Solving Homogeneous Linear Equations over Polynomial Semirings

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

Abstract
For a subset $B$ of $\mathbb{R}$, denote by $U(B)$ be the semiring of (univariate) polynomials in $\mathbb{R}[X]$ that are strictly positive on $B$. Let $\mathbb{N}[X]$ be the semiring of (univariate) polynomials with non-negative integer coefficients. We study solutions of homogeneous linear equations over the polynomial semirings $U(B)$ and $\mathbb{N}[X]$. In particular, we prove local-global principles for solving single homogeneous linear equations over these semirings. We then show PTIME decidability of determining the existence of non-zero solutions over $\mathbb{N}[X]$ of single homogeneous linear equations.

Our study of these polynomial semirings is largely motivated by several semigroup algorithmic problems in the wreath product $\mathbb{Z} \wr \mathbb{Z}$. As an application of our results, we show that the Identity Problem (whether a given semigroup contains the neutral element?) and the Group Problem (whether a given semigroup is a group?) for finitely generated sub-semigroups of the wreath product $\mathbb{Z} \wr \mathbb{Z}$ is decidable when elements of the semigroup generator have the form $(y, \pm 1)$.

2012 ACM Subject Classification Computing methodologies → Symbolic and algebraic manipulation
Keywords and phrases wreath product, identity problem, polynomial semiring, positive polynomial
Digital Object Identifier 10.4230/LIPIcs.STACS.2023.26
Funding The author acknowledges support from UKRI Frontier Research Grant EP/X033813/1.

Acknowledgements The author would like to thank Markus Schweighofer for useful discussions and feedback and for pointing out the references [24] and [25].

1 Introduction

Linear equations over semirings appear in various domains in mathematics and computer science, such as automata theory, optimization, and algebra of formal processes [2, 3, 6, 11]. There have been numerous studies on linear equations over different semirings [12], for example the semiring of natural numbers (integer programming), tropical semirings [23] and polynomial semirings [9, 22]. Given a semiring $S$, define $S[X]$ to be the set of polynomials in variable $X$ whose coefficients are elements of $S$. The set $S[X]$ is again a semiring. One of the simplest polynomial semirings is the semiring $\mathbb{N}[X]$ of single variable polynomials with non-negative integer coefficients. The problem of solving a system of linear equations over $\mathbb{N}[X]$ was shown to be undecidable by Narendran [22] using a reduction from Hilbert’s tenth problem. More precisely, given integer polynomials $h_{ij}, g_j \in \mathbb{Z}[X], i = 1, \ldots, n, j = 1, \ldots, k$, it is undecidable whether the system of equations

$$f_1 h_{1j} + \cdots + f_n h_{nj} = g_j, \quad j = 1, \ldots, k,$$

has a solution $(f_1, \ldots, f_n)$ over $\mathbb{N}[X]$. This contrasts with the decidability of solving systems of linear equations over $\mathbb{N}$ and over $\mathbb{Z}[X]$ (using respectively integer programming [15] and Smith canonical forms [16]).
In this paper, we show a decidability result for finding a non-zero solution of a single homogeneous linear equation over \( \mathbb{N}[X] \). In particular, we are concerned with the following problem: given integer polynomials \( h_1, \ldots, h_n \in \mathbb{Z}[X] \), does the equation
\[
f_1 h_1 + \cdots + f_n h_n = 0
\]
(admit a solution \((f_1, \ldots, f_n)\) over \( \mathbb{N}[X] \setminus \{0\} \) (i.e. none of the \( f_i \) is zero)?

In Section 6 of this paper we give a PTIME algorithm that decides this problem. Our algorithm relies on a local-global principle which we prove in Section 5, and reduces the decision problem to the existential theory of the reals in one variable. Formal definitions of these results will be given in Section 2.

It turns out that the problem of solving linear equations over the semiring \( \mathbb{N}[X] \) is closely related to solving the same equation over the semiring \( \mathbb{U}(B) \), consisting of polynomials in \( \mathbb{R}[X] \) that are strictly positive on a subset \( B \) of \( \mathbb{R} \). It is also related to the semiring \( \mathbb{W}(B) \) of polynomials that are non-negative on \( B \). The characterization of polynomials in \( \mathbb{U}(B) \) and \( \mathbb{W}(B) \) is a central subject in the theory of real algebra. In particular, when \( B \) is a semialgebraic set, variants of the positivity constraint over a subset of \( \mathbb{R} \) give explicit descriptions of the semirings \( \mathbb{U}(B) \) and \( \mathbb{W}(B) \). This theory can be traced back to the celebrated Hilbert’s seventeenth problem: given a polynomial that takes only non-negative values over the reals, can it be represented as a sum of squares of rational functions? This has been answered positively by Artin [1] using a model theoretic approach. The techniques proposed by Artin have since developed into the rich theory of real algebra; for a comprehensive account of this subject, see [24] or [25]. An important result in solving homogeneous linear equations over \( \mathbb{W}(\mathbb{R}) \) is the Bröcker-Prestel’s local-global principle for weak isotropy of quadratic forms [24, Theorem 8.12, 8.13]. Applied over the function field \( \mathbb{R}(X) \), the Bröcker-Prestel local-global principle relates the existence of non-trivial solutions over sums of squares in \( \mathbb{R}(X) \) (and hence over \( \mathbb{W}(\mathbb{R}) \)) of a homogeneous linear equation, to the behaviour of the equation in all Henselizations of \( \mathbb{R}(X) \). In Section 4 of this paper we prove a “strictly positive” version of the Bröcker-Prestel local-global principle, which characterizes the existence of solutions over \( \mathbb{U}(B) \). This will serve as a base for proving further results in Section 5 and 6. Our proof is inspired by Prestel’s proof of the original theorem. However, several new ideas are introduced to deal with the strict positivity as well as the positivity constraint over a subset of \( \mathbb{R} \).

An important motivation for studying linear equations over \( \mathbb{N}[X] \) comes from a semigroup algorithmic problem in the wreath product \( \mathbb{Z} \wr \mathbb{Z} \). The wreath product is a fundamental construction in group and semigroup theory. Given two groups \( G \) and \( H \), their wreath product \( G \wr H \) is defined in the following way. Let \( G^H \) be the set of all functions \( y: H \to G \) with finite support; it is a group with respect to pointwise multiplication. The group \( H \) acts on \( G^H \) as a group of automorphisms: if \( h \in H, y \in G^H \), then \( y^h(b) = y(bh^{-1}) \) for all \( b \in H \). The wreath product \( G \wr H \) is then defined as the semi-direct product \( G^H \rtimes H \), that is, the set of all pairs \((y, h)\) where \( y \in G^H, h \in H \), with multiplication operation given by
\[
(y, h)(z, k) = (y^h z, hk).
\]

One easy way to understand the group \( \mathbb{Z} \wr \mathbb{Z} \) is through its isomorphism to a matrix group over the Laurent polynomial ring \( \mathbb{Z}[X, X^{-1}] \) [19]:
\[
\varphi: \mathbb{Z} \wr \mathbb{Z} \simeq \left\{ \begin{pmatrix} 1 & f \\ 0 & X^b \end{pmatrix} \right\}, \text{ where } f \in \mathbb{Z}[X, X^{-1}], b \in \mathbb{Z}, \quad (y, b) \mapsto \left( \begin{pmatrix} 1 & \sum_{k \in \mathbb{Z}} y(k)X^k \\ 0 & X^b \end{pmatrix} \right).
\]
A large number of important groups are constructed using the wreath product, such as the lamplighter group \( Z_2 \wr Z \) [13] and groups resulting from the Magnus embedding theorem [19]. The wreath product also plays an important role in the algebraic theory of automata. The Krohn–Rhodes theorem states that every finite semigroup (and correspondingly, every finite automaton) can be decomposed into elementary components using wreath products [17].

In Section 7 we give an application of our results to the Identity Problem in \( Z \wr Z \). Given a finite set of elements \( G = \{A_1, \ldots, A_k\} \) in a group \( G \) as well as a target element \( A \in G \), denote by \( \langle G \rangle \) the semigroup of generated by \( G \), and by \( \langle G \rangle_{\text{grp}} \) the group generated by \( G \). Consider the following decision problems:

(i) (Group Membership Problem) whether \( A \in \langle G \rangle_{\text{grp}} \)?
(ii) (Semigroup Membership Problem) whether \( A \in \langle G \rangle \)?
(iii) (Identity Problem) whether the neutral element \( I \) of \( G \) is contained in \( \langle G \rangle \)?

All three problems remain undecidable even when the ambient group \( G \) is restricted to relatively simple groups, such as the direct product \( F_2 \times F_2 \) of two free groups over two generators [5, 21]. Indeed, one of the first undecidability results in algorithmic theory was the undecidability of the Semigroup Membership Problem for integer matrices, obtained by Markov [20]. Some decidability results for the Identity Problem include its NP-completeness in \( \text{SL}(2, \mathbb{Z}) \) [4] and its PTIME decidability in nilpotent groups of class at most ten [10].

Let \( p \in \mathbb{Z}_{>0} \). The group \( Z \wr Z \) shares some common properties with the wreath product \( (Z/pZ) \wr Z \) and with the Baumslag-Solitar group \( BS(1, p) \). Similar to the isomorphism (3), both \( (Z/pZ) \wr Z \) and \( BS(1, p) \) can be represented as 2 \times 2 upper triangular matrix groups:

\[
(Z/pZ) \wr Z \cong \left\{ \begin{pmatrix} 1 & f \\ 0 & X^b \end{pmatrix} \left| f \in (Z/pZ)[X, X^{-1}], b \in Z \right. \right\},
\]

\[
BS(1, p) \cong \left\{ \begin{pmatrix} 1 & f \\ 0 & p^b \end{pmatrix} \left| f \in \mathbb{Z}[1/p], b \in \mathbb{Z} \right. \right\}.
\]

Lohrey, Steinberg and Zetzsche showed decidability of the Rational Subset Membership Problem (which subsumes all three decision problems mentioned above) in \( H \wr V \), where \( H \) is a finite and \( V \) is virtually free [18]. This notably implies its decidability in \( (Z/pZ) \wr Z \). Cadilhac, Chistikov and Zetzsche proved its decidability in \( BS(1, p) \) [7]. For \( Z \wr Z \), decision problems are much harder due to higher encoding power of the ring \( \mathbb{Z}[X, X^{-1}] \). The Group Membership Problem in \( Z \wr Z \) can be reduced to the membership problem for modules over the ring \( \mathbb{Z}[X, X^{-1}] \), and is hence decidable [26]. As for the Semigroup Membership Problem in \( Z \wr Z \), Lohrey et al. showed its undecidability using an encoding of 2-counter machines [18].

