# The Identity Problem in $\mathbb{Z} \wr \mathbb{Z}$ Is Decidable

**Ruiwen Dong** ✉
Department of Computer Science, University of Oxford, UK

## Abstract

We consider semigroup algorithmic problems in the wreath product $\mathbb{Z} \wr \mathbb{Z}$. Our paper focuses on two decision problems introduced by Choffrut and Karhumäki (2005): the *Identity Problem* (does a semigroup contain the neutral element?) and the *Group Problem* (is a semigroup a group?) for finitely generated sub-semigroups of $\mathbb{Z} \wr \mathbb{Z}$. We show that both problems are decidable. Our result complements the undecidability of the *Semigroup Membership Problem* (does a semigroup contain a given element?) in $\mathbb{Z} \wr \mathbb{Z}$ shown by Lohrey, Steinberg and Zetzsche (ICALP 2013), and contributes an important step towards solving semigroup algorithmic problems in general metabelian groups.

**2012 ACM Subject Classification** Computing methodologies → Symbolic and algebraic manipulation

**Keywords and phrases** wreath product, algorithmic group theory, identity problem, polynomial semiring, positive coefficients

**Digital Object Identifier** 10.4230/LIPIcs.ICALP.2023.124

**Category** Track B: Automata, Logic, Semantics, and Theory of Programming

**Related Version** *Full Version*: `https://arxiv.org/abs/2302.05939`

**Funding** The author acknowledges support from UKRI Frontier Research Grant EP/X033813/1.

**Acknowledgements** The author would like to thank Markus Schweighofer and David Sawall for useful discussions.

## 1 Introduction

The computational theory of groups and semigroups is one of the oldest and most well-developed parts of computational algebra. Dating back to the work of Markov [24] in the 1940s, the area plays an essential role in analysing system dynamics, with notable applications in automata theory and program analysis [5, 9, 11, 16]. See [19] for an all-encompassing survey on this topic. Among the most prominent problems in this area are *Semigroup Membership* and *Group Membership*, proposed respectively by Markov and Mikhailova in the 1940s and 1960s. For these decision problems, we work in a fixed group $G$. The input is a finite set of elements $\mathcal{G} \subseteq G$, plus a distinguished element $g \in G$. Denote by $\langle \mathcal{G} \rangle$ the semigroup generated by $\mathcal{G}$, and by $\langle \mathcal{G} \rangle_{grp}$ the group generated by $\mathcal{G}$.

**(i)** *(Semigroup Membership)* decide whether $\langle \mathcal{G} \rangle$ contains $g$.
**(ii)** *(Group Membership)* decide whether $\langle \mathcal{G} \rangle_{grp}$ contains $g$.

In this paper, we consider two problems closely related to (i) and (ii): the *Identity Problem* and the *Group Problem*, both introduced by Choffrut and Karhumäki [9] in 2005.

**(iii)** *(Identity Problem)* decide whether $\langle \mathcal{G} \rangle$ contains the neutral element $I$ of $G$.
**(iv)** *(Group Problem)* decide whether $\langle \mathcal{G} \rangle$ is a group, in other words, whether $\langle \mathcal{G} \rangle = \langle \mathcal{G} \rangle_{grp}$.

In general matrix groups, Semigroup Membership is undecidable by a classical result of Markov [24]. All four problems remain undecidable even for integer matrix groups of dimension four [4, 25]. Notably, using an embedding of the *Identity Correspondence Problem*, Bell and Potapov [4] showed undecidability of the Identity Problem and the Group Problem in the group $\mathsf{SL}(4, \mathbb{Z})$ of $4 \times 4$ integer matrices of determinant one. On the other hand, in the


50th International Colloquium on Automata, Languages, and Programming (ICALP 2023).
Editors: Kousha Etessami, Uriel Feige, and Gabriele Puppis; Article No. 124; pp. 124:1–124:20
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

group $\mathsf{SL}(2, \mathbb{Z})$, all four problems are decidable with various degrees of complexity [3, 9, 21]. In particular, the Identity Problem and the Group Problem in $\mathsf{SL}(2, \mathbb{Z})$ are both **NP**-complete by a result of Bell, Hirvensalo, and Potapov [3].

In this paper we focus on these decision problems in the *wreath product* $\mathbb{Z} \wr \mathbb{Z}$. The wreath product is a fundamental construction in group and semigroup theory. A great number of important groups can be constructed using the wreath product, notably *metabelian groups*. Metabelian groups are groups whose commutator is abelian: these are the simplest generalization of abelian groups. Algorithmic problems in metabelian groups have been the focus of active research since the 1970s [2, 8, 26], with a classic result of Romanovskii [27] showing decidability of Group Membership in all finitely presented metabelian groups. A key part of Romanovskii's proof is to embed metabelian groups into quotients of wreath products. In fact, the Magnus embedding theorem [23] states that every finitely generated free metabelian group can be embedded in a wreath product $\mathbb{Z}^m \wr \mathbb{Z}^n$. Therefore, understanding the wreath product $\mathbb{Z} \wr \mathbb{Z}$ is the most crucial step towards studying general metabelian groups. Apart from its interest within group theory, the wreath product also plays an important role in the algebraic theory of automata. The Krohn–Rhodes theorem [20] states that every finite semigroup (and correspondingly, every finite automaton) can be decomposed into elementary components using wreath products.

One easy way to understand the wreath product $\mathbb{Z} \wr \mathbb{Z}$ is through its isomorphism to a matrix group [23] over the Laurent polynomial ring $\mathbb{Z}[X^{\pm}]$:

$$\mathbb{Z} \wr \mathbb{Z} \cong \left\{ \begin{pmatrix} X^b & y \\ 0 & 1 \end{pmatrix} \;\middle|\; y \in \mathbb{Z}[X^{\pm}], b \in \mathbb{Z} \right\}. \tag{1}$$

Consider the four aforementioned decision problems in $\mathbb{Z} \wr \mathbb{Z}$. Since $\mathbb{Z} \wr \mathbb{Z}$ is metabelian [17], the classic result of Romanovskii [27] shows decidability of Group Membership in $\mathbb{Z} \wr \mathbb{Z}$. If we retrace the proof of Romanovskii, one can reduce Group Membership in $\mathbb{Z} \wr \mathbb{Z}$ to solving systems of linear equations over the ring $\mathbb{Z}[X^{\pm}]$, which can then be decided using Gröbner bases. For Semigroup Membership in $\mathbb{Z} \wr \mathbb{Z}$, Lohrey, Steinberg and Zetzsche showed its undecidability using an encoding of 2-counter machines [22]. Decidability of the Identity Problem and the Group Problem in $\mathbb{Z} \wr \mathbb{Z}$ remained an intricate open problem. A recent paper by Dong [12] gave a partial decidability result when the generators all satisfy $b = \pm 1$. Dong's idea was to represent a product of elements in $\mathbb{Z} \wr \mathbb{Z}$ as a walk on $\mathbb{Z}$. When the generators all satisfy $b = \pm 1$, this walk can be decomposed into simple cycles, and the Group Problem reduces to solving a *single* homogeneous linear equation over the semiring $\mathbb{N}[X]$. Extending Dong's result to arbitrary generators is highly challenging: the structure of the walk becomes much more complex when we allow steps of arbitrary length. In this paper, we combine a series of new ideas from graph theory and algebraic geometry to show full decidability of the Identity Problem and the Group Problem in $\mathbb{Z} \wr \mathbb{Z}$.

The first main idea of this paper is to reduce both problems to solving a *system* of homogeneous linear equations over the semiring $\mathbb{N}[X^{\pm}]$, in addition to two *degree constraints*. We use a highly non-trivial graph theoretic construction to establish this reduction. The second main idea of this paper is to generalize a local-global principle by Einsiedler, Mouat and Tuncel [13] to solve these linear equations with degree constraints. In particular, the original local-global principle by Einsiedler et al. is not compatible with the degree constraints which are essential in our reduction. We introduce new ideas to prove a generalized local-global principle that incorporates these additional degree constraints.

We now mention some other known decidability results in wreath products. In [14], Ganardi, König, Lohrey and Zetzsche showed that for every non-trivial finitely generated abelian group $G$, the *knapsack problem* in $G \wr \mathbb{Z}$ is **NP**-complete. Notably, this result applies to $\mathbb{Z} \wr \mathbb{Z}$. In [22], Lohrey, Steinberg and Zetzsche showed decidability of the *Rational Subset*

*Membership Problem* (which subsumes all four decision problems mentioned in the beginning) in the wreath product $H \wr V$, where $H$ is a finite and $V$ is virtually free. In [7], Cadilhac, Chistikov and Zetzsche proved decidability of Rational Subset Membership in the *Baumslag-Solitar groups* $\mathsf{BS}(1,p)$. This group can be considered as an analogue of $(\mathbb{Z}/p\mathbb{Z}) \wr \mathbb{Z}$ "with carrying". In [17], Kharlampovich, López, and Myasnikov showed decidability of solving Diophantine equations in certain metabelian groups, including $\mathbb{Z} \wr \mathbb{Z}$ and $\mathsf{BS}(1,p)$. Many of these results are closely related to automata theory, which we draw inspiration from.

A natural follow-up to our work would be trying to solve the Identity Problem and the Group Problem in *all* finitely presented metabelian groups. This boils down to deciding both problems in quotients of $\mathbb{Z}^m \wr \mathbb{Z}^n$. One encounters some difficulties when trying to generalize our approach to $\mathbb{Z}^m \wr \mathbb{Z}^n$. Notably, decomposition of walks in $\mathbb{Z}^n$ are much more complex, and we can no longer reduce these problems to solving a finite system of equations. We also point out that one cannot go much further beyond metabelian groups (which are 2-step solvable groups), since there exist 3-step solvable groups with undecidable word problem [18].

## 2 Preliminaries

### Words, semigroups and graphs

Let $G$ be an arbitrary group. Let $\mathcal{G} = \{g_1, \ldots, g_a\}$ be a finite set of elements in $G$. Considering $\mathcal{G}$ as an alphabet, denote by $\mathcal{G}^*$ the set of words over $\mathcal{G}$. For an arbitrary word $w = g_{i_1} g_{i_2} \cdots g_{i_m} \in \mathcal{G}^*$, by multiplying consecutively the elements appearing in $w$, we can evaluate $w$ as an element $\pi(w)$ in $G$. We say that the word $w$ *represents* the element $\pi(w)$. The semigroup $\langle \mathcal{G} \rangle$ generated by $\mathcal{G}$ is hence the set of elements in $G$ that are represented by *non-empty* words in $\mathcal{G}^*$.

A word $w$ over the alphabet $\mathcal{G}$ is called *full-image* if every letter in $\mathcal{G}$ has at least one occurrence in $w$. The following observation shows that deciding the Group Problem amounts to finding a full-image word representing the neutral element.

▶ **Lemma 2.1.** *Let $\mathcal{G} = \{g_1, \ldots, g_a\}$ be a set of elements in a group $G$. The semigroup $\langle \mathcal{G} \rangle$ is a group if and only if the neutral element $I$ of $G$ is represented by a full-image word over $\mathcal{G}$.*

The following lemma shows that decidability of the Group Problem implies decidability of the Identity Problem.

▶ **Lemma 2.2** ([4]). *Given a finite subset $\mathcal{G}$ of a group $G$, the semigroup $\langle \mathcal{G} \rangle$ contains the neutral element $I$ if and only if there exists a non-empty subset $\mathcal{H} \subseteq \mathcal{G}$ such that $\langle \mathcal{H} \rangle$ is a group. In particular, if the Group Problem is decidable in the group $G$, then the Identity Problem is also decidable.*

For detailed definition of graph theory terms, see [6]. All graphs considered in this paper will be directed multigraphs. For a graph $G$, we denote by $V(G)$ its set of vertices and by $E(G)$ its set of edges. For a (directed) edge $e$, we denote by $s(e)$ the starting vertex of $e$.

A *loop* is an edge that starts and ends at the same vertex. A *circuit* is a path that starts and ends at the same vertex. An *Euler path* of a graph $G$ is a path that uses each edge exactly once. An *Euler circuit* is an Euler path that starts and ends at the same vertex. We call a graph *Eulerian* if it contains an Euler circuit. It is easy to see that attaching a circuit to an Eulerian graph still results in an Eulerian graph.

