Computability of Equivariant Gröbner bases

Anonymous Author(s)

Abstract

Let $\mathbb{K}$ be a field, $\mathcal{X}$ be an infinite set (of indeterminates), and $\mathcal{G}$ be a group acting on $\mathcal{X}$. An ideal in the polynomial ring $\mathbb{K}[\mathcal{X}]$ is called equivariant if it is invariant under the action of $\mathcal{G}$. We show Gröbner bases for equivariant ideals are computable are hence the equivariant ideal membership is decidable when $\mathcal{G}$ and $\mathcal{X}$ satisfies the Hilbert's basis property, that is, when every equivariant ideal in $\mathbb{K}[\mathcal{X}]$ is finitely generated. Moreover, we give a sufficient condition for the undecidability of the equivariant ideal membership problem. This condition is satisfied by the most common examples not satisfying the Hilbert's basis property. Our results imply decidability of solvability of orbit-finite systems of linear equations and the reachability problem for reversible data Petri nets for a large class of data domains.

Keywords

equivariant ideal, Hilbert basis, ideal membership problem, orbit finite, oligomorphic, well-quasi-ordering

ACM Reference Format:

Anonymous Author(s). 2018. Computability of Equivariant Gröbner bases. *J. ACM* 37, 4, Article 111 (August 2018), 17 pages. https://doi.org/XXXXXXX.XXXXXXX

This document uses knowledge: a notion points to its *definition*.

1 Introduction

For a field $\mathbb{K}$ and a non-empty set $\mathcal{X}$ of indeterminates, we use $\mathbb{K}[\mathcal{X}]$ to denote the ring of polynomials with coefficients from $\mathbb{K}$ and indeterminates/variables from $\mathcal{X}$. A fundamental result in commutative algebra is *Hilbert's basis theorem*, stating that when $\mathcal{X}$ is finite, every ideal in $\mathbb{K}[\mathcal{X}]$ is finitely generated [17], where an ideal is a non-empty subset of $\mathbb{K}[\mathcal{X}]$ that is closed under addition and multiplication by elements of $\mathbb{K}[\mathcal{X}]$. This property follows from Hilbert's basis theorem, stating that for every ring $\mathcal{A}$ that is *Noetherian*, the polynomial ring $\mathcal{A}[x]$ in one variable over $\mathcal{A}$ is also *Noetherian* [23, Theorem 4.1].

In this paper, we will assume that elements of $\mathbb{K}$ can be effectively represented and that basic operations on $\mathbb{K}$ are computable ($+$, $-$, $\times$, $/$, and equality test). In this setting, a Gröbner basis is a specific kind of generating set of a polynomial ideal which allows easy checking of membership of a given polynomial in that ideal. Gröbner bases were introduced by Buchberger who showed when $\mathcal{X}$ is finite, every ideal in $\mathbb{K}[\mathcal{X}]$ has a finite Gröbner basis and that, for a given a set of polynomials in $\mathbb{K}[\mathcal{X}]$, one can compute a finite Gröbner basis of the ideal generated by them via the so-called *Buchberger algorithm* [8]. The existence and computability of Gröbner bases implies the decidability of the ideal membership problem: given a polynomial f and set of polynomial H, decide whether f is in the ideal generated by H. More generally, Gröbner bases provide effective representations of ideals, over which one can decide inclusion, equality, and compute sums or intersections of ideals [9].

In addition to their interest in commutative algebra, these decidability results have important applications in other areas of computer science. For instance, the so-called "Hilbert Method" that reduces verifications of certain problems on automata and transducers to computations on polynomial ideals has been successfully applied to polynomial automata, and equivalence of string-to-string transducers of linear growth, and we refer to [7] for a survey on these applications.

In this paper, we are interested in extending the theory of Gröbner bases to the case where the set $\mathcal{X}$ of indeterminates is infinite. As an example, let us consider $\mathcal{X}$ to be the set of variables x_i for $i \in \mathbb{N}$, and the ideal $\mathcal{Z}$ generated by the set $\{x \mid x \in \mathcal{X}\}$. It is clear that $\mathcal{Z}$ is not finitely generated. As a consequence, Hilbert's basis theorem, and a fortiori the theory of Gröbner bases, does not extend to the case of infinite sets of indeterminates.

Thankfully, the infinite set $\mathcal{X}$ of variables (data) often comes with an extra structure, usually given by relations and functions defined on $\mathcal{X}$, and one is often interested in systems that are invariant under the action of the group $\mathcal{G}$ of structure preserving bijections of $\mathcal{X}$. For instance, in the above example, one may not be interested in the ideal $\mathcal{Z}$ generated by the set $\{x \mid x \in \mathcal{X}\}$, but rather in the equivariant ideal generated by the set $\{x \mid x \in \mathcal{X}\}$, which is the smallest ideal that contains it and is invariant under the action of $\mathcal{G}$. In this case, this ideal is finitely generated by any single indeterminate $x \in \mathcal{X}$. This motivates the study of equivariant ideals, that is highly dependent on the specific choice of group action $\mathcal{G} \curvearrowright \mathcal{X}$: for instance, the ideal $\mathcal{Z}$ is not finitely generated as an equivariant ideal with respect to the trivial group. A general analysis of the equivariant Hilbert basis property stating that "every equivariant ideal is orbit finitely generated" has been recently given in [15], and this paper aims at providing a computational counterpart.

1.1 Contributions.

In this paper, we bridge the gap between the theoretical understanding of the *equivariant Hilbert basis property* [15, Property 4], and the computational aspects of equivariant ideals, by showing that under mild assumptions on the group action, one can compute an equivariant Gröbner basis of an equivariant ideal, hence, that one can decide the equivariant ideal membership problem.

We divide our hypotheses in two parts. First, we will require some computability assumptions to be satisfied by the group action that are fairly standard in the literature on computation with infinite data. Then, we will require a semantic assumption on the set

ACM 1557-735X/2018/8-ART111
https://doi.org/XXXXXXX.XXXXXXX

of indeterminates that will guarantee the termination of our procedures, that we call being well-structured, and implies that the set of monomials is well-quasi-ordered with respect to divisibility. Both of these will be formally introduced in Section 2. Our main positive result states that under these assumptions, one can compute an equivariant Gröbner basis of an equivariant ideal.

Theorem 1.1 (Equivariant Gröbner Basis). *Let $\mathcal{X}$ be a totally ordered set of indeterminates equipped with a group action $\mathcal{G} \curvearrowright \mathcal{X}$, that satisfies our computability assumptions and is well-structured. Then, one can compute a equivariant Gröbner bases of equivariant ideals.*

Using standard techniques on polynomial ideals, we then use our Theorem 1.1 to provide an effective representation of equivariant ideals under the same assumptions.

Corollary 1.2. *Assume that $\mathcal{G} \curvearrowright \mathcal{X}$ is effectively oligomorphic and well-structured. Then one has an* effective representation *of the equivariant ideals of $\mathbb{K}[\mathcal{X}]$, such that:*

1. *One can obtain a representation from an orbit-finite set of generators,*
2. *One can effectively decide the equivariant ideal membership problem given a representation,*
3. *The following operations are computable at the level of representations: the union of two equivariant ideals, the product of two equivariant ideals, the intersection of two equivariant ideals, and checking whether two equivariant ideals are equal.*

▹ Proven p.15

Then, we illustrate how our positive results find applications in numerous situations. This is done by providing families of indeterminates that satisfy our computability assumptions and are well-structured, and show that these are closed under disjoint sums and lexicographic products. Furthermore, we circumvent the requirement that a total ordering is present on the indeterminates by defining nicely orderable actions (Theorem 5.11). Examples of indeterminates that we can therefore deal with are:

1. Equality Atoms: the indeterminates are an infinite set and $\mathcal{G}$ is all permutations.
2. Dense Linear Orders: the indeterminates are $\mathbb{Q}$, and $\mathcal{G}$ is all order-preserving bijections.
3. Dense Meet Tree: the indeterminates are elements of the infinite dense meet tree, and $\mathcal{G}$ is its group of automorphisms.

We then leverage our positive results (Theorem 1.1 and Corollary 1.2) to obtain decision procedures for the following problems, where $\mathcal{G} \curvearrowright \mathcal{X}$ is a nicely orderable group action:

1. Theorem 5.13: The zeroness problem for orbit finite polynomial automata,
2. Theorem 5.14: The reachability problem for reversible Petri nets with data,
3. Theorem 5.16: The solvability problem for orbit-finite linear systems of equations.

Finally, we provide undecidability results for the equivariant ideal membership problem in the case where our effective assumptions are satisfied, but the action is not well-structured. This aims at illustrating the fact that our assumptions are close to optimal. One classical obstruction for a group action to be well-structured is to have the ability to represent an *infinite path* (a formal definition will be given in Section 6). We prove that whenever one can (effectively) represent an infinite path in the set of monomials $\mathsf{Mon}(\mathcal{X})$, then the equivariant ideal membership problem is undecidable.

Theorem 1.3 (Undecidability of Equivariant Ideal Membership). *Let $\mathcal{X}$ be a totally ordered set of indeterminates equipped with a group action $\mathcal{G} \curvearrowright \mathcal{X}$, under our computability assumptions. If $\mathcal{X}$ contains an infinite path then the equivariant ideal membership problem is undecidable.*

As corollaries of our results we obtain decidability of the reachability problem of reversible Petri nets with data and of the solvability problem for orbit-finite systems of linear equations for data domains that are reducts of totally ordered and well-structured structures (Section 5.3). The class of such data domains include both equality and ordered atoms, but also dense tree atoms.

Note that the decidability of the reachability problem of data Petri nets is still open for equality atoms, and for ordered atoms this problem is known to be undecidable [32]. Orbit-finite systems of linear equations were known to solvable only for equality atoms, ordered atoms, and their lexicographic products ([15]).

1.2 Related Research

Let us call Equality Atoms the infinite set of indeterminates with all permutations acting on them. The fact that Hilbert's basis property holds for polynomials with indeterminates being the Equality Atoms is a frequently rediscovered fact [1, 2, 18, 19]. Recently, Ghosh and Lasota provided a general answer to characterize which group actions enjoy Hilbert's basis property [15, Theorem 11 and 12], and provided in some limited setting a version of Buchberger's algorithm [15, Section 6]. Let us recall their precise statements in order to compare it with our contributions.