Decidability of the Identity Problem in \( Z \wr Z \) remains an intricate open problem. In this paper we give a decidability result in the case where all the elements of the generator \( G \) are of the form \((y, \pm 1)\).

## 2 Main results

In this section we sum up the main results of this paper. For a subset \( B \) of \( \mathbb{R} \), denote by \( U(B) \) the set of polynomials in \( \mathbb{R}[X] \) that are strictly positive on \( B \):

\[
U(B) := \{ f \in \mathbb{R}[X] \mid f(x) > 0 \text{ for all } x \in B \}.
\]

Define \( \mathcal{B} \) to be the closure of \( B \) in \( \mathbb{R} \) under the Euclidean topology. Our first result is a local-global principle for solutions of homogeneous linear equations over \( U(B) \). Theorem 2.1 will be proved in Section 4.
Theorem 2.1. Let \( B \) be a subset of \( \mathbb{R} \). Assume that \( h_1, \ldots, h_n \in \mathbb{R}[X] \) are polynomials that satisfy \( \gcd(h_1, \ldots, h_n) = 1 \). If the equation \( f_1h_1 + \cdots + f_nh_n = 0 \) has no solution \((f_1, \ldots, f_n)\) over \( U(B) \), then there exists a real number \( t \in \overline{B} \), such that the values \( h_i(t), i = 1, \ldots, n \), are either all non-negative or all non-positive.

Our second result is a corollary of the previous theorem, it provides a similar local-global principle for solutions over \( \mathbb{N}[X] \setminus \{0\} \). Theorem 2.2 will be proved in Section 5.

Theorem 2.2. Given polynomials \( h_1, \ldots, h_n \in \mathbb{Z}[X] \) with \( \gcd(h_1, \ldots, h_n) = 1 \). If the equation \( f_1h_1 + \cdots + f_nh_n = 0 \) has no solution \((f_1, \ldots, f_n)\) over \( \mathbb{N}[X] \setminus \{0\} \), then there exists \( t \in \mathbb{Z}_{\geq 0} \), such that the values \( h_i(t), i = 1, \ldots, n \), are either all non-negative or all non-positive.

Our next result shows that it is decidable in PTIME whether a linear homogeneous equation is solvable over \( \mathbb{N}[X] \setminus \{0\} \). The input size is defined as the total number of bits used to encode all the coefficients of all \( h_i \). Theorem 2.3 will be proved in Section 6.

Theorem 2.3. Given as input \( h_1, \ldots, h_n \in \mathbb{Z}[X] \). It is decidable in polynomial time whether the equation \( f_1h_1 + \cdots + f_nh_n = 0 \) has solutions \( f_1, \ldots, f_n \) over \( \mathbb{N}[X] \setminus \{0\} \).

An application of this theorem is the following partial decidability result on the Identity Problem in the wreath product \( \mathbb{Z} \wr \mathbb{Z} \). This will be the main topic of Section 7.

Theorem 2.4. Given a finite set of elements \( \mathcal{G} = \{(y_1, b_1), \ldots, (y_n, b_n)\} \) in \( \mathbb{Z} \wr \mathbb{Z} \), where \( b_i = \pm 1 \) for all \( i \). The following are decidable:
1. (Group Problem) whether the semigroup \( \langle \mathcal{G} \rangle \) generated by \( \mathcal{G} \) is a group.
2. (Identity Problem) whether the neutral element \( 1 \) is in the semigroup \( \langle \mathcal{G} \rangle \).

3 Preliminaries

In this section we introduce the necessary mathematical tools on (semi)orderings of fields as well as orderings. Most notations and definitions follow those given in Prestel’s book [24].

3.1 Orderings and semiorderings

Definition 3.1 (Ordering). A linear ordering of a set \( S \) is a binary relation that satisfies
(i) \( a \leq a \),
(ii) \( a \leq b, b \leq c \Rightarrow a \leq c \),
(iii) \( a \leq b, b \leq a \Rightarrow a = a \),
(iv) \( a \leq b \) or \( b \leq a \) for all \( a, b, c \in S \).

Given a field \( F \) of characteristic zero, a (field) ordering of \( F \) is a linear ordering \( \leq \) of the underlying set of \( F \) that additionally satisfies
(i) \( a \leq b \Rightarrow a + c \leq b + c \),
(ii) \( 0 \leq a, 0 \leq b \Rightarrow 0 \leq ab \)
for all \( a, b, c \in F \). A field is called formally real if it admits at least one ordering.

The semiordering of a field, defined below, is a weaker version of the field ordering.

Definition 3.2 (Semiordering). A semiordering of a field \( F \) is a linear ordering \( \leq \) of the underlying set of \( F \) that satisfies
(i) \( a \leq b \Rightarrow a + c \leq b + c \),
(ii) \( 0 \leq 1 \),
(iii) \( 0 \leq a \Rightarrow 0 \leq ab^2 \)
for all \( a, b, c \in F \).
In a field $F$ with semiordering $\leq$, we have $0 \leq x^2$ for all $x \in F$. The field of real numbers $\mathbb{R}$ hence admits a unique semiordering, since every positive real can be written as a square. This semiordering is simply the natural ordering on $\mathbb{R}$.

It is easy to see that an ordering is always a semiordering. Conversely, a semiordering need not be an ordering. However, in any field, the existence of a semiordering implies that of an ordering.

**Lemma 3.3 ([24, Corollary 1.15]).** A field $F$ is formally real (admits an ordering) if and only if it admits a semiordering.

For any subset $P$ of $F$, define $-P := \{ -x \mid x \in P \}$. For a semiordering $\leq$ of $F$, the set $P := \{ a \in F \mid 0 \leq a \}$ satisfies

(i) $P + P \subseteq P$,
(ii) $F^2 \cdot P \subseteq P$ and $1 \in P$,
(iii) $P \cap -P = \{0\}$,
(iv) $P \cup -P = F$.

Such a set will be called a *semicone* of $F$. A semicone $P$ of $F$ determines a semiordering $\leq$ of $F$ by $a \leq b \iff b - a \in P$. Therefore, we will sometimes call $P$ a semiordering as well.

The *pre-semicone* is yet a weaker version of the semiordering (or semicone).

**Definition 3.4 (Pre-semicone).** A pre-semicone of a field $F$ is a subset $P$ of $F$ that satisfies

(i) $P + P \subseteq P$,
(ii) $F^2 \cdot P \subseteq P$,
(iii) $P \cap -P = \{0\}$.

The only difference between a pre-semicone and a semicone is the absence of the rule (iv) and the condition $1 \in P$ in (ii). Obviously every semicone is also a pre-semicone. Conversely, a pre-semicone need not be a semicone, but it can always be extended to one.

**Lemma 3.5 ([24, Lemma 1.13]).** For every pre-semicone $P_0$ of a formally real field $F$ there exists a set $P \supseteq P_0$ such that $P$ or $-P$ is a semicone of $F$.

Suppose $F$ is of characteristic zero. A semiordering or an ordering $\leq$ of $F$ is called archimedean if for each $a \in F$ there exists $n \in \mathbb{N} \subseteq F$ such that $a \leq n$.

**Lemma 3.6 ([24, Lemma 1.20]).** Every archimedean semiordering is an ordering.

### 3.2 Valuations

Let $F$ be a field. A **valuation** of $F$ is a surjective map $v: F \to \Gamma \cup \{ \infty \}$, where the **value group** $\Gamma$ is an abelian totally ordered group\(^1\), such that the following conditions are satisfied for all $a, b \in F$:

(i) $v(a) = \infty$ if and only if $a = 0$,
(ii) $v(ab) = v(a) + v(b)$,
(iii) $v(a + b) \geq \min\{v(a), v(b)\}$, with equality if $v(a) \neq v(b)$.

A valuation is called **non-trivial** if $\Gamma \neq \{0\}$. A **valued field** is a pair $(F, v)$ where $F$ is a field and $v$ is a valuation of $F$. Its **valuation ring** $A_v$ is defined as

$$A_v := \{ a \in F \mid v(a) \geq 0 \}.$$  

\(^1\) An abelian totally ordered group $\Gamma$ is an abelian group equipped with a linear ordering $\leq$, such that $a \leq b \implies a + c \leq b + c$ for all $a, b, c \in \Gamma$. Here, the group law of $\Gamma$ is written additively. The ordering and the group law on $\Gamma$ can be extended to the set $\Gamma \cup \{ \infty \}$ by defining $a \leq \infty$ and $a + \infty = \infty + a = \infty + \infty = \infty$ for all $a \in \Gamma$. 

---

**STACS 2023**
We have $A_v \neq F$ if and only if $v$ is non-trivial. $A_v$ is a ring with a unique maximal ideal

\[ M_v := \{ a \in F \mid v(a) > 0 \}. \]

The quotient $F_v := A_v/M_v$ is called the residue field of $(F,v)$. It is indeed a field since $M_v$ is maximal. A valuation $v$ is called a real place of $F$ if the residue field $F_v$ is formally real.

Consider the field $F = \mathbb{R}(X)$. The following proposition gives a well-known characterization (up to isomorphism of the value group $\Gamma$) of the set of all non-trivial real places $\mathbb{R}(X)$ whose valuation ring contains the subfield $\mathbb{R}$.

**Proposition 3.7.** Let $v$ be a non-trivial real place of $\mathbb{R}(X)$ such that $\mathbb{R} \subseteq A_v$. Then $v$ belongs to one of the two following types of real places:

1. For every $t \in \mathbb{R}$ there is a real place $v_t: \mathbb{R}(X) \to \mathbb{Z} \cup \{\infty\}$, defined by $v_t(y) = a$, where $a \in \mathbb{Z}$ is such that $y = (X-t)^a \cdot \frac{f}{g}$, with $f,g$ being polynomials in $\mathbb{R}[X]$ not divisible by $X-t$. The residue field $\mathbb{R}(X)_{v_t}$ is isomorphic to $\mathbb{R}$ by the natural homomorphism $y + M_{v_t} \mapsto y(t)$.

2. There is a real place $v_\infty: \mathbb{R}(X) \to \mathbb{Z} \cup \{\infty\}$, defined by $v_\infty(y) = \deg g - \deg f$, where $f,g$ are polynomials in $\mathbb{R}[X]$. The residue field $\mathbb{R}(X)_{v_\infty}$ is isomorphic to $\mathbb{R}$ by the natural homomorphism $y + M_{v_\infty} \mapsto \lim_{t \to \infty} y(t)$.

Let $P$ be a semicone of a field $F$, and $F_0$ be a subfield of $F$. Denote by $\mathbb{P}$ the corresponding semiordering of $P$; define the set

\[ A_F^P := \{ a \in F \mid a \leq b \text{ and } -a \leq b \text{ for some } b \in F_0 \}. \tag{4} \]

The following lemmas show that $A_F^P$ is a valuation ring, and that its corresponding residue field admits a semiordering induced by $P$ under additional conditions.

