von Syzygien mit dem verallgemeinerten Weierstraßschen Divisionssatz," Master's thesis, Fakultät für Mathematik, Universität Hamburg, 1980.

[31] D. Eisenbud, *Commutative algebra: with a view toward algebraic geometry*. Springer Science & Business Media, 2013, vol. 150.

[32] E. I. Khukhro, *Nilpotent Groups and their Automorphisms*. Berlin, New York: De Gruyter, 1993.

[33] J. C. Lennox and D. J. Robinson, *The theory of infinite soluble groups*. Clarendon press, 2004.

[34] P. S. Kim and Y. Kim, "Note on groups with finite base," *Comm. Korean Math. Soc.*, vol. 11, no. 2, pp. 303–310, 1996.

[35] O. G. Kharlampovich, "A finitely presented solvable group with unsolvable word problem," *Izvestiya Rossiiskoi Akademii Nauk. Seriya Matematicheskaya*, vol. 45, no. 4, pp. 852–873, 1981.

[36] G. Arzhantseva, J.-F. Lafont, and A. Minasyan, "Isomorphism versus commensurability for a class of finitely presented groups," *Journal of Group Theory*, vol. 17, no. 2, pp. 361–378, 2014. [Online]. Available: https://doi.org/10.1515/jgt-2013-0050

[37] M. Kambites, P. V. Silva, and B. Steinberg, "On the rational subset problem for groups," *Journal of Algebra*, vol. 309, no. 2, pp. 622–639, 2007.

[38] R. H. Gilman, "Groups with a rational cross-section," in *Combinatorial group theory and topology*, vol. 111, 1987, pp. 175–183.

[39] G. Baumslag, F. B. Cannonito, and C. F. Miller III, "Computable algebra and group embeddings," *Journal of Algebra*, vol. 69, no. 1, pp. 186–212, 1981.

[40] A. Tarski, *A Decision Method for Elementary Algebra and Geometry*. second ed., rev., Univ. of California Press, Berkeley, 1951.

Appendix A
Omitted proofs

Lemma 3.1. *Let $T \leq \mathsf{T}(d, \mathbb{K})$ be a finite index normal subgroup of $G = \langle A_1, \ldots, A_m \rangle_{\mathrm{grp}}$, given by a finite set of generators. Then, $\langle A_1, \ldots, A_m \rangle$ is a group if and only if $S \coloneqq \langle A_1, \ldots, A_m \rangle \cap T$ is a group. Furthermore, S is a rational subsemigroup of T, whose automaton can be effectively computed from $A_1, \ldots, A_m$ and the generators of T.*

Proof. If $\langle A_1, \ldots, A_m \rangle$ is a group then obviously $\langle A_1, \ldots, A_m \rangle \cap T$ is a group. Suppose that $\langle A_1, \ldots, A_m \rangle \cap T$ is a group, we show that every element in $\langle A_1, \ldots, A_m \rangle$ is invertible. Take any $s \in \langle A_1, \ldots, A_m \rangle$, then since $|G/T| < \infty$, we have $s^{|G/T|} \in \langle A_1, \ldots, A_m \rangle \cap T$. Since $\langle A_1, \ldots, A_m \rangle \cap T$ is a group, we have $s^{-|G/T|} \in \langle A_1, \ldots, A_m \rangle \cap T$. Thus, $s^{-1} = \underbrace{ss \cdots s}_{|G/T|-1} \cdot s^{-|G/T|} \in \langle A_1, \ldots, A_m \rangle$. Therefore, $\langle A_1, \ldots, A_m \rangle$ is a group.

Let $B_1 \coloneqq I, B_2 \ldots, B_s \in G$ be the representatives of the left quotient $T \backslash G$. These can be effectively computed using the following saturation procedure. Start with the set $\mathcal{B} \coloneqq \{I, A_1, \ldots, A_m\}$. For $i = 1, \ldots, m$, we remove A_i

from $\mathcal{B}$ if there exists $j > i$ such that $A_i A_j^{-1} \in T$. Note that membership in T is decidable since T is solvable [16]. We then repeat the following process: check for all pairs of elements $B_i, B_j \in \mathcal{B}$, whether there exists some element $B_k \in \mathcal{B}$ such that $B_i B_j B_k^{-1} \in T$. If there exists a pair of element $B_i, B_j \in \mathcal{B}$, such that $B_i B_j B_k^{-1} \notin T$ for all $B_k \in S$, then we append the matrix $B_i B_j$ to the set $\mathcal{B}$. Otherwise we stop the process. Note that at each point of the process, the set $\mathcal{B}$ contains representatives for different equivalent classes in $T\backslash G$. By the finiteness of $T\backslash G$, the process must terminate, by which point $\mathcal{B}$ contains the complete set of representatives for $T\backslash G$.

We then construct an automaton $\mathcal{A}$ over T with states $q_1, \dots, q_s$ using the method from [37, Lemma 3.3]. For each $A_i, B_j, i \in \{1, \dots, m\}, j \in \{1, \dots, s\}$, there exists $\varphi(j,i) \in \{1, \dots, s\}$ such that $B_j A_i \in T B_{\varphi(j,i)}$. Compute $T_{ji} \in T$ be such that $B_j A_i = T_{ji} B_{\varphi(j,i)}$. For each $i \in \{1, \dots, m\}, j \in \{1, \dots, s\}$, we add a transition δ_{mj-m+i} in $\mathcal{A}$ from the state q_j to $q_{\varphi(j,i)}$, with evaluation T_{ji}. We claim that $\mathrm{ev}(\mathcal{A}) = \langle A_1, \dots, A_m \rangle \cap T$.

Indeed, take any product $A_{i_1} A_{i_2} \cdots A_{i_p} \in \langle A_1, \dots, A_m \rangle \cap T$. Let $TB_{j_1}, TB_{j_2}, TB_{j_3}, \dots, TB_{j_{p+1}}$, respectively denote the equivalent classes of $I, A_{i_1}, A_{i_1} A_{i_2}, \dots, A_{i_1} A_{i_2} \cdots A_{i_p}$ in $T\backslash G$. In particular, for $l = 1, \dots, p$, we have $TB_{j_l} A_{i_l} = TB_{j_{l+1}}$, so $\varphi(j_l, i_l) = j_{l+1}$. Consider the path $\delta_{mj_1-m+i_1} \delta_{mj_2-m+i_2} \cdots \delta_{mj_p-m+i_p}$ in $\mathcal{A}$. It is indeed a path because for each $l = 1, \dots, p$, the transition $\delta_{mj_l-m+i_l}$ originates at the state q_{j_l} and ends at state $q_{\varphi(j_l,i_l)} = q_{j_{l+1}}$. Furthermore, the path originates at q_1 because $TB_{j_1} = T$ so $j_1 = 1$. It ends at q_1 because $A_{i_1} A_{i_2} \cdots A_{i_p} \in T$, so $TB_{j_{p+1}} = T$ and $j_{p+1} = 1$. Therefore, $A_{i_1} A_{i_2} \cdots A_{i_p} = \mathrm{ev}(\delta_{mj_1-m+i_1} \delta_{mj_2-m+i_2} \cdots \delta_{mj_p-m+i_p}) \in \mathrm{ev}(\mathcal{A})$. Thus, $\langle A_1, \dots, A_m \rangle \cap T \subseteq \mathrm{ev}(\mathcal{A})$.

To prove $\mathrm{ev}(\mathcal{A}) \subseteq \langle A_1, \dots, A_m \rangle \cap T$, take any accepting run $\delta_{mj_1-m+i_1} \delta_{mj_2-m+i_2} \cdots \delta_{mj_p-m+i_p}$ of $\mathcal{A}$. Then $j_1 = \varphi(j_p, i_p) = 1$, and $\varphi(j_l, i_l) = j_{l+1}$ for $l = 1, \dots, p-1$. Therefore,

$$\begin{aligned}
&\mathrm{ev}(\delta_{mj_1-m+i_1} \delta_{mj_2-m+i_2} \cdots \delta_{mj_p-m+i_p}) \\
&= T_{j_1 i_1} T_{j_2 i_2} \cdots T_{j_p i_p} \\
&= B_{j_1} A_{i_1} B_{\varphi(j_1,i_1)}^{-1} \cdot B_{j_2} A_{i_2} B_{\varphi(j_2,i_2)}^{-1} \cdot \cdots \cdot B_{j_p} A_{i_p} B_{\varphi(j_p,i_p)}^{-1} \\
&= A_{i_1} A_{i_2} \cdots A_{i_p} \in \langle A_1, \dots, A_m \rangle .
\end{aligned}$$

Thus, $\mathrm{ev}(\mathcal{A}) \subseteq \langle A_1, \dots, A_m \rangle \cap T$. We therefore conclude that $\mathrm{ev}(\mathcal{A}) = \langle A_1, \dots, A_m \rangle \cap T$. □

Lemma 3.3. *Let S be a rational subsemigroup of T, then $\langle S \rangle_{\mathrm{grp}}$ is finitely generated. Furthermore, given an automaton over T that recognizes S, one can compute an automaton over $\langle S \rangle_{\mathrm{grp}}$ that recognizes S, as well as compute a set of generators for $\langle S \rangle_{\mathrm{grp}}$.*

Proof. The proof uses standard techniques for automata over groups, see for example [38] for similar results. Let $\mathcal{A}$ be an automaton over T such that $\mathrm{ev}(\mathcal{A}) = S$. Without loss of generality suppose $\mathcal{A}$ to be trim. For each state $q_i, i = 2, \dots, s$, of $\mathcal{A}$, let w_i denote a path from q_i to q_1 and write $B_i := \mathrm{ev}(w_i)$. Define additionally $B_1 := I$. Let $\mathcal{A}'$ be the automaton constructed as follows. The states of $\mathcal{A}'$ are the same as $\mathcal{A}$. For each transition δ_ℓ in $\mathcal{A}$, there is a transition δ'_ℓ in $\mathcal{A}'$ with the same origin and destination states, such that $\mathrm{ev}(\delta'_\ell) = B_{\Omega(\ell)}^{-1} \mathrm{ev}(\delta_\ell) B_{\Delta(\ell)}$. We will show that $\mathcal{A}'$ is an automaton over $\langle \mathrm{ev}(\mathcal{A}) \rangle_{\mathrm{grp}}$ and $\mathrm{ev}(\mathcal{A}') = \mathrm{ev}(\mathcal{A})$.

First, we show $\mathrm{ev}(\mathcal{A}') = \mathrm{ev}(\mathcal{A})$. Note that $\delta'_{\ell_1} \cdots \delta'_{\ell_m}$ is an accepting run of $\mathrm{ev}(\mathcal{A}')$ if and only if $\delta_{\ell_1} \cdots \delta_{\ell_m}$ is an accepting run of $\mathrm{ev}(\mathcal{A})$. Furthermore, when they are accepting runs, we have

$$\begin{aligned}
&\mathrm{ev}(\delta'_{\ell_1} \cdots \delta'_{\ell_m}) \\
&= \left(B_{\Omega(\ell_1)}^{-1} \mathrm{ev}(\delta_{\ell_1}) B_{\Delta(\ell_1)}\right) \cdot \left(B_{\Omega(\ell_2)}^{-1} \mathrm{ev}(\delta_{\ell_2}) B_{\Delta(\ell_2)}\right) \cdot \cdots \\
&\qquad \cdot \left(B_{\Omega(\ell_m)}^{-1} \mathrm{ev}(\delta_{\ell_m}) B_{\Delta(\ell_m)}\right) \\
&= \mathrm{ev}(\delta_{\ell_1}) \cdots \mathrm{ev}(\delta_{\ell_m}) \\
&= \mathrm{ev}(\delta_{\ell_1} \cdots \delta_{\ell_m}).
\end{aligned}$$

Therefore $\mathrm{ev}(\mathcal{A}') = \mathrm{ev}(\mathcal{A})$.

Next, we show that $\langle \mathrm{ev}(\delta'_1), \dots, \mathrm{ev}(\delta'_t)) \rangle_{\mathrm{grp}} = \langle \mathrm{ev}(\mathcal{A}) \rangle_{\mathrm{grp}}$. We claim that $B_{\Omega(\ell)}^{-1} \mathrm{ev}(\delta_\ell) B_{\Delta(\ell)} \in \langle \mathrm{ev}(\mathcal{A}) \rangle_{\mathrm{grp}}$ for all ℓ. Since $\mathcal{A}$ is trim, for each $i = 1, \dots, s$, there exists a path v_i from q_1 to q_i. Then $\mathrm{ev}(v_{\Omega(\ell)}) \mathrm{ev}(\delta_\ell) B_{\Delta(\ell)} = \mathrm{ev}(v_{\Omega(\ell)} \delta_\ell w_{\Delta(\ell)}) \in \mathrm{ev}(\mathcal{A})$. Similarly, $\mathrm{ev}(v_{\Omega(\ell)}) B_{\Omega(\ell)} = \mathrm{ev}(v_{\Omega(\ell)} w_{\Omega(\ell)}) \in \mathrm{ev}(\mathcal{A})$. Therefore,

$$\mathrm{ev}(\delta'_\ell) = B_{\Omega(\ell)}^{-1} \mathrm{ev}(\delta_\ell) B_{\Delta(\ell)} = \left(\mathrm{ev}(v_{\Omega(\ell)}) B_{\Omega(\ell)}\right)^{-1} \left(\mathrm{ev}(v_{\Omega(\ell)}) \mathrm{ev}(\delta_\ell) B_{\Delta(\ell)}\right) \in \langle \mathrm{ev}(\mathcal{A}) \rangle_{\mathrm{grp}} .$$

Since every element in $\mathrm{ev}(\mathcal{A}')$ is a product of $\mathrm{ev}(\delta'_1), \dots, \mathrm{ev}(\delta'_t)$, we have

$$\begin{aligned}
\langle \mathrm{ev}(\mathcal{A}') \rangle_{\mathrm{grp}} &\leq \langle \mathrm{ev}(\delta'_1), \dots, \mathrm{ev}(\delta'_t)) \rangle_{\mathrm{grp}} \\
&\leq \langle \mathrm{ev}(\mathcal{A}) \rangle_{\mathrm{grp}} = \langle \mathrm{ev}(\mathcal{A}') \rangle_{\mathrm{grp}} .
\end{aligned}$$

So $\langle \mathrm{ev}(\mathcal{A}) \rangle_{\mathrm{grp}} = \langle \mathrm{ev}(\delta'_1), \dots, \mathrm{ev}(\delta'_t)) \rangle_{\mathrm{grp}}$ is finitely generated, and the transitions of $\mathcal{A}'$ actually evaluates in $\langle \mathrm{ev}(\mathcal{A}) \rangle_{\mathrm{grp}}$. □

Lemma 3.6 (Composition of [29, Lemma 2] and [14, Lemma B.3])**.** *Let $\mathbb{K}$ be an algebraic number field. Suppose we are given a finitely generated subgroup T of $\mathsf{T}(d, \mathbb{K})$, let $N := T \cap \mathsf{UT}(d, \mathbb{K})$. One can compute an embedding $\varphi \colon T/[N,N] \hookrightarrow (\mathcal{Y} \rtimes \mathbb{Z}^n)/H$, where*

(i) *$n \in \mathbb{N}$ and $\mathcal{Y}$ is a finitely presented $\mathbb{Z}[X_1^{\pm}, \dots, X_n^{\pm}]$-module.*

(ii) *H is a subgroup of $\mathbb{Z}^n \leq \mathcal{Y} \rtimes \mathbb{Z}^n$, and elements of H commute with all elements in $\mathcal{Y} \rtimes \mathbb{Z}^n$.*

In particular, given any $g \in T$, one can compute $(y, z) \in \mathcal{Y} \rtimes \mathbb{Z}^n$ such that $\varphi(g[N,N]) = (y, z)H$.

Proof. By [29, Lemma 2], we can compute a finite presentation of $T/[N,N]$ in the variety of metabelian groups (see for example [33, Chapter 9] for the definition of finite presentation in varieties). Using this finite presentation, [14, Lemma B.3] shows that $T/[N,N]$ can be effectively embedded in a quotient $(\mathcal{Y} \rtimes \mathbb{Z}^n)/H$ satisfying the conditions (i) and (ii). □

Lemma 3.7. *Let $\varphi(\overline{S})$ be a rational subsemigroup of $(\mathcal{Y} \rtimes \mathbb{Z}^n)/H$ recognized by a given automaton. Then one can compute an automaton over $\mathcal{Y} \rtimes \mathbb{Z}^n$ that recognizes the subsemigroup $\varphi(\overline{S})H$.*

Proof. Let $\mathcal{A}$ be an automaton over $(\mathcal{Y} \rtimes \mathbb{Z}^n)/H$ recognizing $\varphi(\overline{S})$. Denote by $\delta_1, \dots, \delta_t$ its transitions. Let $\mathcal{A}'$ be the automaton over $\mathcal{Y} \rtimes \mathbb{Z}^n$ obtained from $\mathcal{A}$ by replacing the evaluations $\mathrm{ev}(\delta_1) = (y_1, a_1)H, \dots, \mathrm{ev}(\delta_t) = (y_t, a_t)H$, respectively by $(y_1, a_1), \dots, (y_t, a_t)$. Denote by $(0, h_1), \dots, (0, h_m)$ the generators of H as a semigroup. We then append m transitions to $\mathcal{A}'$, whose origins and destinations are the accepting state q_1, and whose evaluations are respectively $(0, h_1), \dots, (0, h_m)$. We thus obtain an automaton over $\mathcal{Y} \rtimes \mathbb{Z}^n$ that recognizes $\varphi(S)H$, because $(0, h_1), \dots, (0, h_m)$ commute with $(y_1, a_1), \dots, (y_t, a_t)$. □

Lemma 4.1. *Suppose we are given a trim automaton $\mathcal{A}$ over $\mathcal{Y} \rtimes \mathbb{Z}^n$. One can compute $\widetilde{n} \in \mathbb{N}$, a finitely presented $\mathbb{Z}[\widetilde{X_1}^{\pm}, \dots, \widetilde{X_{\widetilde{n}}}^{\pm}]$-module $\widetilde{\mathcal{Y}}$, and a primitive trim automaton $\widetilde{\mathcal{A}}$ over $\widetilde{\mathcal{Y}} \rtimes \mathbb{Z}^{\widetilde{n}}$, such that $\mathrm{ev}(\mathcal{A})$ is a group if and only if $\mathrm{ev}(\widetilde{\mathcal{A}})$ is a group.*

Proof. Denote by π the projection $\mathcal{Y} \rtimes \mathbb{Z}^n \to \mathbb{Z}^n$. Define $L \coloneqq \pi(\mathrm{ev}(\mathcal{A}^{\pm}))$. Fix $i \in \{2, \dots, s\}$. Let w_i be a path in $\mathcal{A}^{\pm}$ from q_1 to q_i, and define $z_i \coloneqq \pi(\mathrm{ev}(w_i))$. Then every path w from q_1 to q_i satisfies $\pi(\mathrm{ev}(w)) \in z_i + L$, because one can concatenate w with the "inverse" w_i^- to obtain an accepting run of $\mathcal{A}^{\pm}$, so $\pi(\mathrm{ev}(w)) - z_i = \pi(\mathrm{ev}(ww_i^-)) \in L$. Therefore, we have $a_\ell \in z_{\Delta(\ell)} - z_{\Omega(\ell)} + L$, for all ℓ.