Theorem 1.4 ([15, Theorem 11 and 12]). *Let $\mathcal{X}$ be a set of indeterminates equipped with a group action $\mathcal{G} \curvearrowright \mathcal{X}$. Then, Item 1 implies Item 2 implies Item 3, where*

1. *The action is ω-well-structured and the indeterminates are equipped with a total order compatible with the group action,*
2. *The equivariant Hilbert basis property holds for $\mathbb{K}[\mathcal{X}]$,*
3. *The action is ω-well-structured.*

Let us briefly state that being ω-well-structured is *a priori* a weaker condition than being well-structured, but that the two are conjectured to be equivalent [29, Problems 9]. Similarly, it is conjectured that Item 3 and Item 1 are equivalent[1] [29, Problems 12]. As a consequence, our Theorem 1.1 is conjectured to hold whenever the equivariant Hilbert basis property does. Beware that Theorems 1.1 and 1.4 are incomparable: the former does not talk about decidability, while the latter only considers equivariant ideals that are already finitely presented, and we will show in Example 6.1 an example where equivariant Gröbner bases are computable, but the equivariant Hilbert basis property fails.

Let us now comment on the decision procedures provided in the literature. First, most results focus on Dense Linear Orders or Equality Atoms, which are only special cases of our general

[1] Up to modifying the group action to respect the ordering.

result. A reason why this happens is that, until this paper, the only way to provide a decision procedure was to assume that the ordering on the indeterminates was *well-founded* [15, Section 6], or to encode the behaviour of the indeterminates in a set with a *well-founded total ordering* [15, Section 7, Reduction Game]. We provide the first result that gets rid of the assumption that the ordering is *well-founded.* As a consequence, we can deal with the Dense Linear Order without using any encoding tricks. Furthermore, we provided with the Dense Meet Tree an example of group action that was not shown to have decidable equivariant ideal membership problem prior to this work. Our applications to the decidability of other problems in theoretical computer science strictly extend those given in [15, Section 4, 8, and 9]. Indeed, their encoding of *orbit finite weighted automata* did not require the ability to test inclusion of equivariant ideals, while it is central to our result on orbit finite polynomial automata (that strictly generalise weighted automata). Furthermore, their solutions to the problems concerning reversible Petri-nets with data and orbit-finite linear systems of equations only apply when the indeterminates are equipped with a *well-founded* total ordering, which we do not require.

Finally, our results are part of a larger research direction that aims at establishing an algorithmic theory of computation with orbit-finite sets. For instance, [27] studies equivariant subspaces of vector spaces generated by orbit-finite sets, [14, 24] study solvability of orbit-finite systems of linear equations and inequalities, and [14, 27, 30] study duals of vector spaces generated by orbit-finite sets.

Organisation. The rest of the paper is organised as follows. In Section 2, we introduce formally the notions of Gröbner bases, effectively oligomorphic actions, and well-quasi-orderings, which are the main assumptions of our positive results. After that, we introduce in Section 3 an adaptation of Buchberger's algorithm to the equivariant case, that computes a weak equivariant Gröbner basis of an equivariant ideal. In Section 4, we use weak equivariant Gröbner bases to prove our main positive Theorem 1.1, and we show that it provides a way to effectively represent equivariant ideals (Corollary 1.2). We continue by showing in Section 5.2 that the assumptions of our Theorem 1.1 are closed under natural operations (Corollary 5.10 and Theorem 5.11). The positive results regarding the equivariant ideal membership problem are then leveraged to obtain several decision procedures. Finally, in Section 6, we show that our assumptions are close to optimal by proving that the equivariant ideal membership problem is undecidable whenever one can find infinite paths in the set of indeterminates (Theorem 1.3), which is conjectured to be a complete characterisation of the undecidability of the equivariant ideal membership problem (Conjecture 6.3).

2 Preliminaries

Partial orders, ordinals, well-founded sets, and well-quasi-ordered sets. We assume basic familiarity with partial orders, well-founded sets, and ordinals. We will use the notation ω for the first infinite ordinal (that is, $(\mathbb{N}, \leq)$), and write $X + Y$ for the lexicographic sum of two partial orders X and Y. Similarly, the notation $X \times Y$ will denote the product of two partial orders equipped with the lexigographic ordering, i.e. $(x_1, y_1) \leq (x_2, y_2)$ if either $x_1 < x_2$, or $x_1 = x_2$ and $y_1 \leq y_2$. We will also use the usual notations for finite ordinals, writing n for the finite ordinal of size n. For instance, $\omega + 1$ is the total order $\mathbb{N} \uplus \{+\infty\}$, where $+\infty$ is the new largest element.

In order to guarantee the termination of the algorithms presented in this paper, a key ingredient will be the notion of *well-quasi-ordering* (WQO), that are sets $(X, \leq)$ such that every infinite sequence $(x_i)_{i\in\mathbb{N}}$ of elements of X contains a pair $i < j$ such that $x_i \leq x_j$. Examples of well-quasi-orderings include finite sets with any ordering, or $\mathbb{N}\times\mathbb{N}$ with the product ordering. We refer the reader to [11] for a comprehensive introduction to well-quasi-orderings and their applications in computer science.

Polynomials, monomials, divisibility. We assume basic familiarity with the theory of commutative algebra, and polynomials. We will use the notation $\mathbb{K}[\mathcal{X}]$ for the ring of polynomials with coefficients from a field $\mathbb{K}$ and indeterminates/variables from a set $\mathcal{X}$, and $\mathsf{Mon}(\mathcal{X})$ for the set of monomials in $\mathbb{K}[\mathcal{X}]$. Letters p, q, r are used to denote polynomials, $\mathfrak{m}, \mathfrak{n}$ are used to denote monomials, and a, b, α, β are used to denote coefficients in $\mathbb{K}$.

A classical example of a WQO is the set of monomials $\mathsf{Mon}(\mathcal{X})$, endowed with the divisibility relation $\sqsubseteq^{\mathrm{div}}$ whenever $\mathcal{X}$ is finite. We recall that a monomial $\mathfrak{m}$ *divides* a monomial $\mathfrak{n}$ if there exists a monomial $\mathfrak{l}$ such that $\mathfrak{m} \times \mathfrak{l} = \mathfrak{n}$. In this case, we write $\mathfrak{m} \sqsubseteq^{\mathrm{div}} \mathfrak{n}$. Note that monomials can be seen as functions from $\mathcal{X}$ to $\mathbb{N}$ having a finite support, and that the divisibility relation can be extended to monomials that are functions from $\mathcal{X}$ to $(Y, \leq)$, where Y is any partially ordered set. In this case, we write $\mathfrak{m} \sqsubseteq^{\mathrm{div}} \mathfrak{n}$ if for every $x \in \mathcal{X}$, we have $\mathfrak{m}(x) \leq \mathfrak{n}(x)$. We will write $\mathsf{Mon}_{\omega+1}(\mathcal{X})$ (resp. $\mathsf{Mon}_{\omega^2}(\mathcal{X})$) for the set of monomials that are functions from $\mathcal{X}$ to $\omega + 1$ (resp. ω^2).

Unless otherwise specified, we will assume that the set of indeterminates $\mathcal{X}$ comes equipped with a total ordering $\leq_{\mathcal{X}}$. Using this order, we define the *reverse lexicographic* (revlex) ordering on monomials as follows: $\mathfrak{n} \sqsubset^{\mathrm{RevLex}} \mathfrak{m}$ if there exists an indeterminate $x \in \mathcal{X}$ such that $\mathfrak{n}(x) < \mathfrak{m}(x)$, and such that for every $y \in \mathcal{X}$, if $x <_{\mathcal{X}} y$ then $\mathfrak{n}(y) = \mathfrak{m}(y)$. Remark that if $\mathfrak{n} \sqsubseteq^{\mathrm{div}} \mathfrak{m}$, then in particular $\mathfrak{n} \sqsubseteq^{\mathrm{RevLex}} \mathfrak{m}$.

We can now use the reverse lexicographic ordering to identify particular elements in a given polynomial. Namely, for a polynomial $p \in \mathbb{K}[\mathcal{X}]$, we define the *leading monomial* $\mathsf{LM}(p)$ of p as the largest monomial appearing in p with respect to the revlex ordering, and the *leading coefficient* $\mathsf{LC}(p)$ of p as the coefficient of $\mathsf{LM}(p)$ in p. We can then define the *leading term* $\mathsf{LT}(p)$ of p as the product of its leading monomial and its leading coefficient, and the *characteristic monomial* $\mathsf{CM}(p)$ of p as the product of its leading monomial and all the indeterminates appearing in p. We also define the *domain* of $\mathfrak{m}$ as the set $\mathsf{dom}(\mathfrak{m})$ of indeterminates $x \in \mathcal{X}$ such that $\mathfrak{m}(x) \neq 0$. Because the coefficients and monomial in question are highly dependent on the ordering $\leq_{\mathcal{X}}$, we allow ourselves to write $\mathsf{LM}_{\mathcal{X}}(p)$ to highlight the precise ordered set of variables that was used to compute the leading monomial of p. We extend dom from monomials to polynomials by defining $\mathsf{dom}(p)$ as the union of the domains of all monomials appearing in p.

Remark 2.1. In the case of a finite set of indeterminates, one can choose any total ordering on $\mathsf{Mon}(\mathcal{X})$, as long as it contains the divisibility quasi-ordering, and is compatible with the product of monomials.[2] In our case, having an infinite number of indeterminates, we rely on a connection between $\mathsf{LM}(p)$ and $\mathsf{dom}(p)$: $\mathsf{dom}(p) \subseteq \downarrow \mathsf{dom}(\mathsf{LM}(p))$, where $\downarrow S$ is the downwards closure of a set $S \subseteq \mathcal{X}$, i.e. the set of all indeterminates $x \in \mathcal{X}$ such that $y \leq x$ for some $y \in S$. This means that the leading monomial encodes a *global property* of the polynomial, and it will be crucial in our termination arguments. This is already at the core of the classical *elimination theorems* [9, Chapter 3, Theorem 2].