**Lemma 3.8 ([24, Lemma 7.13]).** Let $P$ be a semiordering of a field $F$ and $F_0$ a subfield of $F$. Then $A_F^P$ is a valuation ring of some valuation of $F$.

**Lemma 3.9 ([24, Lemma 7.15]).** Let $P$ be a semiordering of a field $F$ and $F_0$ a subfield of $F$, such that there exists $b \in F$ with $a \leq b$ for all $a \in F_0$. Let the valuation $v$ of $F$ correspond to $A_F^P$. Then $(A_v \cap P)/M_v$ is a semiordering of $F_v$.

### 4 Local-global principle over strictly positive polynomials

For a subset $B$ of $\mathbb{R}$, define the set $W(B)$ of polynomials that are non-negative on $B$:

\[ W(B) := \{ f \in \mathbb{R}[X] \mid f(x) \geq 0 \text{ for all } x \in B \}. \]

Observe that $W(0) \subseteq W(B)$. For $f,g \in W(\mathbb{R}) \setminus \{0\}$, by the fundamental theorem of algebra, one can write (uniquely)

\[ f = c \prod_{j \in J} (x - r_j)^{d_j} \prod_{k \in K} (x^2 + a_kx + b_k)^{e_k}, \quad g = c' \prod_{j \in J} (x - r_j)^{d'_j} \prod_{k \in K} (x^2 + a_kx + b_k)^{e'_k} \]

where $c,c',r_j,a_k,b_k \in \mathbb{R}$ and $d_j,d'_j,e_k,e'_k$ are non-negative integers, and the polynomials $x^2 + a_kx + b_k$ have no real root. Here, $J$ indexes all real roots of $f$ and $g$, and $K$ indexes all conjugate pairs of imaginary roots of $f$ and $g$. Since $f$ and $g$ are non-negative on $\mathbb{R}$, all $d_j$ and $d'_j$ are even, and $c,c'$ are positive. Therefore, the greatest common divisor of $f$ and $g$, defined by
\[ \gcd(f, g) = \prod_{j \in J} (x - r_j)^{\min\{d_j, a_j\}} \prod_{k \in K} (x^2 + a_k x + b_k)^{\min\{e_k, c_k\}} \] 

is also non-negative on \( \mathbb{R} \). It follows that the polynomials \( \gcd(f, g) \), \( f/\gcd(f, g) \) and \( g/\gcd(f, g) \) are all in \( W(\mathbb{R}) \).

We now give a proof of our first main result, which can be considered as a “strictly positive” version of the Bröcker-Prestel local-global principle. A comparison of our proof with the proof of the original theorem is given in Appendix C.

\[ \mathbf{Theorem 2.1.} \text{ Let } B \text{ be a subset of } \mathbb{R}. \text{ Assume that } h_1, \ldots, h_n \in \mathbb{R}[X] \text{ are polynomials that satisfy } \gcd(h_1, \ldots, h_n) = 1. \text{ If the equation } f_1 h_1 + \cdots + f_n h_n = 0 \text{ has no solution } (f_1, \ldots, f_n) \text{ over } U(B), \text{ then there exists a real number } t \in B, \text{ such that the values } h_i(t), i = 1, \ldots, n, \text{ are either all non-negative or all non-positive.} \]

\[ \text{Proof.} \text{ The theorem is trivially true if } B \text{ is empty, hence we suppose } B \neq \emptyset. \text{ Suppose } f_1 h_1 + \cdots + f_n h_n = 0 \text{ has no solution } (f_1, \ldots, f_n) \text{ over } U(B). \text{ Consider the following subset of the field } \mathbb{R}(X): \]

\[ P_0 := \left\{ \frac{g}{G}, \text{ where all } f_i \in U(B) \text{ and } g, G \in W(\mathbb{R}) \setminus \{0\} \right\}. \]

Since \( f_1 h_1 + \cdots + f_n h_n = 0 \) has no solution \((f_1, \ldots, f_n)\) over \( U(B) \), we have \( 0 \notin P_0 \). We claim that \( P_0 \supseteq P_0 \cup \{0\} \) is a pre-semicolon of \( \mathbb{R}(X) \). Indeed, we verify the three conditions given in Definition 3.4:

\( P_0 \supseteq P_0 \cup \{0\} \) if \( 0 \notin P_0 \). It suffices to show \( P_0 + P_0 \subseteq P_0 \). Let \( c = c' = \sum_{i=1}^n f_i h_i \) be elements of \( P_0 \). Without loss of generality we can suppose \( \gcd(g, G) = \gcd(g', G') = 1 \).

Write \( d := \gcd(g, g') \), \( D := \gcd(G, G') \), then the polynomials \( d, \frac{g}{G} + D, \frac{g'}{G'} \) are all elements of \( W(\mathbb{R}) \setminus \{0\} \), and \( \gcd(\frac{g}{G} + D, \frac{g'}{G'}) = 1 \). Hence,

\[ c + c' = \sum_{i=1}^n \left( f_i \frac{g}{G} + f'_i \frac{g'}{G'} \right) h_i = \frac{dD}{G'G} \sum_{i=1}^n \left( f_i \frac{g}{G} + f'_i \frac{g'}{G'} \right) h_i \]

(5)

For any \( x \in B \), we have \( \frac{g}{G}(x) \geq 0 \) and \( \frac{g'}{G'}(x) \geq 0 \). Since \( \gcd(\frac{g}{G}, \frac{g'}{G'}) = 1 \), the two polynomials \( \frac{g}{G}, \frac{g'}{G'} \) cannot both vanish at \( x \). Therefore either \( \frac{g}{G}(x) > 0 \) or \( \frac{g'}{G'}(x) > 0 \). Because \( f_i(x) > 0 \) and \( f'_i(x) > 0 \), it follows that \( \left( \frac{g}{G} + f'_i \frac{g'}{G'} \right)(x) > 0 \). So \( f_i \frac{g}{G} + f'_i \frac{g'}{G'} \in U(B) \), and \( c + c' \in P_0 \).

(\( i \)) \( \mathbb{R}(X)^2 \cdot P_0 \subseteq P_0 \). This is obvious since \( \mathbb{R}[X]^2 \cdot W(\mathbb{R}) \subseteq W(\mathbb{R}) \).

(\( ii \)) \( P_0 \cap -P_0 = \{0\} \). It suffices to show \( P_0 \cap -P_0 = \emptyset \). On the contrary suppose \( c \in P_0 \cap -P_0 \), then \( 0 = c + (-c) = P_0 + P_0 \subseteq P_0 \), a contradiction.

By Lemma 3.5, \( P_0 \) can be extended to some \( P \) such that either \( P \) or \( -P \) is a semicone of the field \( \mathbb{R}(X) \). Without loss of generality suppose \( P \supseteq P_0 \), then \( P_0 \) is a semicone, otherwise we can replace all \( h_i \) by \( -h_i \). Since the field \( \mathbb{R}(X) \) has no archimedean ordering [25, Example 1.1.4(2)], the semiordering corresponding to \( P \) must be non-archimedean (otherwise by Lemma 3.6 it must be an archimedean ordering). Consider the subfield \( \mathbb{R} \) of \( \mathbb{R}(X) \), by Lemma 3.8 the valuation ring \( A_R^p \) (as defined in (4)) corresponds to some valuation \( v \) of \( \mathbb{R}(X) \). Since \( P \) is non-archimedean, there exists some \( a \in \mathbb{R}(X) \) such that \( a - r \in P \) for all \( r \in \mathbb{R} \), hence \( A_R^p \neq \mathbb{R}(X) \). Also, Lemma 3.9 shows that the residue field \( F_v \) admits a semiordering \( (P \cap A_R^p)/M_v \). By Lemma 3.3, \( F_v \) is formally real. Therefore, \( v \) is a non-trivial real place of \( \mathbb{R}(X) \), and from the definition of \( A_R^p \) we have \( \mathbb{R} \subseteq A_R^p = A_v \).
Using the classification of real places of $\mathbb{R}(X)$ given in Proposition 3.7, consider the following three cases. Since $F_v$ is isomorphic to $\mathbb{R}$, the semiring $(P \cap A_v)/M_v$ corresponds to the only ordering on $\mathbb{R}$.

1. The real place $v$ is equivalent to a place $v_t$ for some $t \in B \subseteq \mathbb{R}$. In this case $\mathbb{R}[X] \subseteq A_v$. We show that $h_i(t) \geq 0$ for all $i$. By symmetry it suffices to show $h_1(t) \geq 0$. For every $t \in (\mathbb{R}_{>0}, \mathbb{R}_{>0})$, we have $t \in U(B)$, so $h_1 + \varepsilon(h_2 + \cdots + h_n) \in P_0 \subseteq P$. Since $h_1 + \varepsilon(h_2 + \cdots + h_n) \in \mathbb{R}[X] \subseteq A_v$, we have $h_1 + \varepsilon(h_2 + \cdots + h_n) \in P \cap A_v$, which gives

$$h_1 + \varepsilon(h_2 + \cdots + h_n) + M_v \in (P \cap A_v)/M_v.$$  

(6)

Since the residue field $\mathbb{R}(X)_v$ is isomorphic to $\mathbb{R}$ by the natural homomorphism $y + M_v \mapsto y(t)$, Equation (6) yields

$$h_1(t) + \varepsilon(h_2(t) + \cdots + h_n(t)) \geq 0.$$  

Since this is true for all $\varepsilon > 0$, we conclude that $h_1(t) \geq 0$ and thus $h_i(t) \geq 0$ for all $i$.

2. The real place $v$ is equivalent to a place $v_t$ for some $t \in \mathbb{R} \setminus B$. There exists a polynomial $H_B \in \mathbb{R}[X]$, such that $H_B(x) > 0$ for all $x \in B$ but $H_B(t) < 0$. Indeed, since $t \not\in B$, there exists an interval $(t - \delta, t + \delta)$ disjoint from $B$; it then suffices to take $H_B := (X - t)^2 - \delta^2$. As in the previous case, we have $h_1(t) \geq 0$. Furthermore, since $H_B \in U(B)$ by its definition, we have $H_Bh_1 + \varepsilon(h_2 + \cdots + h_n) \in P_0 \subseteq P$ for all $\varepsilon \in \mathbb{R}_{>0}$. This yields $\{H_Bh_1(t) \geq 0\}$. However, we have $H_B(t) < 0$ by its definition. This together with $h_1(t) \geq 0$ yields $h_1(t) = 0$. By symmetry we can prove $h_i(t) = 0$ for all $i$, this contradicts the condition $\gcd(h_1, \ldots, h_n) = 1$.