Next, consider the automaton $\mathcal{A}'$ obtained from $\mathcal{A}$ as follows: the states of $\mathcal{A}'$ are the same as $\mathcal{A}$, and the transitions of $\mathcal{A}'$ are $\delta'_1, \dots, \delta'_t$, where $\delta'_\ell, \ell = 1, \dots, t$, has the same origin and target as δ_ℓ, but $\mathrm{ev}(\delta'_\ell) = (0, -z_{\Omega(\ell)}) \cdot \mathrm{ev}(\delta_\ell) \cdot (0, z_{\Delta(\ell)})$. We claim that $\mathrm{ev}(\mathcal{A}') = \mathrm{ev}(\mathcal{A})$, by the same argument as in the proof of Lemma 3.3. Indeed, take any accepting run $w = \delta_{\ell_1}\delta_{\ell_2}\cdots\delta_{\ell_p}$ of $\mathcal{A}$, we have $1 = \Omega(\ell_1), \Delta(\ell_1) = \Omega(\ell_2), \dots, \Delta(\ell_{p-1}) = \Omega(\ell_p), \Delta(\ell_p) = 1$. Then the run $w' = \delta'_{\ell_1}\delta'_{\ell_2}\cdots\delta'_{\ell_p}$ of $\mathcal{A}'$ is accepting, and

$$\begin{aligned}
&\mathrm{ev}(w') \\
&= (0, -z_{\Omega(\ell_1)}) \cdot \mathrm{ev}(\delta_{\ell_1}) \cdot (0, z_{\Delta(\ell_1)}) \cdot \\
&\quad (0, -z_{\Omega(\ell_2)}) \cdot \mathrm{ev}(\delta_{\ell_2}) \cdot (0, z_{\Delta(\ell_2)}) \cdot \\
&\quad\quad \cdots (0, -z_{\Omega(\ell_p)}) \cdot \mathrm{ev}(\delta_{\ell_p}) \cdot (0, z_{\Delta(\ell_p)}) \\
&= \mathrm{ev}(\delta_{\ell_1})\,\mathrm{ev}(\delta_{\ell_2}) \cdots \mathrm{ev}(\delta_{\ell_p}) \\
&= \mathrm{ev}(w).
\end{aligned}$$

Similarly, if $w' = \delta'_{\ell_1}\delta'_{\ell_2}\cdots\delta'_{\ell_p}$ is an accepting run of $\mathcal{A}'$, then $w = \delta_{\ell_1}\delta_{\ell_2}\cdots\delta_{\ell_p}$ is an accepting run of $\mathcal{A}$ such that $\mathrm{ev}(w) = \mathrm{ev}(w')$. Therefore $\mathrm{ev}(\mathcal{A}') = \mathrm{ev}(\mathcal{A})$. The same argument shows $\mathrm{ev}(\mathcal{A}'^{\pm}) = \mathrm{ev}(\mathcal{A}^{\pm})$, and hence $\pi(\mathrm{ev}(\mathcal{A}'^{\pm})) = \pi(\mathrm{ev}(\mathcal{A}^{\pm})) = L$. Note that for $\ell = 1, \dots, t$, we have $\pi(\mathrm{ev}(\delta'_\ell)) = -z_{\Omega(\ell)} + a_\ell + z_{\Delta(\ell)} \in L$. Therefore, we can without loss of generality replace $\mathcal{A}$ with $\mathcal{A}'$, and suppose $a_\ell = \pi(\mathrm{ev}(\delta_\ell)) \in L$ for all ℓ.

Finally, let $\beta_1, \dots, \beta_{\widetilde{n}} \in \mathbb{Z}^n$ denote a basis of lattice L, and define the new variables $\widetilde{X_i} \coloneqq \overline{X}^{\beta_i}, i = 1, \dots, \widetilde{n}$. Let $\widetilde{\mathcal{Y}}$ be the $\mathbb{Z}[\widetilde{X_1}^{\pm}, \dots, \widetilde{X_{\widetilde{n}}}^{\pm}]$-module generated by $y_1, \dots, y_t$, then a finite presentation of $\widetilde{\mathcal{Y}}$ can be effectively computed [39, Theorem 2.14]. Thus, each element (y_ℓ, a_ℓ) can now be represented as an element in $\widetilde{\mathcal{Y}} \rtimes \mathbb{Z}^{\widetilde{n}}$. The automaton $\mathcal{A}$ is thus considered as an automaton $\widetilde{\mathcal{A}}$ over $\widetilde{\mathcal{Y}} \rtimes \mathbb{Z}^{\widetilde{n}}$. Since $\mathcal{A}$ and $\widetilde{\mathcal{A}}$ recognize the same elements under different presentations, $\mathrm{ev}(\mathcal{A})$ is a group if and only if $\mathrm{ev}(\widetilde{\mathcal{A}})$ is a group. Furthermore, by the definition L, we have $\pi(\mathrm{ev}(\widetilde{\mathcal{A}}^{\pm})) = \mathbb{Z}^{\widetilde{n}}$; so $\widetilde{\mathcal{A}}$ is primitive. □

Proposition 4.2. *The semigroup $\mathrm{ev}(\mathcal{A})$ is a group if and only if $\mathcal{A}$ admits an Identity Traversal.*

Proof. Suppose $\mathrm{ev}(\mathcal{A})$ is a group. Let w be any accepting traversal, then $\mathrm{ev}(w) \in \mathrm{ev}(\mathcal{A})$. Since $\mathrm{ev}(\mathcal{A})$ is a group, we have $\mathrm{ev}(w)^{-1} \in \mathrm{ev}(\mathcal{A})$. Let v be an accepting run that evaluates to $\mathrm{ev}(w)^{-1}$. Then the concatenation wv is an accepting traversal and $\mathrm{ev}(wv) = \mathrm{ev}(w)\,\mathrm{ev}(v) = (0, 0^n)$.

Suppose there exists an Identity Traversal w. Each transition $\delta_\ell, \ell = 1, \dots, t$, appears at least once in w. For each $\ell = 1, \dots, t$, write $w = u_\ell\delta_\ell v_\ell$, and define w_ℓ to be the concatenation $v_\ell u_\ell$: it is a path that starts at the destination of δ_ℓ and ends at the origin of δ_ℓ, such that $\mathrm{ev}(w_\ell) = \mathrm{ev}(\delta_\ell)^{-1}$. In order to show that $\mathrm{ev}(\mathcal{A})$ is a group, let $w = \delta_{\ell_1}\delta_{\ell_2}\cdots\delta_{\ell_p}$ be any accepting run and we prove $\mathrm{ev}(w)^{-1} \in M$. Consider the concatenation $w' \coloneqq w_{\ell_p}\cdots w_{\ell_2}w_{\ell_1}$, then w' is an accepting run and $\mathrm{ev}(w') = \mathrm{ev}(w_{\ell_p})\cdots\mathrm{ev}(w_{\ell_2})\,\mathrm{ev}(w_{\ell_1}) = \mathrm{ev}(\delta_{\ell_m})^{-1}\cdots\mathrm{ev}(\delta_{\ell_2})^{-1}\,\mathrm{ev}(\delta_{\ell_1})^{-1} = \mathrm{ev}(w)^{-1}$. Therefore $\mathrm{ev}(w)^{-1} = \mathrm{ev}(w') \in \mathrm{ev}(\mathcal{A})$. □

Lemma 4.5. *There exists an Identity Traversal of $\mathcal{A}$ if and only if there exists a full-image Eulerian $\mathcal{A}$-graph that represents 0.*

Proof. Let w be an Identity Traversal, then $\mathrm{ev}(w) = (0, 0^n)$. This shows that the graph $\Gamma(w)$ represents the element $0 \in \mathcal{Y}$. Furthermore, $\Gamma(w)$ is a path starting at the vertex $(b_1, 0^n)$ and ends in $(b_1, 0^n + 0^n)$, hence it is Eulerian. Since w contains transitions of every label, $\Gamma(w)$ is full-image.

Let Γ be a full-image Eulerian $\mathcal{A}$-graph that represents 0. By translating Γ we can suppose Γ to contain the vertex $(b_1, 0^n)$, this does not change the fact that Γ represents 0. Let P be an Eulerian circuit of Γ that starts and ends in $(b_1, 0^n)$. We trace the labels $\ell_1, \dots, \ell_p$, of edges in P to obtain a run $w(P) = \delta_{\ell_1}\delta_{\ell_2}\cdots\delta_{\ell_p}$ in $\mathcal{A}$. The run $w(P)$ is accepting because the P starts and ends in the lattice Λ_1. Let $(y, z) \in \mathcal{Y} \rtimes \mathbb{Z}^n$ denote the evaluation $\mathrm{ev}(w(P))$. We have $y = 0$ because Γ represents $0 \in \mathcal{Y}$. We have $z = \sum_{e \in E(\Gamma)} a_{\lambda(e)} = 0^n$ because the P is an Eulerian circuit. Therefore P is an accepting run that evaluates to the neutral element. Furthermore, P uses every transition at least once because Γ is full-image, so P is an Identity Traversal. □

Proposition 4.8. *A trim primitive automaton $\mathcal{A}$ admits an Identity Traversal if and only if there exists a full-image symmetric face-accessible $\mathcal{A}$-graph that represents 0.*

Proof. If the automaton $\mathcal{A}$ admits an Identity Traversal, then Lemma 4.5 shows there exists a full-image Eulerian $\mathcal{A}$-graph

representing 0: this Eulerian graph is symmetric and face-accessible.

If there is a full-image symmetric face-accessible Eulerian $\mathcal{A}$-graph Γ representing 0, then by Theorem 4.7, some a union of translations $\widehat{\Gamma} \coloneqq \bigcup_{i=1}^{m} \Gamma + (0^s, z_i)$ is an Eulerian graph. The graph $\widehat{\Gamma}$ represents the element $\sum_{i=1}^{m} \overline{X}^{z_i} \cdot 0 = 0$, and it is full-image because it contains the full-image graph $\Gamma + (0^s, z_1)$ as a subgraph. Therefore, by Lemma 4.5, the automaton $\mathcal{A}$ admits an Identity Traversal. □

Lemma 4.9. *Let Γ be an $\mathcal{A}$-graph with position polynomials $\boldsymbol{f} = (f_1, \dots, f_t) \in \mathbb{N}[\overline{X}^{\pm}]^t$.*

(i) *Γ is full-image if and only if $f_\ell \in \mathbb{N}[\overline{X}^{\pm}]^* \coloneqq \mathbb{N}[\overline{X}^{\pm}] \setminus \{0\}$, for $\ell = 1, \dots, t$.*

(ii) *Γ is symmetric if and only if for each $i = 1, \dots, s$, we have $\sum_{\ell\colon \Omega(\ell)=i} f_\ell = \sum_{\ell\colon \Delta(\ell)=i} f_\ell \cdot \overline{X}^{a_\ell}$.*

(iii) *Γ represents 0 if and only if $\sum_{\ell=1}^{t} f_\ell \cdot y_\ell = 0$.*

Proof. (i) Γ is full-image if and only if each label appears at least once, meaning $f_\ell \neq 0$ for all ℓ.

(ii) For $i \in \{1, \dots, s\}$, we have

$$\sum_{\ell\colon \Omega(\ell)=i} f_\ell = \sum_{\ell\colon \Omega(\ell)=i,\, e\in E(\Gamma), \lambda(e)=\ell} \overline{X}^{\pi_{\mathbb{Z}^n}(\sigma(e))} = \sum_{e\in E(\Gamma), \sigma(e)\in\Lambda_i} \overline{X}^{\pi_{\mathbb{Z}^n}(\sigma(e))},$$

and

$$\begin{aligned} &\sum_{\ell\colon \Delta(\ell)=i} f_\ell \cdot \overline{X}^{a_\ell} \\ &= \sum_{\ell\colon \Delta(\ell)=i} \sum_{e\in E(\Gamma), \lambda(e)=\ell} \overline{X}^{\pi_{\mathbb{Z}^n}(\sigma(e))} \cdot \overline{X}^{a_\ell} \\ &= \sum_{\ell\colon \Delta(\ell)=i,\, e\in E(\Gamma), \lambda(e)=\ell} \overline{X}^{\pi_{\mathbb{Z}^n}(\tau(e))} \\ &= \sum_{e\in E(\Gamma), \tau(e)\in\Lambda_i} \overline{X}^{\pi_{\mathbb{Z}^n}(\tau(e))}. \end{aligned}$$

These two sums are equal if and only if the in-degree equals the out-degree at every vertex in Λ_i. Therefore, Γ is symmetric if and only if $\sum_{\ell\colon \Omega(\ell)=i} f_\ell = \sum_{\ell\colon \Delta(\ell)=i} f_\ell \cdot \overline{X}^{a_\ell}$ holds for all $i \in \{1, \dots, s\}$.

(iii) Γ represents the element

$$\sum_{e\in E(\Gamma)} \overline{X}^{\pi_{\mathbb{Z}^n}(\sigma(e))} \cdot y_{\lambda(e)} = \sum_{\ell=1}^{t} \sum_{e\in E(\Gamma), \lambda(e)=\ell} \overline{X}^{\pi_{\mathbb{Z}^n}(\sigma(e))} \cdot y_\ell = \sum_{\ell=1}^{t} f_\ell \cdot y_\ell,$$

which is 0 if and only if $\sum_{\ell=1}^{t} f_\ell \cdot y_\ell = 0$. □

Lemma 4.12. *Let Γ be a symmetric $\mathcal{A}$-graph with position polynomials $\boldsymbol{f} = (f_1, \dots, f_t) \in \mathbb{N}[\overline{X}^{\pm}]^t$. Then Γ is face-accessible if and only if for every partial contraction $(S, \mathcal{T}, \rho)$, we have*

$$\left(O_v(S, \mathcal{T}, \rho) \cup \Delta^{-1}(S)^{\complement}\right) \cap M_v((S, \mathcal{T}, \rho), \boldsymbol{f}) \neq \emptyset \qquad (4)$$

for every $v \in (\mathbb{R}^n)^*$.

Proof. We show the contrapositive: the convex hull C of $V(\Gamma)$ has a non-accessible face if and only if $\exists (S, \mathcal{T}, \rho), \exists v \in (\mathbb{R}^n)^*$, such that

$$\left(O_v(S, \mathcal{T}, \rho) \cup \Delta^{-1}(S)^{\complement}\right) \cap M_v((S, \mathcal{T}, \rho), \boldsymbol{f}) = \emptyset.$$

1. Suppose C has a non-accessible face F. Then every edge of Γ that starts inside F and ends inside F. We will show that there exists a partial contraction $(S, \mathcal{T}, \rho)$ and some vector $v \in (\mathbb{R}^n)^*$, such that $\left(O_v(S, \mathcal{T}, \rho) \cup \Delta^{-1}(S)^{\complement}\right) \cap M_v((S, \mathcal{T}, \rho), \boldsymbol{f}) = \emptyset$.

Let $(b, v) \in (\mathbb{R}^{s+n})^*$ be such that F is the extremal face of C at direction (b, v). That is, $F = \{x \in C \mid \forall x' \in C, (b, v) \cdot x \geq (b, v) \cdot x'\}$. Let $\widetilde{S}$ denote the set of indices i such that $V(\Gamma) \cap F \cap \Lambda_i \neq \emptyset$. Let $E_{(b,v)}$ denote the set of edges in Γ whose source and target are both in F, and let $\widetilde{\mathcal{T}}_{(b,v)}$ be the set of labels appearing in $E_{(b,v)}$. Consider the subautomaton $\widetilde{\mathcal{A}}$ of $\mathcal{A}$ whose set of states is $\{q_i \mid i \in \widetilde{S}\}$ and whose set of transitions is $\{\delta_\ell \mid \ell \in \widetilde{\mathcal{T}}_{(b,v)}\}$. Choose any $S \subseteq \widetilde{S}$ such that $\{q_i \mid i \in S\}$ is a connected component of $\widetilde{\mathcal{A}}$, and choose $\mathcal{T} \subseteq \widetilde{\mathcal{T}}_{(b,v)}$ such that $\{\delta_\ell \mid \ell \in \mathcal{T}\}$ is an undirected spanning tree of this connected component. Let ρ be any element of S, we will show that

$$\left(O_v(S, \mathcal{T}, \rho) \cup \Delta^{-1}(S)^{\complement}\right) \cap M_v((S, \mathcal{T}, \rho), \boldsymbol{f}) = \emptyset.$$

Take any $\ell \in M_v((S, \mathcal{T}, \rho), \boldsymbol{f}) \subseteq \Omega^{-1}(S)$, we will show that $\ell \notin \Delta^{-1}(S)^{\complement}$ and $\ell \notin O_v(S, \mathcal{T}, \rho)$. By the definition of $M_v((S, \mathcal{T}, \rho), \boldsymbol{f})$, there is a monomial $c\overline{X}^z$ appearing in $f_\ell^{(S,\mathcal{T},\rho)}$, such that $v \cdot z$ is maximal among all monomials appearing in $f_{(S,\mathcal{T},\rho),\ell'}, \ell' \in \Omega^{-1}(S)$. This yields an edge e with label ℓ, starting at $(b_{\Omega(\ell)}, z) \in F \cap \Lambda_{\Omega(\ell)}$ with $\Omega(\ell) \in S$.

(i) First we show $\ell \notin \Delta^{-1}(S)^{\complement}$, which is equivalent to $\Delta(\ell) \in S$.

Since $\Omega(\ell) \in S$, all edges starting in $V(\Gamma) \cap (F \cap \Lambda_{\Omega(\ell)})$ end in F. Since $\{q_i \mid i \in S\}$ is a connected component of $\widetilde{\mathcal{A}}$, all all edges starting in $V(\Gamma) \cap (F \cap \Lambda_{\Omega(\ell)})$ actually ends in $\bigcup_{i\in S}(F \cap \Lambda_i)$. Therefore $\Delta(\ell) \in S$, so $\ell \notin \Delta^{-1}(S)^{\complement}$.

(ii) Next we show $\ell \notin O_v(S, \mathcal{T}, \rho)$, which is equivalent to $a_\ell^{(S,\mathcal{T},\rho)} \perp v$. If $\Delta(\ell) \notin S$ then $a_\ell^{(S,\mathcal{T},\rho)} = 0^n \perp v$, so consider the case where $\Delta(\ell) \in S$. By the definition of $\mathcal{T} \subseteq \widetilde{\mathcal{T}}_{(b,v)}$, every label $\ell' \in \mathcal{T}$ satisfy $(b_{\Delta(\ell')} - b_{\Omega(\ell')}, a_{\ell'}) = \tau(e) - \sigma(e) \perp (b, v)$, where e is an edge contained within F with label ℓ'. Let $P_{\Omega(\ell)}$ be the path consisting of transitions in $\{\delta_l \mid l \in \mathcal{T}\} \cup \{\delta_l^- \mid l \in \mathcal{T}\}$ that connects from $q_{\Omega(\ell)}$ to q_ρ, and write $\mathrm{ev}(P_{\Omega(\ell)})$ as $(y_{P_{\Omega(\ell)}}, z_{P_{\Omega(\ell)}})$. Then

$$(b_\rho - b_{\Omega(\ell)}, z_{P_{\Omega(\ell)}}) = \sum_{\delta_l^{\pm} \in P_{\Omega(\ell)}} \pm(b_{\Delta(l)} - b_{\Omega(l)}, a_l) \perp (b, v). \qquad (9)$$

Similarly, let $P_{\Delta(\ell)}$ be the path consisting of transitions in $\{\delta_l \mid l \in \mathcal{T}\} \cup \{\delta_l^- \mid l \in \mathcal{T}\}$ that connects from $q_{\Delta(\ell)}$ to q_ρ,

and write $\mathrm{ev}(P_{\Delta(\ell)})$ as $(y_{P_{\Delta(\ell)}}, z_{P_{\Delta(\ell)}})$. Then we have

$$(b_\rho - b_{\Delta(\ell)}, z_{P_{\Delta(\ell)}}) = \sum_{\delta_l^\pm \in P_{\Delta(\ell)}} \pm(b_{\Delta(l)} - b_{\Omega(l)}, a_l) \perp (b, v). \tag{10}$$

Furthermore, since both the source and target of the edge e (with label ℓ) are in F, we have

$$(b_{\Delta(\ell)} - b_{\Omega(\ell)}, a_\ell) \perp (b, v). \tag{11}$$

Taking (10)+(11)−(9) yields $(0^s, z_{P_{\Delta(\ell)}} + a_\ell - z_{P_{\Omega(\ell)}}) \perp (b, v)$. Therefore $a_\ell^{(S,\mathcal{T},\rho)} = (a_\ell + z_{P_{\Delta(\ell)}} - z_{P_{\Omega(\ell)}}) \perp v$.