## Laurent polynomials and the wreath product $\mathbb{Z} \wr \mathbb{Z}$

A (univariate) *Laurent polynomial* with coefficients over $\mathbb{R}$ is an expression of the form

$$f = \sum_{i=p}^{q} a_i X^i, \quad \text{where } p, q \in \mathbb{Z} \text{ and } a_i \in \mathbb{R}, i = p, p+1, \ldots, q.$$

If $p > q$, then $f$ is understood to be zero. Otherwise, $p \leq q$, and we suppose $a_p \neq 0$, $a_q \neq 0$. In this case, we call $p$ the *negative degree* of $f$, denoted by $\deg_-(f)$, and call $q$ the *positive degree* of $f$, denoted by $\deg_+(f)$. We call $a_p$ the *negative leading coefficient* of $f$, denoted by $\mathrm{lc}_-(f)$, and call $a_q$ the *positive leading coefficient* of $f$, denoted by $\mathrm{lc}_+(f)$. Define additionally $\deg_-(0) = +\infty$, $\deg_+(0) = -\infty$ and $\mathrm{lc}_-(0) = \mathrm{lc}_+(0) = 0$. In this paper, all polynomials will be univariate Laurent polynomials. The set of all polynomials with coefficients over $\mathbb{R}$ forms a ring and is denoted by $\mathbb{R}[X^{\pm}]$. One can define $\mathbb{Q}[X^{\pm}]$ and $\mathbb{Z}[X^{\pm}]$ similarly by restricting the coefficients $a_i$ to $\mathbb{Q}$ and $\mathbb{Z}$.

Given a tuple of polynomials $\boldsymbol{f} = (f_1, \ldots, f_n) \in (\mathbb{R}[X^{\pm}])^n$ and $r \in \mathbb{R}$, one naturally defines the evaluation $\boldsymbol{f}(r) \coloneqq (f_1(r), \ldots, f_n(r)) \in \mathbb{R}^n$. The definition of leading coefficients also extends to tuples of polynomials by $\mathrm{lc}_*(\boldsymbol{f}) \coloneqq (\mathrm{lc}_*(f_1), \ldots, \mathrm{lc}_*(f_n)) \in \mathbb{R}^n$, where $* \in \{+, -\}$.

Consider the semiring $\mathbb{R}_{\geq 0}[X^{\pm}]$ of polynomials with positive coefficients: these are expressions of the form $f = \sum_{i=p}^{q} a_i X^i$ where $p, q \in \mathbb{Z}$ and $a_i \in \mathbb{R}_{\geq 0}, i = p, p+1, \ldots, q$. Define further $\mathbb{R}_{\geq 0}[X^{\pm}]^* \coloneqq \mathbb{R}_{\geq 0}[X^{\pm}] \setminus \{0\}$. One can define $\mathbb{N}[X^{\pm}]$ and $\mathbb{N}[X^{\pm}]^*$ similarly by restricting the coefficients $a_i$ to $\mathbb{N}$.

An element $f = \sum_{i=p}^{q} a_i X^i \in \mathbb{R}_{\geq 0}[X^{\pm}]^*$ is called *gap-free* if $a_i \neq 0$ for all $i = p, p+1, \ldots, q$. Is it easy to see that, given arbitrary $M, N \in \mathbb{Z}_{>0}$ and $f \in \mathbb{R}_{\geq 0}[X^{\pm}]^*$, the polynomial $(X^{-M} + X^{-M+1} + \cdots + X^N)^n \cdot f$ is gap-free for all large enough $n$.

A *monomial* is a polynomial $f = a_i X^i$ with only one term (including zero). Let $d \geq 1$ be a positive integer. One can define the semirings

$$\mathbb{N}[X^{\pm d}] \coloneqq \left\{ \sum_{i=p}^{q} a_{di} X^{di} \in \mathbb{N}[X^{\pm}] \right\}, \quad \mathbb{N}[X^{\pm d}]^* \coloneqq \mathbb{N}[X^{\pm d}] \setminus \{0\}.$$

These are polynomials whose monomials have degrees divisible by $d$. Similarly, if $a_{di} \neq 0$ for all $i = p, \ldots, q$, we will call $\sum_{i=p}^{q} a_{di} X^{di}$ gap-free. Note that whether a polynomial is gap-free depends on the polynomial ring we consider it in.

Similarly one can define the rings $\mathbb{Z}[X^{\pm d}]$, $\mathbb{Q}[X^{\pm d}]$ and $\mathbb{R}[X^{\pm d}]$. Furthermore, we define the field of rational functions $\mathbb{Q}(X)$ to be the set of expressions of the form $\frac{f}{g}$, where $f, g \in \mathbb{Q}[X^{\pm}]$. Similarly, $\mathbb{Q}(X^d)$ is defined as the set of expressions $\frac{f}{g}$, where $f, g \in \mathbb{Q}[X^{\pm d}]$.

The wreath product $\mathbb{Z} \wr \mathbb{Z}$ has several equivalent definitions. Here, we introduce the one most convenient to our purpose.

▶ **Definition 2.3.** The wreath product $\mathbb{Z} \wr \mathbb{Z}$ is a group whose elements are pairs of the form $(y, b)$, where $y \in \mathbb{Z}[X^{\pm}]$ and $b \in \mathbb{Z}$. The neutral element in $\mathbb{Z} \wr \mathbb{Z}$ is given by $(0, 0)$. Multiplication is defined by $(y, b) \cdot (y', b') = (y + X^b \cdot y', b + b')$, and inversion is defined by $(y, b)^{-1} = (X^{-b} \cdot y, -b)$. Note that the element $(y, b)$ corresponds to the matrix $\begin{pmatrix} X^b & y \\ 0 & 1 \end{pmatrix}$ under the isomorphism (1) in the introduction.

The wreath product $\mathbb{Z} \wr \mathbb{Z}$ can be embedded into the larger group $\mathbb{Q}(X) \rtimes \mathbb{Z}$, whose elements are pairs of the form $(y, b)$ with $y \in \mathbb{Q}(X)$ and $b \in \mathbb{Z}$ and whose multiplication and inversion are defined using the same formulas as in $\mathbb{Z} \wr \mathbb{Z}$.

## 3 Overview of proof

The main result of this paper is the decidability of the Identity Problem and the Group Problem in $\mathbb{Z} \wr \mathbb{Z}$. In view of Lemma 2.2, it suffices to prove decidability of the Group Problem. In this section we give an overview of its proof.

Our proof proceeds in three steps. As a first step we reduce the Group Problem in $\mathbb{Z} \wr \mathbb{Z}$ to deciding whether a system of linear equations in $\mathbb{R}[X^{\pm}]$ has solution in $\mathbb{R}_{\geq 0}[X^{\pm}]^*$ with two additional degree constraints (see Proposition 3.2 and Corollary 3.3). As the second step we prove a local-global principle that further reduces solving linear equations over $\mathbb{R}_{\geq 0}[X^{\pm}]^*$ to solving a family of "local" equations over $\mathbb{R}_{>0}$ (see Proposition 3.4). As the third step, we show that solving these "local" equations can be done using the first order theory of the reals as well as Gröbner basis techniques (see Proposition 3.5 and 3.6).

Let $\mathcal{G}$ be a finite subset of $\mathbb{Z} \wr \mathbb{Z}$. Write $\mathcal{G} = \{(y_a, b_a) \mid a \in A\}$ where $A$ is a finite set of indices. Divide $A$ into three subsets of indices $A = I \cup J \cup K$ where

$$I := \{i \mid b_i > 0\}, \quad J := \{j \mid b_j < 0\}, \quad K := \{k \mid b_k = 0\}. \tag{2}$$

First, we exclude the easy case where $I$ or $J$ is empty.

▶ **Proposition 3.1.** *Suppose $I = \emptyset$ or $J = \emptyset$. The semigroup $\langle \mathcal{G} \rangle$ is a group if and only if $I = J = \emptyset$ and $\sum_{k \in K} n_k y_k = 0$ for some positive integers $n_k \in \mathbb{Z}_{>0}$. In particular, this is decidable by integer programming.*

A simple proof of Proposition 3.1 is given in the Appendix A. For the rest of this paper, we will suppose $I \neq \emptyset$ and $J \neq \emptyset$.

Define

$$d := \gcd\left(\{b_a \mid a \in I \cup J\}\right).$$

For each pair $(i, j) \in I \times J$, define the rational function

$$h_{(i,j)} := \frac{y_i}{1 + X^d + \cdots + X^{b_i - d}} + \frac{y_j}{X^{-d} + X^{-2d} + \cdots + X^{-|b_j|}} \in \mathbb{Q}(X). \tag{3}$$

By direct computation we have

$$(y_i, b_i)^{|b_j|} \cdot (y_j, b_j)^{b_i} = \left(h_{(i,j)} \cdot (1 + X^d + \cdots + X^{b_i |b_j| - d}), 0\right). \tag{4}$$

One can also take (4) as the definition of $h_{(i,j)}$.

A subset $S$ of $I \times J$ is called *double-full* if for every $i \in I$ there exists $j_i \in J$ such that $(i, j_i) \in S$, and for every $j \in J$ there exists $i_j \in I$ such that $(i_j, j) \in S$. The following proposition reduces the Group Problem in $\mathbb{Z} \wr \mathbb{Z}$ to solving linear equations over $\mathbb{N}[X^{\pm d}]^*$.

▶ **Proposition 3.2.** *The semigroup $\langle \mathcal{G} \rangle$ is a group if and only if there exist a double-full set $S \subset I \times J$ and polynomials $f_{(i,j)}, f_k \in \mathbb{N}[X^{\pm d}]^*$ for $(i, j) \in S, k \in K$ that satisfy the following three conditions.*

**(i)** ***(Single linear equation)*** *The following equation over $\mathbb{Q}(X)$ is satisfied:*

$$\sum_{(i,j) \in S} f_{(i,j)} \cdot h_{(i,j)} + \sum_{k \in K} f_k \cdot y_k = 0. \tag{5}$$

**(ii)** ***(Positive degree bound)*** *We have:*

$$\deg_+\left(\sum\nolimits_{(i,j) \in S} f_{(i,j)}\right) + d \geq \deg_+\left(\sum\nolimits_{k \in K} f_k\right). \tag{6}$$

**(iii)** ***(Negative degree bound)*** *We have:*

$$\deg_-\left(\sum\nolimits_{(i,j)\in S} f_{(i,j)}\right) \leq \deg_-\left(\sum\nolimits_{k\in K} f_k\right). \tag{7}$$

The proof of Proposition 3.2 will be given in Section 4. The idea is roughly as follows. By Lemma 2.1, $\langle \mathcal{G} \rangle$ is a group if and only if there is a full-image word $w \in \mathcal{G}^*$ that represents the neutral element. For the "only if" statement of Proposition 3.2, we will represent $w$ as a walk over $\mathbb{Z}$, and decompose the walk into "primitive circuits". Each primitive circuit contributes a multiple of $h_{(i,j)}$ or $y_k$ to the element represented by $w$. Since $w$ represents the neutral element, this results in the linear equation in Condition (i). Conditions (ii) and (iii) will stem from the connectedness of the walk. The "if" statement is significantly harder. Given the polynomials $f_{(i,j)}, f_k$, we will construct an Eulerian graph $G$ by attaching long "elementary circuits" in a way that corresponds to the coefficients of $f_{(i,j)}, f_k$. We then read a word $w$ from an Euler circuit of $G$. Condition (i) will make sure $w$ represents the neutral element. However, making sure $G$ is connected is highly non-trivial and will be the main difficulty of the proof. In particular, Conditions (ii)-(iii) will be crucial. This concludes the idea of the proof for Proposition 3.2.