3. The real place $v$ is equivalent to the place $v_\infty$. We divide $\{h_1, \ldots, h_n\}$ into two parts according to the parity of its degree. Without loss of generality, suppose $h_1, \ldots, h_k$ have even degree, and $h_{k+1}, \ldots, h_n$ have odd degree.

Define the leading coefficient of a polynomial as the coefficient of its highest degree monomial. First we claim that the leading coefficients of $h_1, \ldots, h_k$ are all positive. By symmetry, we only prove positivity of the leading coefficients of $h_1$.

Let $m = \max\{\deg h_1, \ldots, \deg h_n\} + 1$. Since $(X^2 + 1)^m \in U(B)$ and $X^{\deg h_1} \in W(\mathbb{R})$, we have

$$h_1 \frac{(X^2 + 1)^m}{(X^2 + 1)^{\frac{m}{2}}} (h_2 + \cdots + h_n) + M_v \in (P \cap A_v)/M_v.$$  

(7)

Since the residue field $\mathbb{R}(X)_v$ is isomorphic to $\mathbb{R}$ by the natural homomorphism $y + M_v \mapsto \lim_{t \to \infty} y(t)$, Equation (7) shows that the leading coefficient of $h_1$ is positive. Therefore by symmetry, the leading coefficient of $h_i$ is positive for all $1 \leq i \leq k$.

We then separate four cases.

a. If $B$ is bounded, that is, $B \subseteq (a, b)$ for some $a, b \in \mathbb{R}$. Let $s > \max\{|a|, |b|\} \in U(B)$. Since $\deg h_n$ is odd, we have $X^{\deg h_n+1} \in W(\mathbb{R})$. Therefore,

$$\frac{(X + s)^{-\deg h_n}}{X^{\deg h_n+1}} + \frac{(X^2 + 1)^m}{(X^2 + 1)^{\frac{m}{2}}} (h_1 + \cdots + h_{n-1}) + M_v \in (P \cap A_v)/M_v.$$  

(8)

This shows that the leading coefficient of $h_n$ is positive.

b. If $B$ contains $-s \in U(B)$, we can replace $(X + s)$ with $(-X + s)$ in Equation (8). This shows that the leading coefficient of $h_n$ is negative. Therefore $h_n$ does not exist, so all $h_1, \ldots, h_n$ must have even degree. But then $(X+1-a)(b+1-X) \in U(B)$, so

$$\frac{(X + 1 - a)(b + 1 - X)h_1}{X^{\deg h_1+1}} + \frac{(X^2 + 1)^m}{(X^2 + 1)^{\frac{m}{2}}} (h_2 + \cdots + h_n) + M_v \in (P \cap A_v)/M_v.$$  

(9)

This shows that the leading coefficient of $h_n$ is positive.

However, we also have $-X + s \in U(B)$, so we can replace $(X + s)$ with $(-X + s)$ in Equation (8). This shows that the leading coefficient of $h_n$ is negative. Therefore $h_n$ does not exist, so all $h_1, \ldots, h_n$ must have even degree. But then $(X+1-a)(b+1-X) \in U(B)$, so

$$\frac{(X + 1 - a)(b + 1 - X)h_1}{X^{\deg h_1+1}} + \frac{(X^2 + 1)^m}{(X^2 + 1)^{\frac{m}{2}}} (h_2 + \cdots + h_n) + M_v \in (P \cap A_v)/M_v.$$  

(9)
This shows that the leading coefficient of \( h_1 \) is negative, a contradiction.

b. If \( B \subset (a, +\infty) \) for some \( a \in \mathbb{R} \), and \( B \) contains arbitrarily large positive reals, that is, \( B \cap (b, +\infty) \neq \emptyset \) for all \( b \in \mathbb{R} \). Then \( X + 1 - a \in U(B) \), so
\[
\frac{(X + 1 - a)h_n}{X^\deg h_n + 1} + \frac{(X^2 + 1)^m}{(X^2 + 1)^{2m}}(h_1 + \cdots + h_{n-1}) + M_v \in (P \cap A_v)/M_v. \tag{10}
\]
This shows that the leading coefficient of \( h_n \) is positive. By symmetry, the leading coefficients of \( h_{k+1}, \ldots, h_n \) are all positive. Therefore, for large enough \( t \in B \), \( h_1(t), \ldots, h_n(t) \) are all positive.

c. If \( B \subset (-\infty, a) \) for some \( a \in \mathbb{R} \), and \( B \) contains arbitrarily small reals, that is, \( B \cap (-\infty, b) \neq \emptyset \) for all \( b \in \mathbb{R} \). Then \( a + 1 - X \in U(B) \), so
\[
\frac{(a + 1 - X)h_n}{X^\deg h_n + 1} + \frac{(X^2 + 1)^m}{(X^2 + 1)^{2m}}(h_1 + \cdots + h_{n-1}) + M_v \in (P \cap A_v)/M_v. \tag{11}
\]
This shows that the leading coefficient of \( h_n \) is negative. By symmetry, the leading coefficients of \( h_{k+1}, \ldots, h_n \) are all negative. Therefore, for small enough \( 0 > t \in B \), \( h_1(t), \ldots, h_n(t) \) are all positive.

d. If \( B \) contains arbitrarily large and arbitrarily small reals. We claim that the leading coefficients of \( h_{k+1}, \ldots, h_n \) all have the same sign. Suppose on the contrary that they have different signs, denote by \( a_i \) the leading coefficient of \( h_i \), so \( h_i = a_iX^{\deg h_i} + H_i \) for some polynomial \( H_i \) of degree at most \( \deg h_i - 1 \). Then there exist strictly positive reals \( r_{k+1}, \ldots, r_n \) such that \( r_{k+1}a_{k+1} + \cdots + r_na_n = 0 \). Then, for any \( s \in \mathbb{R} \), we have
\[
X^2 - 2sX + s^2 + 1 \in U(B), \quad \text{so}
\]
\[
\frac{(X^2 + 1)^m}{(X^2 + 1)^{2m}}(h_1 + \cdots + h_k) + \frac{r_{k+1}(X^2 - 2sX + s^2 + 1)}{X^{\deg h_{k+1} + 1}}h_{k+1} + \frac{r_{k+2}}{X^{\deg h_{k+2} - 1}}h_{k+2} + \cdots + \frac{r_n}{X^{\deg h_n - 1}}h_n + M_v \in (P \cap A_v)/M_v. \tag{12}
\]
The limit of the left hand side when \( X \) tends to infinity is equal to
\[
g(s) := \lim_{X \to \infty} \left( \frac{r_{k+1}(X^2 - 2sX)}{X^{\deg h_{k+1} + 1}}h_{k+1}(X) + \sum_{j=k+2}^n \frac{r_j}{X^{\deg h_j - 1}}h_j(X) \right)
\]
\[
= -2sa_{k+1}r_{k+1} + \lim_{X \to \infty} \left( \sum_{j=k+1}^n \frac{r_j}{X^{\deg h_j - 1}}H_j(X) \right)
\]
because \( r_{k+1}a_{k+1} + \cdots + r_na_n = 0 \). According to whether \( a_{k+1}r_{k+1} \) is positive or negative, we can take a positive or negative \( s \) with large enough absolute value, so that the value of \( g(s) \) is negative. This contradicts Equation (12), which shows that the limit of the left hand side when \( X \to \infty \) is positive.

We therefore conclude that the leading coefficients of \( h_{k+1}, \ldots, h_n \) all have the same sign. If they are positive, then for large enough \( t \in B \), \( h_1(t), \ldots, h_n(t) \) are all positive.

If they are negative, then for small enough \( t \in B \), \( h_1(t), \ldots, h_n(t) \) are all positive.

To sum up, in all possible cases, we have \( t \in B \) with \( h_i(t) \geq 0 \) for all \( i \). If \( -P \) is a semicone instead of \( P \), analogously we can find \( t \in B \) such that \( h_i(t) \leq 0 \) for all \( i \). \( \blacksquare \)

5 Local-global principle over \( \mathbb{N}[X] \)

In this section we prove Theorem 2.2. Omitted proofs are given in Appendix A. The key to bridging the difference between the semirings \( U(B) \) and \( \mathbb{N}[X] \) is Pólya’s Theorem:
Lemma 5.1 (Pólya’s Theorem [14, Theorem 56]). If a homogeneous polynomial \( f \in \mathbb{R}[X_1, \ldots, X_n] \) is strictly positive for all \((X_1, \ldots, X_n)\) on \((\mathbb{R}_{\geq 0})^n \setminus \{0\}\), then there exists \( p \in \mathbb{N} \) such that \((X_1 + \cdots + X_n)^p \cdot f \in \mathbb{R}_{\geq 0}[X_1, \ldots, X_n]\).

The following proposition reduces Theorem 2.2 to real polynomials.

Proposition 5.2. Given \( h_1, \ldots, h_n \in \mathbb{Z}[X] \). The equation \( f_1h_1 + \cdots + f_nh_n = 0 \) has a solution \((f_1, \ldots, f_n)\) over \( \mathbb{N}[X] \setminus \{0\} \) if and only if it has a solution over \( \mathbb{R}_{\geq 0}[X] \setminus \{0\} \).

The next proposition further reduces it to \( U(\mathbb{R}_{\geq 0}) \). The key to its proof is Lemma 5.1.

Proposition 5.3. Given \( h_1, \ldots, h_n \in \mathbb{Z}[X] \). The equation \( f_1h_1 + \cdots + f_nh_n = 0 \) has a solution \((f_1, \ldots, f_n)\) over \( \mathbb{R}_{\geq 0}[X] \setminus \{0\} \) if and only if it has a solution over \( U(\mathbb{R}_{\geq 0}) \).

This justifies the need for a “strictly positive” version of the Bröcker-Prestel principle, since Proposition 5.3 no longer holds if we replace \( U(\mathbb{R}_{\geq 0}) \) with \( W(\mathbb{R}_{\geq 0}) \setminus \{0\} \) (see Remark A.1).

We now prove the local-global principle for homogeneous linear equations over \( \mathbb{N}[X] \).

Theorem 2.2. Given polynomials \( h_1, \ldots, h_n \in \mathbb{Z}[X] \) with \( \gcd(h_1, \ldots, h_n) = 1 \). If the equation \( f_1h_1 + \cdots + f_nh_n = 0 \) has no solution \((f_1, \ldots, f_n)\) over \( \mathbb{N}[X] \setminus \{0\} \), then there exists \( t \in \mathbb{R}_{\geq 0} \), such that the values \( h_i(t) \), \( i = 1, \ldots, n \) are either all non-negative or all non-positive.