2. Suppose there exists a partial contraction $(S, \mathcal{T}, \rho)$ and some vector $v \in (\mathbb{R}^n)^*$, such that

$$\left(O_v(S, \mathcal{T}, \rho) \cup \Delta^{-1}(S)^{\complement}\right) \cap M_v((S, \mathcal{T}, \rho), \boldsymbol{f}) = \emptyset.$$

We will show that some strict face of C is not accessible. For a set X we denote by $\mathrm{conv}(X)$ its convex hull.

For $i = 1, \ldots, s$, define $C_i \coloneqq \mathrm{conv}(V(\Gamma) \cap \Lambda_i)$, and let F_i be the extremal face of C_i at direction $(0^s, v)$. Let $b = (\beta_1, \ldots, \beta_s) \in \mathbb{R}^s$ be such that

(i) $(b, v) \perp (b_{\Delta(\ell)} - b_{\Omega(\ell)}, a_\ell)$ for all $\ell \in \mathcal{T}$.

(ii) the extremal face F of $\mathrm{conv}(V(\Gamma))$ at direction (b, v) satisfies $V(\Gamma) \cap F = \bigcup_{i \in S}(V(\Gamma) \cap F_i)$. In other words, F is so that its intersection with $\mathrm{conv}(V(\Gamma))$ contains and only contains vertices in the lattices $\Lambda_i, i \in S$.

Such b can always be found. Indeed, since transitions with label $\mathcal{T}$ form a tree with states of index S, we have $|\mathcal{T}| = |S| - 1$. So condition (i) can be satisfied by choosing the coordinates $\beta_i, i \in S$. Then, condition (ii) can be satisfied by choosing the coordinates $\beta_i, i \notin S$ to be sufficiently small compared to $\beta_i, i \in S$.

We will show that F is not accessible. Let e be an edge with label ℓ starting in $(b_{\Omega(\ell)}, z) \in V(\Gamma) \cap F$.

(i) First, we show $\ell \in M_v((S, \mathcal{T}, \rho), \boldsymbol{f})$. Since $\sigma(e) \in \Lambda_i$ with $i \in S$, we have $\ell \in \Omega^{-1}(S)$. Take any label $\ell' \in \Omega^{-1}(S)$ and let $c'\overline{X}^{z'}$ be the monomial with largest $\deg_v$ in $f_{\ell'}$. Then there is an edge e' starting in $(b_{\Omega(\ell')}, z')$. Since $V(\Gamma) \cap F = \bigcup_{i \in S}(V(\Gamma) \cap F_i) \supseteq V(\Gamma) \cap F_{\Omega(\ell')}$, there is an edge e'' with $\sigma(e'') = (b_{\Omega(\ell')}, z'') \in F_{\Omega(\ell')}$. Therefore $(\beta, v) \cdot (b_{\Omega(\ell')}, z'') \geq (\beta, v) \cdot (b_{\Omega(\ell')}, z')$, yielding

$$v \cdot z'' \geq v \cdot z'. \tag{12}$$

Let $P_{\Omega(\ell)}$ be the path consisting of transitions in $\{\delta_l \mid l \in \mathcal{T}\} \cup \{\delta_l^- \mid l \in \mathcal{T}\}$ that connects from $q_{\Omega(\ell)}$ to q_ρ, and write $\mathrm{ev}(P_{\Omega(\ell)})$ as $(y_{P_{\Omega(\ell)}}, z_{P_{\Omega(\ell)}})$. Then

$$(b_\rho - b_{\Omega(\ell)}, z_{P_{\Omega(\ell)}}) = \sum_{\delta_l^\pm \in P_{\Omega(\ell)}} \pm(b_{\Delta(l)} - b_{\Omega(l)}, a_l) \perp (b, v). \tag{13}$$

Similarly, let $P_{\Omega(\ell')}$ be the path consisting of transitions in $\{\delta_l \mid l \in \mathcal{T}\} \cup \{\delta_l^- \mid l \in \mathcal{T}\}$ that connects from $q_{\Omega(\ell')}$ to q_ρ, and write $\mathrm{ev}(P_{\Omega(\ell')})$ as $(y_{P_{\Omega(\ell')}}, z_{P_{\Omega(\ell')}})$. Then

$$(b_\rho - b_{\Omega(\ell')}, z_{P_{\Omega(\ell')}}) = \sum_{\delta_l^\pm \in P_{\Omega(\ell')}} \pm(b_{\Delta(l)} - b_{\Omega(l)}, a_l) \perp (b, v). \tag{14}$$

Furthermore, since both $(b_{\Omega(\ell)}, z)$ and $(b_{\Omega(\ell')}, z'')$ are in F, we have

$$(b_{\Omega(\ell')} - b_{\Omega(\ell)}, z'' - z) \perp (b, v). \tag{15}$$

Computing (14)+(15)−(13) yields $(0^s, z_{P_{\Omega(\ell')}} + z'' - z - z_{P_{\Omega(\ell)}}) \perp (b, v)$. Therefore,

$$\begin{aligned}\deg_v(f_\ell^{(S,\mathcal{T},\rho)}) &= v \cdot (z + z_{P_{\Omega(\ell)}}) = v \cdot (z'' + z_{P_{\Omega(\ell')}}) \\ &\geq v \cdot (z' + z_{P_{\Omega(\ell')}}) = \deg_v(f_{\ell'}^{(S,\mathcal{T},\rho)}).\end{aligned}$$

So we indeed have $\ell \in M_v((S, \mathcal{T}, \rho), \boldsymbol{f})$.

(ii) Next, we show that the target $\tau(e)$ of e must be in F. Indeed, since $\ell \in M_v((S, \mathcal{T}, \rho), \boldsymbol{f})$ and $\left(O_v(S, \mathcal{T}, \rho) \cup \Delta^{-1}(S)^{\complement}\right) \cap M_v((S, \mathcal{T}, \rho), \boldsymbol{f}) = \emptyset$, we have $\ell \notin O_v(S, \mathcal{T}, \rho)$ and $\ell \notin \Delta^{-1}(S)^{\complement}$. The condition $\ell \notin \Delta^{-1}(S)^{\complement}$ shows $\Delta(\ell) \in S$, so $\tau(e) \in \bigcup_{i \in S}(V(\Gamma) \cap \Lambda_i)$. The $\ell \notin O_v(S, \mathcal{T}, \rho)$ shows $a_\ell + z_{P_{\Delta(\ell)}} - z_{P_{\Omega(\ell)}} = a_\ell^{(S,\mathcal{T},\rho)} \perp v$. Therefore,

$$\begin{aligned}&\tau(e) - \sigma(e) \\ &= (b_{\Delta(\ell)} - b_{\Omega(\ell)}, a_\ell) \\ &= (b_{\Delta(\ell)} - b_{\Omega(\ell)}, z_{P_\Omega(\ell)} - z_{P_\Delta(\ell)} + a_\ell^{(S,\mathcal{T},\rho)}) \\ &= (b_\rho - b_{\Omega(\ell)}, z_{P_{\Omega(\ell)}}) - (b_\rho - b_{\Delta(\ell)}, z_{P_{\Delta(\ell)}}) + (0^s, a_\ell^{(S,\mathcal{T},\rho)}) \\ &\perp (b, v)\end{aligned}$$

by Equations (13) and (14). Since $\sigma(e) \in F$ and F is the extremal face at direction (b, v), we conclude that $\tau(e) \in F$. We have thus shown that every edge e starting in $V(\Gamma) \cap F$ ends in F. Therefore F is not accessible.

□

Proposition 4.13. *There exists a full-image symmetric face-accessible $\mathcal{A}$-graph Γ, if and only if there exists $\widetilde{\boldsymbol{f}} \in \widetilde{\mathcal{M}_\mathbb{Z}} \cap \left(\mathbb{N}[\overline{X}^\pm]^*\right)^K$, satisfying*

$$\left(O_v \cup J_{(S,\mathcal{T},\rho)}\right) \cap M_v\left(I_{(S,\mathcal{T},\rho)}, \widetilde{\boldsymbol{f}}\right) \neq \emptyset, \tag{7}$$

for every $v \in (\mathbb{R}^n)^*$, $(S, \mathcal{T}, \rho) \in \mathcal{PC}$.

Proof. Suppose there exists a full-image symmetric face-accessible $\mathcal{A}$-graph Γ. Take the tuple of position polynomials $\boldsymbol{f}$ of Γ. Then by Lemma 4.9, we have $\boldsymbol{f} \in \left(\mathbb{N}[\overline{X}^\pm]^*\right)^t$ and $\boldsymbol{f} \in \mathcal{M}_\mathbb{Z}$. Therefore $\widetilde{\boldsymbol{f}} \in \widetilde{\mathcal{M}_\mathbb{Z}} \cap \left(\mathbb{N}[\overline{X}^\pm]^*\right)^K$. Since Γ is face-accessible, the tuple $\boldsymbol{f}$ satisfies the condition (4) in Lemma 4.12 for every partial contraction $(S, \mathcal{T}, \rho) \in \mathcal{PC}$. This is equivalent to $\widetilde{\boldsymbol{f}}$ satisfying condition (7).

Suppose there exists $\widetilde{\boldsymbol{f}} \in \widetilde{\mathcal{M}_\mathbb{Z}} \cap \left(\mathbb{N}[\overline{X}^\pm]^*\right)^K$ that satisfies condition (7). We recover $\boldsymbol{f} \in \mathcal{M}_\mathbb{Z} \cap \left(\mathbb{N}[\overline{X}^\pm]^*\right)^t$ as a sub-tuple of $\widetilde{\boldsymbol{f}}$. There exists an $\mathcal{A}$-graph Γ whose position polynomials are $\boldsymbol{f}$. Since $\boldsymbol{f} \in \mathcal{M}_\mathbb{Z} \cap \left(\mathbb{N}[\overline{X}^\pm]^*\right)^t$, it satisfies the conditions (i), (ii) and (iii) in Lemma 4.9. Therefore Γ is full-image symmetric and represents 0. Finally, since $\widetilde{\boldsymbol{f}}$ satisfies condition (7), the tuple $\boldsymbol{f}$ satisfies the condition (4) in Lemma 4.12 for every partial contraction $(S, \mathcal{T}, \rho) \in \mathcal{PC}$. Therefore, Γ is face-accessible. □

Lemma 4.15. *There exists an element $\widetilde{\boldsymbol{f}} \in \widetilde{\mathcal{M}_{\mathbb{Z}}} \cap \left(\mathbb{N}[\overline{X}^{\pm}]^*\right)^K$ satisfying Property (7), if and only if there exists $\boldsymbol{f} \in \mathcal{M} \cap \left(\mathbb{R}_{\geq 0}[\overline{X}^{\pm}]^*\right)^K$ satisfying Property (7).*

Proof. An element $\widetilde{\boldsymbol{f}} \in \widetilde{\mathcal{M}_{\mathbb{Z}}} \cap \left(\mathbb{N}[\overline{X}^{\pm}]^*\right)^K$ satisfying Property (7) is obviously an element in $\mathcal{M} \cap \left(\mathbb{R}_{\geq 0}[\overline{X}^{\pm}]^*\right)^K$. Therefore it suffices to prove the "if" implication.

Suppose we have an element $\boldsymbol{f} \in \mathcal{M} \cap \left(\mathbb{R}_{\geq 0}[\overline{X}^{\pm}]^*\right)^K$ satisfying Property (7). Write $\boldsymbol{f} = (f_1, \dots, f_K)$ where for $i = 1, \dots, K$,

$$f_i = \sum_{b \in B_i} c_{i,b} \overline{X}^b.$$

Here, the *support* B_i is a non-empty finite subset of $\mathbb{Z}^n$, and $c_{i,b} \in \mathbb{R}_{>0}$ for all $b \in B_i$. Since Property (7) depends only on the supports $B_1, \dots, B_K$, it suffices to show that there exists $\widetilde{\boldsymbol{f}} = (\widetilde{f}_1, \dots, \widetilde{f}_K) \in \widetilde{\mathcal{M}_{\mathbb{Z}}} \cap \left(\mathbb{N}[\overline{X}^{\pm}]^*\right)^K$ where

$$\widetilde{f}_i = \sum_{b \in B_i} \widetilde{c}_{i,b} \overline{X}^b$$

and $\widetilde{c}_{i,b} \in \mathbb{Z}_{>0}$ for all $b \in B_i$.

Since $\boldsymbol{f} \in \mathcal{M}$, we have $\boldsymbol{f} = \sum_{j=1}^m h_j \cdot \boldsymbol{g}_j$ for some $h_1, \dots, h_m \in \mathbb{R}[\overline{X}^{\pm}]$. For each $j \in \{1, \dots, m\}$, write $h_j = \sum_{b \in H_j} h_{j,b} \overline{X}^b$, where H_j is a finite subset of $\mathbb{Z}^n$. Then the equation $\boldsymbol{f} = \sum_{j=1}^m h_j \cdot \boldsymbol{g}_j$ can be rewritten as a finite system of linear equations over $\mathbb{R}$, where the left hand sides are 0 or $c_{i,b}, b \in B_i, i = 1, \dots, K$, and the right hand sides are $\mathbb{Z}$-linear combinations of the variables $h_{j,b}, j \in \{1, \dots, m\}, b \in H_j$ (because the coefficients of $\boldsymbol{g}_j$ are integers for all j).

Since this system of linear equations is homogeneous and the coefficients are all in $\mathbb{Z}$, it has a solution $h_{j,b} \in \mathbb{R}, j \in \{1, \dots, m\}, b \in H_j$ and $c_{i,b} \in \mathbb{R}_{>0}, b \in B_i, i = 1, \dots, K$, if and only if it has a solution with $h_{j,b} \in \mathbb{Q}, c_{i,b} \in \mathbb{Q}_{>0}$ for all i, j, b. By multiplying all $h_{j,b}, c_{i,b}$ with their common denominator, we obtain a solution $\widetilde{h}_{j,b} \in \mathbb{Z}, \widetilde{c}_{i,b} \in \mathbb{Z}_{>0}$ for all i, j, b. Then, $\widetilde{f}_i := \sum_{b \in B_i} \widetilde{c}_{i,b} \overline{X}^b, i = 1, \dots, K$ and $\widetilde{h}_j = \sum_{b \in H_j} \widetilde{h}_{j,b} \overline{X}^b, j = 1, \dots, m$, satisfy $\widetilde{\boldsymbol{f}} = \sum_{j=1}^m \widetilde{h}_j \cdot \boldsymbol{g}_j$. Hence, $\widetilde{\boldsymbol{f}} = (\widetilde{f}_1, \dots, \widetilde{f}_K) \in \widetilde{\mathcal{M}_{\mathbb{Z}}} \cap \left(\mathbb{N}[\overline{X}^{\pm}]^*\right)^K$. The element $\widetilde{\boldsymbol{f}}$ satisfies Property (7) since the condition depends only on the supports $B_1, \dots, B_K$. □

Appendix B
Proof of Theorem 4.7

In this appendix we prove Theorem 4.7. Figure 11 illustrates the main steps of the proof.

Theorem 4.7. *Suppose $\mathcal{A}$ is trim and primitive. Let Γ be a full-image, symmetric and face-accessible $\mathcal{A}$-graph. Then there exist $z_1, \dots, z_m \in \mathbb{Z}^n$, such that the union of translations $\widehat{\Gamma} := \bigcup_{i=1}^m \Gamma + (0^s, z_i)$ is an Eulerian graph.*

Our main strategy is to reduce to the case $s = 1$, which has already been proved in [14, Theorem 3.3]. Let Γ be a full-image, symmetric and face-accessible $\mathcal{A}$-graph. Recall that a directed graph is Eulerian if and only if it is symmetric and connected (for symmetric graphs, strong and weak connectivity are equivalent). Since Γ is full-image and symmetric, any union of translations $\widehat{\Gamma} = \bigcup_{i=1}^m \Gamma + (0^s, z_i)$ is also full-image and symmetric when $m \geq 1$. Therefore it suffices to find $z_1, \dots, z_m \in \mathbb{Z}^n$ such that $\widehat{\Gamma} = \bigcup_{i=1}^m \Gamma + (0^s, z_i)$ is connected.

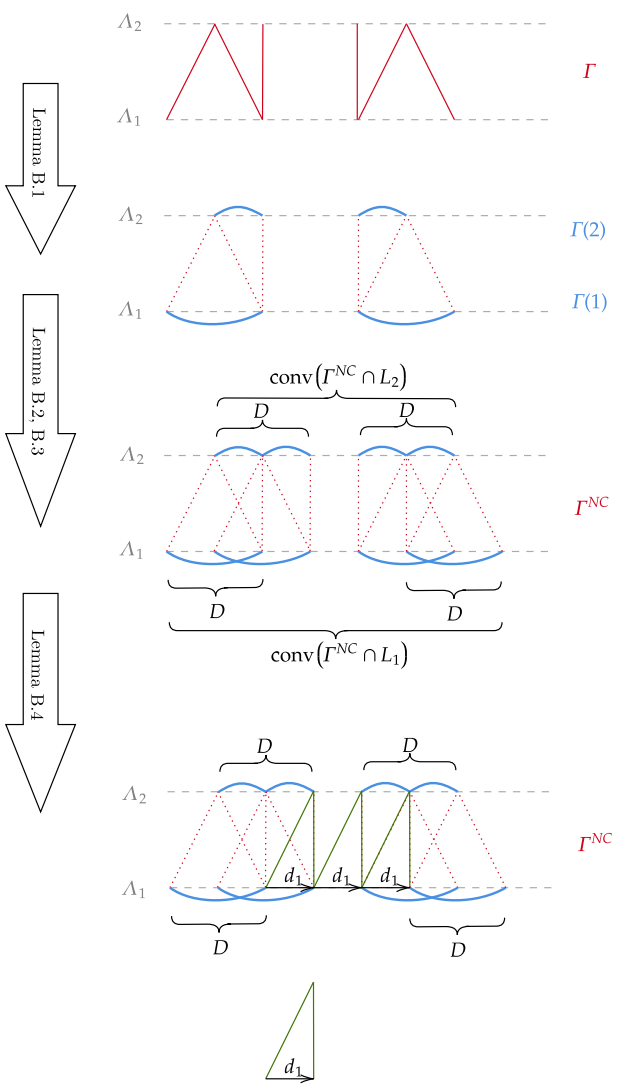

Fig. 11. Proof of Theorem 4.7

For an edge e from $\sigma(e)$ to $\tau(e)$, we denote by e^- its *inverse*, that is, an edge from $\tau(e)$ to $\sigma(e)$. Since strong and weak connectivity are equivalent for symmetric graphs, for each edge e in Γ we add its inverse e^- into Γ, this will not change the connectivity of Γ or the eventually constructed $\widehat{\Gamma}$. Hence, we can suppose without loss of generality that for each $e \in E(\Gamma)$ we have added e^- in $E(\Gamma)$, and Γ is actually an $\mathcal{A}^{\pm}$-graph.

For a sequence sequence of polytopes $P_1, \dots, P_m \subseteq \mathbb{R}^n$, we define their *Minkowski sum*

$$P_1 + \cdots + P_m := \{p_1 + \cdots + p_m \mid p_i \in P_i, i = 1, \dots, m\}.$$

For simplicity we denote by mP the sum $\underbrace{P+P+\cdots+P}_{m \text{ times}}$. Since P is convex, mP is also equal to the set $\{m\cdot p \mid p \in P\}$.

For each $i \in \{1,\dots,s\}$, consider the set of vertices $V(\Gamma)\cap\Lambda_i$: these are the vertices of Γ appearing in the lattice Λ_i. The convex hull of $V(\Gamma)\cap\Lambda_i$ is a polytope of the form $\{b_i\}\times C_i$, where C_i is a polytope in $\mathbb{R}^n$.

Consider the Minkowski sum $C \coloneqq C_1+\cdots+C_s$. Then C is of dimension n since $\mathcal{A}$ is primitive and Γ is full-image. Indeed, if C is of dimension less than n, then $C_1,\dots,C_s$ are all contained in the some hyperplane $H \subsetneq \mathbb{R}^n$. The vertices in Λ_1 reachable by any concatenation of edges will be contained in H, which contradicts the definition of primitiveness of $\mathcal{A}$.