Ideals, and Gröbner Bases. An *ideal* $\mathcal{I}$ of $\mathbb{K}[\mathcal{X}]$ is a non-empty subset of $\mathbb{K}[\mathcal{X}]$ that is closed under addition and multiplication by elements of $\mathbb{K}[\mathcal{X}]$. Given a set $H \subseteq \mathbb{K}[\mathcal{X}]$, we denote by $\langle H \rangle$ the ideal generated by H, i.e. the smallest ideal that contains H. The *ideal membership problem* is the following decision problem: given a polynomial $p \in \mathbb{K}[\mathcal{X}]$ and a set of polynomials $H \subseteq \mathbb{K}[\mathcal{X}]$, decide whether p belongs to the ideal $\langle H \rangle$ generated by H. We know that this problem is decidable when $\mathcal{X}$ is finite, and that it is even EXPTIME-complete [26]. The classical approach to the ideal membership problem is to use the Gröbner basis theory that was developed in the 70s by Buchberger [8]. A set $\mathcal{B}$ of polynomials is called a *Gröbner basis* of an ideal $\mathcal{I}$ if, $\langle \mathcal{B} \rangle = \mathcal{I}$ and for every polynomial $p \in \mathcal{I}$, there exists a polynomial $q \in \mathcal{B}$ such that $\mathsf{LM}_{\mathcal{X}}(q) \sqsubseteq^{\mathrm{div}} \mathsf{LM}_{\mathcal{X}}(p)$.

Given a Gröbner basis $\mathcal{B}$ of an ideal $\mathcal{I}$, and a polynomial p, it suffices to iteratively reduce the leading monomial of p by subtracting multiples of elements in $\mathcal{B}$, until one cannot apply any reductions. If the result is 0, then p belongs to $\mathcal{I}$, and otherwise it does not.

Example 2.2. Let $\mathcal{X} \triangleq \{x, y, z\}$ with $z < y < x$ The set $\mathcal{B} \triangleq \{x^2y - z, x^2 - y\}$ is not a Gröbner basis of the ideal $\mathcal{I}$ it generates, because the polynomial $p \triangleq y^2 - z$ belongs to $\mathcal{I}$ but its leading monomial y^2 is not divisible by $\mathsf{LM}(x^2y - z) = x^2y$ nor by $\mathsf{LM}(x^2 - y) = x^2$.

Group actions and equivariance. A *group* $\mathcal{G}$ is a set equipped with a binary operation that is associative, has an identity element and has inverses. In our setting, we are interested in infinite sets $\mathcal{X}$ of indeterminates that is equipped with a *group action* $\mathcal{G} \curvearrowright \mathcal{X}$. This means that for each $\pi \in \mathcal{G}$, we have a bijection $\mathcal{X} \xrightarrow{\simeq} \mathcal{X}$ that we denote by $x \mapsto \pi \cdot x$. A set $S \subseteq \mathcal{X}$ is *equivariant* under the action of $\mathcal{G}$ if for all $\pi \in \mathcal{G}$ and $x \in S$, we have $\pi \cdot x \in S$. We give in Example 2.3 an example and a non-example of *equivariant ideals*.

Example 2.3. Let $\mathcal{X}$ be any infinite set, and $\mathcal{G}$ be the group of all bijections of $\mathcal{X}$. Then the set $S_0 \subset \mathbb{K}[\mathcal{X}]$ of all polynomials whose set of coefficients sums to 0 is an equivariant ideal. Conversely, the set of all polynomials that are multiple of $x \in X$ is an ideal that is not equivariant.

Proof. Let $p, q \in S_0$, and $r \in \mathbb{K}[\mathcal{X}]$. Then, $p \times r + q$ is in S_0. Remark that p, r and q belong to a subset $\mathbb{K}[\mathcal{X}]$ of the polynomials that uses only finitely many indeterminates. In this subset, the sum of all coefficients is obtained by applying the polynomials to the value 1 for every indeterminate $y \in \mathcal{X}$. We conclude that $(p \times r + q)(1, \ldots, 1) = p(1, \ldots, 1) \times r(1, \ldots, 1) + q(1, \ldots, 1) = 0 \times r(1, \ldots, 1) + 0 = 0$, hence that $p \times r + q$ belongs to S_0. Because 0 is in S_0, we conclude that S_0 is an ideal. Furthermore, if $\pi \in \mathcal{G}$ and $p \in S_0$, then the sum of the coefficients $\pi \cdot p$ is exactly the sum of the coefficients of p, hence is 0 too. This shows that S_0 is equivariant.

It is clear that all multiples of a given polynomial $x \in \mathcal{X}$ is an ideal of $\mathbb{K}[\mathcal{X}]$. This is not an equivariant ideal: take any bijection $\pi \in \mathcal{G}$ that does not map x to x (it exists because $\mathcal{X}$ is infinite and $\mathcal{G}$ is all permutations), then $\pi \cdot x$ is not a multiple of x, and therefore does not belong to the ideal. □

Orbit finiteness. An equivariant set is said to be *orbit finite* if it is the union of finitely many *orbits* under the action of $\mathcal{G}$. We denote $\mathsf{orbit}_{\mathcal{G}}(E)$ for the set of all elements $\pi \cdot x$ for $\pi \in \mathcal{G}$ and $x \in E$. Equivalently, an *orbit finite set* is a set of the form $\mathsf{orbit}_{\mathcal{G}}(E)$ for some finite set E. Not every equivariant subset is orbit finite, as shown in Example 2.4. However, orbit finite sets are robust in the sense that equivariant subsets of orbit finite sets are also orbit finite, and similarly, an equivariant subset of E^n is orbit finite whenever E is orbit finite and $n \in \mathbb{N}$ is finite. For algorithmic purposes, orbit finite sets are the ones that can be taken as input as a finite set of representatives (one for each orbit). The notions of equivariance and orbit finite sets from a computational perspective are discussed in [6], and we refer the reader to this book for a more comprehensive introduction to the topic.

We will mostly be interested in *orbit-finitely generated* equivariant ideals, i.e. equivariant ideals that are generated by an orbit finite set of polynomials, for which the *equivariant ideal membership problem* is as follows: given a polynomial $p \in \mathbb{K}[\mathcal{X}]$ and an orbit finite set $H \subseteq \mathbb{K}[\mathcal{X}]$, decide whether p belongs to the equivariant ideal $\langle H \rangle_{\mathcal{G}}$ generated by H.

Example 2.4. Let $\mathcal{X} = \mathbb{N}$, and $\mathcal{G}$ be all permutations that fixes prime numbers. The set of all polynomials whose coefficients sum to 0 is an equivariant ideal, but it is not orbit finite, since all the polynomials $x_p - x_q$ for $p \neq q$ primes are in distinct orbits under the action of $\mathcal{G}$.

A function $f : X \to Y$ between two sets X and Y equipped with actions $\mathcal{G} \curvearrowright X$ and $\mathcal{G} \curvearrowright Y$ is said to be *equivariant* if for all $\pi \in \mathcal{G}$ and $x \in X$, we have $f(\pi \cdot x) = \pi \cdot f(x)$. For instance, the domain of a monomial is an equivariant function if $\pi \in \mathcal{G}$, then $\pi \cdot \mathsf{dom}(\mathfrak{m}) = \mathsf{dom}(\pi \cdot \mathfrak{m})$. Let us point out that the image of an orbit finite set under an equivariant function is orbit finite, and that the algorithms that we will develop in this paper will all be equivariant.

Computability assumptions. We say that the action is *effectively oligomorphic* if:

(1) It is *oligomorphic*, i.e. for every $n \in \mathbb{N}$, $\mathcal{X}^n$ is orbit finite,
(2) There exists an algorithm that decides whether two elements $\vec{x}, \vec{y} \in \mathcal{X}^*$ are in the same orbit under the action of $\mathcal{G}$ on $\mathcal{X}^*$.
(3) There exists an algorithm which on input $n \in \mathbb{N}$ outputs a set $A \subseteq_{\mathrm{fin}} \mathcal{X}^n$ such that $|A \cap U| = 1$ for every orbit $U \subseteq \mathcal{X}^n$.

In particular, $\mathcal{X}$ itself is orbit finite under the action of $\mathcal{G}$.

A group action $\mathcal{G} \curvearrowright \mathcal{X}$ is said to be *compatible* with an ordering $\leq$ on $\mathcal{X}$ if for all $\pi \in \mathcal{G}$ and $x, y \in \mathcal{X}$, we have $x \leq y$ if and only if $\pi \cdot x \leq \pi \cdot y$. Let us point out that in this case, $\sqsubseteq^{\mathrm{RevLex}}$ is also compatible with the action of $\mathcal{G}$ on $\mathsf{Mon}(\mathcal{X})$, i.e. for all $\pi \in \mathcal{G}$ and monomials $\mathfrak{m}, \mathfrak{n} \in \mathsf{Mon}(\mathcal{X})$, we have $\mathfrak{m} \sqsubseteq^{\mathrm{RevLex}} \mathfrak{n}$ if and only if

[2]This is often called a *monomial ordering*, see [9].

$\pi \cdot \mathfrak{m} \sqsubseteq^{\mathsf{RevLex}} \pi \cdot \mathfrak{n}$. Our *computability assumptions* on the tuple $(\mathcal{X}, \mathcal{G}, \leq)$ will therefore be that $\mathcal{G}$ acts effectively oligomorphic on $\mathcal{X}$, and that its action is compatible with the ordering $\leq$ on $\mathcal{X}$.

Example 2.5. Let $\mathcal{X} \triangleq \mathbb{Q}$ and $\mathcal{G}$ be the group of all order preserving bijections of $\mathbb{Q}$. Then, $\mathcal{G}$ acts effectively oligomorphically on $\mathcal{X}$, and its action is compatible with the ordering of $\mathbb{Q}$ by definition.

Note that under our computability assumptions, the set of polynomials $\mathbb{K}[\mathcal{X}]$ is also effectively oligomorphic under the action of $\mathcal{G}$ on $\mathcal{X}$ when restricted to polynomials with bounded degree. This is because a polynomial $p \in \mathbb{K}[\mathcal{X}]$ can be seen as an element of $(\mathbb{K} \times \mathcal{X}^{\leq d})^n$ where n is the number of monomials in p, and d is the maximal degree of a monomial appearing in p. Beware that the set of all polynomials $\mathbb{K}[\mathcal{X}]$ is not orbit finite, precisely because the orbit of a polynomial p under the action of $\mathcal{G}$ cannot change the degree of p, and that there are polynomials of arbitrarily large degree.