Note that Proposition 3.2 involves finding solutions over $\mathbb{N}[X^{\pm d}]^*$ for linear equations with coefficients in $\mathbb{Q}(X)$. When $d > 1$, this is inconvenient, so we now further reduce Proposition 3.2 to finding solutions over $\mathbb{R}_{\geq 0}[X^{\pm}]^*$ for a *system* of linear equations. For each $(i,j) \in I \times J$, since the denominator of $h_{(i,j)}$ is an element in $\mathbb{Q}[X^{\pm d}]$, there exist $h_{(i,j),0}, \ldots, h_{(i,j),d-1} \in \mathbb{Q}(X)$ such that $h_{(i,j)}$ can be written as

$$h_{(i,j)} = h_{(i,j),0}(X^d) + h_{(i,j),1}(X^d) \cdot X + \cdots + h_{(i,j),d-1}(X^d) \cdot X^{d-1}. \tag{8}$$

Similarly, for each $k \in K$, there exist $y_{k,0}, \ldots, y_{k,d-1} \in \mathbb{Q}[X^{\pm}]$ so that $y_k$ can be written as

$$y_k = y_{k,0}(X^d) + y_{k,1}(X^d) \cdot X + \cdots + y_{k,d-1}(X^d) \cdot X^{d-1}. \tag{9}$$

The following corollary shows that, using the elements $h_{(i,j),m}, y_{k,m}$ defined in (8) and (9), we can rewrite the conditions in Proposition 3.2 using only variables in $\mathbb{R}_{\geq 0}[X^{\pm}]^*$ instead of $\mathbb{N}[X^{\pm d}]^*$. See Appendix A for a simple proof of Corollary 3.3.

▶ **Corollary 3.3.** *The semigroup $\langle \mathcal{G} \rangle$ is a group if and only if there exist a double-full set $S \subset I \times J$ and polynomials $f_S, f_K, f_{(i,j)}, f_k \in \mathbb{R}_{\geq 0}[X^{\pm}]^*$ for $(i,j) \in S, k \in K$ that satisfy the following three conditions.*

**(i)** ***(System of linear equations)*** *The following linear equations over $\mathbb{R}(X)$ are satisfied:*

$$\sum_{(i,j)\in S} f_{(i,j)} h_{(i,j),m} + \sum_{k\in K} f_k y_{k,m} = 0, \quad m = 0, \ldots, d-1, \tag{10}$$

$$f_S = \sum_{(i,j)\in S} f_{(i,j)}, \qquad f_K = \sum_{k\in K} f_k. \tag{11}$$

**(ii)** ***(Positive degree bound)*** *We have:*

$$\deg_+(f_S) + 1 \geq \deg_+(f_K). \tag{12}$$

**(iii)** ***(Negative degree bound)*** *We have:*

$$\deg_-(f_S) \leq \deg_-(f_K). \tag{13}$$

For brevity, from now on we denote $\mathbb{A} \coloneqq \mathbb{R}[X^{\pm}]$ and $\mathbb{A}^+ \coloneqq \mathbb{R}_{\geq 0}[X^{\pm}]^*$. Denote also $n \coloneqq 2 + |S| + |K|$. Define the following subset of $\mathbb{A}^n$:

$$\mathcal{M} \coloneqq \left\{ \boldsymbol{f} = \left(f_S, f_K, (f_{(i,j)})_{(i,j)\in S}, (f_k)_{k\in K}\right) \in \mathbb{A}^n \;\middle|\; \boldsymbol{f} \text{ satisfies (10) and (11)} \right\}. \tag{14}$$

That is, $\mathcal{M}$ is the set of solutions of the linear equations (10)-(11). Using linear algebra over the polynomial ring $\mathbb{A}$ (see [1]), one can effectively compute a set of vectors $\boldsymbol{g}_1, \ldots, \boldsymbol{g}_m \in \mathbb{A}^n$ such that

$$\mathcal{M} = \{\phi_1 \boldsymbol{g}_1 + \cdots + \phi_m \boldsymbol{g}_m \mid \phi_1, \ldots, \phi_m \in \mathbb{A}\}. \tag{15}$$

One can even suppose $\boldsymbol{g}_1, \ldots, \boldsymbol{g}_m \in (\mathbb{Q}[X^{\pm}])^n$ since $h_{(i,j)}$ and $y_k$ all have rational coefficients. A set $\mathcal{M}$ of the form (15) will be called a $\mathbb{A}$-*submodule* of $\mathbb{A}^n$, and the elements $\boldsymbol{g}_1, \ldots, \boldsymbol{g}_m$ will be called a *basis* of $\mathcal{M}$.

Corollary 3.3 actually states the following: the semigroup $\langle \mathcal{G} \rangle$ is a group if and only if $\mathcal{M}$ contains an element $\boldsymbol{f} = (f_S, f_K, \ldots) \in (\mathbb{A}^+)^n$ such that $\deg_+(f_S) + 1 \geq \deg_+(f_K)$ and $\deg_-(f_S) \leq \deg_-(f_K)$. The key to deciding the existence of $\boldsymbol{f}$ is the following proposition, which can be considered as a local-global principle that generalizes a result of Einsiedler, Mouat and Tuncel [13].

▶ **Proposition 3.4.** *Let $\mathcal{M}$ be a $\mathbb{A}$-submodule of $\mathbb{A}^n$. Then $\mathcal{M}$ contains an element $\boldsymbol{f} = (f_S, f_K, \ldots) \in (\mathbb{A}^+)^n$ with $\deg_+(f_S) + 1 \geq \deg_+(f_K)$ and $\deg_-(f_S) \leq \deg_-(f_K)$, if and only if the following three conditions are all satisfied.*

**(i)** ***(Existence of $\boldsymbol{f}_r$ for all $r \in \mathbb{R}_{>0}$)*** *For each $r \in \mathbb{R}_{>0}$, there exists $\boldsymbol{f}_r \in \mathcal{M}$ such that*

$$\boldsymbol{f}_r(r) \in \mathbb{R}^n_{>0}. \tag{16}$$

**(ii)** ***(Existence of $\boldsymbol{f}_\infty$)*** *There exists $\boldsymbol{f}_\infty = (f_{\infty,S}, f_{\infty,K}, \ldots) \in \mathcal{M}$ such that*

$$\mathrm{lc}_+(\boldsymbol{f}_\infty) \in \mathbb{R}^n_{>0} \quad \textit{and} \quad \deg_+(f_{\infty,S}) + 1 \geq \deg_+(f_{\infty,K}). \tag{17}$$

**(iii)** ***(Existence of $\boldsymbol{f}_0$)*** *There exists $\boldsymbol{f}_0 = (f_{0,S}, f_{0,K}, \ldots) \in \mathcal{M}$ such that*

$$\mathrm{lc}_-(\boldsymbol{f}_0) \in \mathbb{R}^n_{>0} \quad \textit{and} \quad \deg_-(f_{0,S}) \leq \deg_-(f_{0,K}). \tag{18}$$

The proof of Proposition 3.4 will be given in Section 5. The original result of Einsiedler et al. [13, Theorem 1.3] gives a similar local-global principle without the degree constraints on $f_S$ and $f_K$. While our proof follows the main steps of the original proof, we need to introduce new arguments in order for the degree constraint to stay compatible with the local-global principle.

One direction of the implication in Proposition 3.4 is clear. In fact, if $f \in \mathbb{A}^+$ and $r \in \mathbb{R}_{>0}$, then we have $f(r) \in \mathbb{R}_{>0}$ and $\mathrm{lc}_+(f), \mathrm{lc}_-(f) \in \mathbb{R}_{>0}$. Therefore, if $\mathcal{M}$ contains an element $\boldsymbol{f} = (f_S, f_K, \cdots) \in (\mathbb{A}^+)^n$ with $\deg_+(f_S) + 1 \geq \deg_+(f_K)$ and $\deg_-(f_S) \leq \deg_-(f_K)$, then simply take $\boldsymbol{f}_r = \boldsymbol{f}_\infty = \boldsymbol{f}_0 = \boldsymbol{f}$ for all $r$: Equation (16) is satisfied for all $r$ as well as (17) and (18); hence all three conditions are satisfied.

On the other hand, if the Equation (16) as well as (17) and (18) can be satisfied *individually* by different $\boldsymbol{f}_r, \boldsymbol{f}_\infty, \boldsymbol{f}_0$, we cannot *a priori* find an element $\boldsymbol{f} \in \mathcal{M}$ in $(\mathbb{A}^+)^n$. Such an element $\boldsymbol{f}$ would *simultaneously* satisfy Equations (16) for all $r \in \mathbb{R}_{>0}$ as well as (17) and (18). The key idea of proving this non-trivial direction is that if all three conditions (i)-(iii) are satisfied, then we can "glue" these different $\boldsymbol{f}_r, \boldsymbol{f}_\infty$ and $\boldsymbol{f}_0$ together to obtain a single $\boldsymbol{f}$ that satisfies Equation (16) for *all* $r$ as well as (17) and (18). While this idea comes from the original

proof, the difficult part in our generalization is to make sure the degree constraints are still satisfied after the gluing procedure. In the end, we multiply this $\boldsymbol{f}$ by a "large enough" polynomial to obtain an element in $(\mathbb{A}^+)^n$, using a theorem of Handelman (Theorem 5.3).

The following two propositions show that Conditions (i), (ii) and (iii) of Proposition 3.4 are all decidable.

▶ **Proposition 3.5.** *Let $\mathcal{M}$ be an $\mathbb{A}$-submodule of $\mathbb{A}^n$. Given as input a finite basis of $\mathcal{M}$, it is decidable whether for every $r \in \mathbb{R}_{>0}$ there exists $\boldsymbol{f}_r \in \mathcal{M}$ with $\boldsymbol{f}_r(r) \in \mathbb{R}^n_{>0}$.*

▶ **Proposition 3.6.** *Let $* \in \{+, -\}$, $a \in \mathbb{Z}$ and $\mathcal{M}$ be an $\mathbb{A}$-submodule of $\mathbb{A}^n$. Given as input a finite basis of $\mathcal{M}$, it is decidable whether there exists $\boldsymbol{f} = (f_S, f_K, \cdots) \in \mathcal{M}$ such that*

$$\mathrm{lc}_*(\boldsymbol{f}) \in \mathbb{R}^n_{>0} \quad \textit{and} \quad \deg_*(f_S) + a \geq \deg_*(f_K)\,. \tag{19}$$

Proposition 3.5 and 3.6 will be proven in Section 6. The idea of proving Proposition 3.5 is to reduce the statement to the first order theory of the reals; while for proving Proposition 3.6 we will use the *super Gröbner basis* introduced in the original proof of Einsiedler et al. [13].

We are now ready to prove our main theorem by bridging the remaining gaps.

▶ **Theorem 3.7.** *The Identity Problem and the Group Problem in $\mathbb{Z} \wr \mathbb{Z}$ are decidable.*

**Proof.** First we show decidability of the Group Problem. Given a finite set $\mathcal{G} = \{(y_a, b_a) \mid a \in A\}$ in $\mathbb{Z} \wr \mathbb{Z}$, define the index sets $I, J, K$ as in (2). If $I$ or $J$ is empty, then Proposition 3.1 shows that the Group Problem for $\mathcal{G}$ is decidable. If $I$ and $J$ are not empty, we enumerate all double-full sets $S \subset I \times J$. For each $S$ we compute a finite basis of $\mathcal{M}$ defined in (14). Corollary 3.3 together with Proposition 3.4 shows that the Group Problem for $\mathcal{G}$ has a positive answer if and only if for some $S$, the three conditions in Proposition 3.4 are all satisfied. For each $S$, Condition (i) can be decided using Proposition 3.5; Condition (ii) can be decided using Proposition 3.6 by taking $* = +, a = 1$; Condition (iii) can be decided using Proposition 3.6 by swapping the coordinates $S$ and $K$ and taking $* = -, a = 0$. Therefore the Group Problem in $\mathbb{Z} \wr \mathbb{Z}$ is decidable. By Lemma 2.2, the Identity Problem in $\mathbb{Z} \wr \mathbb{Z}$ is also decidable. ◀

# 4 From semigroup to polynomial equations

## 4.1 Definition of $\mathcal{G}$-graphs

Section 4 is dedicated to the proof of Proposition 3.2. In this subsection, we will define the notion of a *$\mathcal{G}$-graph*. Let $A$ be a finite set of indices. Let $\mathcal{G} = \{(y_a, b_a) \mid a \in A\}$ be a finite set of elements in the group $\mathbb{Z} \wr \mathbb{Z}$ or $\mathbb{Q}(X) \rtimes \mathbb{Z}$. We define the following notion of a $\mathcal{G}$-graph.