Consider the $\mathcal{A}$-graph

$$\Gamma^C \coloneqq \bigcup_{z\in C\cap\mathbb{Z}^n} \Gamma + (0^s, z).$$

Then for each $i \in \{1,\dots,s\}$, the convex hull $\mathrm{conv}(\Gamma^C \cap \Lambda_i)$ is equal to $\{b_i\}\times(C+C_i)$.

Lemma B.1. *Fix $i \in \{1,\dots,s\}$. Let F be a strict face of $C+C_i \subsetneq \mathbb{R}^n$. Then there exists a path in Γ^C starting in $\{b_i\}\times F$ and ending in $\{b_i\}\times((C+C_i)\setminus F)$.*

Proof. See Figure 12 and 13 for an illustration of this proof. Without loss of generality suppose $i=1$. Let $v \in (\mathbb{R}^n)^*$ be such that F is the extremal face of $C+C_1$ at direction v. That is, $F = \{x \in C+C_1 \mid \forall x' \in C+C_1, v\cdot x \geq v\cdot x'\}$. Let $F_1, F_2, \dots, F_s$ be respectively the extremal face of $C_1, C_2, \dots, C_s$ at direction v, then $F_1+F_2+\cdots+F_s+F_1 \subseteq F$. Indeed, take $x_1 \in F_1,\dots,x_s \in F_s, x_{s+1} \in F_1$ and any $x' \in C+C_1 = C_1+C_2+\cdots+C_s+C_1$. Write $x' = x'_1+\cdots+x'_s+x'_{s+1}$ with $x'_1 \in C_1,\dots,x'_s \in C_1, x'_{s+1} \in C_1$, then we have $v\cdot x_1 \geq v\cdot x'_1,\dots,v\cdot x_{s+1} \geq v\cdot x'_{s+1}$. Therefore $v\cdot(x_1+\cdots+x_{s+1}) \geq v\cdot x'$ for every $x' \in C+C_1$, which yields $x_1+\cdots+x_{s+1} \in F$. This shows $F_1+F_2+\cdots+F_s+F_1 \subseteq F$.

We claim that we can find a sequence of edges $e_1,\dots,e_M$ in $E(\Gamma)$ satisfying the following conditions. (See Figure 12 for an illustration.)

(i) $\sigma(e_1) \in \{b_1\}\times F_1$.
(ii) For each $j=2,\dots,M$, there exists an index $i_j \in \{2,\dots,s\}$ such that the source vertex $\sigma(e_j)$ is in $\{b_{i_j}\}\times F_{i_j}$.
(iii) The indices $i_1 \coloneqq 1, i_2, i_3, \dots, i_M$ are distinct.
(iv) For $j=2,\dots,M$, the target vertex $\tau(e_{j-1})$ is in the lattice Λ_{i_j}.
(v) there exists $j \in \{1,\dots,M\}$ such that $\tau(e_{j-1})$ is in $\{b_{i_j}\}\times\left(C_{i_j}\setminus F_{i_j}\right)$.
(vi) $\tau(e_M) \in \Lambda_{i_m}$ for some $1 \leq m \leq M$.

For $i,j \in \{1,\dots,s\}$, we write $i \leftrightarrow j$ if there is an edge in $E(\Gamma)$ between $\{b_i\}\times F_i$ and $\{b_j\}\times F_j$. Let $\sim$ denote the transitive closure of the relation $\leftrightarrow$. That is, $i \sim j$ if and only if there exists a sequence of indices $l_1 = i, l_2, l_3, \dots, l_p = j$ such that for $k=1,\dots,p-1$, some edge $e_k \in E(\Gamma)$ starts in $\{b_{l_k}\}\times F_{l_k}$ and ends in $\{b_{l_{k+1}}\}\times F_{l_{k+1}}$.

We perform the following procedure. Let I_1 be the equivalent class of $\{1,\dots,s\}/\sim$ containing 1. Take a closed halfspace $\mathcal{H}$ of $\mathbb{R}^{s+n}$ such that $\mathcal{H}\cap\mathrm{conv}(\Gamma)\cap\Lambda = \bigcup_{i\in I_1}\{b_i\}\times F_i$. Since the strict face $\mathcal{H}\cap\mathrm{conv}(\Gamma)$ is accessible, there exists an edge e_{I_1} in Γ from $\bigcup_{i\in I_1}(\{b_i\}\times F_i)$ to $(\mathrm{conv}(\Gamma)\cap\Lambda)\setminus\bigcup_{i\in I_1}(\{b_i\}\times F_i)$. Since $\sim$ is the transitive closure of $\leftrightarrow$, the target of e_{I_1} must be in $\{b_j\}\times(C_j\setminus F_j)$ for some j. Otherwise, $\tau(e_{I_1}) \in \{b_j\}\times F_j$ for some j, so $j \in I_1$ by the definition of I_1, contradicting $\tau(e_{I_1}) \notin \bigcup_{i\in I_1}(\{b_i\}\times F_i)$.

If $j \in I_1$ then we stop the procedure, otherwise we denote by I_2 the $\sim$-equivalence class of j and repeat the above procedure. We stop repeating the procedure when we have found equivalence classes $I_1, I_2, \dots, I_T$ and an edge e_{I_T}, such that the target of e_{I_T} is in $\{b_j\}\times(C_j\setminus F_j)$ for some $j \in I_t$ with $1 \leq t \leq T$.

For $k=1,\dots,T-1$, there exists an edge $e_{I_k} \in E(\Gamma)$ from $\bigcup_{i\in I_k} F_i$ to $\bigcup_{i\in I_{k+1}}(C_i\setminus F_i)$. Also, there exists an edge

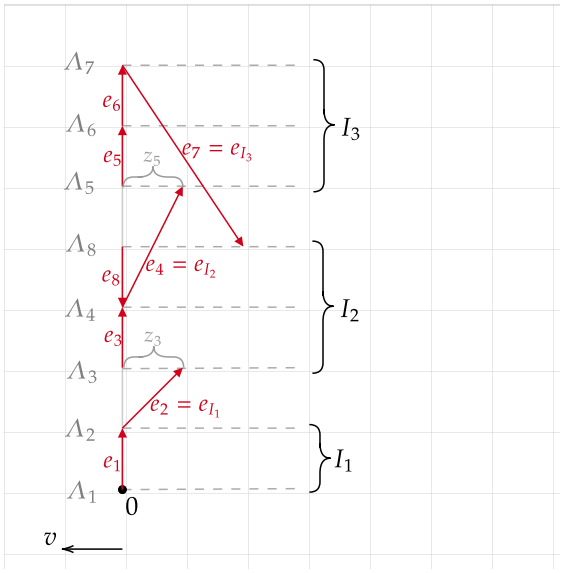

Fig. 12. edges e_i in the graph Γ

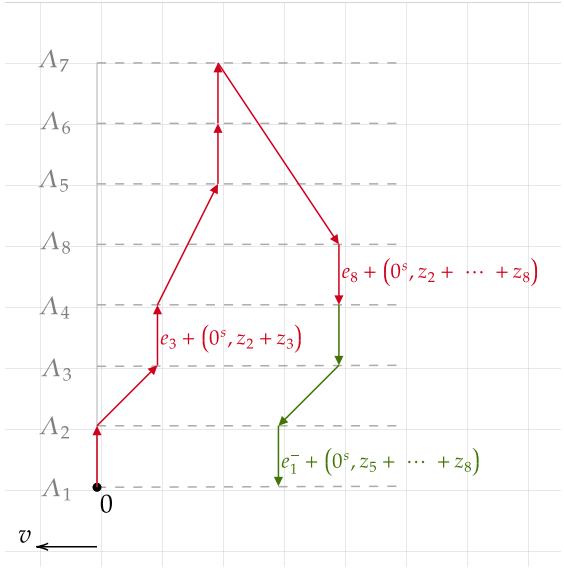

Fig. 13. the concatenated path P in Γ^C

$e_{I_T} \in E(\Gamma)$ from $\bigcup_{i\in I_T} F_i$ to $\bigcup_{i\in I_t}(C_i \setminus F_i)$. The vertices $\tau(e_{I_{k-1}})$ and $\sigma(e_{I_k})$ are both in $\bigcup_{i\in I_k}(\{b_i\}\times F_i)$, so there exists a distinct sequence of indices $i_{k,1},\dots,i_{k,l_k} \in I_k$, such that $\tau(e_{I_{k-1}}) \in \{b_{i_{k,1}}\}\times F_{i_{k,1}}, \sigma(e_{I_k}) \in \{b_{i_{k,l_k}}\}\times F_{i_{k,l_k}}$, and for $j = 1,\dots,l_k-1$, there exists an edge $e_{i_{k,j}}$ from $\{b_{i_{k,j}}\}\times F_{i_{k,j}}$ to $\{b_{i_{k,j+1}}\}\times F_{i_{k,j+1}}$.

Thus we get a sequence of edges

$$e_{i_{1,1}},\dots,e_{i_{1,l_1}},e_{I_1},e_{i_{2,1}},\dots,e_{i_{2,l_2}},e_{I_2},\\ \dots,e_{i_{T,1}},\dots,e_{i_{T,l_T}},e_{I_T}, \quad (16)$$

from the above procedure. We extend this sequence in the following way. Recall that $\tau(e_{I_T}) \in \{b_j\}\times(C_j\setminus F_j)$ for some $j \in I_t$ with $1 \le t \le T$. If j already appears among the indices $\{i_{t,1},\dots,i_{t,l_t}\}$, then we do not extend the sequence (16). Otherwise, since $j, i_{t,l_t} \in I_t$, there exists a sequence of indices $i_{T+1,1},\dots,i_{T+1,l_{T+1}} \in I_t \setminus \{i_{t,1},\dots,i_{t,l_t}\}$, such that $\tau(e_{I_T}) \in F_{i_{T+1,1}}$, and for $j = 1,\dots,l_{T+1}-1$, there exists an edge $e_{i_{T+1,j}}$ from $F_{i_{T+1,j}}$ to $F_{i_{T+1,j+1}}$. Furthermore, there exists an edge $e_{i_{T+1,l_{T+1}}}$ from $F_{i_{T+1,l_T}}$ to F_j with $j \in \{i_{t,1},\dots,i_{t,l_t}\}$. We then extend the sequence (16) with $e_{i_{T+1,1}},\dots,e_{i_{T+1,l_{T+1}}}$ and obtain a sequence

$$e_{i_{1,1}},\dots,e_{i_{1,l_1}},e_{I_1},e_{i_{2,1}},\dots,e_{i_{2,l_2}},e_{I_2},\\ \dots,e_{i_{T,1}},\dots,e_{i_{T,l_T}},e_{I_T},e_{i_{T+1,1}},\dots,e_{i_{T+1,l_{T+1}}}. \quad (17)$$

We rename this sequence of edges as $e_1,\dots,e_m$, and verify it satisfies the conditions (i)-(vi) listed at the beginning of this proof. The conditions (i), (ii), (iii), (iv) directly follow from the construction of the sequence (17). For condition (v) it suffices to note that the edge e_{I_1} defined in the construction has target in $(\mathrm{conv}(\Gamma)\cap\Lambda)\setminus\bigcup_{i\in I_1}(\{b_i\}\times F_i)$. For (vi) it suffices to note that the last edge $e_{i_{T+1,l_{T+1}}}$ in the sequence has target in F_j with $j \in \{i_{t,1},\dots,i_{t,l_t}\}$: in other words the index j has appeared earlier in the sequence.

By renaming the lattices $\Lambda_1,\dots,\Lambda_s$, we can suppose without loss of generality that $\sigma(e_i) \in \Lambda_i$ for $i = 1,2,\dots,M$, and $\tau(e_m) \in \Lambda_m$. In other words, the indices $i_1,\dots,i_M$ in conditions (i)-(vi) can respectively be assumed to be exactly $1,\dots,m$.

Notice that by applying a suitable linear transformation in $\mathsf{SL}(s+n,\mathbb{Z})$ to Γ and $\mathbb{Z}^{s+n}$, we can translate Λ_i by any vector in $\{0\}^s\times\mathbb{Z}^n$, without moving $\Lambda_j, j\neq i$. This translates the set C_i by the same vector, and therefore also translates C by a vector in $\{0\}^s\times\mathbb{Z}^n$. Therefore, the effect of this transformation on Γ^C is an *affine* transformation (a linear transformation plus a translation) that stabilizes Λ, and does not change the properties we are interested in for Γ^C. Therefore we can without loss of generality suppose that $\sigma(e_i) = b_i\times 0^n, i = 1,\dots,M$, and $b_i\times 0^n \in F_i$ for $i = M+1,\dots,s$. In particular, $0^n \in C_i$ for all $1\le i\le s$.

For each $i = 2,\dots,M$, let $z_i \in \mathbb{Z}^n$ be such that $\tau(e_{i-1}) = (0^s,z_i)+\sigma(e_i)$. Since $\sigma(e_i) = b_i\times 0^n$ and $\tau(e_{i-1}) \in \{b_i\}\times C_i$, we have $z_i \in C_i$. Recall that for an edge e we denote by e^- its inverse. Denote by P the concatenation of edges

$$e_1, e_2+(0^s,z_2), e_3+(0^s,z_2+z_3),\dots,\\ e_M+(0^s,z_2+z_3+\cdots+z_M),\\ e^-_{m-1}+(0^s,z_2+\cdots+z_{m-2}+z_m+\cdots+z_M),\\ \dots,e_1^-+(0^s,z_m+\cdots+z_M).$$

We claim that P is a path in Γ^C, and furthermore it starts in $\{b_1\}\times F$ and ends in $\{b_1\}\times((C+C_1)\setminus F)$.

Recall that $\sigma(e_1) \in \{b_1\}\times F_1$ by (i). Since $F_1 = F_1 + \{0^n\}+\cdots+\{0^n\} \subseteq F_1+F_2+\cdots+F_s+F_1 = F$, we indeed have $\sigma(e_1)\in\{b_1\}\times F$. Since $z_i\in C_i$ for each $i=2,\dots,m$ and $0^n\in C_1$, we have $z_2+\cdots+z_i \in C$ for all $2\le i\le M$ and $z_2+\cdots+z_i+z_m+\cdots+z_M\in C$ for all $1\le i\le m-1$. Therefore, each edge $e_i+(0^s,z_2+\cdots+z_i)\in e_i+\{0^s\}\times C$ and each edge $e_i^-+(0^s,z_2+\cdots+z_i+z_m+\cdots+z_M)\in e_i^-+\{0^s\}\times C$, is in $\Gamma^C = \sum_{z\in C\cap\mathbb{Z}^n}\Gamma+(0^s,z)$. Consequently, every edge in P belongs to Γ^C. We now show it ends in $\{b_i\}\times((C+C_i)\setminus F)$.

It suffices to show that $z_m+\cdots+z_M$ is not orthogonal to v. Indeed, each edge $e_i, i=1,\dots,M$ starts in F_i, meaning $v\cdot z_i = (0^s,v)\cdot(\sigma(e_i)-\tau(e_{i-1}))\ge 0$. Furthermore, condition (v) shows there exists $j\in\{1,\dots,M\}$ such that $\tau(e_{j-1})\in\{b_{i_j}\}\times\left(C_{i_j}\setminus F_{i_j}\right)$, meaning $v\cdot z_j$ is strictly positive. We therefore conclude that P is a path in Γ^C starting in $\{b_1\}\times F$ and ending in $\{b_1\}\times((C+C_1)\setminus F)$. □

We now without loss of generality replace Γ with Γ^C, this does not change the fact that Γ is full-image and symmetric. Thus by Lemma B.1, the new Γ satisfies the following property: for each $i\in\{1,\dots,s\}$, and each strict face $\{b_i\}\times F$ of the convex hull $\mathrm{conv}(\Gamma\cap\Lambda_i)$, there exists a path in Γ starting in $\{b_i\}\times F$ and ending in $\mathrm{conv}(\Gamma\cap\Lambda_i)\setminus F$. Furthermore, each $\mathrm{conv}(\Gamma\cap\Lambda_i)$ is of dimension n.

Now, the convex hull of $V(\Gamma)\cap\Lambda_i$ is a polytope of the form $\{b_i\}\times C_i$, where C_i is a polytope in $\mathbb{R}^n$. This time, each C_i is of dimension n. Consider the Minkowski sum $C \coloneqq C_1+\cdots+C_s$.

For each $N\in\mathbb{N}$, define

$$\Gamma^{NC} \coloneqq \sum_{z\in NC\cap\mathbb{Z}^n}\Gamma+(0^s,z).$$

We will show that there exists N such that Γ^{NC} is connected.

Fix $i\in\{1,\dots,s\}$, consider the (undirected) graph $\Gamma(i)$ over $\mathbb{Z}^n$, defined as follows. The set of vertices of $\Gamma(i)$ is $\{v\in\mathbb{Z}^n \mid (b_i,v)\in V(\Gamma)\cap\Lambda_i\}$. Two vertices v,v' in $\Gamma(i)$ are connected by an edge if v and v' are connected by a path in Γ. Then by Lemma B.1, the graph $\Gamma(i)$ satisfies the following property: for each strict face F of $\mathrm{conv}(\Gamma(i))$ there exists an edge with source in F and target outside F. This is exactly the definition of face-accessibility as in [14, Section 3.1].

Define

$$\Gamma(i)^{(N-1)C_i} \coloneqq \bigcup_{z\in(N-1)C_i}\Gamma(i)+z,$$

then $\mathrm{conv}(\Gamma(i)^{(N-1)C_i}) = (N-1)C_i+C_i = NC_i$. For $c\in\mathbb{R}^n, R\in(0,1), S\subseteq\mathbb{R}^n$, define

$$scale(S,c,R) \coloneqq \{c+R\cdot(x-c)\mid x\in S\}.$$

Intuitively, $scale(S, c, R)$ is the scaling of the set S with proportion R, and c is the invariant point of the scaling.

Lemma B.2 ([14, Lemma 4.6]). *Let $c_0 \in \mathbb{Q}^n$ be an interior point of C_i. There exists $N_i \in \mathbb{N}, R \in (0,1)$, such that if $N > 0$ is divisible by N_i, then every vertex in the graph $\Gamma(i)^{(N-1)C_i}$ is connected by a path to some vertex in $scale(NC_i, Nc_0, R)$.*[7]

See Figure 14 for an illustration of Lemma B.2.

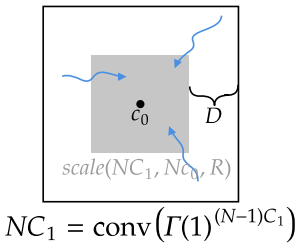

Fig. 14. Illustration of Lemma B.2 with $n = 2$, $i = 1$.

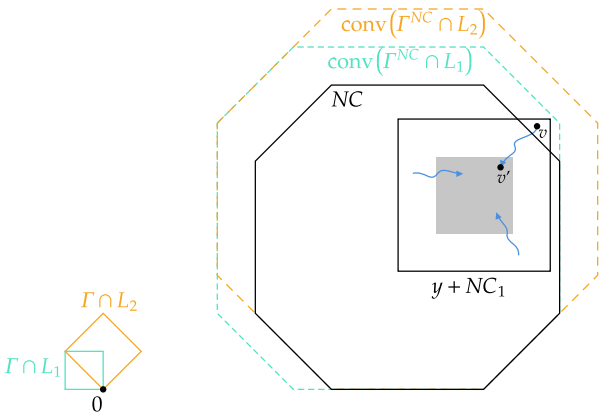

Fig. 15. Illustration for Lemma B.3, projected on $\mathbb{Z}^n$. Here, $n = 2, s = 2, i = 1$.

Denote by $d_j \in \mathbb{Z}^n, j = 1, \ldots, n$ the natural basis of $\mathbb{Z}^n$, that is, d_j is the vector with 1 on the j-th coordinate and 0 elsewhere. Since $\mathcal{A}$ is primitive and Γ is full-image, for each $d_j, j = 1, \ldots, n$, there exists a concatenation Q_{1j} of $(\{0\}^s \times \mathbb{Z}^n)$-translations of edges in Γ that goes from $(b_1, 0^n)$ to (b_1, d_j). (Recall that for each $e \in E(\Gamma)$ we have added $e^- \in E(\Gamma)$.) For $i = 1, \ldots, s$, by additionally appending paths to and from Λ_i, we obtain a concatenation Q_{ij} of $(\{0\}^s \times \mathbb{Z}^n)$-translations of edges in Γ that goes from $(b_i, 0^n)$ to (b_i, d_j).