Proof. Suppose the equation \( f_1h_1 + \cdots + f_nh_n = 0 \) has no solution \((f_1, \ldots, f_n)\) over \( \mathbb{N}[X] \setminus \{0\} \). By Proposition 5.2 and 5.3, it has no solution over \( U(\mathbb{R}_{\geq 0}) \). Hence, by Theorem 2.1, there exists a real number \( t \in \mathbb{R}_{\geq 0} = \mathbb{R}_{\geq 0} \) such that \( h_i(t) \) are all non-negative or all non-positive. ▶

6 Decidability

In this section we show our main decidability result.

Theorem 2.3. Given as input \( h_1, \ldots, h_n \in \mathbb{Z}[X] \). It is decidable in polynomial time whether the equation \( f_1h_1 + \cdots + f_nh_n = 0 \) has solutions \( f_1, \ldots, f_n \) over \( \mathbb{N}[X] \setminus \{0\} \).

Proof. (A summary of the algorithm constructed in this proof is given in Appendix B.) By the homogeneity of the linear equation, we can divide \( h_1, \ldots, h_n \) by their greatest common divisor and suppose \( \gcd(h_1, \ldots, h_n) = 1 \). Computing the greatest common divisor can be done in polynomial time using the Euclidean algorithm.

We then show that we can simplify the equation so that \( h_1, \ldots, h_n \) satisfy

\[
h_i(0) > 0, h_j(0) < 0, \quad \text{for some } i, j.
\]

Suppose this is not already the case, that \( h_i(0) \geq 0 \) for all \( i \) or \( h_i(0) \leq 0 \) for all \( i \). Without loss of generality suppose \( h_i(0) \geq 0 \) for all \( i \). We write \( h_1(0) = 0, \ldots, h_k(0) = 0, h_{k+1}(0) > 0, \ldots, h_n(0) > 0 \). Then \( X \mid h_i \) for \( i = 1, \ldots, k \).

If \( k = 0 \), that is \( h_i(0) > 0 \) for all \( i \), then \( f_1h_1 + \cdots + f_nh_n = 0 \) has no solution over \( \mathbb{N}[X] \setminus \{0\} \). Indeed, suppose on the contrary that \( (f_1, \ldots, f_n) \) is such a solution. Dividing all \( f_i \) by a suitable power of \( X \) we can suppose \( f_s(0) \neq 0 \) for some \( s \). Then \( f_i(0) \geq 0 \) for all \( i \) while \( f_s(0) > 0 \), which yields \( f_1(0)h_1(0) + \cdots + f_n(0)h_n(0) > 0 \), a contradiction.

If \( k \geq 1 \), we show that the equation

\[
f_1h_1 + \cdots + f_nh_n = 0
\]

has a solution over \( \mathbb{N}[X] \setminus \{0\} \) if and only if the equation

\[
f_1 \cdot \frac{h_1}{X} + \cdots + f_k \cdot \frac{h_k}{X} + f_{k+1}h_{k+1} + \cdots + f_nh_n = 0
\]
has a solution over $\mathbb{N}[X] \setminus \{0\}$. Let $(f_1, \ldots, f_n)$ be a solution over $\mathbb{N}[X] \setminus \{0\}$ of Equation (14), then $f_1(0)h_1(0) + \cdots + f_n(0)h_n(0) = 0$. Since $h_i(0) = 0$ for all $i = 1, \ldots, k$, $h_i(0) > 0$ for $i = k + 1, \ldots, n$ and $f_i(0) > 0$ for $i = 1, \ldots, n$, we must have $f_{k+1}(0) = 0, \ldots, f_n(0) = 0$. That is, $X | f_{k+1}, \ldots, X | f_n$. Therefore $(f_1, \ldots, f_k, f_{k+1}/X, \ldots, f_n/X)$ is a solution over $\mathbb{N}[X] \setminus \{0\}$ of Equation (15). This shows that we can divide $h_1, \ldots, h_k$ by $X$ without changing the existence of the solutions of Equation (14). Repeating this division process, one eventually terminates by obtaining $h_i$ such that either: $h_i(0)$ are all strictly positive or all strictly negative, in which case Equation (14) has no solution over $\mathbb{N}[X] \setminus \{0\}$; or $h_i(0) > 0$ and $h_j(0) < 0$ for some $i, j$, in which case we have achieved the desired simplification to Condition (13). This procedure is repeated at most $\deg h_1 + \cdots + \deg h_n$ times, and therefore terminates in polynomial time.

Supposing Condition (13), we claim that $f_1h_1 + \cdots + f_nh_n = 0$ has no solution over $\mathbb{N}[X] \setminus \{0\}$ if and only if there exists $t \in \mathbb{R}_{\geq 0}$ such that $h_i(t)$ are all non-positive or all non-negative. The first implication is given by Theorem 2.2. Conversely, suppose $h_i(t)$ are all non-positive or all non-negative. Without loss of generality suppose $h_i(t) \geq 0$ for all $i$. By Condition (13), we have $t \neq 0$. Suppose on the contrary that $(f_1, \ldots, f_n)$ is a solution over $\mathbb{N}[X] \setminus \{0\}$, then $f_i(t) > 0$ for all $i$ since $t > 0$. Since $\gcd(h_1, \ldots, h_n) = 1$, at least one of $h_i(t)$ must be non-zero. Since $h_i(t) \geq 0$ for all $i$, we have $f_1(t)h_1(t) + \cdots + f_n(t)h_n(t) > 0$, a contradiction.

Thus, it suffices to decide whether there exists $t \geq 0$ such that $h_i(t)$ are all non-positive or all non-negative. This can be expressed in the existential theory of the reals:

$$\exists X (X^{\geq 0} \land h_1(X) \geq 0 \land \cdots \land h_n(X) \geq 0) \lor (X^{\geq 0} \land h_1(X) \leq 0 \land \cdots \land h_n(X) \leq 0).$$  \hspace{1cm} (16)

Deciding the existential theory of the reals in one variable can be done in polynomial time with respect to the total bit length used to encode the sentence, due to a classic result by Collins\(^2\) [8]. Therefore, one can decide the correctness of the sentence (16) in polynomial time. Combining all the steps, we conclude that the total complexity is in PTIME.

\section{Application to wreath product}

In this section we show the following result on wreath products.

\textbf{Theorem 2.4.} Given a finite set of elements $G = \{(y_1, b_1), \ldots, (y_n, b_n)\}$ in $\mathbb{Z} \times \mathbb{Z}$, where $b_i = \pm 1$ for all $i$. The following are decidable:

1. (Group Problem) whether the semigroup $\langle G \rangle$ generated by $G$ is a group.

2. (Identity Problem) whether the neutral element $I$ is in the semigroup $\langle G \rangle$.

Let $\varphi$ be the isomorphism defined in (3). Fix a finite set of elements $G$ as in Theorem 2.4. For $i = 1, \ldots, n$, denote by $H_i \in \mathbb{Z}[X, X^{-1}]$ the Laurent polynomial in the upper-right entry of the image of $\varphi((y_i, b_i))$. Write $G = G_+ \cup G_-$ where $G_+ := \{(y_i, b_i) \in G \mid b_i = 1\}$ and $G_- := \{(y_i, b_j) \in G \mid b_j = -1\}$. Let $\varphi(G), \varphi(G_+), \varphi(G_-)$ be the set of matrices that are images under $\varphi$ of elements in $G, G_+, G_-$. Define the sets of indices

$I := \{i \mid b_i = 1\}, \quad J := \{i \mid b_i = -1\}.$

\(^2\) The algorithm by Collins \cite{Collins1975} has complexity $L^3(n d)^{O(K)}$, where $L$ is the total coefficient bit length, $n$ the number of polynomials, $d$ the total degree of the polynomials, and $K$ the number of variables. In the one variable case, $K = 1$, the algorithm takes polynomial time with respect to the total bit length.
For simplicity, we write $A_i, i \in I$ for the matrices in $\varphi(\mathcal{G}_+)$, and $B_j, j \in J$ the matrices in $\varphi(\mathcal{G}_-)$. For every tuple $(i, j) \in I \times J$, define the matrix

$$h_{ij} := X^{-1}H_i + H_j \in \mathbb{Z}[X, X^{-1}].$$

This is the upper-right entry of the matrix $A_iB_j$.

For a subset $S \subseteq I \times J$, denote by $\pi_S(S)$ its projection onto the $I$ coordinates, that is, $\pi_S(S) := \{ i \in I \mid \exists j \in J, (i, j) \in S \}$. Define $\pi_S$ likewise. The key to proving the partial decidability of the Group Problem in $\mathbb{Z} \wr \mathbb{Z}$ is the following proposition that relates sub-semigroups of $\mathbb{Z} \wr \mathbb{Z}$ to equations over $\mathbb{N}[X] \setminus \{0\}$.

**Proposition 7.1.** Given a set $\mathcal{G} = \mathcal{G}_+ \cup \mathcal{G}_-$ of generators as above. Let $h_{ij} \in \mathbb{Z}[X, X^{-1}]$ be the polynomials defined in (17). The semigroup $\langle \mathcal{G} \rangle$ is a group if and only if there exists a set $S \subseteq I \times J$ satisfying $\pi_S(S) = I, \pi_S(S) = J$, such that the equation $\sum_{(i,j) \in S} f_{ij}h_{ij} = 0$ has a solution $(f_{ij})_{(i,j) \in S}$ over $\mathbb{N}[X] \setminus \{0\}$.

**Proof.** For a word $w$ in the alphabet $\varphi(\mathcal{G})$, define its product $\pi(w)$ to be the matrix obtained by multiplying all the matrices in $w$ consecutively. Denote by $|w|_+$ (respectively, $|w|_-$) the number of letters in $w$ belonging in $\varphi(\mathcal{G}_+)$ (respectively, $\varphi(\mathcal{G}_-)$). Define the height of the word $w$ to be $h(w) := |w|_+ - |w|_-$, then we have $\pi(w) = \begin{pmatrix} 1 & * \\ 0 & X^{h(w)} \end{pmatrix}$, where $*$ is some element in $\mathbb{Z}[X, X^{-1}]$.

For a finite alphabet $A$, denote by $A^+$ the set of non-empty words over $A$. We claim that for any non-empty word $w \in \varphi(\mathcal{G})^+$ such that $h(w) = 0$, the upper right entry of $\pi(w)$ can be written as a sum $\sum_{(i,j) \in I \times J} f_{ij}h_{ij}$, where $f_{ij}$ are elements in $\mathbb{N}[X, X^{-1}]$. We prove this by induction on the length of the word $w$. For the sake of simplicity, denote $U(\pi(w))$ the upper right entry of $\pi(w)$.