▶ **Definition 4.1** ($\mathcal{G}$-graphs)**.** A *$\mathcal{G}$-graph* is a directed multigraph $G$, whose set of vertices $V(G)$ is a finite subset of $\mathbb{Z}$, and its edges are each labeled with an index in $A$. Furthermore, if an edge from vertex $d_1$ to vertex $d_2$ has label $a$, then $d_2 = d_1 + b_a$.

For a word $w$ over the alphabet $\mathcal{G}$, we associate to it a unique $\mathcal{G}$-graph $G(w)$, defined as follows. Write $w = (y_{a_1}, b_{a_1}) \cdots (y_{a_p}, b_{a_p})$. For each $i = 0, \ldots, p-1$, we add an edge starting at the vertex $b_{a_1} + \cdots + b_{a_i}$, ending at the vertex $b_{a_1} + \cdots + b_{a_{i+1}}$, with the label $a_i$. (If $i = 0$ then the edge starts at 0 and ends at $b_{a_1}$.) The graph $G(w)$ is then obtained by taking the connected component of the vertex 0. See Figure 1 for the illustration of an example.

By reading the letters in $w$ one by one and tracing the corresponding edges of $G(w)$, we obtain an Euler path of $G(w)$. Furthermore, if the word $w$ represents the neutral element (or any element of the form $(y, 0)$), then this Euler path is an Euler circuit.

We point out that the element which $w$ represents is uniquely determined by $G(w)$:

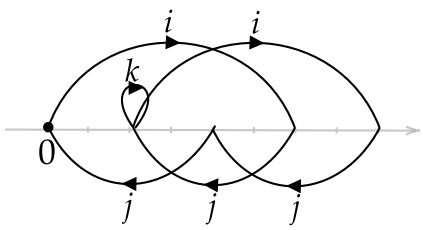


**Figure 1** Illustration of $G(w)$. Here, $A = \{i, j, k\}$, $\mathcal{G} = \{(y_i, 6), (y_j, -4), (y_k, 0)\}$, $w = (y_i, 6)(y_j, -4)(y_k, 0)(y_i, 6)(y_j, -4)(y_j, -4)$.

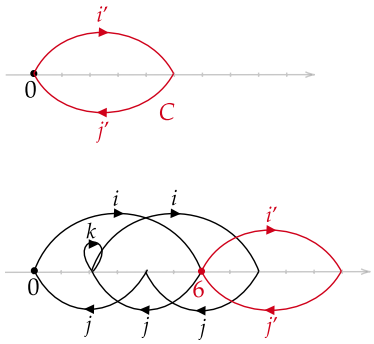


**Figure 2** Attaching the circuit $C$ to $G(w)$ at vertex 6.

▶ **Fact 4.2** (Product of associated graph)**.** Let $w$ be a word over the alphabet $\mathcal{G}$, and let $G = G(w)$ be its associated $\mathcal{G}$-graph. For an edge $e \in E(G)$, denote by $\ell(e)$ the label of $e$, denote by $s(e) \in \mathbb{Z}$ the starting vertex of $e$, then $w$ represents the element

$$\left( \sum_{e \in E(G)} X^{s(e)} \cdot y_{\ell(e)}, \sum_{e \in E(G)} b_{\ell(e)} \right). \tag{20}$$

For an arbitrary $\mathcal{G}$-graph $G$, the element in Expression (20) will be called the *product* of the graph $G$. It is easy to see that, if $G$ contains an Eulerian path, then by following this path we obtain a word $w$ that represents the product of $G$.

Let $C$ be a another Eulerian $\mathcal{G}$-graph (seen as a circuit). We define the following action of *attaching $C$ to $G$ at vertex $v$*: For each edge $e$ of $C$, starting at vertex $s(e)$ with label $\ell(e)$, we add an edge $e'$ to $G$, starting at vertex $s(e) + v$ with label $\ell(e)$. See Figure 2 for the illustration of an example. The product of the resulting graph is uniquely determined by $G$, $C$ as well as $v$:

▶ **Fact 4.3** (Effect of attaching circuit to a graph)**.** Let $G$ be an arbitrary $\mathcal{G}$-graph and $C$ be an Eulerian $\mathcal{G}$-graph. Denote by $(y_G, b_G)$ the product of $G$ and by $(y_C, 0)$ the product of $C$. Then attaching $C$ to $G$ at vertex $v$ results in a graph with product $(y_G + X^v \cdot y_C, b_G)$.

## 4.2 Group Problem implies polynomial equations

In this subsection, we prove the "only if" part of Proposition 3.2. We will show that if $\langle \mathcal{G} \rangle$ is a group then there exists a double-full set $S \subset I \times J$ and polynomials $f_{(i,j)}, f_k \in \mathbb{N}[X^{\pm d}]^*$ for $(i, j) \in S, k \in K$ satisfying (i)-(iii) of Proposition 3.2.

Recall that $d \coloneqq \gcd\left(\{b_a \mid (y_a, b_a) \in \mathcal{G}\}\right)$. Define the alphabet $\widehat{\mathcal{G}}$ of *radical* elements:

$$\widehat{\mathcal{G}} \coloneqq \left\{ (\widehat{y}_a, \widehat{b}_a) \;\middle|\; (y_a, b_a) \in \mathcal{G} \right\},$$

where

$$(\widehat{y}_a, \widehat{b}_a) \coloneqq \begin{cases} \left( \frac{y_a}{1 + X^d + \cdots + X^{b_a - d}}, d \right) & a \in I \quad \text{(or equivalently, } b_a > 0\text{)}, \\ \left( \frac{y_a}{1 + X^{-d} + \cdots + X^{-(|b_a| - d)}}, -d \right) & a \in J \quad \text{(or equivalently, } b_a < 0\text{)}, \\ (y_a, 0) & a \in K \quad \text{(or equivalently, } b_a = 0\text{)}. \end{cases}$$

Note that these elements are in $\mathbb{Q}(X) \rtimes \mathbb{Z}$ instead of $\mathbb{Z} \wr \mathbb{Z}$. Direct computation shows that

$$(\widehat{y}_a, \widehat{b}_a)^{|b_a|/d} = (y_a, b_a) \tag{21}$$

for $a \in I \cup J$. Equation (21) can also be taken as the definition of $(\widehat{y}_a, \widehat{b}_a)$.

Since $\langle \mathcal{G} \rangle$ is a group, by Lemma 2.1 there exists a full-image word $w \in \mathcal{G}^*$ that represents the neutral element. Replacing the letters $(y_a, b_a)$ in $w$ by the words $\underbrace{(\widehat{y}_a, \widehat{b}_a) \cdots (\widehat{y}_a, \widehat{b}_a)}_{|b_a|/d \text{ times}}$ for every $a \in I \cup J$, we obtain a word $\widehat{w} \in \widehat{\mathcal{G}}^*$. By Equation (21), $\widehat{w}$ also represents the neutral element. To the word $\widehat{w}$ we associate a $\widehat{\mathcal{G}}$-graph $G(\widehat{w})$. See Figure 3 for the illustration of an example of $G(\widehat{w})$; one can compare it with Figure 1 which illustrates $G(w)$ for the same $w$.

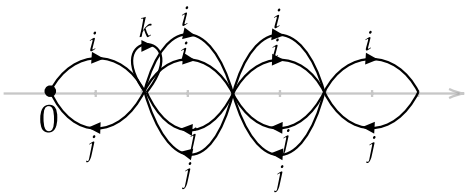


**Figure 3** Decomposition of $G(\widehat{w})$. Here $\mathcal{G}$ and $w$ are the same as in Figure 1.

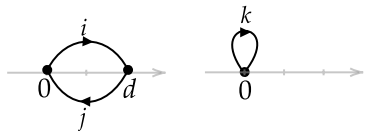


**Figure 4** Primitive circuits of type $(i, j)$ and $k$.

Since $\widehat{w}$ represents the neutral element, the graph $G(\widehat{w})$ is Eulerian. Since $\widehat{b}_a = \pm d$ or $0$ for all indices $a \in I \cup J \cup K$, the graph $G(\widehat{w})$ can be decomposed into two classes of smaller circuits. The first class of circuits is an edge with some label $i \in I$ (edge directed to the right) followed by an edge with some label $j \in J$ (edge directed to the left); we call such a circuit *of the type* $(i, j)$. The second class is a loop with label $k \in K$; we call such a circuit *of the type* $k$. We call these two classes of circuits *primitive*. See Figure 4 for an illustration.

▶ **Lemma 4.4.** *The graph $G(\widehat{w})$ can be constructed by starting with an edgeless graph with a single vertex $0$ and gradually attaching primitive circuits.*

Recall the definition of $h_{(i,j)}$ in Equation (3). In fact, $h_{(i,j)}$ is the product of a primitive circuit of type $(i, j)$, meaning $(\widehat{y}_i, \widehat{b}_i) \cdot (\widehat{y}_j, \widehat{b}_j) = (h_{(i,j)}, 0)$. Similarly, the product of a circuit of type $k$ is $(h_k, 0) \coloneqq (y_k, 0)$. By Lemma 4.4, $G(\widehat{w})$ can be decomposed into primitive circuits. For each primitive circuit $C$ in the decomposition, denote by $s(C) \in d\mathbb{Z}$ the vertex where $C$ is attached, and by $type(C)$ the type of $C$. Denote by $\mathcal{C}$ the set of circuits in the decomposition of $G(\widehat{w})$ into primitive circuits. By Fact 4.3, the product of $G(\widehat{w})$ can be written as

$$\left( \sum_{C \in \mathcal{C}} X^{s(C)} \cdot h_{type(C)}, 0 \right) = (0, 0). \tag{22}$$

For each $(i, j) \in I \times J$ and $k \in K$, define the following polynomials in $\mathbb{N}[X^{\pm d}]$:

$$f_{(i,j)} \coloneqq \sum_{C \in \mathcal{C} \text{ of type } (i,j)} \left(X^d\right)^{\frac{s(C)}{d}}, \quad f_k \coloneqq \sum_{C \in \mathcal{C} \text{ of type } k} \left(X^d\right)^{\frac{s(C)}{d}}. \tag{23}$$

Let $S \coloneqq \{(i, j) \in I \times J \mid f_{(i,j)} \neq 0\}$. We point out that $f_k \neq 0$ for all $k \in K$, because $\widehat{w}$ is full-image, meaning $G(\widehat{w})$ contains a loop of label $k$ for each $k \in K$. Equation (22) becomes

$$\sum_{(i,j) \in S} f_{(i,j)} \cdot h_{(i,j)} + \sum_{k \in K} f_k \cdot y_k = 0. \tag{24}$$

This is exactly Condition (i) of Proposition 3.2. It suffices to show the following to complete the proof of the first implication of Proposition 3.2.

▶ **Lemma 4.5.** *Let $f_{(i,j)}, f_k \in \mathbb{N}[X^{\pm d}]$ and $S \subset I \times J$ be defined as above, then:*

**(i)** *$S$ is double-full.*

**(ii)** $\deg_+ \left(\sum_{(i,j)\in S} f_{(i,j)}\right) + d \geq \deg_+ \left(\sum_{k\in K} f_k\right)$.

**(iii)** $\deg_- \left(\sum_{(i,j)\in S} f_{(i,j)}\right) \leq \deg_- \left(\sum_{k\in K} f_k\right)$.

**Sketch of proof.** For (i), $S$ is double full since $G(\widehat{w})$ contains edges of each type of labels. For (ii) and (iii), it suffices to notice that $G(\widehat{w})$ must be connected while $\max(V(G(\widehat{w}))) = \deg_+ \left(\sum_{(i,j)\in S} f_{(i,j)}\right) + d$ and $\min(V(G(\widehat{w}))) = \deg_- \left(\sum_{(i,j)\in S} f_{(i,j)}\right)$. ◀

**Proof of "only if" part of Proposition 3.2.** If $\langle \mathcal{G} \rangle$ is a group, then there exists a full-image word $w \in \mathcal{G}^*$ that represents the neutral element. Consider $G(\widehat{w})$ and let $f_{(i,j)}, f_k \in \mathbb{N}[X^{\pm d}]^*, (i,j) \in S, k \in K$, be as defined in (23). The Conditions (i)-(iii) of Proposition 3.2 follow directly from Equation (24) and Lemma 4.5. ◀

## 4.3 Polynomial equation implies Group Problem

In this subsection, we prove the "if" part of Proposition 3.2. Given a double-full set $S \subset I \times J$ and positive polynomials $f_{(i,j)}, f_k \in \mathbb{N}[X^{\pm d}]^*$ for $(i,j) \in S, k \in K$ that satisfy Conditions (i)-(iii) of Proposition 3.2, we will construct an Eulerian $\mathcal{G}$-graph $G$ with product zero. The main difficulty here is that the length of the edges of a $\mathcal{G}$-graph are no longer identical, as opposed to $\widehat{\mathcal{G}}$-graphs. Therefore one can no longer decompose $\mathcal{G}$-graphs into primitive circuits. The key idea is a work-around that simulates primitive circuits using longer circuits.