Equivariant Gröbner bases. We know from [15] that a necessary condition for the equivariant Hilbert basis property to hold is that the set $\mathsf{Mon}(\mathcal{X})$ of monomials is a well-quasi-ordering when endowed with the *divisibility up-to $\mathcal{G}$* relation ($\sqsubseteq^{\mathrm{div}}_{\mathcal{G}}$), which is defined as follows: for $\mathfrak{m}_1, \mathfrak{m}_2 \in \mathsf{Mon}(\mathcal{X})$, we write $\mathfrak{m}_1 \sqsubseteq^{\mathrm{div}}_{\mathcal{G}} \mathfrak{m}_2$ if there exists $\pi \in \mathcal{G}$ such that $\mathfrak{m}_1$ divides $\pi \cdot \mathfrak{m}_2$. This relation also extends to monomials that are functions from $\mathcal{X}$ to $(Y, \leq)$ with finite support, where Y is any partially ordered set. We say that a set $\mathcal{B} \subseteq \mathbb{K}[\mathcal{X}]$ is an *equivariant Gröbner basis* of an equivariant ideal $\mathcal{I}$ if $\mathcal{B}$ is equivariant, $\langle \mathcal{B} \rangle = \mathcal{I}$, and for every polynomial $p \in \mathcal{I}$, there exists $q \in \mathcal{B}$ such that $\mathsf{LM}_{\mathcal{X}}(q) \sqsubseteq^{\mathrm{div}}_{\mathcal{G}} \mathsf{LM}_{\mathcal{X}}(p)$ and $\mathsf{dom}(q) \subseteq \mathsf{dom}(p)$, following the definition of [15].

We say that a group action $\mathcal{G} \curvearrowright \mathcal{X}$ is *well-structured* if the set $(\mathsf{Mon}_Y(\mathcal{X}), \sqsubseteq^{\mathrm{div}}_{\mathcal{G}})$ is well-quasi-ordered, for every well-quasi-order $(Y, \leq)$. We say that it is *ω-well-structured* if $(\mathsf{Mon}(\mathcal{X}), \sqsubseteq^{\mathrm{div}}_{\mathcal{G}})$ is well-quasi-ordered.

Beware that even in the case of a finite set of variables, a Gröbner basis is not necessarily an equivariant Gröbner basis, because of the domain condition. However, every equivariant Gröbner basis is a Gröbner basis.

Example 2.6. Let $\mathcal{X} \triangleq \{x_1, x_2\}$, with $x_1 \leq_{\mathcal{X}} x_2$, and $\mathcal{G}$ be the trivial group. Let us furthermore consider the ideal $\mathcal{I}$ generated by $\{x_1, x_2\}$. Then, the set $\mathcal{B} \triangleq \{x_2 - x_1, x_1\}$ is a Gröbner basis of $\mathcal{I}$, but not an equivariant Gröbner basis. Indeed, $x_2 \in \mathcal{I}$, but there is no polynomial $q \in \mathcal{B}$ such that $\mathsf{LM}(q) \sqsubseteq^{\mathrm{div}} x_2$ and $\mathsf{dom}(q) \subseteq \mathsf{dom}(x_2)$.

3 Weak Equivariant Gröbner Bases

In this section we prove that a natural adaptation of Buchberger's algorithm to the equivariant setting computes a weak equivariant Gröbner basis of an equivariant ideal. This can be seen as an analysis of the classical algorithm in the equivariant setting. We will assume for the rest of the section that $\mathcal{X}$ is a set of indeterminates equipped with a group $\mathcal{G}$ acting effectively oligomorphically on $\mathcal{X}$, and that $\mathcal{X}$ is equipped with a total ordering $\leq_{\mathcal{X}}$ that is compatible with the action of $\mathcal{G}$. The crucial object of this section is the notion of decomposition of a polynomial with respect to a set H.

Definition 3.1. Let H be a set of polynomials. A *decomposition* of p with respect to H is given by a finite sequence $\mathfrak{d} \triangleq ((a_i, \mathfrak{m}_i, h_i))_{i \in I}$ such that

$$p = \sum_{i \in I} a_i \mathfrak{m}_i h_i \quad , \tag{1}$$

where $a_i \in \mathbb{K}$, $\mathfrak{m}_i \in \mathsf{Mon}(\mathcal{X})$, and $h_i \in H$ for all $i \in I$. The *domain of the decomposition* that we write $\mathsf{dom}(\mathfrak{d})$ is defined as the union of the domains of the polynomials $\mathfrak{m}_i h_i$ for all $i \in I$. The *leading monomial of the decomposition* is defined as $\mathsf{LM}(\mathfrak{d}) \triangleq \max((\mathsf{LM}(\mathfrak{m}_i h_i))_{i \in I})$.

Leveraging the notion of decomposition, we can define a weakening of the notion of equivariant Gröbner basis, that essentially mimics the classical notion of equivariant Gröbner basis at the level of decompositions instead of polynomials.

Definition 3.2. An equivariant set $\mathcal{B}$ of polynomials is a *weak equivariant Gröbner basis* of an equivariant ideal $\mathcal{I}$ if $\langle \mathcal{B} \rangle = \mathcal{I}$, and if for every polynomial $p \in \mathcal{I}$, and decomposition $\mathfrak{d}$ of p with respect to $\mathcal{B}$, there exists a decomposition $\mathfrak{d}'$ of p with respect to $\mathcal{B}$ such that $\mathsf{dom}(\mathfrak{d}') \subseteq \mathsf{dom}(\mathfrak{d})$, and such that $\mathsf{LM}(\mathfrak{d}') = \mathsf{LM}(p)$.

To compute weak equivariant Gröbner bases, we will use a rewriting relation. Given $p, r \in \mathbb{K}[\mathcal{X}]$, we write $p \to_H r$ if and only if there exists $q \in H$, $a \in \mathbb{K}$, and $\mathfrak{m} \in \mathsf{Mon}(\mathcal{X})$ such that $p = a\mathfrak{m}q + r$, $\mathsf{dom}(r) \subseteq \mathsf{dom}(p)$, and $\mathsf{LM}_{\mathcal{X}}(r) \sqsubset^{\mathsf{RevLex}} \mathsf{LM}_{\mathcal{X}}(p)$. In order to simplify the notations, we will write $r \prec p$ to denote $\mathsf{dom}(r) \subseteq \mathsf{dom}(p)$, and $\mathsf{LM}_{\mathcal{X}}(r) \sqsubset^{\mathsf{RevLex}} \mathsf{LM}_{\mathcal{X}}(p)$, leaving the ordered set of indeterminates $\mathcal{X}$ implicit. The relation $\preceq$ is extended to decompositions by using the analogues of dom and LM for decompositions.

Lemma 3.3. *The quasi-ordering $\preceq$ is compatible with the action of $\mathcal{G}$, and is well-founded on polynomials, and on decompositions of polynomials.*

Proof. The first property is immediate because dom, LM, and $\sqsubseteq^{\mathsf{RevLex}}$ are compatible with the group action $\mathcal{G}$. The second property follows from the fact that $\sqsubset^{\mathsf{RevLex}}$ is a total well-founded ordering whenever one has fixed finitely many possible indeterminates. In a decreasing sequence, the support of the leading monomials is also decreasing, so that sequence only contains finitely many indeterminates, hence we conclude. The same proof works for decompositions. ◻

As a consequence of Lemma 3.3, we know that the rewriting relation $\to_H$ is *terminating* for every set H. Given a set H of polynomials, and given a polynomial $p \in \mathbb{K}[\mathcal{X}]$, we say that p is *normalised* with respect to H if there are no transitions $p \to_H r$. The set of *remainders* of p with respect to H is denoted $\mathsf{Rem}_H(p)$, and is defined as the set of all polynomials r such that $p \to_H^* r$ and r is normalised with respect to H. The following lemma states that $\mathsf{Rem}_H(\cdot)$ is a computable function from our setting.

Lemma 3.4. *Let H be an orbit finite set of polynomials, and let $p \in \mathbb{K}[\mathcal{X}]$ be a polynomial. Then $\mathsf{Rem}_H(p)$ is finite. Furthermore, this computation is equivariant. In particular, $\mathsf{Rem}_H(K)$ is a computable orbit finite set for every orbit finite set K of polynomials.* ▷ Proven p.14

Now that we have a quasi-ordering on polynomials, we will prove that given an orbit finite set H of generators, we can compute a weak equivariant Gröbner basis. The computation will closely follow the classical Buchberger's algorithm. The main idea being to saturate the set of generators H to remove some *critical pairs* of the rewriting relation $\to_H$. Namely, given two polynomials p and q in H, we compute the set $\mathsf{C}_{p,q}$ of cancellations between p and q as the set of polynomials of the form $r = \alpha\mathfrak{n}p + \beta\mathfrak{m}q$ such that $\mathsf{LM}(r) < \max(\mathfrak{n}\,\mathsf{LM}(p), \mathfrak{m}\,\mathsf{LM}(q))$, where $\alpha, \beta \in \mathbb{K}$, and where $\mathfrak{n}, \mathfrak{m} \in \mathsf{Mon}(\mathcal{X})$. Let us recall that given two monomials $\mathfrak{n}, \mathfrak{m} \in \mathsf{Mon}(\mathcal{X})$, one can compute $\mathsf{LCM}(\mathfrak{n}, \mathfrak{m})$ as the least common multiple of the two monomials, and that this in an equivariant operation. Using this, we can introduce the *S-polynomial* of two polynomials p and q as in Equation (2).

$$\mathsf{S}(p,q) \triangleq \frac{\mathsf{LCM}(\mathsf{LM}(p),\mathsf{LM}(q))}{\mathsf{LT}(p)} \times p - \frac{\mathsf{LCM}(\mathsf{LM}(p),\mathsf{LM}(q))}{\mathsf{LT}(q)} \times q \quad . \tag{2}$$

Lemma 3.5 (S-polynomials). *Let p and q be two polynomials in $\mathbb{K}[\mathcal{X}]$. All the polynomials in $\mathsf{C}_{p,q}$ are obtained by multiplying a monomial with their S-polynomial $\mathsf{S}(p,q)$.* ▹ Proven p.14

Remark that the S-polynomial is equivariant: if $\pi \in \mathcal{G}$, then $\mathsf{S}(\pi \cdot p, \pi \cdot q) = \pi \cdot \mathsf{S}(p,q)$. Given a set H, we write $\mathsf{SSet}(H) \triangleq \bigcup_{p,q \in H} \mathsf{Rem}_H(\mathsf{S}(p,q))$. We are now ready to define the saturation algorithm that will compute weak equivariant Gröbner bases, described in Algorithm 1. Let us remark that Algorithm 1 is an actual algorithm (Lemma 3.6) that is equivariant.