[7]Note that by taking Γ in [14, Section 4] to be the graph $\Gamma(i)$ defined here and by taking C to be C_i, the graph Γ_N defined in [14, Section 4] corresponds to the graph $\Gamma(i)^{(N-1)C_i}$ defined above. This is because the set $S_N := \{z \in \mathbb{Z}^n \mid z + C \subset NC\}$ defined in the beginning of [14, Section 4] corresponds exactly to $\mathbb{Z}^n \cap (N-1)C_i$. Indeed, using the notation of [14, Section 4], we have $(N-1)C + C = NC$, so $(N-1)C \subseteq \{z \in \mathbb{R}^n \mid z + C \subset NC\}$. On the other hand, take $v \notin (N-1)C$, taking a linear transformation we can suppose $v = 0^n$, then $v + C = C \not\subset NC$ because the distance from NC to 0^n is strictly larger than the distance from C to 0^n. Therefore $v \notin \{z \in \mathbb{R}^n \mid z + C \subset NC\}$. We conclude that $\mathbb{Z}^n \cap (N-1)C = \mathbb{Z}^n \cap \{z \in \mathbb{R}^n \mid z + C \subset NC\} = S_N$.

More precisely, for every $i \in \{1, \ldots, s\}, j \in \{1, \ldots, n\}$, there exist edges $e_1, \ldots, e_m$ in Γ, satisfying the following properties.

(i) $\sigma(e_1), \tau(e_m) \in \Lambda_i$.

(ii) For $k = 2, \ldots, m$, both $\tau(e_{k-1})$ and $\sigma(e_k)$ are in some same lattice Λ_{l_k}. In particular, both $\tau(e_{k-1})$ and $\sigma(e_k)$ belong to $\{b_{l_k}\} \times C_{l_k}$. Write $\tau(e_{k-1}) - \sigma(e_k) = (0^s, z_k)$ with $z_k \in \mathbb{Z}^n$.

(iii) The concatenation of $e_1, e_2 + (0^s, z_2), e_3 + (0^s, z_2 + z_3), \ldots, e_m + (0^s, z_2 + \cdots + z_m)$ is a path from $\sigma(e_1)$ to $\sigma(e_1) + (0^s, d_j)$. We denote by Q_{ij} this concatenation.

(iv) We additionally define the value $D_{ij} := \max\{\|z_2\|, \|z_2 + z_3\|, \ldots, \|z_2 + \cdots + z_m\|\} \in \mathbb{R}_{\geq 0}$.

For two sets $S, S' \subseteq \mathbb{R}^n$, define their *distance* as $\mathrm{dist}(S, S') := \inf_{x \in S, x' \in S'} \|x - x'\|$. For a set $S \subseteq \mathbb{R}^n$, define its *diameter* as $\mathrm{diam}(S) := \sup_{x, x' \in S} \|x - x'\|$. Denote

$$D := \max_{1 \leq i \leq s, 1 \leq j \leq n} \{D_{ij}\} + \sqrt{n} + \max_{1 \leq i \leq s} \{\mathrm{diam}(C_i)\}.$$

Lemma B.3. *There exists an integer $N \in \mathbb{N}$ such that in the graph Γ^{NC}, for every $i \in \{1, \ldots, s\}$, every vertex $(b_i, v) \in V(\Gamma^{NC} \cap \Lambda_i)$ is connected to some other vertex $(b_i, v') \in V(\Gamma^{NC} \cap \Lambda_i)$ that is of distance at least D from the boundary of $\mathrm{conv}(\Gamma^{NC} \cap \Lambda_i)$.*

Proof. See Figure 15 for an illustration of the proof. Let $N_i, i = 1, \ldots, s$, be as defined in Lemma B.2. Let N be a large enough multiple of $N_1 N_2 \cdots N_s$, such that the distance between $scale(NC_i, Nc_0, R)$ and the boundary of C_i is at least D. Let (b_i, v) be a vertex of $\Gamma^{NC} \cap \Lambda_i$, it appears in some translated graph $\Gamma + (0^s, z)$ with $z \in NC$. Then, $(b_i, v - z) \in V(\Gamma)$. Since $z \in NC$, there exists some translation $y + (N-1)C_i$ of $(N-1)C_i$ such that $z \in y + (N-1)C_i \subseteq NC$. By Lemma B.2, (b_i, v) is connected in $y + \Gamma(i)^{(N-1)C_i}$, and hence also in Γ^{NC}, to some vertex (b_i, v') in $y + scale(NC_i, Nc_0, R)$. Since v' is of distance at least D from the boundary of $(b_i, y) + NC_i$, it is also of distance at least D from the boundary of $\mathrm{conv}(\Gamma^{NC} \cap \Lambda_i) = NC + (b_i, 0^n) + C_i \supseteq (b_i, y) + (N-1)C_i + C_i = (b_i, y) + NC_i$. □

Lemma B.4 (Generalization of [14, Lemma 4.7]). *Two vertices $(b_i, v_1), (b_i, v_2) \in V(\Gamma^{NC} \cap \Lambda_i)$ of distance at least D from the boundary of $\mathrm{conv}(\Gamma^{NC} \cap \Lambda_i)$ are connected in Γ^{NC}.*

Proof. Upon applying a transformation in $\mathsf{SL}(s+n, \mathbb{Z})$ to $\Gamma \subseteq \mathbb{Z}^{s+n}$, we now without loss of generality suppose $0^n \in C_i$ for all i.

For two points $x, x' \in \mathbb{R}^n$, define the *segment* $seg(x, x') := \{rx + (1-r)x' \mid r \in [0,1]\} \subseteq \mathbb{R}^n$. Since $(b_i, v_1), (b_i, v_2) \in \Lambda_i$, are of distance at least D from the boundary of $\mathrm{conv}(\Gamma^{NC} \cap \Lambda_i) \subseteq \{b_i\} \times (NC + C_i)$, they are of distance at least $D - \mathrm{diam}(C_i) \geq \max_{i,j}\{D_{ij}\} + \sqrt{n}$ from the boundary of $\{b_i\} \times NC$. Hence, every point in the segment $seg(v_1, v_2)$ is of distance at least $\max_{i,j}\{D_{ij}\} + \sqrt{n}$ from the boundary of NC.

There exists a path $P_{\mathbb{Z}^n}(v_1, v_2)$ in the lattice Λ_i from (b_i, v_1) to (b_i, v_2), consisting of translations of the segments $\{b_i\} \times seg(0^n, d_k), k = 1, \ldots, n$, such that each point in

$P_{\mathbb{Z}^n}(v_1, v_2)$ is of distance at most $\sqrt{n}$ from the segment $\{b_i\} \times seg(v_1, v_2)$. For $k = 1, \ldots, n$, replacing each segment $\{b_i\} \times (z + seg(0^n, d_k))$ in $P_{\mathbb{Z}^n}(v_1, v_2)$ by the translation $Q_{ik} + (0^n, z)$ of the path Q_{ik}, we obtain a path $P_\Gamma(v_1, v_2)$. We now show that each edge of $P_\Gamma(v_1, v_2)$ is in $E(\Gamma^{NC})$.

By definition of the concatenation Q_{ik}, Each edge in $Q_{ik} + (0^n, z)$ appears in a translation $\Gamma + (0^n, z + z')$ of the graph Γ satisfying $\|z'\| \leq D_{ik}$. Since (b_i, z) is of distance at most $\sqrt{n}$ from the segment $\{b_i\} \times seg(v_1, v_2)$, and every point in the segment $\{b_i\} \times seg(v_1, v_2)$ is of distance at least $\max_{i,j}\{D_{ij}\} + \sqrt{n}$ from the boundary of $\{b_i\} \times NC$, we conclude that (b_i, z) is of distance at least $\max_{i,j}\{D_{ij}\}$ from the boundary of $\{b_i\} \times NC$. Therefore, $(b_i, z+z')$ is within the boundary of $\{b_i\} \times NC$ because $\|z'\| \leq \max\{D_{ij}\}$. In other words, $z + z' \in NC$, the translation $\Gamma + (0^n, z + z')$ appears as a subgraph of Γ^{NC}. This shows that the path $P_\Gamma(v_1, v_2)$ connecting v_1 and v_2 is a subgraph of Γ^{NC}. □

Proof of Theorem 4.7. See Figure 11 for an illustration of the proof. Let N be the integer defined in Lemma B.3, we show that $\widehat{\Gamma} := \Gamma^{NC} = \sum_{z \in NC \cap \mathbb{Z}^n} \Gamma + (0^s, z)$ is connected. First we show that for any $i \in \{1, \ldots, s\}$, every two vertices $(b_i, v), (b_i, w)$ in $\Gamma^{NC} \cap \Lambda_i$ are connected. Indeed, by Lemma B.3, (b_i, v) and (b_i, w) are respectively connected to vertices $(b_i, v'), (b_i, w')$, which are of distance at least D from the boundary of $\mathrm{conv}(\Gamma^{NC} \cap \Lambda_i)$. By Lemma B.4, (b_i, v') and (b_i, w') are connected in Γ^{NC}. Therefore, (b_i, v) and (b_i, w) are connected in Γ^{NC}.

This shows that for any $i \in \{1, \ldots, s\}$, all vertices in $\Gamma^{NC} \cap \Lambda_i$ lie in the same connected component of Γ^{NC}. Since the $\mathcal{A}$-graph Γ^{NC} is full-image and the automaton $\mathcal{A}$ is trim, the different lattices $\Gamma^{NC} \cap \Lambda_i$ connected to each other by edges in Γ^{NC} form a single connected component. Therefore Γ^{NC} is connected. Since Γ^{NC} is also symmetric, it is Eulerian. □

APPENDIX C
PROOF OF THEOREM 4.14

In this section of the appendix we prove Theorem 4.14:

Theorem 4.14. *Denote $\mathbb{A} := \mathbb{R}[\overline{X}^{\pm}], \mathbb{A}^+ := \mathbb{R}_{\geq 0}[\overline{X}^{\pm}]^*$. Fix $n \in \mathbb{N}$ and let Ξ be a finite set of indices. Suppose we are given as input a set of generators $\boldsymbol{g}_1, \ldots, \boldsymbol{g}_m \in \mathbb{A}^K$ with integer coefficients, the vectors $\widetilde{a}_1, \ldots, \widetilde{a}_K \in \mathbb{Z}^n$, as well as subsets $I_\xi, J_\xi \subseteq \{1, \ldots, K\}$ for each $\xi \in \Xi$. Denote by $\mathcal{M}$ be the $\mathbb{A}$-submodule of $\mathbb{A}^K$ generated by $\boldsymbol{g}_1, \ldots, \boldsymbol{g}_m$. It is decidable whether there exists $\boldsymbol{f} \in \mathcal{M} \cap (\mathbb{A}^+)^K$ satisfying*

$$(O_v \cup J_\xi) \cap M_v(I_\xi, \boldsymbol{f}) \neq \emptyset, \quad \text{for every } v \in (\mathbb{R}^n)^*, \xi \in \Xi. \tag{8}$$

Here, if $n = 0$ then $\mathbb{A}$ is understood as $\mathbb{R}$, and Property (8) is considered trivially true.

Our proof strictly follows the proof of [14, Theorem 3.9] provided in [14, Sections 5-6]. We recall [14, Theorem 3.9] for comparison:

Theorem C.1 ([14, Theorem 3.9])**.** *Denote $\mathbb{A} := \mathbb{R}[\overline{X}^{\pm}], \mathbb{A}^+ := \mathbb{R}_{\geq 0}[\overline{X}^{\pm}]^*$. Fix $n \in \mathbb{N}$. Suppose we are given as input a set of generators $\boldsymbol{g}_1, \ldots, \boldsymbol{g}_m \in \mathbb{A}^K$ with integer coefficients, as well as the vectors $\widetilde{a}_1, \ldots, \widetilde{a}_K \in \mathbb{Z}^n$ and two subsets I, J of $\{1, \ldots, K\}$. Denote by $\mathcal{M}$ be the $\mathbb{A}$-submodule of $\mathbb{A}^K$ generated by $\boldsymbol{g}_1, \ldots, \boldsymbol{g}_m$. It is decidable whether there exists $\boldsymbol{f} \in \mathcal{M} \cap (\mathbb{A}^+)^K$ satisfying*

$$(O_v \cup J) \cap M_v(I, \boldsymbol{f}) \neq \emptyset, \quad \text{for every } v \in (\mathbb{R}^n)^*. \tag{18}$$

Here, if $n = 0$ then $\mathbb{A}$ is understood as $\mathbb{R}$, and Property (18) is considered trivially true.

We need to add the quantifier "for all $\xi \in \Xi$" in appropriate places of the proof and modify a few definitions and lemmas accordingly.

A. Local-global principle

Given $f \in \mathbb{A}$ and $v \in (\mathbb{R}^n)^*$, the *initial polynomial* of f is defined as the sum of all monomials in f having the maximal degree $\deg_v(\cdot)$:

$$\mathrm{in}_v(f) := \sum\nolimits_{\deg_v(\overline{X}^b) = \deg_v(f)} c_b \overline{X}^b, \quad \text{where } f = \sum c_b \overline{X}^b.$$

For $\boldsymbol{f} = (f_1, \ldots, f_K) \in \mathbb{A}^K$, we naturally denote $\mathrm{in}_v(\boldsymbol{f}) := (\mathrm{in}_v(f_1), \ldots, \mathrm{in}_v(f_K)) \in \mathbb{A}^K$.

In this subsection we prove the following local-global principle:

Theorem C.2 (Generalization of [14, Theorem 3.8])**.** *Let $\mathcal{M}$ be an $\mathbb{A}$-submodule of $\mathbb{A}^K$ and $I_\xi, J_\xi, \xi \in \Xi$ be subsets of $\{1, \ldots, K\}$. There exists $\boldsymbol{f} \in \mathcal{M} \cap (\mathbb{A}^+)^K$ satisfying*

$$(O_v \cup J_\xi) \cap M_v(I_\xi, \boldsymbol{f}) \neq \emptyset, \quad \text{for every } v \in (\mathbb{R}^n)^*, \xi \in \Xi \tag{19}$$

if and only if the two following conditions are satisfied:

1. **(LocR):** *For every $r \in \mathbb{R}^n_{>0}$, there exists $\boldsymbol{f}_r \in \mathcal{M}$ such that $\boldsymbol{f}_r(r) \in \mathbb{R}^K_{>0}$.*
2. **(LocInf):** *For every $v \in (\mathbb{R}^n)^*$, there exists $\boldsymbol{f}_v \in \mathcal{M}$,*
   a) $\mathrm{in}_v(\boldsymbol{f}_v) \in (\mathbb{A}^+)^K$.
   b) Denote $I'_\xi := M_v(I_\xi, \boldsymbol{f}_v), J'_\xi := O_v \cup J_\xi$. We have

$$\left(O_w \cup J'_\xi\right) \cap M_w(I'_\xi, \mathrm{in}_v(\boldsymbol{f}_v)) \neq \emptyset \tag{20}$$

for every $w \in (\mathbb{R}^n)^*, \xi \in \Xi$.

Define the quotient $D_n := (\mathbb{R}^n)^* / \mathbb{R}_{>0}$. That is, elements of D_n are of the form $v\mathbb{R}_{>0}, v \in (\mathbb{R}^n)^*$, where $v\mathbb{R}_{>0} = v'\mathbb{R}_{>0}$ if and only if $v = r \cdot v'$ for some $r \in \mathbb{R}_{>0}$. The quotient D_n can be identified with the unit sphere of dimension n since every $v\mathbb{R}_{>0}$ is equal to exactly one $v'\mathbb{R}_{>0}$ with $||v'|| = 1$. We equip D_n with the standard topology of the unit sphere. Note that $\mathrm{in}_v(\cdot), M_v(\cdot)$ and O_v are invariant when scaling v by any positive real number.

Lemma C.3 ([14, Theorem 5.1])**.** *Fix $v \in (\mathbb{R}^n)^*$, a set $I_\xi \subseteq \{1, \ldots, K\}$ and $\boldsymbol{f} \in \mathbb{A}^K$. There exists an open neighbourhood $U \subseteq D_n$ of $v\mathbb{R}_{>0}$, such that for every $w \in (\mathbb{R}^n)^*$ with $(v + w)\mathbb{R}_{>0} \in U$, we have*

$$\mathrm{in}_{v+w}(\boldsymbol{f}) = \mathrm{in}_w(\mathrm{in}_v(\boldsymbol{f})),$$
$$M_{v+w}(I_\xi, \boldsymbol{f}) = M_w(M_v(I_\xi, \boldsymbol{f}), \mathrm{in}_v(\boldsymbol{f})),$$

and $O_{v+w} = O_v \cup O_w$. (21)

With Lemma C.3 we can prove the "only if" part of Theorem C.2:

Proof of "only if" part of Theorem C.2. Suppose $\boldsymbol{f} \in \mathcal{M} \cap (\mathbb{A}^+)^K$ satisfies Property (19). To show (LocR), simply take $\boldsymbol{f}_r \coloneqq \boldsymbol{f}$ for all $r \in \mathbb{R}^n_{>0}$, then $\boldsymbol{f}(r) \in \mathbb{R}^K_{>0}$. As for (LocInf), for every $v \in (\mathbb{R}^n)^*$ we show that $\boldsymbol{f}_v \coloneqq \boldsymbol{f}$ satisfies Properties (LocInf)(a) and (b). Property (LocInf)(a) is satisfied by the definition of $\boldsymbol{f}$. We now show Property (LocInf)(b). Take any $w \in (\mathbb{R}^n)^*$ and $\xi \in \Xi$.

When $w \in v\mathbb{R}_{>0}$, we have $O_w \cup J'_\xi = O_w \cup O_v \cup J_\xi = O_v \cup J_\xi$ and

$$\begin{aligned} M_w(I'_\xi, \mathrm{in}_v(\boldsymbol{f})) &= M_w(M_v(I_\xi, \boldsymbol{f}), \mathrm{in}_v(\boldsymbol{f})) \\ &= M_v(M_v(I_\xi, \boldsymbol{f}), \mathrm{in}_v(\boldsymbol{f})) = M_v(I_\xi, \boldsymbol{f}), \end{aligned}$$

so Property (LocInf)(b) is equivalent to $(O_v \cup J_\xi) \cap M_v(I_\xi, \boldsymbol{f}) \neq \emptyset$. This is exactly the Property (19) satisfied by $\boldsymbol{f}$.

When $w \notin v\mathbb{R}_{>0}$, let $U \subseteq D_n$ be the open neighbourhood of $v\mathbb{R}_{>0}$ defined in Lemma C.3. Scaling w by a small enough positive real we can suppose $(v+w)\mathbb{R}_{>0} \in U$. We have

$$\begin{aligned} &\mathrm{in}_{v+w}(\boldsymbol{f}) = \mathrm{in}_w(\mathrm{in}_v(\boldsymbol{f})), \\ &M_{v+w}(I_\xi, \boldsymbol{f}) = M_w(I'_\xi, \mathrm{in}_v(\boldsymbol{f})), \\ \text{and } &O_{v+w} = O_v \cup O_w. \end{aligned}$$

where $I'_\xi = M_v(I_\xi, \boldsymbol{f})$. Therefore $(O_{v+w} \cup J_\xi) \cap M_{v+w}(I_\xi, \boldsymbol{f}) = (O_w \cup O_v \cup J_\xi) \cap M_w(I'_\xi, \mathrm{in}_v(\boldsymbol{f})) = \left(O_w \cup J'_\xi\right) \cap M_w(I'_\xi, \mathrm{in}_v(\boldsymbol{f}))$. Since $\boldsymbol{f}$ satisfies Property (19), we have $(O_{v+w} \cup J_\xi) \cap M_{v+w}(I_\xi, \boldsymbol{f}) \neq \emptyset$. Therefore we also have $\left(O_w \cup J'_\xi\right) \cap M_w(I'_\xi, \mathrm{in}_v(\boldsymbol{f})) \neq \emptyset$ for all $w \notin v\mathbb{R}_{>0}$. □

We now start working towards proving the "if" part of Theorem C.2. The main idea is a "gluing" procedure. The following lemma is the foundation of this gluing argument. It shows the "continuity" of the property (LocInf) when changing the direction v by a small amount.