For $(i,j) \in I \times J$, we define an *elementary circuit of the type* $(i,j)$ to be a circuit that starts with $|b_j|$ edges of label $i$, followed by $b_i$ edges of label $j$. See Figure 5 for an example.

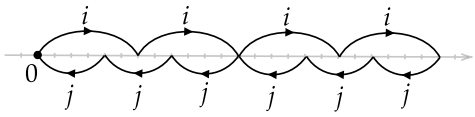


**Figure 5** An elementary circuit of type $(i,j)$. Here, $b_i = 6, b_j = -4$.

▶ **Lemma 4.6.** *Suppose $S \subset I \times J$ be double-full. There exists an Eulerian $\mathcal{G}$-graph $A$ with $d \in V(A)$, obtained by attaching together elementary circuits of types in $S$.*

The idea of constructing $A$ is illustrated in Figure 6, with a detailed proof given in Appendix A. We now characterize the product of $A$. An elementary circuit of type $(i,j)$ attached at vertex $dv$ contributes $X^{dv}(1 + X^d + \cdots + X^{b_i|b_j|-d}) \cdot h_{(i,j)}$ to the product (see Equation (4)). Since $A$ is a combination of elementary circuits, the product of $A$ can written as $\sum_{(i,j)\in S} a_{(i,j)} h_{(i,j)}$ for some $a_{(i,j)} \in \mathbb{N}[X^{\pm d}]$.

Let $N := \prod_{i\in I\cup J} |b_i|$. Note that simultaneously multiplying all $f_{(i,j)}$ and $f_k$ by any polynomial $g \in \mathbb{N}[X^{\pm d}]^*$ does not change the fact that $f_{(i,j)}, f_k \in \mathbb{N}[X^{\pm d}]^*$, and they still satisfy Conditions (i)-(iii) of Proposition 3.2. Also note that $1 + X^d + \cdots + X^{b_i|b_j|-d} \mid 1 + X^d + \cdots + X^{N-d}$. Therefore, by simultaneously multiplying all $f_{(i,j)}$ and $f_k$ by $p \cdot (X^{-d} + 1 + \cdots + X^{N-2d})^q$ for large enough $p, q \in \mathbb{N}$, we can suppose that for all $(i,j) \in S$,

$$g_{(i,j)} := \frac{f_{(i,j)} - a_{(i,j)} \cdot (1 + X^d + \cdots + X^{N-d})}{1 + X^d + \cdots + X^{b_i|b_j|-d}} \in \mathbb{N}[X^{\pm d}]^* \quad \text{is gap-free,} \tag{25}$$

and

$$\deg_+ \left(f_{(i,j)}\right) > \deg_+(a_{(i,j)}) + N - d, \qquad \deg_- \left(f_{(i,j)}\right) < \deg_-(a_{(i,j)}). \tag{26}$$

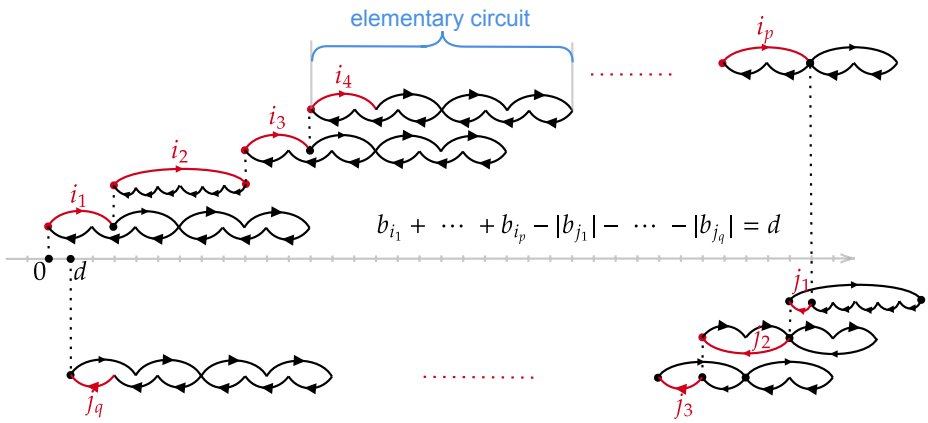


**Figure 6** Graph $A$ from Lemma 4.6.

▶ **Proposition 4.7.** *Suppose $S$ is double-full and $f_{(i,j)}, f_k \in \mathbb{N}[X^{\pm d}]^*, (i,j) \in S, k \in K$, satisfy Equations (25), (26) and Conditions (ii)-(iii) of Proposition 3.2, then there exists an Eulerian $\mathcal{G}$-graph $G$ whose product is $\sum_{(i,j)\in S} f_{(i,j)} \cdot h_{(i,j)} + \sum_{k\in K} f_k \cdot y_k$.*

**Proof.** We construct $G$ in three steps. See Figure 7 for an illustration.

**Step 1: Constructing the foundation $A'$.** We start with the $\mathcal{G}$-graph $A$ constructed in Lemma 4.6. We then attach to it another $N/d - 1$ copies of $A$, where the $k$-th copy is attached at vertex $dk$. The resulting graph is still Eulerian because $d \in V(A)$. We denote by $A'$ the $\mathcal{G}$-graph obtained by this attachment. Then we have $0, d, \cdots, N - d \in V(A')$.

**Step 2: Attaching elementary circuits of type $(i,j) \in S$.** For each pair $(i,j) \in S$, we want to attach elementary circuits of type $(i,j)$ to the graph $A'$, such that the total contribution of these circuits to the product is $g_{(i,j)} \cdot \left(1 + X^d + \cdots + X^{b_i|b_j|-d}\right) \cdot h_{(i,j)}$, where $g_{(i,j)}$ is defined in (25). Write $g_{(i,j)} = \sum_{t=p}^{q} \gamma_t X^{dt}$. We attach a total of $\sum_{t=p}^{q} \gamma_t$ elementary circuits of type $(i,j)$ to $A'$, where for $t = p, p+1, \ldots, q$, exactly $\gamma_t$ of these circuits are attached at the vertex $dt$. The resulting graph is connected (and Eulerian) because $g_{(i,j)}$ is gap-free. In fact, for each $t \in [\deg_-(g_{(i,j)})/d, \left(\deg_+(g_{(i,j)}) + b_i|b_j|\right)/d] \cap \mathbb{Z}$ and $u \in [0, N)$, such that $dt \equiv du \mod b_i|b_j|$, the vertex $dt$ is connected to $du \in V(A')$ by a chain of circuits of type $(i,j)$. Denote by $A''$ the resulting graph after doing the above attachments for all $(i,j) \in S$. Then

$$dt \in V(A'') \text{ for all } t \in [\deg_-(g_{(i,j)})/d, \left(\deg_+(g_{(i,j)}) + b_i|b_j|\right)/d] \cap \mathbb{Z},\ (i,j) \in S. \tag{27}$$

**Step 3: Attaching loops of type $k \in K$.** For each $k \in K$, we want to attach loops of label $k \in K$ to $A''$, such that the total contribution of these loops to the product is $f_k \cdot y_k$. Write $f_k = \sum_{t=p}^{q} \beta_t X^{dt}$, we attach a total of $\sum_{t=p}^{q} \beta_t$ loops of label $k$ to $A''$, where for $t = p, p+1, \ldots, q$, exactly $\beta_t$ of these loops are attached at the vertex $dt$.

We need to prove that the resulting graph $G$ is still connected (and hence Eulerian). In view of Property (27) of the graph $A''$, it suffices to prove $\deg_-(f_k) \geq \min_{(i,j)\in S}\left\{\deg_-(g_{(i,j)})\right\}$ and $\deg_+(f_k) \leq \max_{(i,j)\in S}\left\{\deg_+(g_{(i,j)}) + b_i|b_j|\right\}$ for all $k \in K$. By Equations (25) and (26), we have $\deg_-(g_{(i,j)}) = \deg_-(f_{(i,j)})$ and $\deg_+(g_{(i,j)}) + b_i|b_j| - d = \deg_+(f_{(i,j)})$ for all $(i,j) \in S$. Then, by Conditions (ii) and (iii) of Proposition 3.2, we have

$$\deg_-(f_k) \geq \deg_-\left(\sum_{k\in K} f_k\right) \geq \min_{(i,j)\in S}\{\deg_-(f_{(i,j)})\} = \min_{(i,j)\in S}\{\deg_-(g_{(i,j)})\},$$
$$\deg_+(f_k) \leq \deg_+\left(\sum_{k\in K} f_k\right) \leq \max_{(i,j)\in S}\{\deg_+(f_{(i,j)})\} + d = \max_{(i,j)\in S}\{\deg_-(g_{(i,j)}) + b_i|b_j|\},$$

for all $k \in K$. Therefore, the resulting graph $G$ is still connected.

Finally, we count the product of $G$. The product of $A'$ is $(1 + X^d + \cdots + X^{N-d}) \cdot \sum_{(i,j)\in S} a_{(i,j)} h_{(i,j)}$. The total contribution of elementary circuits in Step 2 is $\sum_{(i,j)\in S} g_{(i,j)} \cdot \left(1 + X^d + \cdots + X^{b_i|b_j|-d}\right) \cdot h_{(i,j)}$. The total contribution of loops in Step 3 is $\sum_{k\in K} f_k \cdot y_k$. Thus, by Equation (25), the product of $G$ is $\sum_{(i,j)\in S} f_{(i,j)} \cdot h_{(i,j)} + \sum_{k\in K} f_k \cdot y_k$. ◀