Input: An orbit finite set H of polynomials
Output: An orbit finite set $\mathcal{B}$ that is a weak equivariant Gröbner basis of $\langle H \rangle_{\mathcal{G}}$

begin
  $\mathcal{B} \leftarrow H$;
  repeat
    $\mathcal{B} \leftarrow \mathcal{B} \cup \mathsf{SSet}(\mathcal{B})$;
  until *$\mathcal{B}$ stabilizes*;
  return $\mathcal{B}$;
end

Algorithm 1: Computing weak equivariant Gröbner bases using the algorithm `weakgb`.

Lemma 3.6. *Algorithm 1 is computable and equivariant, and produces an orbit finite set $\mathcal{B}$ if it terminates.*

Proof. Observe that it is enough to show that $\mathsf{SSet}\,\mathcal{B}$ is orbit-finite for every orbit-finite set $\mathcal{B}$. First, we compute $\mathcal{B}^2$, which is an orbit finite set of pairs, because $\mathcal{B}$ is orbit finite and $\mathcal{X}$ is effectively oligomorphic. Then, noting that $\mathsf{S}(-,-)$ is computable and equivariant, we conclude that $\bigcup_{p,q \in H} \mathsf{S}(p,q)$ is computable and orbit-finite. Now using Lemma 3.4 one can compute the set $\mathsf{SSet}(\mathcal{B})$ which is also orbit-finite. Furthermore, one can decide whether the set $\mathcal{B}$ stabilizes, because the membership of a polynomial p in $\mathcal{B}$ is decidable, since $\mathcal{G} \curvearrowright \mathcal{X}$ is effectively oligomorphic and $\mathcal{B}$ is orbit finite. □

Let us now use the semantic assumptions to prove the termination of Algorithm 1 (Lemma 3.7) and the correctness of the resulting orbit finite set (Lemma 3.8).

Lemma 3.7. *Assume that the action $\mathcal{G} \curvearrowright \mathcal{X}$ is ω-well-structured. Then, Algorithm 1 terminates on every orbit finite set H of polynomials.* ▹ Proven p.14

Lemma 3.8. *Assume that $\mathcal{B}$ is the output of Algorithm 1. Then, it is a weak equivariant Gröbner basis of the ideal $\langle H \rangle_{\mathcal{G}}$.*

Proof. It is clear that $\mathcal{B}$ is a generating set of $\langle H \rangle_{\mathcal{G}}$, because one only add polynomials that are in the ideal generated by H at every step.

Let $p \in \langle H \rangle_{\mathcal{G}}$ be a polynomial, and let $\mathfrak{d}$ be a decomposition of p with respect to $\mathcal{B}$, that is, a decomposition of the form

$$p = \sum_{i \in I} \alpha_i \mathfrak{m}_i p_i \quad . \tag{3}$$

Where $\alpha_i \in \mathbb{K}$, $p_i \in \mathcal{B}$, and $\mathfrak{m}_i \in \mathsf{Mon}(\mathcal{X})$, for all $i \in I$.

Leveraging Lemma 3.3, we know that the ordering $\preceq$ is well-founded. As a consequence, we can consider a minimal decomposition $\mathfrak{d}'$ of p with respect to $\mathcal{B}$ such that $\mathfrak{d}' \preceq \mathfrak{d}$. We now distinguish two cases, depending on whether the leading monomial $\mathsf{LM}(\mathfrak{d}')$ of the decomposition $\mathfrak{d}'$ is equal to the leading monomial of p or not.

Case 1: $\mathsf{LM}(\mathfrak{d}') = \mathsf{LM}(p)$. In this case, we conclude immediately, as we also have by assumption $\mathsf{dom}(\mathfrak{d}') \subseteq \mathsf{dom}(\mathfrak{d})$.

Case 2: $\mathsf{LM}(\mathfrak{d}') \neq \mathsf{LM}(p)$. In this case, it must be that the set J the set of indices such that $\mathfrak{l} \triangleq \mathsf{LM}(\mathfrak{m}_i p_i) = \mathsf{LM}(\mathfrak{d}')$ is non-empty. Let us remark that the sum of leading coefficients of the polynomials in J must vanish: $\sum_{i \in J} \alpha_i\,\mathsf{LC}(p_i) = 0$. As a consequence, the set J has size at least 2. Let us distinguish one element $\star \in J$, and write $J_\star = J \setminus \{\star\}$. We conclude that $\alpha_\star = -\sum_{i \in J_\star} \alpha_i\,\mathsf{LC}(p_i)/\mathsf{LC}(p_\star)$. Let us now rewrite p as follows:

$$p = \sum_{i \in J_\star} \alpha_i \left(\mathfrak{m}_i p_i - \frac{\mathsf{LC}(p_i)}{\mathsf{LC}(p_\star)} \mathfrak{m}_\star p_\star \right) + \sum_{i \in I \setminus J} \alpha_i \mathfrak{m}_i p_i \quad . \tag{4}$$

Now, by definition, polynomials $\alpha_i \mathfrak{m}_i p_i$ for $i \in I \setminus J$ have leading monomials strictly smaller than $\mathfrak{l}$. Furthermore, the polynomials $\mathfrak{m}_i p_i - \frac{\mathsf{LC}(p_i)}{\mathsf{LC}(p_\star)} \mathfrak{m}_\star p_\star$ for $i \in J_\star$ cancel their leading monomials, hence they belong to the set $\mathsf{C}_{p_i,p_\star}$. By Lemma 3.5, we know that these polynomials are obtained by multiplying the S-polynomial $\mathsf{S}(p_i, p_\star)$ by some monomial. Because Algorithm 1 terminated, we know that $\mathsf{S}(p_i, p_\star) \to_{\mathcal{B}}^* 0$ by construction.

By definition of the rewriting relation, we conclude that one can rewrite $\mathsf{S}(p_i, p_\star)$ as combination of polynomials in $\mathcal{B}$ that have smaller or equal leading monomials, and do not introduce new indeterminates.

We conclude that the whole sum is composed of polynomials with leading monomials strictly smaller than $\mathfrak{l}$, and using a subset of the indeterminates used in $\mathfrak{d}'$, leading to a contradiction because of the minimality of the latter. □

As a consequence of the above lemmas, we can now conclude that the Algorithm 1 computes a weak equivariant Gröbner basis of the ideal $\langle H \rangle_{\mathcal{G}}$, as stated in Theorem 3.9.

Theorem 3.9. *Assume that the action $\mathcal{G} \curvearrowright \mathcal{X}$ is ω-well-structured and satisfies our computability assumptions. Then, the algorithm* weakgb *that takes as input an orbit finite set H of generators of an* *equivariant ideal $\mathcal{I}$ and computes a weak equivariant Gröbner basis $\mathcal{B}$ of $\mathcal{I}$.*

4 Computing the Equivariant Gröbner Basis

The goal of this section is to prove Theorem 1.1, that is, to show that one can effectively compute an equivariant Gröbner basis of an equivariant ideal. To that end, we will apply the algorithm weakgb on a slightly modified set of polynomials, and then show that the result is indeed an equivariant Gröbner basis.

Let us fix a set $\mathcal{X}$ of indeterminates equipped with a total ordering $\leq_{\mathcal{X}}$. We define $\mathcal{Y} \triangleq \mathcal{X} + \mathcal{X}$, that is, the disjoint union of two copies of $\mathcal{X}$, ordered. It will be useful to refer to the first copy (lower copy) and the second copy (upper copy), noting the isomorphism between $\mathcal{Y}$ and $\{\text{first}, \text{second}\} \times \mathcal{X}$, ordered lexicographically, where first $<$ second. We will also define $\mathsf{forget}\colon \mathcal{Y} \to \mathcal{X}$ that maps a colored variable to its underlying variable. Beware that forget is not an order preserving map. We extend forget as a morphism from polynomials in $\mathbb{K}[\mathcal{Y}]$ to polynomials in $\mathbb{K}[\mathcal{X}]$.

Given a subset $V \subset_{\text{fin}} \mathcal{X}$, we build the injection $\mathsf{col}_V\colon \mathcal{X} \to \mathcal{Y}$ that maps variables x in V to (first, x), and variables x not in V to (second, x). Again, we extend these maps as morphisms from $\mathbb{K}[\mathcal{X}]$ to $\mathbb{K}[\mathcal{Y}]$. We say that a polynomial $p \in \mathbb{K}[\mathcal{Y}]$ is *V-compatible* if $p \in \mathsf{col}_V(\mathbb{K}[\mathcal{X}])$. Using these definitions, we create freecol that maps a set H of polynomials to the union over all finite subsets V of $\mathcal{X}$ of the set $\mathsf{col}_V(H)$. Beware that freecol does not equal forget^{-1}, since we only consider V-compatible polynomials (for some finite set V).

We are now ready to write our algorithm to compute an equivariant Gröbner basis by computing the "congugacy"

$$\mathsf{egb} \triangleq \mathsf{forget} \circ \mathsf{weakgb} \circ \mathsf{freecol} \quad . \tag{5}$$

To prove the correctness of our algorithm, let us first argue that one can indeed compute the weak equivariant Gröbner basis algorithm.

Lemma 4.1. *Assume that $\mathcal{G} \curvearrowright \mathcal{X}$ is is effectively oligomorphic, and that $(\mathsf{Mon}_{\mathbb{N}\times\mathbb{N}}(\mathcal{X}), \sqsubseteq_{\mathcal{G}}^{\text{div}})$ is a well-quasi-order. Then* egb *is a computable function, and the function* weakgb *is called on correct inputs.* ▹ Proven p.14

Let us now argue that the result of egb is indeed a generating set of the ideal (Lemma 4.2), and then refine our analysis to prove that it is an equivariant Gröbner basis (Lemma 4.3).