Lemma C.4 (Generalization of [14, Lemma 5.2])**.** *Suppose $v \in (\mathbb{R}^n)^*$ and $\boldsymbol{f}_v \in \mathcal{M}$ satisfy properties (LocInf)(a) and (b) of Theorem C.2. Then there exists an open neighbourhood $U_v \subseteq D_n$ of $v\mathbb{R}_{>0}$ such that for every $v'\mathbb{R}_{>0} \in U_v, \xi \in \Xi$,*

(i) $\mathrm{in}_{v'}(\boldsymbol{f}_v) \in (\mathbb{A}^+)^K$.

(ii) $(O_{v'} \cup J_\xi) \cap M_{v'}(I_\xi, \boldsymbol{f}_v) \neq \emptyset$.

Proof. We use Lemma C.3 on v, I_ξ and $\boldsymbol{f}_v$ to obtain an open neighbourhood $U_{v,\xi} \subseteq D_n$ of $v\mathbb{R}_{>0}$, where for all $(v+w)\mathbb{R}_{>0} \in U_{v,\xi}$ we have

$$\begin{aligned} &\mathrm{in}_{v+w}(\boldsymbol{f}_v) = \mathrm{in}_w(\mathrm{in}_v(\boldsymbol{f}_v)), \\ &M_{v+w}(I_\xi, \boldsymbol{f}_v) = M_w(M_v(I_\xi, \boldsymbol{f}_v), \mathrm{in}_v(\boldsymbol{f}_v)), \\ \text{and } &O_{v+w} = O_v \cup O_w. \end{aligned}$$

Note that $\mathrm{in}_v(\boldsymbol{f}_v) \in (\mathbb{A}^+)^K$ by Property (LocInf)(a) of $\boldsymbol{f}_v$. Take $U_v \coloneqq \bigcap_{\xi \in \Xi} U_{v,\xi}$. Since taking the initial polynomial of any polynomial in $\mathbb{A}^+$ yields an element of $\mathbb{A}^+$, we have $\mathrm{in}_{v+w}(\boldsymbol{f}_v) = \mathrm{in}_w(\mathrm{in}_v(\boldsymbol{f}_v)) \in (\mathbb{A}^+)^K$. Furthermore, $(O_{v+w} \cup J_\xi) \cap M_{v+w}(I_\xi, \boldsymbol{f}_v) = \left(O_w \cup J'_\xi\right) \cap M_w(I'_\xi, \mathrm{in}_v(\boldsymbol{f}_v))$, which is non-empty by Property (LocInf)(b) of $\boldsymbol{f}_v$. Therefore, both (i) and (ii) are satisfied for $v'\mathbb{R}_{>0} \in U_v$. □

The following lemma shows that one can "glue" all different $\boldsymbol{f}_v, v \in (\mathbb{R}^n)^*$ together to obtain a single $\boldsymbol{f}$ that has positive initial polynomial at every direction $v \in (\mathbb{R}^n)^*$.

Lemma C.5 (Generalization of [14, Lemma 5.3])**.** *Suppose Condition (LocInf) of Theorem C.2 is satisfied. Then there exists $\boldsymbol{f} \in \mathcal{M}$ that satisfies*

(i) $\mathrm{in}_v(\boldsymbol{f}) \in (\mathbb{A}^+)^K$ *for all* $v \in (\mathbb{R}^n)^*$.

(ii) $(O_v \cup J_\xi) \cap M_v(I_\xi, \boldsymbol{f}) \neq \emptyset$ *for all* $v \in (\mathbb{R}^n)^*, \xi \in \Xi$.

Proof. The exact same proof as [14, Lemma 5.3] works, we only need to replace the usage of [14, Lemma 5.2] by the usage of Lemma C.4. □

Denote by $\boldsymbol{f}_\infty$ the element $\boldsymbol{f} \in \mathcal{M}$ obtained in Lemma C.5. Since $\mathrm{in}_v(\boldsymbol{f}_\infty) \in (\mathbb{A}^+)^K$ for all $v \in (\mathbb{R}^n)^*$, there exists $c > 1$ such that $\boldsymbol{f}_\infty(x) \in \mathbb{R}^K_{>0}$ for all $x \in \mathbb{R}^n_{>0} \setminus [1/c, c]^n$. Define the compact set

$$C \coloneqq [1/(4nc), 4nc]^n \supseteq [1/c, c]^n.$$

Lemma C.6 ([14, Lemma 5.4])**.** *Let $\mathcal{M}$ be an $\mathbb{A}$-submodule of $\mathbb{A}^K$ and $C \subset \mathbb{R}^n_{>0}$ be a compact set. Suppose for all $r \in C$ there exists $\boldsymbol{f}_r \in \mathcal{M}$ with $\boldsymbol{f}_r(r) \in \mathbb{R}^K_{>0}$. Then there exists $\boldsymbol{f} \in \mathcal{M}$ such that $\boldsymbol{f}(x) \in \mathbb{R}^n_{>0}$ for all $x \in C$.*

Denote by $\boldsymbol{f}_C$ the element $\boldsymbol{f} \in \mathcal{M}$ obtained in Lemma C.6.

Lemma C.7 ([14, Corollary 5.6])**.** *Let $\boldsymbol{f} \in \mathbb{A}^K$. There exists $g \in \mathbb{A}^+$ such that $g\boldsymbol{f} \in (\mathbb{A}^+)^K$ if and only if the two following conditions are satisfied:*

(i) For all $r \in \mathbb{R}^n_{>0}$, we have $\boldsymbol{f}(r) \in \mathbb{R}^K_{>0}$.

(ii) For all $v \in (\mathbb{R}^n)^*$ and $r \in \mathbb{R}^n_{>0}$, we have $\mathrm{in}_v(\boldsymbol{f})(r) \in \mathbb{R}^K_{>0}$.

We are now ready to prove the "if" part of Theorem C.2 by "gluing" together the elements $\boldsymbol{f}_\infty, \boldsymbol{f}_C \in \mathcal{M}$ obtained respectively in Lemma C.5 and C.6.

Proof of "if" part of Theorem C.2. Let $\boldsymbol{f}_\infty, \boldsymbol{f}_C \in \mathcal{M}$ be the elements obtained respectively in Lemma C.5 and C.6. Define the polynomial

$$q \coloneqq \frac{1}{2nc} \sum_{i=1}^n (X_i + X_i^{-1}) \in \mathbb{A}^+.$$

It is easy to see that we have $\deg_w(q) > 0$ for all $w \in (\mathbb{R}^n)^*$. By the compactness of the unit sphere, the value $\min_{||w||=1} \deg_w(q)$ exists and is a positive number.

Let $\epsilon > 0$ be such that

$$\epsilon \cdot \boldsymbol{f}_\infty(x) + \boldsymbol{f}_C(x) \in \mathbb{R}^n_{>0} \tag{22}$$

for all $x \in C$. Such an ϵ exists by the compactness of C. We claim that there exists $N \in \mathbb{N}$ such that the vector $\boldsymbol{f} \coloneqq$

$\epsilon q^N \cdot \boldsymbol{f}_\infty + \boldsymbol{f}_C$ satisfies Conditions (i) and (ii) in Corollary C.7 simultaneously.

Let $M \in \mathbb{N}$ be such that $\deg_v(f_{\infty,i}) + M \cdot \min_{||w||=1} \deg_w(q) > \deg_v(f_{C,i})$ for all $v \in (\mathbb{R}^n)^*, ||v|| = 1$ and $i = 1, \dots, K$. Such an M exists by the compactness of the unit sphere and because $\min_{||w||=1} \deg_w(q) > 0$. Let $\boldsymbol{g} \coloneqq \epsilon q^M \cdot \boldsymbol{f}_\infty + \boldsymbol{f}_C$. Then for all $v \in (\mathbb{R}^n)^*, i = 1, \dots, K$, we have $\deg_v(\epsilon q^M \cdot f_{\infty,i}) = M \cdot \deg_v(q) + \deg_v(f_{\infty,i}) > \deg_v(f_{C,i})$. Therefore $\mathrm{in}_v(\boldsymbol{g}) = \mathrm{in}_v(\epsilon q^M \cdot \boldsymbol{f}_\infty) \in (\mathbb{A}^+)^K$ for all $v \in (\mathbb{R}^n)^*$. Therefore, there exists another compact set $[1/d, d]^n \supset C$ such that $\boldsymbol{g}(x) \in \mathbb{R}^K_{>0}$ for all $x \in \mathbb{R}^n_{>0} \setminus [1/d, d]^n$. Since $[1/d, d]^n \supset C = [1/(4nc), 4nc]^n$, we have $d \geq 4nc$. Since the set $[1/d, d]^n \setminus (1/(4nc), 4nc)^n$ is compact and $\boldsymbol{f}_\infty(x) \in \mathbb{R}^K_{>0}$ for all $x \in [1/d, d]^n \setminus (1/(4nc), 4nc)^n$, there exists $N > M$ such that

$$\epsilon f_{\infty,i}(x) \cdot 2^N + f_{C,i}(x) > 0 \tag{23}$$

for all $x \in [1/d, d]^n \setminus (1/(4nc), 4nc)^n$ and all $i = 1, \dots, K$. We prove that for this N, the element $\boldsymbol{f} \coloneqq \epsilon q^N \cdot \boldsymbol{f}_\infty + \boldsymbol{f}_C$ satisfies Conditions (i) and (ii) in Corollary C.7 simultaneously.

Fix any $i \in \{1, \dots, K\}$. For every $x \in \mathbb{R}^n_{>0} \setminus [1/d, d]^n$, we have $q(x) > \frac{d}{2nc} \geq 1$ and $f_{\infty,i}(x) > 0$, so

$$\begin{aligned} f_i(x) &= \epsilon q(x)^N \cdot f_{\infty,i}(x) + f_{C,i}(x) \\ &\geq \epsilon q(x)^M \cdot f_{\infty,i}(x) + f_{C,i}(x) = g_i(x) > 0. \end{aligned}$$

For every $x \in [1/d, d]^n \setminus C = [1/d, d]^n \setminus [1/(4nc), 4nc]^n$, we have $x_{i'} \geq 4nc$ for at least one $i' \in \{1, \dots, K\}$. Since $f_{\infty,i}(x) > 0$ by the definition of C, we have

$$\begin{aligned} f_i(x) &= \epsilon f_{\infty,i}(x) \cdot \left(\sum_{j=1}^n \frac{x_j + x_j^{-1}}{2nc} \right)^N + f_{C,i}(x) \\ &\geq \epsilon f_{\infty,i}(x) \cdot 2^N + f_{C,i}(x) > 0 \end{aligned}$$

by $\sum_{j=1}^n (x_j + x_j^{-1}) > x_{i'} \geq 4nc$ and Inequality (23).

For every $x \in C \setminus [1/c, c]^n$,

$$f_i(x) = \epsilon q(x)^N \cdot f_{\infty,i}(x) + f_{C,i}(x) > 0$$

since $f_{\infty,i}(x) > 0$ for all $x \notin [1/c, c]^n$ and $f_{C,i}(x) > 0$ for all $x \in C$.

For every $x \in [1/c, c]^n$,

$$\begin{aligned} f_i(x) &= \epsilon f_{\infty,i}(x) \cdot \left(\sum_{j=1}^n \frac{x_j + x_j^{-1}}{2nc} \right)^N + f_{C,i}(x) \\ &\geq \min\{\epsilon f_{\infty,i}(x), 0\} + f_{C,i}(x) > 0. \end{aligned}$$

The last inequality is due to $f_{C,i}(x) > 0$ and Inequality (22). The second to last inequality can be justified as follows. If $f_{\infty,i}(x) \geq 0$ then $f_{\infty,i}(x) \cdot \left(\sum_{i=1}^n \frac{x_i + x_i^{-1}}{2nc} \right)^N \geq 0$, otherwise $\left(\sum_{i=1}^n \frac{x_i + x_i^{-1}}{2nc} \right)^N \leq \left(\sum_{i=1}^n \frac{2c}{2nc} \right)^N = 1$ so $f_{\infty,i}(x) \cdot \left(\sum_{i=1}^n \frac{x_i + x_i^{-1}}{2nc} \right)^N \geq f_{\infty,i}(x)$.

Therefore, for every $x \in \mathbb{R}^n_{>0}$, we have $f_i(x) > 0$. In other words, $\boldsymbol{f}$ satisfies Conditions (i) in Corollary C.7. Furthermore, since $N > M$ we have $\deg_v(q^N \cdot f_{\infty,i}) > \deg_v(f_{C,i})$ for $i = 1, \dots, K, v \in (\mathbb{R}^n)^*$. Hence $\mathrm{in}_v(\boldsymbol{f}) = \mathrm{in}_v(\epsilon q^N \cdot \boldsymbol{f}_\infty) \in (\mathbb{A}^+)^K$ and $M_v(I_\xi, \boldsymbol{f}) = M_v(I_\xi, \boldsymbol{f}_\infty)$ for all $v \in (\mathbb{R}^n)^*, \xi \in \Xi$. Therefore, $\boldsymbol{f}$ satisfies Conditions (ii) in Corollary C.7.

Therefore, by Lemma C.7, we can find $g \in \mathbb{A}^+$ such that $g\boldsymbol{f} \in (\mathbb{A}^+)^K$. We have at the same time $g\boldsymbol{f} \in \mathcal{M}$ as well as $(O_v \cup J_\xi) \cap M_v(I_\xi, g\boldsymbol{f}) = (O_v \cup J_\xi) \cap M_v(I_\xi, \boldsymbol{f}) = (O_v \cup J_\xi) \cap M_v(I_\xi, \boldsymbol{f}_\infty) \neq \emptyset$ for all $v \in (\mathbb{R}^n)^*, \xi \in \Xi$. We have thus found the required element $g\boldsymbol{f} \in \mathcal{M} \cap (\mathbb{A}^+)^K$ satisfying Property (19). □

B. Decidability of local conditions

This subsection is dedicated to the proof of Theorem 4.14. By the local-global principle (Theorem C.2), this amounts to showing decidability of the two "local" Conditions (LocR) and (LocInf).

Decidability of the Condition (LocR) is the same as in [14], which uses Tarski's theorem [40].

Proposition C.8 ([14, Proposition 6.2])**.** *Given the generators $\boldsymbol{g}_1, \dots, \boldsymbol{g}_m$ for $\mathcal{M}$, it is decidable whether Condition (LocR) of Theorem C.2 is satisfied.*

We now focus on deciding the Condition (LocInf).

From (LocInf) to shifted initials (LocInfShift).: First, we introduce the *shifted initials*, in order to replace Condition (LocInf) of Theorem C.2 with a new Condition (LocInfShift).

Suppose we are given $\boldsymbol{f} \in \mathbb{A}^K$, $v \in (\mathbb{R}^n)^*$ and $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_K) \in \mathbb{R}^K$. Then define the *shifted initials* $\mathrm{in}_{v,\alpha}(\boldsymbol{f}) = (\mathrm{in}_{v,\alpha}(\boldsymbol{f})_1, \dots, \mathrm{in}_{v,\alpha}(\boldsymbol{f})_K)$, where $\mathrm{in}_{v,\alpha}(\boldsymbol{f})_i$ is defined as

$$\begin{cases} \mathrm{in}_v(f_i) & \text{if } \deg_v(f_i) + \alpha_i = \max_{1 \leq i' \leq K} \{\deg_v(f_{i'}) + \alpha_{i'}\}, \\ 0 & \text{if } \deg_v(f_i) + \alpha_i < \max_{1 \leq i' \leq K} \{\deg_v(f_{i'}) + \alpha_{i'}\}. \end{cases}$$

Lemma C.9 ([14, Lemma 6.3])**.** *Let $\boldsymbol{f} \in \mathbb{A}^K$ and $v \in (\mathbb{R}^n)^*$. We have $\mathrm{in}_v(\boldsymbol{f}) \in (\mathbb{A}^+)^K$ if and only if there exists $\boldsymbol{\alpha} \in \mathbb{R}^K$ such that $\mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{f}) \in (\mathbb{A}^+)^K$. Furthermore, in this case, $\mathrm{in}_v(\boldsymbol{f}) = \mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{f})$ and $\alpha_1 + \deg_v(f_1) = \cdots = \alpha_K + \deg_v(f_K)$.*

Given $v = (v_1, \dots, v_n) \in (\mathbb{R}^n)^*$, define the following set of real numbers:

$$\sum_{k=1}^n \mathbb{Z} v_k \coloneqq \left\{ \sum_{k=1}^n z_k v_k \;\middle|\; z_1, \dots, z_n \in \mathbb{Z} \right\}.$$

Then for every $f \in \mathbb{A}$, we have $\deg_v(f) \in \sum_{k=1}^n \mathbb{Z} v_k$.

Proposition C.10 (Generalization fof [14, Proposition 6.4])**.** *Condition* (LocInf) *of Theorem C.2 is equivalent to the following:*

2. **(LocInfShift):** *For every $v \in (\mathbb{R}^n)^*$, there exists $\boldsymbol{f} \in \mathcal{M}$ as well as $\boldsymbol{\alpha} \in \left(\sum_{k=1}^n \mathbb{Z} v_k\right)^K$ satisfying the following properties:*
   a) $\mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{f}) \in (\mathbb{A}^+)^K$.

b) For every $\xi \in \Xi$, denote $I'_\xi \coloneqq \{i \in I_\xi \mid \alpha_i = \min_{i' \in I_\xi} \alpha_{i'}\}$, $J'_\xi \coloneqq O_v \cup J_\xi$. We have

$$\left(O_w \cup J'_\xi\right) \cap M_w(I'_\xi, \mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{f})) \neq \emptyset$$

for every $w \in (\mathbb{R}^n)^*, \xi \in \Xi$.

Proof. **(LocInf) $\Longrightarrow$ (LocInfShift)**. Suppose Condition (LocInf) of Theorem C.2 is true. Fix a vector $v \in (\mathbb{R}^n)^*$. Then there exists $\boldsymbol{f} \in \mathcal{M}$, such that $\mathrm{in}_v(\boldsymbol{f}) \in (\mathbb{A}^+)^K$ satisfies Property (LocInf)(b). As in Lemma C.9, we can let $\alpha_i \coloneqq -\deg_v(f_i)$ for $i = 1, \dots, K$, then $\mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{f}) = \mathrm{in}_v(\boldsymbol{f}) \in (\mathbb{A}^+)^K$, satisfying (LocInfShift)(a). Furthermore, we have $\boldsymbol{\alpha} \in (\sum_{k=1}^n \mathbb{Z} v_k)^K$ by the definition of $\alpha_i = -\deg_v(f_i)$. Finally, for every $\xi \in \Xi$, we have $\{i \in I_\xi \mid \alpha_i = \min_{i' \in I_\xi} \alpha_{i'}\} = \{i \in I_\xi \mid \deg_v(f_i) = \max_{i' \in I_\xi} \deg_v(f_{i'})\} = M_v(I_\xi, \boldsymbol{f})$, so (LocInf)(b) implies (LocInfShift)(b).