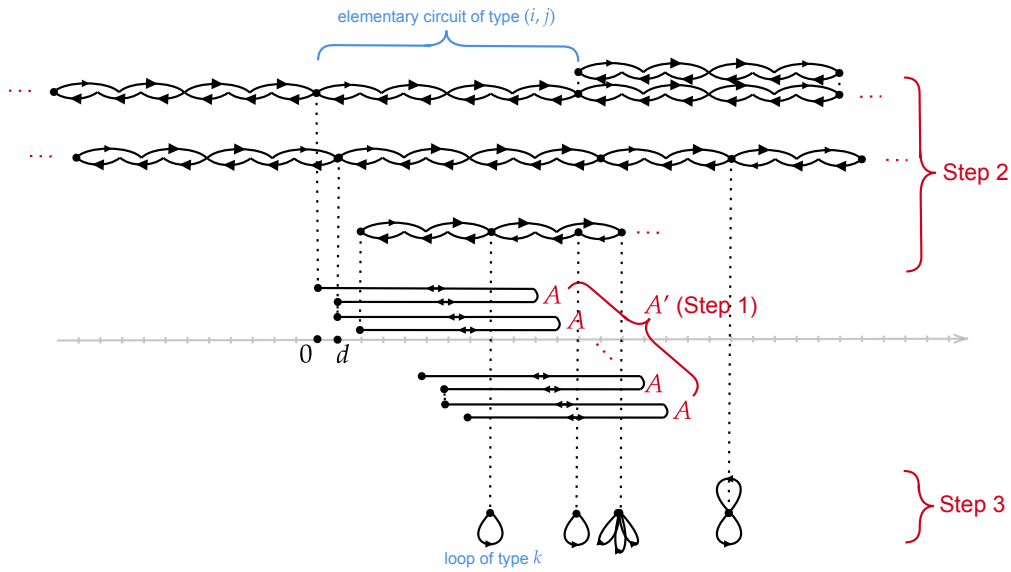


**Figure 7** Graph $G$ from Proposition 4.7.

**Proof of "if" part of Proposition 3.2.** We use Proposition 4.7 to prove the "if" part of Proposition 3.2. Suppose there exist a double-full set $S \subset I \times J$ and polynomials $f_{(i,j)}, f_k \in \mathbb{N}[X^{\pm d}]^*$ for $(i,j) \in S, k \in K$ that satisfy Conditions (i)-(iii). Recall that by simultaneously multiplying all $f_{(i,j)}$ and $f_k$ by $p \cdot (X^{-d} + 1 + X^d + \cdots + X^{N-2d})^q$ for large enough $p, q \in \mathbb{N}$, we can suppose Equations (25) and (26) to be satisfied. Then Proposition 4.7 gives an Eulerian $\mathcal{G}$-graph $G$ whose product is $\left(\sum_{(i,j)\in S} f_{(i,j)} \cdot h_{(i,j)} + \sum_{k\in K} f_k \cdot y_k, 0\right)$. This product is equal to the neutral element due to Conditions (i) of Proposition 3.2. By following an Eulerian cycle of $G$, we obtain a word $w$ representing the neutral element. The word $w$ is full-image because $G$ contains elementary circuits of all types $(i,j) \in S$ and loops of all types $k \in K$, and because $S$ is double-full. Therefore $\langle \mathcal{G} \rangle$ is a group by Lemma 2.1. ◀

## 5 A local-global principle for polynomial equations

In this section we prove Proposition 3.4. We follow the line of proof for the original result of Einsiedler et al. [13], while introducing new elements concerning the degree constraints. See Figure 8 in Appendix A for an illustration of the proof.

▶ **Lemma 5.1.** *Suppose Conditions (ii) and (iii) of Proposition 3.4 hold. Then there exists* $\boldsymbol{f}_{end} = (f_{end,S}, f_{end,K}, \cdots) \in \mathcal{M}$ *such that*

$$\mathrm{lc}_+(\boldsymbol{f}_{end}) \in \mathbb{R}^n_{>0}, \quad \deg_+(f_{end,S}) + 1 \geq \deg_+(f_{end,K}), \text{ and} \tag{28}$$

$$\mathrm{lc}_-(\boldsymbol{f}_{end}) \in \mathbb{R}^n_{>0}, \quad \deg_-(f_{end,S}) \leq \deg_-(f_{end,K}). \tag{29}$$

Since $\mathrm{lc}_\pm(\boldsymbol{f}_{end}) \in \mathbb{R}^n_{>0}$, there exists $c > 1$, such that $\boldsymbol{f}_{end}(x) \in \mathbb{R}^n_{>0}$ for all $x \in \mathbb{R}_{>0} \backslash [1/c, c]$. Define the compact set $C := [1/4c, 4c]$.

▶ **Lemma 5.2.** *Suppose Condition (i) of Proposition 3.4 hold. Let* $C \subset \mathbb{R}_{>0}$ *be a compact set, then there exists* $\boldsymbol{f}_C = (f_{C,S}, f_{C,K}, \cdots) \in \mathcal{M}$ *such that* $\boldsymbol{f}_C(x) \in \mathbb{R}^n_{>0}$ *for all* $x \in C$.

The key ingredient for finding an element in $(\mathbb{A}^+)^n$ is the following corollary of Handelman's Theorem.

▶ **Theorem 5.3** (Corollary of Handelman's Theorem [10, 15])**.** *Let* $\boldsymbol{f} \in \mathbb{A}^n$. *There exists* $g \in \mathbb{A}^+$ *such that* $g \cdot \boldsymbol{f} \in (\mathbb{A}^+)^n$ *if and only if the two following conditions are satisfied:*

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

**(ii)** *We have* $\mathrm{lc}_+(\boldsymbol{f}) \in \mathbb{R}^n_{>0}$ *and* $\mathrm{lc}_-(\boldsymbol{f}) \in \mathbb{R}^n_{>0}$.

We now sketch a proof of Proposition 3.4 by "gluing" the two elements $\boldsymbol{f}_{end}$ and $\boldsymbol{f}_C$ obtained respectively in Lemma 5.1 and 5.2, then applying Theorem 5.3. For an illustration of the proof, see Figure 8.

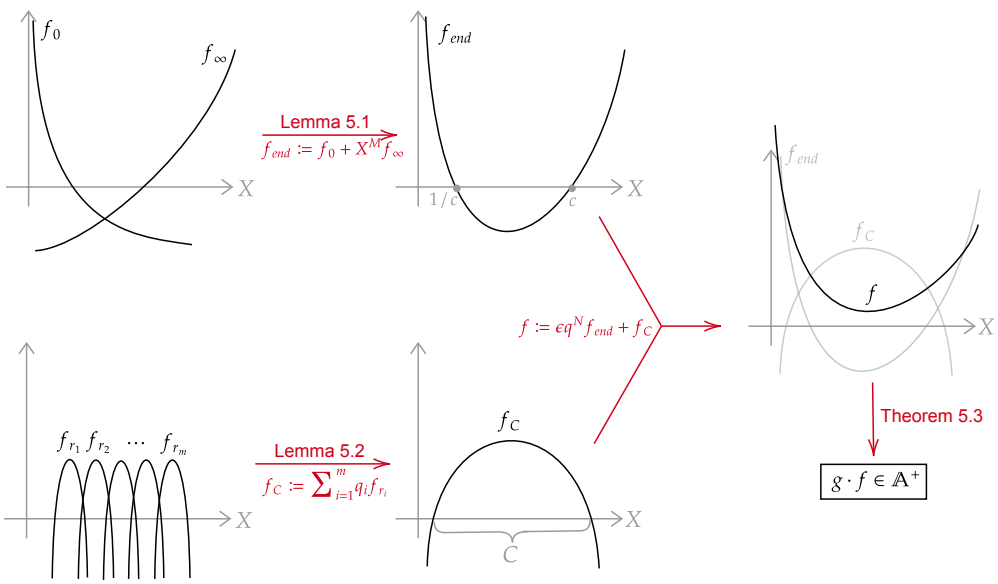


**Figure 8** Proof of Proposition 3.4, illustrated at dimension $n = 1$.

**Sketch of proof of Proposition 3.4.** If $\mathcal{M}$ contains an element $\boldsymbol{f} = (f_S, f_K, \cdots) \in (\mathbb{A}^+)^n$ with $\deg_+(f_S) + 1 \geq \deg_+(f_K)$ and $\deg_-(f_S) \leq \deg_-(f_K)$, then simply take $\boldsymbol{f}_r = \boldsymbol{f}_\infty = \boldsymbol{f}_0 = \boldsymbol{f}$ for all $r \in \mathbb{R}_{>0}$: Equation (16) is satisfied for all $r$ as well as (17) and (18).

Consider the non-trivial direction of implication. Let $\boldsymbol{f}_{end}, \boldsymbol{f}_C \in \mathcal{M}$ be the elements obtained respectively in Lemma 5.1 and 5.2. Define the polynomial $q := \frac{1}{2c}(X + X^{-1})$. Let $\epsilon > 0$ be such that $\epsilon \cdot \boldsymbol{f}_{end}(x) + \boldsymbol{f}_C(x) \in \mathbb{R}^n_{>0}$ for all $x \in C$. Such an $\epsilon$ exists by the compactness of $C$. We claim that there exists $N \in \mathbb{N}$ such that $\boldsymbol{f} := \epsilon q^N \cdot \boldsymbol{f}_{end} + \boldsymbol{f}_C$ satisfies Conditions (i) and (ii) in Theorem 5.3 simultaneously.

Let $M \in \mathbb{N}$ be such that $\deg_+(f_{end,i}) + M > \deg_+(f_{C,i})$ and $\deg_-(f_{end,i}) - M < \deg_-(f_{C,i})$ for every coordinate $i = S, K, \cdots, n$. Let $\boldsymbol{g} \coloneqq \epsilon q^M \cdot \boldsymbol{f}_{end} + \boldsymbol{f}_C$. Then we have $\mathrm{lc}_+(\boldsymbol{g}) = \mathrm{lc}_+(\boldsymbol{f}_{end}) \in \mathbb{R}^n_{>0}$ and $\mathrm{lc}_-(\boldsymbol{g}) = \mathrm{lc}_-(\boldsymbol{f}_{end}) \in \mathbb{R}^n_{>0}$, as well as

$$\deg_+(g_S) + 1 = \deg_+(f_{end,S}) + M + 1 \geq \deg_+(f_{end,K}) + M = \deg_+(g_K),$$
$$\deg_-(g_S) = \deg_-(f_{end,S}) - M \leq \deg_-(f_{end,K}) - M = \deg_-(g_K).$$

Therefore, there exists a compact set $[1/d, d] \supset C$ such that $\boldsymbol{g}(x) \in \mathbb{R}^n_{>0}$ for all $x \in \mathbb{R}_{>0} \setminus [1/d, d]$. Since $[1/d, d]$ is compact, there exists $N > M$ such that $\epsilon f_{end,i}(x) \cdot 2^N + f_{C,i}(x) > 0$ for all $i = S, K, \cdots, n$, and all $x \in [1/d, d]$.

For this $N$, the vector $\boldsymbol{f} \coloneqq \epsilon q^N \cdot \boldsymbol{f}_{end} + \boldsymbol{f}_C$ satisfies both Conditions (i) and (ii) in Theorem 5.3 (see the full proof in Appendix A). Therefore, we can find $g \in \mathbb{A}^+$ such that $g\boldsymbol{f} \in (\mathbb{A}^+)^n$. We have at the same time $g\boldsymbol{f} \in \mathcal{M}$ as well as $\deg_+(gf_S) + 1 \geq \deg_+(gf_K)$ and $\deg_-(gf_S) \leq \deg_-(gf_K)$. We have thus found the required element $g\boldsymbol{f}$. ◀

## 6 Decidability of local conditions

In this section we prove Proposition 3.5 and 3.6. Let $\mathcal{M}$ be an $\mathbb{A}$-submodule of $\mathbb{A}^n$.

▶ **Lemma 6.1.** *Let $\boldsymbol{g}_1, \ldots, \boldsymbol{g}_m$ be a basis of $\mathcal{M}$ and $r \in \mathbb{R}_{>0}$. There exists $\boldsymbol{f} \in \mathcal{M}$ with $\boldsymbol{f}(r) \in \mathbb{R}^n_{>0}$ if and only if there exist $r_1, \ldots, r_m \in \mathbb{R}$ such that $r_1\boldsymbol{g}_1(r) + \cdots + r_m\boldsymbol{g}_m(r) \in \mathbb{R}^n_{>0}$.*

▶ **Proposition 3.5.** *Let $\mathcal{M}$ be an $\mathbb{A}$-submodule of $\mathbb{A}^n$. Given as input a finite basis of $\mathcal{M}$, it is decidable whether for every $r \in \mathbb{R}_{>0}$ there exists $\boldsymbol{f}_r \in \mathcal{M}$ with $\boldsymbol{f}_r(r) \in \mathbb{R}^n_{>0}$.*

**Proof.** By Lemma 6.1, the statement to be decided is equivalent to the following sentence in the first order theory of the reals:

$$\forall r, r > 0 \implies (\exists r_1 \exists r_2 \cdots \exists r_m, r_1\boldsymbol{g}_1(r) + \cdots + r_m\boldsymbol{g}_m(r) \in \mathbb{R}^n_{>0}). \tag{30}$$

Its truth is decidable by Tarski's Theorem [28]. ◀

For Proposition 3.6, we start by the following definitions.

▶ **Definition 6.2.**

**(i)** Suppose $f = \sum_{i=p}^{q} a_i X^i \in \mathbb{A} \setminus \{0\}$, where $a_p a_q \neq 0$. Define $\mathrm{in}_+(f) \coloneqq a_q X^q$ and $\mathrm{in}_-(f) \coloneqq a_p X^p$. Additionally define $\mathrm{in}_+(0) = \mathrm{in}_-(0) = 0$.