Lemma 4.2. *Let $H \subseteq \mathbb{K}[\mathcal{X}]$, then $\mathsf{egb}(H)$ generates $\langle H \rangle_{\mathcal{G}}$.* ▹ Proven p.14

Lemma 4.3. *Let $H \subseteq \mathbb{K}[\mathcal{X}]$, then $\mathsf{egb}(H)$ is an equivariant Gröbner basis of $\langle H \rangle_{\mathcal{G}}$.*

Proof. Let $H_\star = \mathsf{freecol}(H)$, $\mathcal{B}_\star = \mathsf{weakgb}(H_\star)$, and $\mathcal{B} = \mathsf{forget}(\mathcal{B}_\star)$. We want to prove that $\mathcal{B}$ is an equivariant Gröbner basis of $\langle H \rangle$. Let us consider an arbitrary polynomial $p \in \langle H \rangle_{\mathcal{G}}$, our goal is to construct an $h \in \mathcal{B}$ such that $\mathsf{LM}(h) \sqsubseteq^{\text{div}} \mathsf{LM}(p)$ and $\mathsf{dom}(h) \subseteq \mathsf{dom}(p)$.

Let us define $V \triangleq \mathsf{dom}(p)$ and $H_V \triangleq \mathsf{col}_V(H)$. It is clear that $\mathsf{col}_V(p)$ belongs to $\langle H_V \rangle$. Let us write

$$\mathsf{col}_V(p) = \sum_{i=1}^{n} a_i \mathfrak{m}_i h_i$$

Where $a_i \in \mathbb{K}$, $\mathfrak{m}_i \in \mathsf{Mon}(\mathcal{Y})$, and $h_i \in \mathcal{B}_\star$ is V-compatible. Such a decomposition $\mathfrak{d}$ exists because $H_V \subseteq H_\star \subseteq \mathcal{B}_\star$.

Now, because $\mathcal{B}_\star$ is a weak equivariant Gröbner basis of $\langle H_\star \rangle$, there exists a decomposition $\mathfrak{d}'$ of $\mathsf{col}_V(p)$ such that $\mathsf{LM}(\mathsf{col}_V(p)) = \mathsf{LM}(\mathfrak{d}') \sqsubseteq^{\text{RevLex}} \mathsf{LM}(\mathfrak{d})$, and $\mathsf{dom}(\mathfrak{d}') \subseteq \mathsf{dom}(\mathfrak{d})$. In particular, $\mathfrak{d}'$ is a decomposition of $\mathsf{col}_V(p)$ using only V-compatible polynomials in $\mathcal{B}_\star$.

Let us consider some element $(a_i', \mathfrak{m}_i', h_i')$ of the decomposition $\mathfrak{d}'$ such that $\mathsf{LM}(\mathfrak{m}_i' h_i') = \mathsf{LM}(\mathsf{col}_V(p))$, which exists by assumption on $\mathfrak{d}'$. Since $\mathsf{dom}(\mathfrak{m}_i' h_i) \subseteq \downarrow \mathsf{dom}(\mathsf{LM}(\mathsf{col}_V(p)))$, we conclude that all variables of $\mathfrak{m}_i' h_i'$ are in the first copy of $\mathcal{Y}$. Furthermore, since h_i' is V-compatible, we conclude that all variables of h_i' correspond to variables in V in the first copy of $\mathcal{Y}$. Similarly, all variables of $\mathfrak{m}_i'$ correspond to variables in V in the first copy of $\mathcal{Y}$.

Therefore, $\mathsf{col}_V(\mathsf{forget}(h_i')) = h_i'$ and $\mathsf{col}_V(\mathsf{forget}(\mathfrak{m}_i')) = \mathfrak{m}_i'$. If we define $h \triangleq \mathsf{forget}(h_i')$ and $\mathfrak{m} \triangleq \mathsf{forget}(\mathfrak{m}_i')$, we conclude that $\mathsf{LM}(p) = \mathfrak{m}\,\mathsf{LM}(h)$, and $\mathsf{dom}(h) \subseteq V = \mathsf{dom}(p)$. We have proven that $\mathsf{forget}(\mathcal{B}_\star)$ is an equivariant Gröbner basis of $\langle H \rangle_{\mathcal{G}}$. □

As a consequence, egb is the algorithm of Theorem 1.1, and in particular obtain as a corollary that one can decide the equivariant ideal membership problem under our computability assumptions, if the set of indeterminates satisfies that $(\mathsf{Mon}_{\mathbb{N}\times\mathbb{N}}(\mathcal{X}), \sqsubseteq_{\mathcal{G}}^{\text{div}})$ is a well-quasi-ordered set. We can leverage these decidability results to obtain effective representations of equivariant ideals, which can then be used in algorithms as we will see in Section 5.3.

Corollary 1.2. *Assume that $\mathcal{G} \curvearrowright \mathcal{X}$ is effectively oligomorphic and well-structured. Then one has an* effective representation *of the equivariant ideals of $\mathbb{K}[\mathcal{X}]$, such that:*

1. *One can obtain a representation from an orbit-finite set of generators,*
2. *One can effectively decide the equivariant ideal membership problem given a representation,*
3. *The following operations are computable at the level of representations: the union of two equivariant ideals, the product of two equivariant ideals, the intersection of two equivariant ideals, and checking whether two equivariant ideals are equal.*

▹ Proven p.15

5 Applications and examples

In this section, we discuss how our main Theorem 1.1 and its Corollary 1.2 can be applied in practice. First, we give some examples of group actions and discuss whether they satisfy our computability assumptions and whether the divisibility relation up-to-$\mathcal{G}$ is a well-quasi-ordering. We also provide an analogue of Corollary 1.2 allowing us to work in the absence of a total ordering on the set of indeterminates $\mathcal{X}$. Finally, we discuss some applications of our results to several problems in algebra and computer science.

5.1 Examples of group actions

Many of the common examples of group actions $\mathcal{G} \curvearrowright \mathcal{X}$ are obtained by considering $\mathcal{X}$ as set with some structure, described by some relations and functions on that set, and $\mathcal{G}$ is the group $\mathsf{Aut}(\mathcal{X})$ of all automorphisms (i.e. bijections that preserve and reflect the structure) of $\mathcal{X}$. A monomial $\mathfrak{p} \in \mathsf{Mon}_Y(\mathcal{X})$ can be thought as a

Example	W.S.	ω-W.S.
Equality Atoms (5.1)	Yes	Yes
Dense linear order (5.2)	Yes	Yes
Dense tree (5.5)	Yes	Yes
Integers with order (5.6)	No	No
Rado graph (5.3)	No	No
Infinite dim. vector space (5.4)	No	No

Figure 1: Summary of the examples of group actions in Section 5.1. Notice that on all examples, being well-structured (*W.S.*) is equivalent to being ω-well-structured (ω-*W.S.*).

labelling of a finite substructure of $\mathcal{X}$ using elements of Y. If the structure $\mathcal{X}$ is *homogeneous*, that is, if isomorphisms between finite induced substructures extends to automorphisms of the whole structure, then $\sqsubseteq^{\text{div}}_{\mathcal{G}}$ is the same as embedding of labelled finite induced substructures of $\mathcal{X}$.[3] Let us now give some examples of such structures and whether they satisfy our computability assumptions, and whether the divisibility relation up-to-$\mathcal{G}$ is a well-quasi-ordering.

Example 5.1 (Equality Atoms). Let $\mathcal{A}$ be an infinite set without any additional structure other than the equality relation. Up to isomorphism, finite induced substructures of $\mathcal{A}$ are finite sets, monomials in $\text{Mon}_Y(\mathcal{A})$ are finite multisets of elements in Y, and $\sqsubseteq^{\text{div}}_{\text{Aut}(\mathcal{A})}$ is the multiset ordering [11, Section 1.5], which is a WQO [11, Corollary 1.21].

Example 5.2 (Dense linear order). Let $\mathcal{Q}$ be the set of rational numbers ordered by the usual ordering. Note that under this ordering, $\mathcal{Q}$ is a dense linear order without endpoints. Up to isomorphism, finite induced substructures of $\mathcal{Q}$ are finite linear orders, monomials in $\text{Mon}_Y(\mathcal{Q})$ are words in Y^* (i.e. finite linear order labelled with elements of Y) and $\sqsubseteq^{\text{div}}_{\text{Aut}(\mathcal{Q})}$ is the scattered subword ordering, which is a WQO due to Higman's lemma [16].

Example 5.3 (The Rado graph). Let $\mathcal{R}$ be the *Rado graph* ([6, Section 7.3.1],[25, Example 2.2.1]). Up to isomorphism, finite induced substructures of $\mathcal{R}$ are finite undirected graphs, monomials in $\text{Mon}_Y(\mathcal{R})$ are graphs with vertices labelled with Y, and $\sqsubseteq^{\text{div}}_{\text{Aut}(\mathcal{R})}$ is the labelled induced subgraph ordering even when Y is a singleton. For example, cycles of length more than three form an infinite antichain.

Example 5.4 (Infinite dimensional vector space). Let $\mathcal{V}$ be an infinite dimensional vector space over $\mathbb{F}_2$. Up to isomorphism, finite induced substructures of $\mathcal{V}$ are finite dimensional vector spaces over $\mathbb{F}_2$. These are well-quasi-ordered in the absence of labelling. However, even when $Y = \mathbb{N}$, $(\text{Mon}_Y(\mathcal{V}), \sqsubseteq^{\text{div}}_{\text{Aut}(\mathcal{V})})$ is not a WQO as illustrated by the following antichain. Let $\{v_1, v_2, \dots\} \subseteq \mathcal{V}$ be a countable set of linearly independent vectors in $\mathcal{V}$. Let $\oplus$ denote the addition operation of $\mathcal{V}$. For $n \geq 3$ define the monomial $\mathfrak{p}_n \triangleq v_1^2 \dots v_n^2 (v_1 \oplus v_2)(v_2 \oplus v_3) \dots (v_{n-1} \oplus v_n)(v_n \oplus v_1)$. Then, $\{\mathfrak{p}_n \mid n = 3, 4, \dots\}$ forms an infinite antichain.

[3] We refer the reader to [6, Chapter 7] and [25] for more details on homogeneous structures.

The previous Examples 5.1 to 5.4 are well known examples in the theory of *sets with atoms* [6]. Let us now give a new example of well-quasi-ordered divisibility relation up-to-$\mathcal{G}$, by extending Example 5.2 that relied on Higman's lemma [16] via Kruskal's tree theorem [22].