If $w$ has length at most two, then it must be of the form $A_iB_j$ or $B_jA_i$, and the claim is easy to verify. Suppose the claim is true for all words $w$ of length less than $\ell > 2$. We prove the claim for words $w$ of length $\ell$. Distinguish the following two cases.

1. The word $w$ is of the form $A_iw'B_j$ or $B_jw'A_i$ for some $i \in I, j \in J, w' \in \varphi(\mathcal{G})^+$. Since $w'$ has length at most $\ell - 2$ and is of height $0$, by induction hypothesis, $\pi(w') = \begin{pmatrix} 1 & r' \\ 0 & 1 \end{pmatrix}$, with $r$ a linear combination of $h_{ij}$ with coefficients in $\mathbb{N}[X, X^{-1}]$. If $w = A_iw'B_j$, then

$$\pi(w) = \begin{pmatrix} 1 & H_j \\ 0 & X \end{pmatrix} \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & H_i \\ 0 & X^{-1} \end{pmatrix} = \begin{pmatrix} 1 & X^{-1}r + (X^{-1}H_i + H_j) \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & X^{-1}r + h_{ij} \\ 0 & 1 \end{pmatrix}.$$ 

So $U(\pi(w)) = X^{-1}r + h_{ij}$ can also be written as a linear combination of $h_{ij}, i \in I, j \in J$ with coefficients in $\mathbb{N}[X, X^{-1}]$. If $w = B_jw'A_i$, then

$$\pi(w) = \begin{pmatrix} 1 & H_j \\ 0 & X^{-1} \end{pmatrix} \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & H_i \\ 0 & X \end{pmatrix} = \begin{pmatrix} 1 & Xr + H_i + XH_j \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & X(r + h_{ij}) \\ 0 & 1 \end{pmatrix}.$$ 

So $U(\pi(w)) = X(r + h_{ij})$ can also be written as a linear combination of $h_{ij}, i \in I, j \in J$ with coefficients in $\mathbb{N}[X, X^{-1}]$.

2. The word $w$ is of the form $A_iw'A_j$ or $B_jw'B_j$ for some $i, i' \in I$ or $j, j' \in J$. First suppose $w = A_iw'A_j$. Since $h(A_i) = 1 > 0$ and $h(A_iw') = -1 < 0$, there must exist a strict prefix $v$ of $w$ with height zero. This is because by reading the word $w$ letter by letter, this height of consecutive prefixes differs by at most one. We have $w = vv'$ with $h(v) = h(v') = 0$ where $v, v'$ are non-empty words. By induction hypothesis,
where \(w = B_jw'B_j\) is completely analogous.

Combining the two cases concludes the induction. It is easy to see from the induction process that if the letter \(A_i\) appears in \(w\), then the coefficient of the term \(h_{ij}\) in the linear combination is not zero for some \(j \in J\). This is because at some point we have replaced \(r\) with either \(X^{-1}r + h_{ij}\) or \(X(r + h_{ij})\). Similarly, if the letter \(B_j\) appears in \(w\), then the coefficient of the term \(h_{ij}\) in the linear combination is non-zero for some \(i \in I\).

If the semigroup \(\langle \mathcal{G} \rangle\) is a group, then there exists a word \(v\) in the alphabet \(\mathcal{G}\) using all letters in \(\mathcal{G}\), whose corresponding product is the neutral element. Taking the image under \(\varphi\) yields a word \(w = \varphi(v)\) in the alphabet \(\varphi(\mathcal{G})\) such that \(h(w) = 0\) and \(U(\pi(w)) = U(\pi(\varphi(v))) = 0\).

The claim above and the discussion following it show that there exist Laurent polynomials \(f_{ij} \in N[X, X^{-1}]\) such that \(\sum_{(i,j) \in I \times J} f_{ij}h_{ij} = 0\). Furthermore, all letters \(A_i, i \in I\) and \(B_j, j \in J\) appear in \(w\), so for every \(i\), the coefficient \(f_{ij}\) in the linear combination is not zero for some \(j \in J\); and for every \(j\), the coefficient \(f_{ij}\) is not zero for some \(i \in I\). Let \(S := \{(i, j) \in I \times J \mid f_{ij} \neq 0\}\), then \(\sum_{(i,j) \in S} f_{ij}h_{ij} = 0\), and \(\pi_I(S) = I, \pi_J(S) = J\). By the homogeneity of the equation, suppose that there is a tuple \(w = (u, v) \in S\) such that \(X \cdot f_{uv} = 0\). Let \((u, v) \in S\) be a tuple such that \(\deg f_{uv} \geq \deg f_{ij}\) for all \((i, j) \in S\).

Denote by \(N_{\geq 0}[X]\) the set of polynomials of the form \(\sum_{t=0}^d a_tX^t\), where \(d \geq 0\) and \(a_t > 0\) for all \(i\). By multiplying all \(f_{ij}\) by the polynomial \((1 + X)^m\) for a sufficiently large \(m\), we can suppose that \(f_{uv} \in N_{\geq 0}[X], X^{-v_0(f_{uv})}f_{yz} \in N_{\geq 0}[X],\) and \(\deg f_{uv} \geq v_0(f_{yz})\). Indeed, we can take any \(m \geq \max\{\deg f_{uv}, \deg X^{-v_0(f_{uv})}f_{yz}, v_0(f_{yz})\}\). Additionally, the condition that \(\deg f_{yz} \geq \deg f_{ij}\) for all \((i, j) \in S\) is still satisfied after this multiplication.

We now construct a word \(w \in \varphi(\mathcal{G})^+\) that uses every letter in \(\varphi(\mathcal{G})\), such that \(h(\pi(w)) = 0\), \(U(\pi(w)) = \sum_{(i,j) \in S} f_{ij}h_{ij} = 0\). We start with the word

\[
w_0 := A_u^{\deg f_{uv}} A_y^{\deg f_{yz} - \deg f_{uv}} B_z^{\deg f_{yz} - \deg f_{uv}} B_u^{\deg f_{uv}} f_{uv},
\]

which has height 0, and whose product has upper-right entry

\[
U(\pi(w_0)) = h_{uv} \cdot \sum_{i=0}^{\deg f_{uv} - 1} X^i + h_{yz} \cdot \sum_{i=\deg f_{uv}}^{\deg f_{yz} - 1} X^i.
\]

Since \(f_{uv} \in N_{\geq 0}[X], X^{-v_0(f_{uv})}f_{yz} \in N_{\geq 0}[X],\) and \(\deg f_{uv} \geq v_0(f_{yz})\), the polynomials \(\hat{f}_{uv} := f_{uv} - \sum_{i=0}^{\deg f_{uv} - 1} X^i, \hat{f}_{yz} := f_{yz} - \sum_{i=\deg f_{uv}}^{\deg f_{yz} - 1} X^i\) are still polynomials in \(N[X] \setminus \{0\}\).

For \((i, j) \in S\), define

\[
\hat{f}_{ij} := \begin{cases} 
\hat{f}_{uv} & (i, j) = (u, v) \\
\hat{f}_{yz} & (i, j) = (y, z) \\
\hat{f}_{ij} & \text{otherwise}
\end{cases}
\]

These are elements in \(N[X] \setminus \{0\}\) and satisfy \(U(\pi(w_0)) + \sum_{(i,j) \in S} \hat{f}_{ij}h_{ij} = \sum_{(i,j) \in S} f_{ij}h_{ij} = 0\).

We then gradually insert “loops” of the form \(A_iB_j\) into the word \(w_0\). This insertion does not change the height of the word, but it adds a multiple of \(h_{ij}\) to the upper-right entry of the product. Indeed, if \(h(vv') = 0\), then we have \(h(vA_iB_jv') = 0\) and \(U(\pi(vA_iB_jv')) = \ldots\)
Solving Homogeneous Linear Equations over Polynomial Semirings

$U(\pi(w)) + X^{h(w)}h_{ij}$. Note that the initial word $w_0$ has suffixes of all heights from 0 to $\deg f_{yz}$. For each $k = 0, \ldots, \deg f_{yz}$ and each $(i, j) \in S$, after a suffix of height $k$, we insert $\text{Coef}_{X^k}(f_{ij})$ times the "loop" $A_i B_j$, where $\text{Coef}_{X^k}(f_{ij})$ is the coefficient of the monomial $X^k$ in the polynomial $f_{ij}$. The upper-right entry of the product after all these insertions will be

$$U(\pi(w_0)) + \sum_{k=0}^{\deg f_{yz}} \sum_{(i,j) \in S} \text{Coef}_{X^k}(f_{ij})X^k \cdot h_{ij} = U(\pi(w_0)) + \sum_{(i,j) \in S} \hat{f}_{ij} h_{ij} = 0,$$

because $\deg f_{yz} \geq \deg f_{ij}$ for all $(i, j) \in I \times J$. See Figure 1 for an example of this construction.

We have thus constructed a word $w \in \varphi(G)^+$ such that $h(\pi(w)) = 0$, $U(\pi(w)) = 0$. Note that we have inserted at least one loop $A_i B_j$ for each $(i, j) \in S$. Since $\pi(I) = I$, $\pi(J) = J$, the word $w$ contains every letter $A_i, i \in I$ and $B_j, j \in J$. Because $\pi(w)$ is the neutral element, the inverse of every letter in $w$ can be written as a product of matrices in $\varphi(G)$. Indeed, if $w = vX^w$ then $X^{-1} = \pi(v^w)$. Thus the inverse of every element of $\varphi(G)$ is in $\langle \varphi(G) \rangle$. We conclude that $\langle \varphi(G) \rangle$, and thus $\langle G \rangle$, is a group.

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{figure1.png}
\caption{Example of a word constructed in the proof of Proposition 7.1. Here, $S = \{(u, v), (y, z), (1, 2), (3, 1)\}$, and $f_{uv} = 1 + X + X^2 + X^3$, $f_{yz} = X^3 + X^4 + X^5 + X^6$, $f_{12} = X + 2X^2$, $f_{31} = 3 + X^2$. The constructed word is $A_u(A_1 B_2)A_u A_u(A_2 B_1)A_u A_u(A_1 B_2)(A_1 B_2)A_o(A_y B_z)B_z B_z B_z B_z B_z B_z B_z (A_3 B_1)(A_3 B_1)(A_3 B_1)(A_3 B_1)(A_3 B_1).$}
\end{figure}

We have thus established the link between the Group Problem in $\mathbb{Z}/2$ and homogeneous linear equations over $\mathbb{N}[X]$. Theorem 2.4 follows from Proposition 7.1 and the decidability result of Theorem 2.3. Its proof is given in Appendix A.