**(ii)** Given $* \in \{+, -\}$, $\boldsymbol{\alpha} = (\alpha_S, \alpha_K, \ldots) \in \mathbb{Z}^n$ and $\boldsymbol{f} = (f_S, f_K, \ldots) \in \mathbb{A}^n$. Define $\mathrm{sgn}(*) = 1$ when $* = +$, and $\mathrm{sgn}(*) = -1$ when $* = -$. Let

$$m_{*,\boldsymbol{\alpha}}(\boldsymbol{f}) \coloneqq \max\{\mathrm{sgn}(*) \cdot \deg_*(f_S) + \alpha_S, \mathrm{sgn}(*) \cdot \deg_*(f_K) + \alpha_K, \ldots\}.$$

Define $\mathrm{in}_{*,\boldsymbol{\alpha}}(\boldsymbol{f}) \coloneqq (g_S, g_K, \ldots)$, where for $j = S, K, \ldots$,

$$g_j \coloneqq \begin{cases} \mathrm{in}_*(f_j) & \mathrm{sgn}(*) \cdot \deg_*(f_j) + \alpha_j = m_{*,\boldsymbol{\alpha}}(\boldsymbol{f}), \\ 0 & \deg_*(f_j) + \alpha_j < m_{*,\boldsymbol{\alpha}}(\boldsymbol{f}). \end{cases}$$

For a monomial $f = a_i X^i \in \mathbb{A}$, define $\mathrm{coef}(f) \coloneqq a_i$. In particular, $\mathrm{coef}(0) = 0$. Note that for any $* \in \{+, -\}$, $\boldsymbol{f} \in \mathbb{A}^n$ and $\boldsymbol{\alpha} \in \mathbb{Z}^n$, the above defined $\mathrm{in}_{*,\boldsymbol{\alpha}}(\boldsymbol{f})$ is an $n$-tuple of monomials. Writing $\mathrm{in}_{*,\boldsymbol{\alpha}}(\boldsymbol{f}) = (g_S, g_K, \ldots)$, we then extend the definition of coef() to

$$\mathrm{coef}(\mathrm{in}_{*,\boldsymbol{\alpha}}(\boldsymbol{f})) \coloneqq (\mathrm{coef}(g_S), \mathrm{coef}(g_K), \ldots) \in \mathbb{R}^n.$$

▶ **Lemma 6.3.** *Fix $* \in \{+,-\}$ and $a \in \mathbb{Z}$. The two following conditions are equivalent:*

**(i)** *There exists $\boldsymbol{f} = (f_S, f_K, \cdots) \in \mathcal{M}$ such that*

$$\mathrm{lc}_*(\boldsymbol{f}) \in \mathbb{R}^n_{>0} \quad \textit{and} \quad \deg_*(f_S) + a \geq \deg_*(f_K)\,. \tag{31}$$

**(ii)** *There exists $\boldsymbol{\alpha} = (\alpha_S, \alpha_K, \cdots) \in \mathbb{Z}^n$ with $\alpha_S - \alpha_K \leq a$, as well as $\boldsymbol{f} = (f_S, f_K, \cdots) \in \mathcal{M}$, such that $\mathrm{coef}\,(\mathrm{in}_{*,\boldsymbol{\alpha}}(\boldsymbol{f})) \in \mathbb{R}^n_{>0}$.*

We use the notion of a *super Gröbner basis* for $\mathcal{M}$: see [13, Chapter 2] for its exact definition. Readers can simply take the following Lemma 6.4 as its definition, since this will be the only property of the super Gröbner basis that we use in this paper.

▶ **Lemma 6.4** ([13, Lemma 2.1])**.** *Let $* \in \{+,-\}$ and $\boldsymbol{\alpha} \in \mathbb{Z}^n$. Let $\boldsymbol{g}_1, \ldots, \boldsymbol{g}_m$ be a super Gröbner basis for $\mathcal{M}$. For every $\boldsymbol{g} \in \mathcal{M}$, we have $\mathrm{in}_{*,\boldsymbol{\alpha}}(\boldsymbol{g}) = \sum_{i=1}^m p_i \cdot \mathrm{in}_{*,\boldsymbol{\alpha}}(\boldsymbol{g}_i)$ for some $p_1, \ldots, p_m \in \mathbb{A}$.*

By [13, Chapter 2], given a basis for $\mathcal{M}$, a set of super Gröbner basis exists and can be effectively computed. We now fix a set of a super Gröbner basis $\boldsymbol{g}_1, \ldots, \boldsymbol{g}_m$ for $\mathcal{M}$.

▶ **Corollary 6.5.** *Let $* \in \{+,-\}$ and $\boldsymbol{\alpha} \in \mathbb{Z}^n$. Then there exists $\boldsymbol{f} \in \mathcal{M}$ with $\mathrm{coef}\,(\mathrm{in}_{*,\boldsymbol{\alpha}}(\boldsymbol{f})) \in \mathbb{R}^n_{>0}$ if and only if there exist $r_1, \ldots, r_m \in \mathbb{R}$ with $\sum_{i=1}^m r_i \cdot \mathrm{coef}(\mathrm{in}_{*,\boldsymbol{\alpha}}(\boldsymbol{g}_i)) \in \mathbb{R}^n_{>0}$.*

▶ **Lemma 6.6** (Generalization of [13, Lemma 6.1])**.** *Fix $* \in \{+,-\}$. The initial tuples $\mathrm{in}_{*,\boldsymbol{\alpha}}(\boldsymbol{g}_1), \ldots, \mathrm{in}_{*,\boldsymbol{\alpha}}(\boldsymbol{g}_m)$ can take only a finite number of possible values when $\boldsymbol{\alpha}$ varies in the set $\{\boldsymbol{\alpha} = (\alpha_S, \alpha_K, \cdots) \in \mathbb{Z}^n \mid \alpha_S - \alpha_K \leq a\}$. Furthermore, one can effectively compute representatives $\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_p \in \mathbb{Z}^n$, such that the tuples $\big(\mathrm{in}_{*,\boldsymbol{\alpha}_1}(\boldsymbol{g}_i)\big)_{i=1,\ldots,m}, \ldots, \big(\mathrm{in}_{*,\boldsymbol{\alpha}_p}(\boldsymbol{g}_i)\big)_{i=1,\ldots,m}$ are all the possible tuples $\big(\mathrm{in}_{*,\boldsymbol{\alpha}}(\boldsymbol{g}_i)\big)_{i=1,\ldots,m}$ when $\boldsymbol{\alpha}$ varies.*

▶ **Proposition 3.6.** *Let $* \in \{+,-\}$, $a \in \mathbb{Z}$ and $\mathcal{M}$ be an $\mathbb{A}$-submodule of $\mathbb{A}^n$. Given as input a finite basis of $\mathcal{M}$, it is decidable whether there exists $\boldsymbol{f} = (f_S, f_K, \cdots) \in \mathcal{M}$ such that*

$$\mathrm{lc}_*(\boldsymbol{f}) \in \mathbb{R}^n_{>0} \quad \textit{and} \quad \deg_*(f_S) + a \geq \deg_*(f_K)\,. \tag{19}$$

**Proof.** First we compute a set of super Gröbner basis $\boldsymbol{g}_1, \ldots, \boldsymbol{g}_m$ for $\mathcal{M}$. Then for each $* \in \{+,-\}$, by Lemma 6.6 we compute $\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_p \in \mathbb{Z}^n$ such that the tuples $\big(\mathrm{in}_{*,\boldsymbol{\alpha}_1}(\boldsymbol{g}_i)\big)_{i=1,\ldots,m}, \ldots, \big(\mathrm{in}_{*,\boldsymbol{\alpha}_p}(\boldsymbol{g}_i)\big)_{i=1,\ldots,m}$ are all the possible tuples when $\alpha_S - \alpha_K \leq a$. For each of these $\boldsymbol{\alpha} \in \{\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_p\}$, use linear programming to decide whether there exist real numbers $r_1, \ldots, r_m \in \mathbb{R}$ such that $\sum_{i=1}^m r_i \cdot \mathrm{coef}\,(\mathrm{in}_{*,\boldsymbol{\alpha}}(\boldsymbol{g}_i)) \in \mathbb{R}^n_{>0}$. By Corollary 6.5, such $r_1, \ldots, r_m \in \mathbb{R}$ exist if and only if there exists $\boldsymbol{f} \in \mathcal{M}$ with $\mathrm{coef}(\mathrm{in}_{*,\boldsymbol{\alpha}}(\boldsymbol{f})) \in \mathbb{R}^n_{>0}$. By Lemma 6.3, this is true if and only if there exists $\boldsymbol{f} = (f_S, f_K, \cdots) \in \mathcal{M}$ satisfying condition (19). ◀

## References


1. Erwin H. Bareiss. Sylvester's identity and multistep integer-preserving gaussian elimination. *Mathematics of computation*, 22(103):565–578, 1968.
2. Gilbert Baumslag, Frank B. Cannonito, and Derek J. S. Robinson. The algorithmic theory of finitely generated metabelian groups. *Transactions of the American Mathematical Society*, 344(2):629–648, 1994.
3. Paul C. Bell, Mika Hirvensalo, and Igor Potapov. The Identity Problem for matrix semigroups in $\mathsf{SL}_2(\mathbb{Z})$ is NP-complete. In *Proceedings of the Twenty-Eighth Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 187–206. SIAM, 2017.
4. Paul C. Bell and Igor Potapov. On the undecidability of the identity correspondence problem and its applications for word and matrix semigroups. *International Journal of Foundations of Computer Science*, 21(06):963–978, 2010.

5 Vincent D. Blondel, Emmanuel Jeandel, Pascal Koiran, and Natacha Portier. Decidable and undecidable problems about quantum automata. *SIAM Journal on Computing*, 34(6):1464–1473, 2005.

6 J. A. Bondy and U. S. R. Murty. *Graph theory with applications*, volume 290. Macmillan London, 1976.

7 Michaël Cadilhac, Dmitry Chistikov, and Georg Zetzsche. Rational subsets of baumslag-solitar groups. In *47th International Colloquium on Automata, Languages, and Programming, ICALP*, volume 168 of *LIPIcs*, pages 116:1–116:16. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2020.

8 Olivier Chapuis. ∀-free metabelian groups. *The Journal of Symbolic Logic*, 62(1):159–174, 1997.

9 Christian Choffrut and Juhani Karhumäki. Some decision problems on integer matrices. *RAIRO-Theoretical Informatics and Applications-Informatique Théorique et Applications*, 39(1):125–131, 2005.

10 Valerio De Angelis and Selim Tuncel. Handelman's theorem on polynomials with positive multiples. *Codes, systems, and graphical models (Minneapolis, MN, 1999)*, pages 439–445, 2001.

11 Harm Derksen, Emmanuel Jeandel, and Pascal Koiran. Quantum automata and algebraic groups. *Journal of Symbolic Computation*, 39(3-4):357–371, 2005.

12 Ruiwen Dong. Solving homogeneous linear equations over polynomial semirings. *arXiv preprint*, 2022. To appear in STACS 2023. `arXiv:2209.13347`.

13 Manfred Einsiedler, Robert Mouat, and Selim Tuncel. When does a submodule of $(\mathbb{R}[x_1, \ldots, x_k])^n$ contain a positive element? *Monatshefte für Mathematik*, 140(4):267–283, 2003.

14 Moses Ganardi, Daniel König, Markus Lohrey, and Georg Zetzsche. Knapsack problems for wreath products. In *35th Symposium on Theoretical Aspects of Computer Science, STACS 2018, February 28 to March 3, 2018, Caen, France*, volume 96 of *LIPIcs*, pages 32:1–32:13. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2018.

15 David Handelman. *Positive polynomials and product type actions of compact groups*, volume 320. American Mathematical Soc., 1985.

16 Ehud Hrushovski, Joël Ouaknine, Amaury Pouly, and James Worrell. Polynomial invariants for affine programs. In *Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science*, pages 530–539, 2018.