Example 5.5 (Dense Meet Tree). Let $\mathcal{T}$ denote the universal countable dense meet-tree, as defined in [21, Page 2] or [6, Section 7.3.3]. Note that the tree structure is given by the *least common ancestor* (*meet*) operation, and not by its edges. For a subset $S \subset \mathcal{T}$, define its *closure* to be the smallest subtree of $\mathcal{T}$ containing S. Up to isomorphism, finite induced substructures of $\mathcal{T}$ are finite meet-trees. Monomials in $\text{Mon}_Y(\mathcal{T})$ are finite meet-trees labelled with $1 + Y$. Here $1 + Y$ is the WQO containing one more element than Y which is incomparable to elements in Y, and is used to label nodes that are in the closure of the set of variable of a monomial, but not in the monomial itself. The divisibility relation $\sqsubseteq^{\text{div}}_{\text{Aut}(\mathcal{T})}$ is exactly the embedding of labelled meet-trees, which is a WQO due to Kruskal's tree theorem [22].

The above examples using homogeneous structures nicely illustrate the correspondence between monomials and labelled finite substructures, but we can also consider non-homogeneous structures, such as in Example 5.6 below.

Example 5.6. Let $\mathcal{Z}$ be the set of *integers ordered by the usual ordering*. Then $\text{Aut}(\mathcal{Z})$ is the set of all order preserving bijections of $\mathcal{D}$. Note that every order preserving bijection of the set $\mathcal{Z}$ is a translation $n \mapsto n + c$ for some constant $c \in \mathcal{Z}$. By definition, the action $\text{Aut}(\mathcal{Z}) \curvearrowright \mathcal{Z}$ preserves the linear order on $\mathbb{Z}$. However, $(\text{Mon}_Y(\mathcal{Z}), \sqsubseteq^{\text{div}}_{\text{Aut}(\mathcal{Z})})$ is not a WQO even when Y is a singleton. An example of an infinite antichain is the set $\{ab \mid b \in \mathcal{Z} \setminus \{a\}\}$, for any fixed $a \in \mathcal{Z}$.

Recall that in our computability assumptions we require the action $\mathcal{G} \curvearrowright \mathcal{X}$ to be effectively oligomorphic. It is already known that all the structures of the upgoing Examples 5.1 to 5.5 are oligomorphic [6, Theorem 7.6]. The other examples are not ω-well-structured, hence we will not verify effective oligomorphicity for them. Let us argue on an example that they are effectively oligomorphic. It is clear that $\mathcal{Q}$ can be represented by integer fractions, and that the orbit of a tuple $(q_1, q_2, \dots, q_n)$ of rational numbers is given by their relative ordering in $\mathbb{Q}$, which can be effectively computed. Finally, one can enumerate such orderings and produce representatives by selecting n integers. This can be generalised to all the structures mentioned in Examples 5.1 to 5.5, by using dedicated representations (such as [6, Page 244-245] for $\mathcal{T}$), or the general theory of Fraïsse limits [10].

5.2 Closure properties

In this section, we are interested in listing the operations on sets of indeterminates equipped with a group action that preserve our computability assumptions and the well-quasi-ordering property ensuring that our Theorem 1.1 can be applied. Indeed, it is often tedious to prove that a given group action $\mathcal{G} \curvearrowright \mathcal{X}$ satisfies the computability assumptions and the well-quasi-ordering property, and we aim to provide a list of operations that preserve these properties, so that simpler examples (Examples 5.1, 5.2 and 5.5) can serve as building blocks to model complex systems.

Structural operations. Let us first focus on three standard operations on sets of indeterminates: the disjoint sum (that was already at play in Section 4), the direct product (that will fail to preserve our assumptions), and its variant, the lexicographic product. For the remainder of this section, we fix a pair of group actions $\mathcal{H} \curvearrowright \mathcal{X}$ and $\mathcal{G} \curvearrowright \mathcal{Y}$, where $\mathcal{X}$ is equipped with a total order $<_{\mathcal{X}}$ and $\mathcal{Y}$ is equipped with a total order $<_{\mathcal{Y}}$.

The *disjoint sum* $\mathcal{X}+\mathcal{Y}$ is the disjoint union of $\mathcal{X}$ and $\mathcal{Y}$, equipped with the total order obtained by stating that all elements of $\mathcal{X}$ are smaller than all elements of $\mathcal{Y}$, and preserving the original orderings inside $\mathcal{X}$ and $\mathcal{Y}$. The group $\mathcal{G} \times \mathcal{H}$ acts on $\mathcal{X} + \mathcal{Y}$ by acting as $\mathcal{H}$ on $\mathcal{X}$ and as $\mathcal{G}$ on $\mathcal{Y}$.

Lemma 5.7. *If $\mathcal{G} \curvearrowright \mathcal{X}$ and $\mathcal{H} \curvearrowright \mathcal{Y}$ are well-structured (resp. effectively oligomorphic), then so is $\mathcal{G} \times \mathcal{H} \curvearrowright \mathcal{X} + \mathcal{Y}$.*

Proof. The divisibility up to $\mathcal{G} \times \mathcal{H}$ order is essentially the disjoint sum of the orders $\sqsubseteq_{\mathcal{G}}^{\mathrm{div}}$ and $\sqsubseteq_{\mathcal{H}}^{\mathrm{div}}$, hence is a WQO if both orders are WQOs [11, Lemma 1.5]. Furthermore, it is folklore that the disjoint sum of two oligomorphic actions is itself oligomorphic.

Let us now check that the action is effectively oligomorphic when both actions are. It is an easy check that the action defined is compatible with the total ordering on the set of indeterminates. To list representatives of the orbits in $(\mathcal{X} + \mathcal{Y})^n$ for a fixed $n \in \mathbb{N}$, we can list representatives $u_{\mathcal{X}}$ of the orbits in $\mathcal{X}^{\leq n}$, representatives $u_{\mathcal{Y}}$ of the orbits in $\mathcal{Y}^{\leq n}$, and words $u_{\mathrm{tag}} \in \{0,1\}^n$, and consider triples $(u_{\mathcal{X}}, u_{\mathcal{Y}}, u_{\mathrm{tag}})$ such that $|u_{\mathcal{X}}| + |u_{\mathcal{Y}}| = n$, $|u_{\mathrm{tag}}|_0 = |u_{\mathcal{X}}|$, and $|u_{\mathrm{tag}}|_1 = |u_{\mathcal{Y}}|$. It is an easy check that one can effectively decide whether two such triples are in the same orbit. □

The *direct product* $\mathcal{X}\times\mathcal{Y}$ is the Cartesian product $\mathcal{X}\times\mathcal{Y}$, equipped with the lexicographic ordering defined as

$$(x_1, y_1) <_{\mathcal{X}\times\mathcal{Y}} (x_2, y_2) \text{ if } x_1 <_{\mathcal{X}} x_2 \text{ or } (x_1 = x_2 \text{ and } y_1 <_{\mathcal{Y}} y_2) .$$

The group $\mathcal{G} \times \mathcal{H}$ acts on $\mathcal{X} \times \mathcal{Y}$ by acting as $\mathcal{H}$ on the first component and as $\mathcal{G}$ on the second component.

Lemma 5.8. *When $\mathcal{X}$ and $\mathcal{Y}$ are infinite, $(\mathrm{Mon}_Q(\mathcal{X} \times \mathcal{Y}), \sqsubseteq_{\mathcal{G}\times\mathcal{H}}^{\mathrm{div}})$ is not a WQO, even with $Q = \{0, 1\}$.*

Proof. We restate the antichain given in [15, Example 10], that will also be used is Remark 6.10 of Section 6 when discussing the undecidability of the equivariant ideal membership problem. Let $\{x_1, x_2, \dots\}$ and $\{y_1, y_2, \dots\}$ be infinite subsets of $\mathcal{X}$ and $\mathcal{Y}$ respectively. For $n = 3, 4, \dots$, let $\mathfrak{c}_n$ be the monomial

$$\mathfrak{c}_n = (x_1, y_1)(x_1, y_2)(x_2, y_2)(x_2, y_3) \cdots (x_n, y_n)(x_n, y_1) .$$

Then $\{\mathfrak{c}_n \mid n = 3, 4, \dots\}$ is an infinite antichain. □

The failure to consider direct products is somewhat unfortunate, and motivates the introduction of the *lexicographic product* $\mathcal{X} \otimes \mathcal{Y}$, whose underlying set is also $\mathcal{X} \times \mathcal{Y}$, with the same lexicographic ordering as the direct product, but where the group $\mathcal{G}\otimes\mathcal{H}$ is defined as pairs $(\pi, (\sigma^x)_{x\in\mathcal{X}})$, where $\pi \in \mathcal{G}$ and $\sigma^x \in \mathcal{H}$ for every $x \in \mathcal{X}$, and where the multiplication is defined as

$$(\pi_1, (\sigma_1^x)_{x\in\mathcal{X}})(\pi_2, (\sigma_2^x)_{x\in\mathcal{X}}) = (\pi_1\pi_2, (\sigma_1^{\pi_2(x)} \sigma_2^x)_{x\in\mathcal{X}}) \quad . \tag{6}$$

This group is sometimes called the *wreath product* or the *semidirect product* of $\mathcal{G}$ and $\mathcal{H}$. It acts on $\mathcal{X} \otimes \mathcal{Y}$ as

$$(\pi, (\sigma^x)_{x\in\mathcal{X}}) \cdot (x', y') = (\pi \cdot x', \sigma^{x'} \cdot y') \quad , \tag{7}$$

for every $(x', y') \in \mathcal{X} \otimes \mathcal{Y}$. Essentially, it means that every element $x \in \mathcal{X}$ carries its own copy $\{x\} \times \mathcal{Y}$ of the structure $\mathcal{Y}$, and one can act independently on different copies of the structure $\mathcal{Y}$.