References

1. Emil Artin. Über die zerlegung definiter funktionen in quadrate. In Abhandlungen aus dem mathematischen Seminar der Universität Hamburg, volume 5, pages 100–115. Springer, 1927.
2. William Ross Ashby. Automata Studies: Annals of Mathematics Studies. Number 34. Princeton University Press, 1956.
3. François Baccelli, Guy Cohen, Geert Jan Olsder, and Jean-Pierre Quadrat. Synchronization and linearity: an algebra for discrete event systems. John Wiley & Sons Ltd, 1992.
4. Paul C. Bell, Mika Hirvensalo, and Igor 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, pages 187–206. SIAM, 2017.
5. 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.
Proposition 3.7. Let $v$ be a non-trivial real place of $\mathbb{R}(X)$ such that $\mathbb{R} \subseteq A_v$. Then $v$ belongs to one of the two following types of real places:
1. For every $t \in \mathbb{R}$ there is a real place $v_t : \mathbb{R}(X) \to \mathbb{Z} \cup \{\infty\}$, defined by $v_t(y) = a$, where $a \in \mathbb{Z}$ is such that $y$ can be written as $y = (X - t)^a \cdot \frac{f}{g}$, with $f, g$ being polynomials in $\mathbb{R}[X]$ not divisible by $X - t$. The residue field $\mathbb{R}(X)_{v_t}$ is isomorphic to $\mathbb{R}$ by the natural homomorphism $y + M_{v_t} \mapsto y(t)$.

2. There is a real place $v_{\infty} : \mathbb{R}(X) \to \mathbb{Z} \cup \{\infty\}$, defined by $v_{\infty}(\frac{f}{g}) = \deg g - \deg f$, where $f, g$ are polynomials in $\mathbb{R}[X]$. The residue field $\mathbb{R}(X)_{v_{\infty}}$ is isomorphic to $\mathbb{R}$ by the natural homomorphism $y + M_{v_{\infty}} \mapsto \lim_{t \to \infty} y(t)$.

**Proof.** Since $\mathbb{R} \subseteq A_v$, every element $r \in \mathbb{R} \setminus \{0\}$ satisfies $v(r) \geq 0$ and $v(r^{-1}) \geq 0$. But $v(r) + v(r^{-1}) = v(1) = 0$, so $v(r) = 0$. Consider the value $v(X)$, there are two possibilities:

1. If $v(X) \geq 0$. In this case, we have $\mathbb{R} \subseteq A_v$ and $X \in A_v$, therefore $\mathbb{R}[X] \subseteq A_v$. Since $M_v$ is a maximal (hence prime) ideal of $A_v$, the ideal $\mathbb{R}[X] \cap M_v$ is a prime ideal of $\mathbb{R}[X]$. Furthermore, $\mathbb{R}[X] \cap M_v$ is not zero, otherwise every element of $\mathbb{R}[X] \setminus \{0\}$ would be invertible in $A_v$, so $\mathbb{R}(X) \subseteq A_v$, contradicting the non-triviality of $v$. Since $\mathbb{R}[X]$ is a prime ideal domain, the non-zero prime ideal $\mathbb{R}[X] \cap M_v$ is generated by a single irreducible polynomial $\mathbb{R}[X]$. Consider the two cases:

   a. The ideal $\mathbb{R}[X] \cap M_v$ is generated by a polynomial $X - t$ for some $t \in \mathbb{R}$. In this case we have $v(X - t) > 0$. Every polynomial $f \in \mathbb{R}[X]$ not divisible by $(X - t)$ can be written as $f = (X - t) \cdot F + r$ for some $F \in \mathbb{R}[X]$, $r \in \mathbb{R} \setminus \{0\}$. Since $v((X - t) \cdot F) = v(X - t) + v(F) > 0$ and $v(r) = 0$, we have $v(f) = v(r) = 0$. Every element $y \in \mathbb{R}(X)$ can be written as $y = (X - t)^a \cdot \frac{f}{g}$, where $f, g$ are polynomials in $\mathbb{R}[X]$ not divisible by $(X - t)$. Then $v(y) = a \cdot v(X - t) + v(f) - v(g) = av(X - t)$. Under isomorphism of the value group $\Gamma$, we can without loss of generality suppose $v(X - t) = 1$, then we get the valuation $v_t$ of type 1 described in the proposition. Since every element $y \in M_{v_t}$ satisfies $y(t) = 0$, we have that $y + M_{v_t} \mapsto y(t)$ is an isomorphism from the residue field to $\mathbb{R}$; it is a formally real field.

   b. The ideal $\mathbb{R}[X] \cap M_v$ is generated by a polynomial $X^2 + eX + d$ without real roots. In this case, the residue field $A_v/M_v$ is a quadratic extension of $\mathbb{R}$, and is hence isomorphic to the field $\mathbb{C}$. However $\mathbb{C}$ is not formally real. Indeed, suppose on the contrary that $\mathbb{C}$ admits some ordering $\leq$, then since $0 < i^2 = -1$ and $0 < 1^2 = 1$, we have $0 < (-1) + 1 = 0$, a contradiction.

2. If $v(X) < 0$. In this case we have $\mathbb{R}[1/X] \subseteq A_v$ and $1/X \in M_v$. Since $\mathbb{R}[1/X] \cap M_v$ is a prime ideal of $\mathbb{R}[1/X]$ that contains $1/X$, it is generated by $1/X$. Then similar to the case 1a., every element $y \in \mathbb{R}(X)$ can be written as $y = (1/X)^a \cdot \frac{F}{G}$, where $F, G$ are polynomials in $\mathbb{R}[1/X]$ not divisible by $1/X$. Without loss of generality suppose $v(1/X) = 1$, we have $v(y) = a$. Rewriting $y = \frac{G}{F}$, comparing degrees, we have $a = \deg g - \deg f$. So $v$ is the valuation $v_{\infty}$ of type 2 described in the proposition. Since every element $y \in M_{v_{\infty}}$ satisfies $\lim_{t \to \infty} y(t) = 0$, we have that $y + M_{v_{\infty}} \mapsto \lim_{t \to \infty} y(t)$ is an isomorphism from the residue field to $\mathbb{R}$; it is a formally real field.

**Proposition 5.2.** Given $h_1, \ldots, h_n \in \mathbb{Z}[X]$. The equation $f_1h_1 + \cdots + f_nh_n = 0$ has a solution $(f_1, \ldots, f_n)$ over $\mathbb{N}[X] \setminus \{0\}$ if and only if it has a solution over $\mathbb{R}_{\geq 0}[X] \setminus \{0\}$.

**Proof.** A solution over $\mathbb{N}[X] \setminus \{0\}$ is obviously also a solution over $\mathbb{R}_{\geq 0}[X] \setminus \{0\}$. Conversely, let $f_i = \sum_{j=0}^{d_i} a_{ij}X^j$, $i = 1, \ldots, n$, be a solution of $f_1h_1 + \cdots + f_nh_n = 0$. Write $h_i = \sum_{j=0}^{e_i} b_{ij}X^j$, $i = 1, \ldots, n$, then the equation $f_1h_1 + \cdots + f_nh_n = 0$ is equivalent to the system of equations

$$\sum_{i=1}^n \sum_{j=0}^d a_{ij}b_{i,d-j} = 0, \quad d = 1, \ldots, \max_{1 \leq i \leq n} (d_i + e_i).$$

(18)

All the coefficients $b_{ij}$ are integers, and $b_{i,d-j} = 0$ whenever $d - j < 0$. 

---

*Solving Homogeneous Linear Equations over Polynomial Semirings*
If \( f_1 h_1 + \cdots + f_n h_n = 0 \) has a solution over \( \mathbb{R}_{\geq 0}[X] \setminus \{0\} \), then System (18) has a solution \( a_{ij}, i = 1, \ldots, n, j = 1, \ldots, d_i \) over \( \mathbb{R} \), satisfying

\[
a_{ij} \geq 0, \quad i = 1, \ldots, n, \quad j = 1, \ldots, d_i, \tag{19}
\]

and

\[
a_{i1} \neq 0 \text{ or } a_{i2} \neq 0 \text{ or } \ldots \text{ or } a_{id_i} \neq 0, \quad i = 1, \ldots, n. \tag{20}
\]

This condition is a boolean combination of homogeneous linear inequalities with integer coefficients. Since the linear Systems (18), (19) and (20) have only integer coefficients, they have a solution over \( \mathbb{R} \) if and only if they have a solution over \( \mathbb{Q} \). Then, by their homogeneity, they have a solution over \( \mathbb{Q} \) if and only if they have a solution over \( \mathbb{Z} \). Hence, the Systems (18), (19), (20) have a solution over \( \mathbb{Z} \), meaning \( f_1 h_1 + \cdots + f_n h_n = 0 \) has a solution \( f_i = \sum_{j=0}^{d_i} a_{ij} X^j, i = 1, \ldots, n, \) over \( \mathbb{N}[X] \setminus \{0\} \).

\[\text{Proposition 5.3.} \text{ Given } h_1, \ldots, h_n \in \mathbb{Z}[X]. \text{ The equation } f_1 h_1 + \cdots + f_n h_n = 0 \text{ has a solution } (f_1, \ldots, f_n) \text{ over } \mathbb{R}_{\geq 0}[X] \setminus \{0\} \text{ if and only if it has a solution over } \mathbb{U}(\mathbb{R}_{\geq 0}).\]

\[\text{Proof.} \text{ Obviously a solution over } \mathbb{R}_{\geq 0}[X] \setminus \{0\} \text{ is a solution over } \mathbb{U}(\mathbb{R}_{\geq 0}). \]

For the other implication, we use Pólya’s Theorem (Lemma 5.1). Suppose \( f_1 h_1 + \cdots + f_n h_n = 0 \) has a solution \((f_1, \ldots, f_n)\) over \( \mathbb{U}(\mathbb{R}_{\geq 0}) \). Write \( f_i = X^{c_i} \cdot F_i \) where \( c_i \geq 0 \) and \( F_i \in \mathbb{R}[X] \) is such that \( X \notdivides F_i \). Since \( X \notdivides F_i \) we have \( F_i(0) \neq 0 \), we claim that \( F_i(0) > 0 \). In fact, if \( F_i(0) < 0 \), then by the continuity of \( F_i \), there exists \( \varepsilon > 0 \) such that \( F_i(\varepsilon) < 0 \), but then \( f_i(\varepsilon) = e^{c_i} F_i(\varepsilon) < 0 \), contradicting the fact that \( f_i \in \mathbb{U}(\mathbb{R}_{\geq 0}) \). Furthermore, one easily sees that \( F_i(x) = F_i(0) x^{c_i} > 0 \) for all \( x > 0 \). So we have shown \( F_i(x) > 0 \) for all \( x > 0 \).