17 Olga Kharlampovich, Laura López, and Alexei Myasnikov. The diophantine problem in some metabelian groups. *Mathematics of Computation*, 89(325):2507–2519, 2020.

18 Olga G. Kharlampovich. A finitely presented solvable group with unsolvable word problem. *Izvestiya Rossiiskoi Akademii Nauk. Seriya Matematicheskaya*, 45(4):852–873, 1981.

19 Olga G. Kharlampovich and Mark V. Sapir. Algorithmic problems in varieties. *International Journal of Algebra and Computation*, 5(04n05):379–602, 1995.

20 Kenneth Krohn and John Rhodes. Algebraic theory of machines. I. Prime decomposition theorem for finite semigroups and machines. *Transactions of the American Mathematical Society*, 116:450–464, 1965.

21 Markus Lohrey. Subgroup membership in GL(2, Z). In *38th International Symposium on Theoretical Aspects of Computer Science (STACS 2021)*, volume 187 of *LIPIcs*, pages 51:1–51:17. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2021.

22 Markus Lohrey, Benjamin Steinberg, and Georg Zetzsche. Rational subsets and submonoids of wreath products. *Information and Computation*, 243:191–204, 2015.

23 Wilhelm Magnus. On a theorem of Marshall Hall. *Annals of Mathematics*, pages 764–768, 1939.

24 A. Markov. On certain insoluble problems concerning matrices. *Doklady Akad. Nauk SSSR*, 57(6):539–542, 1947.

25 K. A. Mikhailova. The occurrence problem for direct products of groups. *Matematicheskii Sbornik*, 112(2):241–251, 1966.

26 Vitalii Anatol'evich Roman'kov. Equations in free metabelian groups. *Siberian Mathematical Journal*, 20(3):469–471, 1979.

27 N. S. Romanovskii. Some algorithmic problems for solvable groups. *Algebra and Logic*, 13(1):13–16, 1974.

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


## A Some omitted proofs

This appendix contains some omitted proofs from the main article. Other omitted proofs can be found in the full version of this paper.

▶ **Lemma 2.1.** *Let $\mathcal{G} = \{g_1, \dots, g_a\}$ be a set of elements in a group $G$. The semigroup $\langle \mathcal{G} \rangle$ is a group if and only if the neutral element $I$ of $G$ is represented by a full-image word over $\mathcal{G}$.*

**Proof.** Let $w \in \mathcal{G}^*$ be a full-image word with $\pi(w) = I$. Then for every $i$, the word $w$ can be written as $w = vg_iv'$, so $g_i^{-1} = \pi(v')\pi(v) \in \langle \mathcal{G} \rangle$. Therefore, the semigroup $\langle \mathcal{G} \rangle$ contains all the inverse $g_i^{-1}$, and is thus a group.

If $\langle \mathcal{G} \rangle$ is a group, then for all $i$, the inverse $g_i^{-1}$ can be written as $\pi(w_i)$ for some word $w_i \in \mathcal{G}^*$. Then the word $w := g_1w_1g_2w_2 \cdots g_aw_a$ is a full-image word with $\pi(w) = \pi(g_1w_1) \cdots \pi(g_aw_a) = I$. ◀

▶ **Proposition 3.1.** *Suppose $I = \emptyset$ or $J = \emptyset$. The semigroup $\langle \mathcal{G} \rangle$ is a group if and only if $I = J = \emptyset$ and $\sum_{k \in K} n_k y_k = 0$ for some positive integers $n_k \in \mathbb{Z}_{>0}$. In particular, this is decidable by integer programming.*

**Proof.** First suppose $\langle \mathcal{G} \rangle$ is a group. Without loss of generality suppose $I = \emptyset$. Then every element $(y, b) \in \langle \mathcal{G} \rangle$ must satisfy $b \leq 0$. Therefore, for any $(y_j, b_j) \in \mathcal{G}$ with $b_j < 0$, we have $(y_j, b_j)^{-1} = (X^{-b_j} \cdot y_j, -b_j) \notin \langle \mathcal{G} \rangle$ by the positivity of $-b_j$. Hence $J = \emptyset$.

Since $\langle \mathcal{G} \rangle$ is a group, by Lemma 2.1 there exists a full-image word $w \in \mathcal{G}^*$ that represents $(0, 0)$. Let $n_k$ be the number of times the word $(y_k, 0)$ appears in $w$, then $n_k > 0$ and $w$ represents $\left(\sum_{k \in K} n_k y_k, 0\right) = (0, 0)$. This finishes the first implication.

For the converse implication, suppose $I = J = \emptyset$ and $\sum_{k \in K} n_k y_k = 0$ for some integers $n_k \in \mathbb{Z}_{>0}$. Then the word $\prod_{k \in K} (y_k, 0)^{n_k} = (0, 0)$. Therefore there exists a full-image word that represents $(0, 0)$. Hence $\langle \mathcal{G} \rangle$ is a group.

Let $p = \min_{k \in K}\{\deg_-(y_k)\}$ and $q = \max_{k \in K}\{\deg_+(y_k)\}$. For each $k \in K$, write $y_k = \sum_{t=p}^{q} \beta_{k,t} X^t$, then $\sum_{k \in K} n_k y_k = 0$ is equivalent to the system of linear equations

$$\sum_{k \in K} n_k \beta_{k,t} = 0, \quad t = p, p+1, \dots, q. \tag{32}$$

Deciding whether the system (32) has solution over $\mathbb{Z}_{>0}$ can be decided using integer programming. ◀

▶ **Corollary 3.3.** *The semigroup $\langle \mathcal{G} \rangle$ is a group if and only if there exist a double-full set $S \subset I \times J$ and polynomials $f_S, f_K, f_{(i,j)}, f_k \in \mathbb{R}_{\geq 0}[X^{\pm}]^*$ for $(i, j) \in S, k \in K$ that satisfy the following three conditions.*

**(i)** ***(System of linear equations)*** *The following linear equations over $\mathbb{R}(X)$ are satisfied:*

$$\sum_{(i,j)\in S} f_{(i,j)} h_{(i,j),m} + \sum_{k\in K} f_k y_{k,m} = 0, \quad m = 0, \ldots, d-1, \tag{10}$$

$$f_S = \sum_{(i,j)\in S} f_{(i,j)}, \qquad f_K = \sum_{k\in K} f_k. \tag{11}$$

**(ii)** ***(Positive degree bound)*** *We have:*

$$\deg_+ (f_S) + 1 \geq \deg_+ (f_K). \tag{12}$$

**(iii)** ***(Negative degree bound)*** *We have:*

$$\deg_- (f_S) \leq \deg_- (f_K). \tag{13}$$

**Proof.** We show that Corollary 3.3 is equivalent to Proposition 3.2.

By the definition of $h_{(i,j),m}, y_{k,m}, (i,j) \in S, k \in K, m = 0, \ldots, d-1$ in Equation (8) and (9), the Equation (5) in Condition (i) of Proposition 3.2 is equivalent to the following system:

$$\sum_{(i,j)\in S} f'_{(i,j)} h_{(i,j),m} + \sum_{k\in K} f'_k y_{k,m} = 0, \quad m = 0, \ldots, d-1. \tag{33}$$

Where $f'_{(i,j)}, f'_k$ are polynomials in $\mathbb{N}[X^{\pm}]^*$ such that $f_{(i,j)} = f'_{(i,j)}(X^d), f_k = f'_k(X^d)$.

On one hand, suppose there exist polynomials $f_{(i,j)}, f_k \in \mathbb{N}[X^{\pm d}]^*$ that satisfy Conditions (i)-(iii) of Proposition 3.2. Then the polynomials $f'_{(i,j)}, f'_k$ satisfying the system (33) are also in $\mathbb{R}_{\geq 0}[X^{\pm}]$. Then let $f'_S = \sum_{(i,j)\in S} f'_{(i,j)}$ and $f'_K = \sum_{k\in K} f'_k$, so Conditions (i)-(iii) of Corollary 3.3 are satisfied for $f'_S, f'_K, f'_{(i,j)}, f'_k \in \mathbb{R}_{>0}[X^{\pm}]^*$.

On the other hand, suppose there exist polynomials $f'_S, f'_K, f'_{(i,j)}, f'_k \in \mathbb{R}_{>0}[X^{\pm}]^*$ that satisfy Conditions (i)-(iii) of Corollary 3.3. We show that there exist $f_S, f_K, f_{(i,j)}, f_k \in \mathbb{N}[X^{\pm}]^*, (i,j) \in S, k \in K$ that satisfy the same Equations (10)-(11), and such that $\deg_{\pm} f'_{(i,j)} = \deg_{\pm} f_{(i,j)}$, $\deg_{\pm} f'_k = \deg_{\pm} f_k$ for all $(i,j) \in S, k \in K$.

In fact, by the homogeneity of Equations (10)-(11), one can multiply all $h_{(i,j),m}$ and $y_{k,m}$ simultaneously by their common denominator, and suppose $h_{(i,j),m}, y_{k,m} \in \mathbb{Q}[X^{\pm}]$. Then, *fixing the degrees of $f_{(i,j)}$ and $f_k$*, one can rewrite Equations (10)-(11) as a system of homogeneous linear equation where the variables are the coefficients of $f_{(i,j)}$ and $f_k$. We then add to this system of homogeneous linear equations a boolean combination of homogeneous linear inequalities to guarantee $f_{(i,j)}, f_k \in \mathbb{R}_{>0}[X^{\pm}]^*$ (this can be expressed using inequalities for the coefficients of $f_{(i,j)}, f_k$), as well as to guarantee the degree of $f_{(i,j)}, f_k$. Since this system of homogeneous linear equations plus boolean combination of homogeneous linear inequalities has a solution over $\mathbb{R}$, it also has a solution over $\mathbb{Q}$, and even over $\mathbb{Z}$ by the homogeneity. Therefore, we obtain a solution over $\mathbb{Z}$ for the coefficients of $f_{(i,j)}, f_k$. This gives us a solution $f_{(i,j)}, f_k \in \mathbb{N}[X^{\pm}]^*$ with the same fixed degrees.

Consequently, $f_{(i,j)}, f_k, (i,j) \in S, k \in K$, satisfy the system (33). Thus, $f_{(i,j)}(X^d), f_k(X^d)$, $(i,j) \in S, k \in K$. satisfy Conditions (i)-(iii) of Proposition 3.2. ◀

▶ **Lemma 4.4.** *The graph $G(\widehat{w})$ can be constructed by starting with an edgeless graph with a single vertex 0 and gradually attaching primitive circuits.*

**Proof.** Denote by $G_0$ the edgeless graph with a single vertex 0. We show that every Eulerian $\widehat{\mathcal{G}}$-graph $G$ can be constructed by attaching primitive circuits to $G_0$. We use induction on the number of edges in $G$. When there is no edge in $G$, it is $G_0$, and we are done.

When there are loops in $G$, these are loops of some label $k \in K$, and are therefore primitive circuits themselves. Removing them results in another Eulerian graph $G'$ and decreases the number of edges. By the induction hypothesis $G'$ can be constructed by attaching primitive circuits to $G_0$. Then attaching the loops (primitive circuits of type in $K$) to $G'$ results in $G$.

When there are no loops in $G$, denote $m \coloneqq \max(V(G))$. Then since $G$ is Eulerian, there must be an edge $e$ of label $\ell(e)$ starting from the vertex $m$, and an edge $e'$ of label $\ell(e')$ ending at the vertex $m$. Since all the edges in $G$ are of length $d$, the edge $e$ must end at vertex $m - d$, and $e'$ must start at $m - d$. (The length of an edge of label $a$ is $\widehat{b}_a$.) Therefore the circuit consisting of $e$ and $e'$ is primitive of type $(\ell(e), \ell(e'))$. Removing the circuit (and the vertex $m$ if necessary) results in a graph $G'$. $G'$ is connected (and Eulerian) since there is no loop at $m$, and the only possible neighbour of the vertex $m$ is $m - d$. By the induction hypothesis $G'$ can be constructed by attaching primitive circuits to $G_0$. Then attaching to $G'$ the primitive circuits of type $(\ell(e), \ell(e'))$ at vertex $m - d$ results in $G$. ◀