(LocInfShift) $\Longrightarrow$ (LocInf). Suppose Condition (LocInfShift) is true. Fix a vector $v \in (\mathbb{R}^n)^*$. Then there exists $\boldsymbol{f} \in \mathcal{M}$ as well as $\boldsymbol{\alpha} \in (\mathbb{R}^n)^*$, such that $\mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{f}) \in (\mathbb{A}^+)^K$ satisfies Property (LocInfShift)(b). By Lemma C.9, we have $\mathrm{in}_v(\boldsymbol{f}) = \mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{f}) \in (\mathbb{A}^+)^K$, and $\alpha_1 + \deg_v(f_1) = \cdots = \alpha_K + \deg_v(f_K)$. Therefore for every $\xi \in \Xi$, we have $\{i \in I_\xi \mid \alpha_i = \min_{i' \in I_\xi} \alpha_{i'}\} = \{i \in I_\xi \mid \deg_v(f_i) = \min_{i' \in I_\xi} \deg_v(f_{i'})\} = M_v(I_\xi, \boldsymbol{f})$, so (LocInfShift)(b) implies (LocInf)(b). □

Dimension reduction: a special case.: We will further reduce Condition (LocInfShift) to a Condition (LocInfD) (which will be defined in Proposition C.16). We first consider the special case where the vector $v \in (\mathbb{R}^n)^*$ in Condition (LocInfShift) is of the form $(0, \dots, 0, v_{d+1}, \dots, v_n)$, where $v_{d+1}, \dots, v_n \in \mathbb{R}$ are $\mathbb{Q}$-linearly independent.

As in [14, Definition 6.5], we now define the *super Gröbner basis* of an $\mathbb{A}$-module $\mathcal{M}$. Let $v \in (\mathbb{R}^n)^*, \boldsymbol{\alpha} \in \mathbb{R}^K$. Define $\mathrm{in}_{v,\alpha}(\mathcal{M})$ to be the $\mathbb{A}$-module generated by the elements $\mathrm{in}_{v,\alpha}(\boldsymbol{f}), \boldsymbol{f} \in \mathcal{M}$:

$$\mathrm{in}_{v,\alpha}(\mathcal{M}) \coloneqq \sum_{\boldsymbol{f} \in \mathcal{M}} \mathbb{A} \cdot \mathrm{in}_{v,\alpha}(\boldsymbol{f}) = \left\{ \sum_{j=1}^q p_j \cdot \mathrm{in}_{v,\alpha}(\boldsymbol{f}_j) \,\middle|\, q \in \mathbb{N}, p_1, \dots p_q \in \mathbb{A}, \boldsymbol{f}_1, \dots, \boldsymbol{f}_q \in \mathcal{M} \right\}.$$

Definition C.11 (Super Gröbner basis [14, Definition 6.5])**.** A set of generators $\boldsymbol{g}_1, \dots, \boldsymbol{g}_m$ for $\mathcal{M}$ is called a *super Gröbner basis* if for all $v \in (\mathbb{R}^n)^*, \boldsymbol{\alpha} \in \mathbb{R}^K$, the set $\{\mathrm{in}_{v,\alpha}(\boldsymbol{g}_1), \dots, \mathrm{in}_{v,\alpha}(\boldsymbol{g}_m)\}$ generates $\mathrm{in}_{v,\alpha}(\mathcal{M})$ as an $\mathbb{A}$-module.

Lemma C.12 ([14, Lemma 6.6])**.** *Suppose we are given an arbitrary set of generators for a module $\mathcal{M}$. Then a super Gröbner basis of $\mathcal{M}$ is effectively computable.*

Furthermore, if the given generators for $\mathcal{M}$ contain only polynomials with integer coefficients, then Lemma C.12 computes a super Gröbner basis containing only polynomials with integer coefficients.

Let $0 \le d \le n-1$ be an integer. From now on we denote

$$\mathbb{A}_d \coloneqq \mathbb{R}[X_1^\pm, \dots, X_d^\pm], \quad \mathbb{A}_d^+ \coloneqq \mathbb{R}_{\ge 0}[X_1^\pm, \dots, X_d^\pm]^*.$$

In particular, $\mathbb{A}_0 = \mathbb{R}, \mathbb{A}_0^+ = \mathbb{R}_{>0}$.

We now consider the vectors $v \in (\mathbb{R}^n)^*$ with the special form $(0, \dots, 0, v_{d+1}, \dots, v_n)$ where $v_{d+1}, \dots, v_n$ are $\mathbb{Q}$-linearly independent.

Lemma C.13 ([14, Lemma 6.7])**.** *Let $\boldsymbol{g}_1, \dots, \boldsymbol{g}_m$ be a super Gröbner basis of $\mathcal{M}$.*

Let $v = (0, \dots, 0, v_{d+1}, \dots, v_n) \in (\mathbb{R}^n)^*$ be such that $0 \le d \le n-1$ and $v_{d+1}, \dots, v_n$ are $\mathbb{Q}$-linearly independent. Let $\boldsymbol{\alpha} \in \mathbb{R}^K$. Then there exists $b_i \in \{0\}^d \times \mathbb{Z}^{n-d}$ and $c_j \in \{0\}^d \times \mathbb{Z}^{n-d}$ such that $\overline{X}^{b_i} \overline{X}^{c_j} \mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{g}_j)_i \in \mathbb{A}_d$ for $i = 1, \dots, K$ and $j = 1, \dots, m$. See [14, Figure 27] for an illustration.

Suppose $v \in (\mathbb{R}^n)^*$ satisfies $v = (0, \dots, 0, v_{d+1}, \dots, v_n)$ with $v_{d+1}, \dots, v_n$ being $\mathbb{Q}$-linearly independent. Let $\boldsymbol{\alpha} \in \mathbb{R}^K$. For each $j = 1, \dots, m$, define $\mathrm{in}^d_{v,\boldsymbol{\alpha}}(\boldsymbol{g}_j) = (\mathrm{in}^d_{v,\boldsymbol{\alpha}}(\boldsymbol{g}_j)_1, \dots, \mathrm{in}^d_{v,\boldsymbol{\alpha}}(\boldsymbol{g}_j)_K)$ where

$$\mathrm{in}^d_{v,\boldsymbol{\alpha}}(\boldsymbol{g}_j)_i \coloneqq \overline{X}^{b_i} \overline{X}^{c_j} \mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{g}_j)_i \in \mathbb{A}_d, \quad i = 1, \dots, K.$$

Here, b_i and c_j are defined as in Lemma C.13. Note that the vectors $b_i, c_j \in \{0\}^d \times \mathbb{Z}^{n-d}$ are not necessarily uniquely determined. However, when $d, v, \boldsymbol{\alpha}$ are fixed, the polynomials $\mathrm{in}^d_{v,\boldsymbol{\alpha}}(\boldsymbol{g}_j)_i$ are uniquely determined by $\boldsymbol{g}_1, \dots, \boldsymbol{g}_m$. In fact, by Lemma C.13 each $\mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{g}_j)_i$ can be uniquely written as $\overline{X}^s \cdot p$ for some $\overline{X}^s \in \mathbb{R}[X_{d+1}^\pm, \dots, X_n^\pm]$ and $p \in \mathbb{R}[X_1^\pm, \dots, X_d^\pm]$. Therefore $\mathrm{in}^d_{v,\boldsymbol{\alpha}}(\boldsymbol{g}_j)_i$ is uniquely determined as the polynomial p in the decomposition.

Define by $\mathrm{in}^d_{v,\boldsymbol{\alpha}}(\mathcal{M})$ the $\mathbb{A}_d$-module generated by $\mathrm{in}^d_{v,\boldsymbol{\alpha}}(\boldsymbol{g}_1), \dots, \mathrm{in}^d_{v,\boldsymbol{\alpha}}(\boldsymbol{g}_m) \in \mathbb{A}_d^K$:

$$\mathrm{in}^d_{v,\boldsymbol{\alpha}}(\mathcal{M}) \coloneqq \sum_{j=1}^m \mathbb{A}_d \cdot \mathrm{in}^d_{v,\boldsymbol{\alpha}}(\boldsymbol{g}_j) = \left\{ \sum_{j=1}^m p_j \cdot \mathrm{in}^d_{v,\boldsymbol{\alpha}}(\boldsymbol{g}_j) \,\middle|\, p_1, \dots p_m \in \mathbb{A}_d \right\}.$$

Lemma C.14 ([14, Lemma 6.9])**.** *Let $\boldsymbol{g}_1, \dots, \boldsymbol{g}_m$ be a super Gröbner basis of $\mathcal{M}$.*

Let $v = (0, \dots, 0, v_{d+1}, \dots, v_n)$ be such that $0 \le d \le n-1$ and $v_{d+1}, \dots, v_n$ are $\mathbb{Q}$-linearly independent. Let $\boldsymbol{\alpha} \in \left(\sum_{k=d+1}^n \mathbb{Z} v_k\right)^K$. Fix $\xi \in \Xi$. Denote $I'_\xi \coloneqq \{i \in I_\xi \mid \alpha_i = \min_{i' \in I_\xi} \alpha_{i'}\}, J'_\xi \coloneqq O_v \cup J$. Denote by $\pi_d \colon \mathbb{Z}^n \to \mathbb{Z}^d$ the projection onto the first d coordinates. For every $u \in (\mathbb{R}^d)^*$, define $O'_u \coloneqq \{i \in \{1, \dots, K\} \mid \pi_d(a_i) \not\perp u\}$. Then the two following conditions are equivalent:

(i) (Condition in (LocInfShift)*): There exists $\boldsymbol{f} \in \mathcal{M}$ such that $\mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{f}) \in (\mathbb{A}^+)^K$ and*

$$\left(O_w \cup J'_\xi\right) \cap M_w(I'_\xi, \mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{f})) \neq \emptyset \quad \text{for all } w \in (\mathbb{R}^n)^*. \tag{24}$$

(ii) We have $J'_\xi \cap I'_\xi \neq \emptyset$, and there exists $\boldsymbol{f}^d \in \mathrm{in}^d_{v,\boldsymbol{\alpha}}(\mathcal{M}) \cap \left(\mathbb{A}_d^+\right)^K$, such that

$$\left(O'_u \cup J'_\xi\right) \cap M_u(I'_\xi, \boldsymbol{f}^d) \neq \emptyset \quad \text{for every } u \in (\mathbb{R}^d)^*. \tag{25}$$

When $d = 0$, Property (25) *is considered trivially true.*

Dimension reduction: the general case.: Having considered the special case where the vector $v \in (\mathbb{R}^n)^*$ in Condition (LocInfShift) is of the form $(0, \dots, 0, v_{d+1}, \dots, v_n)$, we now consider the general case. The key idea when dealing with the general case of $v \in (\mathbb{R}^n)^*$ is the following *coordinate change*.

Given a matrix $A = (a_{ij})_{1 \le i,j \le n} \in \mathsf{GL}(n, \mathbb{Z})$, define the new variables $X'_1, \dots, X'_n$ where $X'_i \coloneqq X_1^{a_{i1}} X_2^{a_{i2}} \cdots X_n^{a_{in}}$. Then

$$\mathbb{R}[X_1, \dots, X_n] = \mathbb{R}[X'_1, \dots, X'_n].$$

In other words, we can define the ring automorphism

$$\varphi_A \colon \mathbb{A} \to \mathbb{A}, \quad X_i \mapsto X_1^{a_{i1}} X_2^{a_{i2}} \cdots X_n^{a_{in}},$$

such that $\varphi_A(\overline{X}^b) = \overline{X}^{bA}$. The automorphism φ_A extends entry-wise to $\mathbb{A}^K \to \mathbb{A}^K$.

For each $A \in \mathsf{GL}(n, \mathbb{Z})$, denote by $A^{-\top}$ the inverse of its transpose. Then $(vA^{-\top}) \cdot (bA) = v \cdot b$ for all $v \in (\mathbb{R}^n)^*, b \in \mathbb{Z}^n$. Hence, for any $f \in \mathbb{A}$, we have $\mathrm{in}_{vA^{-\top}}(\varphi_A(f)) = \varphi_A(\mathrm{in}_v(f))$, and for any $\boldsymbol{f} \in \mathbb{A}^K, \xi \in \Xi$, we have $M_v(I_\xi, \boldsymbol{f}) = M_{vA^{-\top}}(I_\xi, \varphi_A(\boldsymbol{f}))$. Furthermore, if we replace the vectors $\widetilde{a}_1, \dots, \widetilde{a}_K \in \mathbb{Z}^n$ by the vectors $\widetilde{a}_1 A, \dots, \widetilde{a}_K A \in \mathbb{Z}^n$, then the set O_v becomes $O_{vA^{-\top}}$. It is easy to verify that if $\boldsymbol{g}_1, \dots, \boldsymbol{g}_m$ is a super Gröbner basis for $\mathcal{M}$, then $\varphi_A(\boldsymbol{g}_1), \dots, \varphi_A(\boldsymbol{g}_m)$ is still a super Gröbner basis for $\varphi_A(\mathcal{M}) \coloneqq \{\varphi_A(\boldsymbol{f}) \mid \boldsymbol{f} \in \mathcal{M}\}$.

Let $v \in (\mathbb{R}^n)^*$ and let $A \in \mathsf{GL}(n, \mathbb{Z})$ be such that $vA^{-\top} = (0, \dots, 0, v_{d+1}, \dots, v_n)$ where $v_{d+1}, \dots, v_n$ are $\mathbb{Q}$-linearly independent. Then as in the previous section we define the module $\mathrm{in}^d_{vA^{-\top},\boldsymbol{\alpha}}(\varphi_A(\mathcal{M}))$ to be the module generated by $\mathrm{in}^d_{vA^{-\top},\boldsymbol{\alpha}}(\varphi_A(\boldsymbol{g}_1)), \dots, \mathrm{in}^d_{vA^{-\top},\boldsymbol{\alpha}}(\varphi_A(\boldsymbol{g}_m))$.

The above observation shows the following. Fix $v \in (\mathbb{R}^n)^*$ in (LocInfShift) of Theorem C.2. Given any change of coordinates $A \in \mathsf{GL}(n, \mathbb{Z})$, we can simultaneously (right-)multiply $A^{-\top}$ to v and A to all $a_1, \dots, a_K$, while applying φ_A to the super Gröbner basis $\boldsymbol{g}_1, \dots, \boldsymbol{g}_m$ of $\mathcal{M}$. Then the original properties (LocInfShift)(a)(b) are satisfied by $\boldsymbol{f}$ if and only if they are satisfied by $\varphi_A(\boldsymbol{f})$ after the change of coordinates. We will use this observation to reduce the general case for v to the special case considered in the previous subsection.

Fact C.15 ([14, Fact 6.10])**.** For every $v \in (\mathbb{R}^n)^*$, there exists $A \in \mathsf{GL}(n, \mathbb{Z})$ such that $vA^{-\top} = (0, \dots, 0, v_{d+1}, \dots, v_n)$ with $v_{d+1}, \dots, v_n$ being $\mathbb{Q}$-linearly independent.

Proposition C.16 (Generalization of [14, Proposition 6.11])**.** *Condition* (LocInfShift) *of Proposition C.10 is equivalent to the following:*

2. **(LocInfD):** *For every $v \in (\mathbb{R}^n)^*, A \in \mathsf{GL}(n, \mathbb{Z})$, such that $vA^{-\top} = (0, \dots, 0, v_{d+1}, \dots, v_n)$, $0 \le d \le n-1$ with $v_{d+1}, \dots, v_n$ being $\mathbb{Q}$-linearly independent, there exist $\boldsymbol{\alpha} \in \left(\sum_{k=d+1}^n \mathbb{Z} v_k\right)^K$ and $\boldsymbol{f}^d \in \mathrm{in}^d_{vA^{-\top},\boldsymbol{\alpha}}(\varphi_A(\mathcal{M}))$ satisfying the following properties:*
   (a) $\boldsymbol{f}^d \in \left(\mathbb{A}_d^+\right)^K$.
   (b1) For each $\xi \in \Xi$, denote $I'_\xi \coloneqq \{i \in I_\xi \mid \alpha_i = \min_{i' \in I_\xi} \alpha_{i'}\}, J'_\xi \coloneqq (O_v \cup J_\xi)$. We have
   $$J'_\xi \cap I'_\xi \neq \emptyset \quad \text{for all } \xi \in \Xi. \tag{26}$$
   (Note that this property depends only on v and $\boldsymbol{\alpha}$, but not on $\boldsymbol{f}^d$.)
   (b2) Denote by $\pi_d \coloneqq \mathbb{Z}^n \to \mathbb{Z}^d$ the projection onto the first d coordinates. For $u \in (\mathbb{R}^d)^*$, define $O'_u \coloneqq \{i \in \{1, \dots, K\} \mid \pi_d(\widetilde{a}_i A) \not\perp u\}$, we have
   $$\left(O'_u \cup J'_\xi\right) \cap M_u(I'_\xi, \boldsymbol{f}^d) \neq \emptyset \tag{27}$$
   for every $u \in (\mathbb{R}^d)^*, \xi \in \Xi$.

As in Lemma C.14, Property (27) *is considered trivially true when $d = 0$.*

Proof. Fix a $v = (v_1, \dots, v_n) \in (\mathbb{R}^n)^*$. Take any $A \in \mathsf{GL}(n, \mathbb{Z})$ with $vA^{-\top} = (0, \dots, 0, v'_{d+1}, \dots, v'_n)$ such that $v'_{d+1}, \dots, v'_n$ are $\mathbb{Q}$-linearly independent. Note that $\sum_{k=1}^n \mathbb{Z} v_k = \sum_{k=d+1}^n \mathbb{Z} v'_k$ because $A \in \mathsf{GL}(n, \mathbb{Z})$. Therefore, we can apply Lemma C.14 to the super Gröbner basis $\varphi_A(\boldsymbol{g}_1), \dots, \varphi_A(\boldsymbol{g}_m)$, the vector $vA^{-\top} = (0, \dots, 0, v'_{d+1}, \dots, v'_n)$ and the vectors $\widetilde{a}_1 A, \dots, \widetilde{a}_K A \in \mathbb{Z}^n$. Lemma C.14 shows that there exist $\boldsymbol{\alpha} \in \left(\sum_{k=d+1}^n \mathbb{Z} v'_k\right)^K$ and $\boldsymbol{f}^d \in \mathrm{in}^d_{vA^{-\top},\boldsymbol{\alpha}}(\varphi_A(\mathcal{M}))$ satisfying (LocInfD)(a)(b1)(b2) if and only if there exists $\boldsymbol{\alpha} \in \left(\sum_{k=1}^n \mathbb{Z} v_k\right)^K$ and $\boldsymbol{f} \in \mathcal{M}$ satisfying (LocInfShift)(a)(b). □

Computing cells (LocInfCell).: We further reduce the Condition (LocInfD) to a Condition (LocInfCell) which consists of verifying a *finite* number of $v \in (\mathbb{R}^n)^*$ for each coordinate-change matrix $A \in \mathsf{GL}(n, \mathbb{Z})$.

Let $v \in (\mathbb{R}^n)^*, \boldsymbol{\alpha} \in \mathbb{R}^K$. Denote by $e_1, \dots, e_K$ the canonical basis of the $\mathbb{A}$-module $\mathbb{A}^K$. We introduce the new variables $T_1, \dots, T_K$ and define an $\mathbb{A}$-module homomorphism

$$\phi : \mathbb{A}^K \to \mathbb{R}[X_1^\pm, \dots, X_n^\pm, T_1^\pm, \dots, T_K^\pm], \quad \overline{X}^u e_i \mapsto \overline{X}^u T_i.$$

We have $\phi(\mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{f})) = \mathrm{in}_{(v,\boldsymbol{\alpha})}(\phi(\boldsymbol{f}))$ for every $\boldsymbol{f} \in \mathbb{A}^K$.

As in the previous subsections let $\boldsymbol{g}_1, \dots, \boldsymbol{g}_m$ be a super Gröbner basis of $\mathcal{M}$. Since $\phi(\boldsymbol{g}_i)$ is a polynomial in $\mathbb{R}[X_1^\pm, \dots, X_n^\pm, T_1^\pm, \dots, T_K^\pm]$, there exists a partition of $(\mathbb{R}^n)^* \times \mathbb{R}^K$ such that for any two directions in the same partition element the initial parts of $\phi(\boldsymbol{g}_i)$ are the same. Let $\mathcal{L}_\mathcal{M}$ be the common refinement of the partitions associated to the polynomials $\phi(\boldsymbol{g}_1), \dots, \phi(\boldsymbol{g}_m)$.