We now show that for large enough \( p \in \mathbb{N} \), the polynomials \( \hat{f}_i := (X + 1)^p \cdot f_i \) are all in \( \mathbb{R}_{\geq 0}[X] \). Let \( Y \) be a new variable, and for every \( i \), let \( G_i \) be the homogenization of \( F_i \) using the variable \( Y \). That is, \( G_i = F_i(X/Y) \cdot Y^{\deg(F_i)} \). Since \( F_i(x/y) > 0 \) for all \( x/y \geq 0 \), we have \( G_i(x, y) > 0 \) for all \( x \geq 0, y > 0 \). Whereas for \( x > 0, y = 0 \), \( G_i(x, y)/x^{\deg(F_i)} \) is the leading coefficient of \( F_i \). This is non-zero and thus must be positive because \( \lim_{x \to \infty} F_i(x) > 0 \). Therefore \( G_i(x, y) > 0 \) for \( x > 0, y > 0 \).

We have thus shown \( G_i(x, y) > 0 \) for all \( x \geq 0, y > 0, x + y > 0 \). Applying Pólya’s Theorem yields the existence of a \( p_0 \in \mathbb{N} \) such that \( (X + Y)^{p_0} \cdot G_i \in \mathbb{R}_{\geq 0}[X, Y] \). Taking \( Y = 1 \) we dehomogenize \( G_i \) and obtain \( (X + 1)^{p_0} \cdot F_i \in \mathbb{R}_{\geq 0}[X] \). Let \( p = \max\{p_1, \ldots, p_n\} \), then

\[
\hat{f}_i = (X + 1)^p \cdot f_i = X^{c_i} \cdot (X + 1)^p \cdot F_i \in \mathbb{R}_{\geq 0}[X] \setminus \{0\}
\]

for all \( i \). We have thus found the solution \((\hat{f}_1, \ldots, \hat{f}_n)\) over \( \mathbb{R}_{\geq 0}[X] \setminus \{0\} \) for the equation \( f_1 h_1 + \cdots + f_n h_n = 0 \).

\[\text{Remark A.1.} \text{ Proposition 5.3 no longer holds if we replace } \mathbb{U}(\mathbb{R}_{\geq 0}) \text{ with } \mathbb{W}(\mathbb{R}_{\geq 0}) \setminus \{0\}. \]

For example, take \( n = 2, h_1 = 1, h_2 = -(X - 1)^2 \). Then \( f_1 = (X - 1)^2, f_2 = 1 \) is a solution over \( \mathbb{W}(\mathbb{R}_{\geq 0}) \setminus \{0\} \) of the equation \( f_1 h_1 + f_2 h_2 = 0 \). However, \( f_1 h_1 + f_2 h_2 = 0 \) does not admit a solution over \( \mathbb{R}_{\geq 0}[X] \setminus \{0\} \). Indeed, any solution of \( f_1 - f_2 \cdot (X - 1)^2 = 0 \) over \( \mathbb{R}[X] \) must satisfy \( f_1(1) = 0 \), so \( f_1 \) cannot be in \( \mathbb{R}_{\geq 0}[X] \setminus \{0\} \).

\[\text{Theorem 2.4.} \text{ Given a finite set of elements } \mathcal{G} = \{(y_1, b_1), \ldots, (y_n, b_n)\} \text{ in } \mathbb{Z} \cap \mathbb{Z}, \text{ where } b_i = \pm 1 \text{ for all } i. \text{ The following are decidable:} \]

1. \( \text{(Group Problem)} \) whether the semigroup \( \langle \mathcal{G} \rangle \) generated by \( \mathcal{G} \) is a group.
2. \( \text{(Identity Problem)} \) whether the neutral element \( I \) is in the semigroup \( \langle \mathcal{G} \rangle \).
Proof.
1. For the Group Problem, by Proposition 7.1 it suffices to decide whether there exists a set \( S \subseteq I \times J \) satisfying \( \pi_1(S) = I, \pi_J(S) = J \), such that the equation \( \sum_{(i,j) \in S} f_{ij}h_{ij} = 0 \) has a solution \((f_{ij})_{(i,j) \in S}\) over \( \mathbb{N}[X] \setminus \{0\} \). By the homogeneity of the equation \( \sum_{(i,j) \in S} f_{ij}h_{ij} = 0 \), one can multiply all the Laurent polynomials \( h_{ij} \) by a power of \( X \) and suppose all \( h_{ij} \in \mathbb{Z}[X] \). For every set \( S \subseteq I \times J \) satisfying \( \pi_1(S) = I, \pi_J(S) = J \), we can use Theorem 2.3 to decide whether \( \sum_{(i,j) \in S} f_{ij}h_{ij} = 0 \) has a solution over \( \mathbb{N}[X] \setminus \{0\} \). This shows the decidability of the Group Problem.

2. The neutral element is in \( \langle G \rangle \) if and only if a non-empty subset of \( G \) generates a group (as a semigroup). This is because, if the product of a word \( w \in \langle G \rangle^+ \) is the neutral element, then every element in the set \( C \) of letters used in \( w \) can be inverted in \( \langle C \rangle \), so \( \langle C \rangle \) is a group. Therefore, in order to decide whether the neutral element is in \( \langle G \rangle \), it suffices to check for all subsets of \( G \) whether they generate a group. This is decidable by the above result on the Group Problem.

\[ \square \]

B Algorithm for Theorem 2.2

Algorithm 1 Deciding existence of solutions over \( \mathbb{N}[X] \setminus \{0\} \) of the equation \( f_1h_1 + \cdots + f_nh_n = 0 \).

\[ \begin{align*}
\text{Input: Polynomials } & h_1, \ldots, h_n \in \mathbb{Z}[X]. \\
\text{Output: } & \text{True or False.}
\end{align*} \]

1. Compute \( d := \gcd(h_1, \ldots, h_n) \) and divide all \( h_i \) by \( d \).
2. Repeat the following:
   a. If \( h_i(0) > 0 \) for all \( i \), or \( h_i(0) < 0 \) for all \( i \), return \text{False}.
   b. Else if \( h_i(0) \geq 0 \) for all \( i \), or \( h_i(0) \leq 0 \) for all \( i \), divide all the polynomials \( h_i \)
      that satisfy \( h_i(0) = 0 \) by \( X \).
   c. Else go to 3.
3. Decide the truth of the existential sentence (16) in the theory of reals. If (16) is true, return \text{False}, otherwise return \text{True}.

C Comparison with the Bröcker-Prestel local-global principle

The original Bröcker-Prestel local-global principle ([24, Theorem 8.13]) can be formulated as follows.

\[ \text{Theorem C.1 (Bröcker-Prestel local-global principle).} \]

Let \( F \) be a formally real field, and \( h_1, \ldots, h_n \) be non-zero elements of \( F \). If the equation \( f_1h_1 + \cdots + f_nh_n = 0 \) has no non-trivial solution \((f_1, \ldots, f_n) \neq (0, \ldots, 0)\) over sums of squares of \( F \) (that is, over the set \( S := \{ \sum_{i=1}^n a_i^2 \mid a_i \in F \} \)), then at least one of the following hold:

\begin{enumerate}
   \item \( h_1, \ldots, h_n \) are all of the same sign in some archimedean ordering of \( F \).
   \item \( f_1h_1 + \cdots + f_nh_n = 0 \) has no solution in the Henselization of some real place of \( F \).
\end{enumerate}

For a definition of Henselizations of a formally real field, see [24, Proposition 8.1].

When applied to the field \( F = \mathbb{R}(X) \), the Bröcker-Prestel local-global principle characterizes the absence of non-trivial solutions over sums of squares by condition (iii), since the field \( \mathbb{R}(X) \) has no archimedean orderings. Multiplying by the common denominator and using the fact that any element in \( W(\mathbb{R}) \) can be written as a sum of squares in \( \mathbb{R}(X) \),
Theorem C.1 also characterizes the absence of non-trivial solutions over $W(\mathbb{R})$. However, when considering non-trivial solutions over $U(\mathbb{R})$ and $U(\mathbb{B})$, the situation is quite different; and we now compare the proof of Theorem 2.1 to Theorem C.1.

The proof of Bröcker-Prestel’s original theorem starts with the definition of the pre-semicone

$$P_1 := \left\{ \sum_{i=1}^n f_i h_i, \text{ where } f_i \text{ are sum of squares of elements in } \mathbb{R}(X) \right\}.$$ 

Since it considers solutions over sum of squares, this definition is straightforward. The definition of $P_0$ is our proof of Theorem 2.1 is different and less straightforward. In our theorem, we are considering strictly positive polynomials on $\mathbb{B} \subseteq \mathbb{R}$, therefore we need to replace sum of squares with polynomials in $U(\mathbb{B})$. However, such a naive replacement does not work due to the requirement of a pre-semicone to be closed under multiplication of squares (unlike $W(\mathbb{R})$, the set $U(\mathbb{B})$ is not closed under multiplication by squares). This is why we need to add the rational function $g$ in the definition of $P_0$ and use the fundamental theorem of algebra to guarantee closure under addition.

Note that in order to guarantee the closure under addition of $P_0$, it is essential that we work in the univariate polynomial ring $\mathbb{R}[X]$, so that two polynomials $g, g'$ having a common root implies $\gcd(g, g') \neq 1$. For example, this no longer holds in the bivariate polynomial ring $\mathbb{R}[X, Y]$. Therefore, even when supposing $\gcd\left(\frac{g}{x}, \frac{g'}{y}\right) = 1$, we no longer have $\left(f_i \frac{g'}{x^2} + f'_i \frac{g}{y^2}\right) (x, y) > 0$ in Equation (5). Thus, for the field $\mathbb{R}(X, Y)$, the closure under addition of $P_0$ no longer holds, in contrast with the “non-strict” version $P_1$.

The following step of extracting the valuation ring $A_{P_1}$ from the semiordering $P$ appeared as part of the proof of the original theorem. (The original theorem used the valuation ring $A_{Q_1}$ instead, but they are in fact equivalent.) This is the main part where we drew inspiration from the original local-global principle.

After extracting the valuation ring $A_{P_1}$, our proof again diverges from that of the original theorem. Our new definition of $P_0$ allows us to enforce strict positivity, however it also takes away some convenient properties of the pre-semicone $P_1$ in the original theorem. Notably, we have $h_1 \in P_1$, allowing for a quick conclusion on the positivity of $h_1$ in Henselizations. Whereas for $P_0$, we do not have $h_1 \in P_0$ due to the strict positivity of the coefficients $f_i$. We compensate this by the analytic approach adopted in the second half of our proof, making use of the classification of real places of $\mathbb{R}(X)$ and the continuity of functions in $\mathbb{R}[X]$. This part is absent from the proof of the original theorem, which is purely algebraic and model theoretic.