From now on we use the term "*cell*" to call elements of a given partition. Fix $I_\xi \subseteq \{1, \dots, K\}$. There exists a partition $\mathcal{L}_{I_\xi}$ of $\mathbb{R}^K$ such that for any two vectors $(\alpha_1, \dots, \alpha_K)$, $(\alpha'_1, \dots, \alpha'_K)$ in the same cell, we have $\alpha_i > \alpha_j \iff \alpha'_i > \alpha'_j$ and $\alpha_i < \alpha_j \iff \alpha'_i < \alpha'_j$ for all $i, j \in I_\xi$. Define the partition $\mathcal{L}'_{I_\xi} \coloneqq (\mathbb{R}^n)^* \times \mathcal{L}_{I_\xi}$ of $(\mathbb{R}^n)^* \times \mathbb{R}^K$ where each cell is of the form $(\mathbb{R}^n)^* \times P, P \in \mathcal{L}_{I_\xi}$.

There exists a partition $\mathcal{L}_O$ of $(\mathbb{R}^n)^*$ such that any two vectors v, v' in the same cell satisfy $v \perp \widetilde{a}_i \iff v' \perp \widetilde{a}_i$ for all $i \in \{1, \dots, K\}$. By subdividing $\mathcal{L}_O$ we can suppose that each cell is a convex polyhedron. Similar to the definition of $\mathcal{L}'_{I_\xi}$, we define the partition $\mathcal{L}'_O \coloneqq \mathcal{L}_O \times \mathbb{R}^K$ of $(\mathbb{R}^n)^* \times \mathbb{R}^K$.

For any two partition $\mathcal{B}, \mathcal{B}'$ of the same set S, define $\mathcal{B} \vee \mathcal{B}'$ to be the partition of S whose elements are of the form $B \cap B', B \in \mathcal{B}, B' \in \mathcal{B}'$. Consider the partition $\mathcal{L}$ of $(\mathbb{R}^n)^* \times \mathbb{R}^K$ defined by

$$\mathcal{L} \coloneqq \mathcal{L}_{\mathcal{M}} \vee \mathcal{L}'_O \vee \left(\bigvee_{\xi \in \Xi} \mathcal{L}'_{I_\xi} \right).$$

We point out that the cells of $\mathcal{L}$ are invariant under scaling by a positive real, meaning $x \in Q \iff r \cdot x \in Q$ for all cells $Q \in \mathcal{L}$ and $r \in \mathbb{R}_{>0}$.

Let $\pi\colon (\mathbb{R}^n)^* \times \mathbb{R}^K \to (\mathbb{R}^n)^*, (v, \boldsymbol{\alpha}) \mapsto v$ be the canonical projection. For each $Q \in \mathcal{L}$, define the two-element partition $\{\pi(Q), (\mathbb{R}^n)^* \setminus \pi(Q)\}$ of $(\mathbb{R}^n)^*$, and define

$$\mathcal{P} \coloneqq \bigvee_{Q \in \mathcal{L}} \{\pi(Q), (\mathbb{R}^n)^* \setminus \pi(Q)\}.$$

By this definition, take any $P \in \mathcal{P}$ and $Q \in \mathcal{L}$ with $\pi^{-1}(P) \cap Q \neq \emptyset$; then for $v, v' \in P$, there exists $\boldsymbol{\alpha} \in \mathbb{R}^K$ with $(v, \boldsymbol{\alpha}) \in Q$ if and only if there exists $\boldsymbol{\alpha}' \in \mathbb{R}^K$ with $(v', \boldsymbol{\alpha}') \in Q$. See [14, Figure 28] for an illustration.

It is important to note that the partitions $\mathcal{L}_{\mathcal{M}}, \mathcal{L}_O, \mathcal{L}_{I_\xi}, \xi \in \Xi$, are all defined using equalities and inequalities with *rational* coefficients. Also, each inequality is strict, so every cell $Q \in \mathcal{L}$ and $P \in \mathcal{P}$ is relatively open (a polyhedron is called relative open if it is open in the smallest linear space containing it). In other words, each cell is defined by a combination of equalities and *strict* inequalities. We also point out that, like the cells of $\mathcal{L}$, the cell of $\mathcal{P}$ are invariant under scaling by a positive real, meaning $x \in P \iff r \cdot x \in P$ for all cells $P \in \mathcal{P}$ and $r \in \mathbb{R}_{>0}$. By the definition of $\mathcal{L}$, we immediately obtain the following.

Lemma C.17 ([14, Lemma 6.12])**.** *Fix a change of coordinates $A \in \mathsf{GL}(n, \mathbb{Z})$, two sets $I_\xi, J_\xi \subseteq \{1, \dots, K\}$, and a cell $Q \in \mathcal{L}A^{-\top}$. Then the sets I'_ξ, J'_ξ defined in* (LocInfD)*(b1) are effectively computable and do not depend on $v, \boldsymbol{\alpha}$ as long as $(vA^{-\top}, \boldsymbol{\alpha}) \in Q$. In particular, the Property* (LocInfD)*(b1) is either always true or always false for $v, \boldsymbol{\alpha}, (vA^{-\top}, \boldsymbol{\alpha}) \in Q$.*

Let $Q \in \mathcal{L}$. For $(v, \boldsymbol{\alpha}), (v', \boldsymbol{\alpha}') \in Q$, we have

$$\mathrm{in}_{v, \boldsymbol{\alpha}}(\boldsymbol{g}_j) = \mathrm{in}_{v', \boldsymbol{\alpha}'}(\boldsymbol{g}_j)$$

for all $j = 1, \dots, m$. Thus, if $v = (0, \dots, 0, v_{d+1}, \dots, v_n)$ is such that $v_{d+1}, \dots, v_n$ are $\mathbb{Q}$-linearly independent, then $\mathrm{in}^d_{v, \boldsymbol{\alpha}}(\mathcal{M})$ depends only on the cell $Q \in \mathcal{L}$ containing $(v, \boldsymbol{\alpha})$. Hence, we can denote

$$\begin{aligned} \mathrm{in}^d_Q(\boldsymbol{g}_j) &\coloneqq \mathrm{in}^d_{v, \boldsymbol{\alpha}}(\boldsymbol{g}_j), \quad j = 1, \dots, m, \\ \mathrm{in}^d_Q(\mathcal{M}) &\coloneqq \mathrm{in}^d_{v, \boldsymbol{\alpha}}(\mathcal{M}), \quad \text{where } (v, \boldsymbol{\alpha}) \in Q. \end{aligned}$$

For any coordinate change $A \in \mathsf{GL}(n, \mathbb{Z})$, we similarly define the partitions $\mathcal{L}A^{-\top}$ and $\mathcal{P}A^{-\top}$ based on the super Gröbner basis $\varphi_A(\boldsymbol{g}_1), \dots, \varphi_A(\boldsymbol{g}_m)$ and the vectors $\widetilde{a}_1 A, \dots, \widetilde{a}_K A$. In particular, each cell of $\mathcal{L}A^{-\top}$ is of the form $Q \cdot diag(A^{-\top}, I_K), Q \in \mathcal{L}$, and each cell of $\mathcal{P}A^{-\top}$ is of the form $P \cdot A^{-\top}, P \in \mathcal{P}$. If $vA^{-\top} = (0, \dots, 0, v_{d+1}, \dots, v_n)$ is such that $v_{d+1}, \dots, v_n$ are $\mathbb{Q}$-linearly independent, then $\mathrm{in}^d_{vA^{-\top}, \boldsymbol{\alpha}}(\varphi_A(\mathcal{M}))$ depends only on the cell $Q \in \mathcal{L}A^{-\top}$ containing $(vA^{-\top}, \boldsymbol{\alpha})$. Similarly, for $j = 1, \dots, m$, we can denote

$$\begin{aligned} \mathrm{in}^d_Q(\varphi_A(\boldsymbol{g}_j)) &\coloneqq \mathrm{in}^d_{vA^{-\top}, \boldsymbol{\alpha}}(\varphi_A(\boldsymbol{g}_j)), \\ \mathrm{in}^d_Q(\varphi_A(\mathcal{M})) &\coloneqq \mathrm{in}^d_{vA^{-\top}, \boldsymbol{\alpha}}(\varphi_A(\mathcal{M})), \end{aligned}$$

where $(vA^{-\top}, \boldsymbol{\alpha}) \in Q$.

The inputs in Theorem 4.14 are generators for modules $\mathcal{M}$ over $\mathbb{A} = \mathbb{R}[X_1^{\pm}, \dots, X_n^{\pm}]$, vectors $\widetilde{a}_1, \dots, \widetilde{a}_K$ in $\mathbb{Z}^n$ and pairs of sets $I_\xi, J_\xi, \xi \in \Xi$. Our strategy is to use induction on n to prove Theorem 4.14. The base case $n = 0$ reduces to linear programming. Indeed, when $n = 0$, $\mathbb{A} = \mathbb{R}, \mathbb{A}^+ = \mathbb{R}_{>0}$, the Property (8) is trivially true; and the problem becomes the following: given an $\mathbb{R}$-submodule $\mathcal{M}$ of $\mathbb{R}^K$, decide whether $\mathcal{M} \cap \mathbb{R}^K_{>0}$ contains an element. Since the given generators of $\mathcal{M}$ all have integer coefficients, this is decidable using linear programming.

The following lemma shows that a decision procedure for Theorem 4.14 with smaller n can help us decide for a given cell $Q \in \mathcal{L}$ if the module $\mathrm{in}^d_Q(\varphi_A(\mathcal{M}))$ contains an $\boldsymbol{f}^d$ satisfying the Properties (LocInfD)(a) and (b2).

Lemma C.18 (Generalization of [14, Lemma 6.13])**.** *Fix a change of coordinates $A \in \mathsf{GL}(n, \mathbb{Z})$, sets $I_\xi, J_\xi \subseteq \{1, \dots, K\}$ for each $\xi \in \Xi$, and a number $0 \leq d \leq n-1$. Suppose Theorem 4.14 is true for all n_0, $0 \leq n_0 \leq n-1$. Fix a cell $Q \in \mathcal{L}A^{-\top}$, let $I'_\xi, J'_\xi, \xi \in \Xi$, be the sets defined in* (LocInfD)*(b1). We can decide whether the module $\mathrm{in}^d_Q(\varphi_A(\mathcal{M}))$ contains an element $\boldsymbol{f}^d$ satisfying the Properties* (LocInfD)*(a) and (b2).*

Proof. Suppose Theorem 4.14 is true for all $0 \leq n_0 \leq n-1$. In particular it is true for $d \leq n-1$. Fix a cell $Q \in \mathcal{L}A^{-\top}$.

In (LocInfD), the $\mathbb{A}_d$-submodule $\mathrm{in}^d_{vA^{-\top}, \boldsymbol{\alpha}}(\varphi_A(\mathcal{M})) = \mathrm{in}^d_Q(\varphi_A(\mathcal{M}))$ of $\mathbb{A}_d^K$ is generated by the elements $\mathrm{in}^d_Q(\varphi_A(\boldsymbol{g}_j)), j = 1, \dots, m$. Recall that $\pi_d \coloneqq \mathbb{Z}^n \to \mathbb{Z}^d$ denotes the projection onto the first d coordinates.

We then apply Theorem 4.14 the following way: replace n by d; replace the elements $\boldsymbol{g}_1, \dots, \boldsymbol{g}_m \in \mathbb{A}^K$ by the elements $\mathrm{in}^d_Q(\varphi_A(\boldsymbol{g}_1)), \dots, \mathrm{in}^d_Q(\varphi_A(\boldsymbol{g}_m)) \in \mathbb{A}_d^K$; replace the vectors $\widetilde{a}_1, \dots, \widetilde{a}_K \in \mathbb{Z}^n$ by the vectors $\pi_d(\widetilde{a}_1 A), \dots, \pi_d(\widetilde{a}_K A) \in \mathbb{Z}^d$; and replace the sets $I_\xi, J_\xi, \xi \in \Xi$, by the sets $I'_\xi, J'_\xi, \xi \in \Xi$. Then Theorem 4.14 shows we can decide whether $\mathrm{in}^d_Q(\varphi_A(\mathcal{M}))$ contains an element $\boldsymbol{f}^d$ satisfying $\boldsymbol{f}^d \in \left(\mathbb{A}_d^+\right)^K$ and

$$\left(O'_u \cup J'_\xi\right) \cap M_u(I'_\xi, \boldsymbol{f}^d) \neq \emptyset, \quad \text{for every } u \in \left(\mathbb{R}^d\right)^*, \xi \in \Xi.$$

These are exactly the Properties (LocInfD)(a) and (b2). □

Denote by $Op(A, d)$ the union of all cells $Q \in \mathcal{L}A^{-\top}$ such that the Property (LocInfD)(b1) is true for $(vA^{-\top}, \boldsymbol{\alpha}) \in Q$, and such that $\mathrm{in}^d_Q(\varphi_A(\mathcal{M}))$ contains an element $\boldsymbol{f}^d$ satisfying the Properties (LocInfD)(a)(b2). By Lemma C.17 and C.18, the set $Op(A, d)$ is effectively computable as a finite union of polyhedra defined over rational coefficients (supposing

Theorem 4.14 is true for all $0 \leq n_0 \leq n-1$). See [14, Figure 29] for an illustration of $Op(A,d)$.

Proposition C.19 (Generalization of [14, Proposition 6.14])**.** *Condition* (LocInfD) *of Proposition C.16 is equivalent to the following:*

2. **(LocInfCell):** *For every $A \in \mathsf{GL}(n,\mathbb{Z})$ and every number $0 \leq d \leq n-1$, the following is true:*
   (a) *For every $v = (0,\dots,0,v_{d+1},\dots,v_n) \in \{0\}^d \times (\mathbb{R}^{n-d})^*$ with $v_{d+1},\dots,v_n$ being $\mathbb{Q}$-linearly independent, there exists $\boldsymbol{\alpha} \in \left(\sum_{k=d+1}^{n} \mathbb{Z}v_k\right)^K$ with $(v,\boldsymbol{\alpha}) \in Op(A,d)$.*

Proof. This follows directly from the definition of $Op(A,d)$. □

Lemma C.20 ([14, Lemma 6.15])**.** *Given $A \in \mathsf{GL}(n,\mathbb{Z}), d \in \mathbb{N}$ and given $Op(A,d)$ as a finite union of polyhedra defined over rational coefficients, it is decidable whether the statement* (LocInfCell)(a) *is true.*

Proving Theorem 4.14: induction and a double procedure.: We now give the full proof of Theorem 4.14. As in [14], the overall strategy is to use induction on n, while deciding the Conditions (LocR) and (LocInf) from the local-global principle (Theorem C.2).

Theorem 4.14. *Denote $\mathbb{A} \coloneqq \mathbb{R}[\overline{X}^{\pm}], \mathbb{A}^+ \coloneqq \mathbb{R}_{\geq 0}[\overline{X}^{\pm}]^*$. Fix $n \in \mathbb{N}$ and let Ξ be a finite set of indices. Suppose we are given as input a set of generators $\boldsymbol{g}_1,\dots,\boldsymbol{g}_m \in \mathbb{A}^K$ with integer coefficients, the vectors $\widetilde{a}_1,\dots,\widetilde{a}_K \in \mathbb{Z}^n$, as well as subsets $I_\xi, J_\xi \subseteq \{1,\dots,K\}$ for each $\xi \in \Xi$. Denote by $\mathcal{M}$ be the $\mathbb{A}$-submodule of $\mathbb{A}^K$ generated by $\boldsymbol{g}_1,\dots,\boldsymbol{g}_m$. It is decidable whether there exists $\boldsymbol{f} \in \mathcal{M} \cap (\mathbb{A}^+)^K$ satisfying*

$$(O_v \cup J_\xi) \cap M_v(I_\xi, \boldsymbol{f}) \neq \emptyset, \quad \text{for every } v \in (\mathbb{R}^n)^*, \xi \in \Xi. \tag{8}$$

Here, if $n = 0$ then $\mathbb{A}$ is understood as $\mathbb{R}$, and Property (8) *is considered trivially true.*

Proof. We use induction on n. As remarked earlier, the base case $n = 0$ degenerates into linear programming (given an $\mathbb{R}$-submodule $\mathcal{M}$ of $\mathbb{R}^K$, decide whether $\mathcal{M} \cap \mathbb{R}^K_{>0}$ contains an element). Suppose we have a decision procedure for all $n_0 < n$, we now construct a procedure for n.

By Theorem C.2 it suffices to decide whether the two conditions (LocR) and (LocInf) are both satisfied. First we check if (LocR) is true using Proposition C.8. If (LocR) is false then we return False and conclude there is no $\boldsymbol{f} \in \mathcal{M} \cap (\mathbb{A}^+)^K$ satisfying (8). If (LocR) is true then we proceed.

We now run the two following procedures *in parallel*:

1) **Procedure A:** We recursively enumerate all elements of the $\mathbb{Z}[X_1^{\pm},\dots,X_n^{\pm}]$-module:

$$\widetilde{\mathcal{M}_{\mathbb{Z}}} \coloneqq \left\{ \sum_{j=1}^{m} h_j \cdot \boldsymbol{g}_j \;\middle|\; h_1,\dots,h_m \in \mathbb{Z}[X_1^{\pm},\dots,X_n^{\pm}] \right\}.$$

   For each element $\boldsymbol{f} \in \widetilde{\mathcal{M}_{\mathbb{Z}}}$, check if $\boldsymbol{f}$ is in $(\mathbb{A}^+)^K$ and if it satisfies Property (8). This can be done in the following way: since the entries of $\boldsymbol{f}$ contain finitely many monomials, it suffices to check Property (8) for a finite number of v. Indeed, since each of $f_1,\dots,f_K$ has only finitely many monomials, there exists a partition $\mathcal{L}_{\boldsymbol{f}}$ of $(\mathbb{R}^n)^*$ such that for each cell $L \in \mathcal{L}_{\boldsymbol{f}}$ and for each $\xi \in \Xi$, the set $M_v(I_\xi, \boldsymbol{f})$ is the same for all $v \in L$. Furthermore, for each cell $L \in \mathcal{L}_O$, the set O_v is the same for all $v \in L$. Therefore, it suffices to check Property (8) for one vector v in each cell of the partition $\mathcal{L}_{\boldsymbol{f}} \vee \mathcal{L}_O$. This can be done in finite time for any given $\boldsymbol{f}$. If some element $\boldsymbol{f} \in \widetilde{\mathcal{M}_{\mathbb{Z}}}$ is in $(\mathbb{A}^+)^K$ and satisfies Property (8), we stop the procedure and return True.
2) **Procedure B:** We recursively enumerate all $A \in \mathsf{GL}(n,\mathbb{Z})$ and $d \in \{0,1,\dots,n-1\}$. For each A and d, compute $Op(A,d)$ using Lemma C.18 and the induction hypothesis on n. Using Lemma C.20, we check if the statement (LocInfCell)(a) from Proposition C.19 is false. If for some A, d, the statement (LocInfCell)(a) is false, then we stop the procedure and return False.

We claim that one of the two above procedures must stop.

Indeed, if $\mathcal{M}$ contains an element of $(\mathbb{A}^+)^K$ satisfying Property (8), then there exists an element $\boldsymbol{f} \in \widetilde{\mathcal{M}_{\mathbb{Z}}} \cap (\mathbb{A}^+)^K$ that satisfies Property (8) (see Lemma 4.15). In this case, Procedure A terminates by finding an element $\boldsymbol{f}$ of $\widetilde{\mathcal{M}_{\mathbb{Z}}} \cap (\mathbb{A}^+)^K$ that satisfies Property (8).

If $\mathcal{M}$ does not contain an element of $(\mathbb{A}^+)^K$ satisfying Property (8), then by Theorem C.2, Condition (LocInf) must be false (since we have already checked (LocR) to be true). By the chain of Propositions C.10, C.16 and C.19, the statement (LocInfCell)(a) must be false for some $A \in \mathsf{GL}(n,\mathbb{Z})$ and $d \in \{0,1,\dots,n-1\}$. In this case, Procedure B terminates by finding $A \in \mathsf{GL}(n,\mathbb{Z})$ and $d \in \{0,1,\dots,n-1\}$ where the statement (LocInfCell)(a) is false.

Therefore, by running Procedure A and Procedure B in parallel, we obtain an algorithm that always terminates for n. □