Lemma 5.9 ([15, Lemmas 9 and 39]). *If $\mathcal{G} \curvearrowright \mathcal{X}$ and $\mathcal{H} \curvearrowright \mathcal{Y}$ are well-structured (resp. effectively oligomorphic), then so is $(\mathcal{G}\otimes\mathcal{H}) \curvearrowright (\mathcal{X} \times \mathcal{Y})$.*

Corollary 5.10. *The class of group actions satisfying our computability assumptions and well-quasi-ordering property is closed under disjoint sums and lexicographic products, but not under direct products.*

Reducts and nicely orderable actions. Another important operation on group actions is the notion of reduct, which allows one to encode actions that do not preserve a linear order into actions that do. We say that $\mathcal{G} \curvearrowright \mathcal{X}$ is a *reduct* of another group action $\mathcal{H} \curvearrowright \mathcal{Y}$ if there exists a bijection $f : \mathcal{X} \to \mathcal{Y}$ such that, for every $\theta \in \mathcal{H}$, we have some $\pi \in \mathcal{G}$ such that $f^{-1} \circ \theta \circ f$ acts like π on $\mathcal{X}$. This is called an *effective reduct* if f is computable.

Theorem 5.11. *Let $\mathcal{H} \curvearrowright \mathcal{Y}$ be an action satisfying the requirements of Corollary 1.2, and let $\mathcal{G} \curvearrowright \mathcal{X}$ be an effective reduct of $\mathcal{H} \curvearrowright \mathcal{Y}$. Then one has an* effective representation *of the equivariant ideals of $\mathbb{K}[\mathcal{X}]$ satisfying the properties of Corollary 1.2.*

Theorem 5.11 implies that one can apply our results to an action $\mathcal{G} \curvearrowright \mathcal{X}$ that does not preserve a linear order, as soon as it is a reduct of some another action $\mathcal{H} \curvearrowright \mathcal{X}$ which does preserves a linear order. For example, $\mathrm{Aut}(\mathcal{A}) \curvearrowright \mathcal{A}$ is a reduct of $\mathrm{Aut}(\mathcal{Q}) \curvearrowright \mathcal{Q}$ assuming $\mathcal{A}$ is countable. Similarly, let $\mathcal{T}_<$ be the countable dense-meet tree with a lexicographic ordering, as defined in [21, Remark 6.14].[4] Let $\mathcal{G}$ be the group of bijections of $\mathcal{T}_<$ which do not necessarily preserve the lexicographic ordering. Then $\mathcal{G} \curvearrowright \mathcal{T}_<$ is isomorphic to $\mathrm{Aut}(\mathcal{T}) \curvearrowright \mathcal{T}$, and hence $\mathrm{Aut}(\mathcal{T}) \curvearrowright \mathcal{T}$ is a reduct of $\mathrm{Aut}(\mathcal{T}_<) \curvearrowright \mathcal{T}_<$.

We say that an action $\mathcal{G} \curvearrowright \mathcal{X}$ is *nicely orderable* if there exists another action $\mathcal{H} \curvearrowright \mathcal{Y}$ such that $\mathcal{G} \curvearrowright \mathcal{X}$ is a reduct of $\mathcal{H} \curvearrowright \mathcal{Y}$, $\mathcal{H} \curvearrowright \mathcal{Y}$ preserves a linear order on $\mathcal{Y}$, and $\mathcal{H} \curvearrowright \mathcal{Y}$ satisfies our computability assumptions. In the case of actions originating from homogeneous structures, it is conjectured that being well-structured is equivalent to being nicely orderable [29, Problems 12].

5.3 Applications

Polynomial computations. The fact that (finite control) systems performing polynomial computations can be verified follows from the theory of Gröbner bases on finitely many indeterminates [4, 28]. There were also numerous applications to automata theory, such as deciding whether a weighted automaton could be determinised (resp. desambiguated) [3, 31]. We refer the readers to a nice survey recapitulating the successes of the "Hilbert method" automata theory [7]. A natural consequence of the effective computations of equivariant Gröbner bases is that one can apply the same decision techniques to *orbit finite polynomial computations*. For simplicity and clarity, we will focus on polynomial automata

[4] The remark says that finite meet-trees expanded with a lexicographic ordering is a Fraïsse class, from which it follows that there exists a Fraïsse limit $\mathcal{T}_<$ for that class.

without states or zero-tests [4], but the same reasoning would apply to more general systems.

Before discussing the case of orbit finite polynomial automata, let us recall the setting of polynomial automata in the classical case, as studied by [4], with techniques that dates back to [28]. A *polynomial automaton* is a tuple $A \triangleq (Q, \Sigma, \delta, q_0, F)$, where $Q = \mathbb{K}^n$ for some finite $n \in \mathbb{N}$, Σ is a finite alphabet, $\delta \colon Q \times \Sigma \to Q$ is a transition function such that $\delta(\cdot, a)_i$ is a polynomial in the indeterminates $q_1, \dots, q_n$ for every $a \in \Sigma$ and every $i \in \{1, \dots, n\}$, $q_0 \in Q$ is the initial state, and $F \colon Q \to \mathbb{K}$ is a polynomial function describing the final result of the automaton. The *zeroness problem for polynomial automata* is the following decision problem: given a polynomial automaton A, is it true that for all words $w \in \Sigma^*$, the polynomial $F(\delta^*(q_0, w))$ is zero? It is known that the zeroness problem for polynomial automata is decidable [4], using the theory of Gröbner bases on finitely many indeterminates.

Let us now propose a new model of computation called orbit finite polynomial automata, and prove an analogue decidability result. Let us fix an effectively oligomorphic action $\mathcal{G} \curvearrowright \mathcal{X}$, such that there exists finitely many indeterminates $V \subset_{\mathrm{fin}} \mathcal{X}$ such that $\mathcal{G}$ acts as the identity on V. Given such a function $f \colon \mathcal{X} \to \mathbb{K}$, and given a polynomial $p \in \mathbb{K}[\mathcal{X}]$, we write $p(f)$ for the evaluation of p on f, that belongs to $\mathbb{K}$. Let us emphasis that the model is purposely designed to be simple and illustrate the usage of equivariant Gröbner bases, and not meant to be a fully-fledged model of computation.

Definition 5.12. An *orbit finite polynomial automaton* over $\mathbb{K}$ and $\mathcal{X}$ is a tuple $A \triangleq (Q, \delta, q_0, F)$, where $Q = \mathcal{X} \to \mathbb{K}$, $q_0 \in Q$ is a function that is non-zero for finitely many indeterminates, $\delta \colon \mathcal{X} \times \mathcal{X} \stackrel{\mathrm{eq}}{\to} \mathbb{K}[\mathcal{X}]$ is a polynomial update function, and $F \in \mathbb{K}[V]$ is a polynomial computing the result of the automaton.

Given a letter $a \in \mathcal{X}$ and a state $q \in Q$, the updated state $\delta^*(a, q) \in Q$ is defined as the function from $\mathcal{X}$ to $\mathbb{K}$ defined by $\delta^*(a, q) \colon x \mapsto \delta(a, x)(q)$. The update function is naturally extended to words. Finally, the output of an orbit finite polynomial automaton on a word $w \in \mathcal{X}^*$ is defined as $F(\delta^*(w, q_0))$.

Orbit finite polynomial automata can be used to model programs that read a string $w \in \mathcal{X}^*$ from left to right, having as internal state a dictionary of type `dict[indet, number]`, which is updated using polynomial computations. As for polynomial automata, the *zeroness problem* for orbit finite polynomial automata is the following decision problem: decide if for every input word w, the output $F(\delta^*(w, q_0))$ is zero.

The orbit finite polynomial automata model could be extended to allow for inputs of the form $\mathcal{X}^k$ for some $k \in \mathbb{N}$, or even be recast in the theory of nominal sets [6]. Furthermore, leveraging the closure properties of Corollary 5.10, one can also reduce the equivalence problem for orbit finite polynomial automata to the zeroness problem, by considering the sum action on the registers to compute the difference of the two results. We leave a more detailed investigation of the generalisation of polynomial automata to the orbit finite setting for future work.

Theorem 5.13 (orbit finite polynomial automata). *Let $\mathcal{X}$ be a set of indeterminates that satisfies the computability assumptions and such that $(\mathrm{Mon}_Y(\mathcal{X}), \sqsubseteq_{\mathcal{G}}^{\mathrm{div}})$ is a well-quasi-ordering, for every well-quasi-ordered set $(Y, \leq)$. Then, the zeroness problem is decidable for orbit finite polynomial automata over $\mathbb{K}$ and $\mathcal{X}$.*

Reachability problem of reversible data Petri nets. The classical model of Petri nets was extended to account for arbitrary data attached to tokens to form what is called data Petri nets. We will not discuss the precise definitions of these models, but point out that a reversible data Petri net is exactly what is called a monomial rewriting system [15, Section 8]. Because reachability in such rewriting systems can be decided using equivariant ideal membership queries [15, Theorem 64], we can use Theorem 5.11 to show Theorem 5.14. Note that monomial rewrite systems will be at the center of our undecidability results in Section 6.

Theorem 5.14 (Reachability in Reversible Data Petri Nets). *For every nicely orderable group action $\mathcal{G} \curvearrowright \mathcal{X}$, the reachability problem for reversible Petri nets with data in $\mathcal{X}$ is decidable.*

Remark 5.15. The decidability of reachability for Petri nets with equality data is still open, and the for ordered data this problem is known to be undecidable [32, Proposition 1 and Section 5.2]. Theorem 5.14 implies both of these become decidable when the Petri net is assumed to reversible.

Orbit-finite systems of equations. The classical theory of solving finite systems of linear equations has been generalised to the infinite setting by [14], [15, Section 9]. In this setting, one considers an effectively oligomorphic group action $\mathcal{G} \curvearrowright \mathcal{X}$, and the vector space $\mathrm{Lin}(\mathcal{X}^n)$ generated by the indeterminates $\mathcal{X}^n$ over $\mathbb{K}$. An *orbit-finite linear system of equations* asks whether a given vector $u \in \mathrm{Lin}(\mathcal{X}^n)$ is in the vector space generated by an orbit-finite set of vectors V in $\mathrm{Lin}(\mathcal{X}^n)$ [15, Section 9]. It has been shown that the *solvability* of these systems of equations reduces to the equivariant ideal membership problem [15, Theorem 68], and as a consequence of this reduction and Theorem 5.11 we obtain the following theorem.

Theorem 5.16 (Solvability of Orbit-Finite Systems of Equations). *For every nicely orderable group action $\mathcal{G} \curvearrowright \mathcal{X}$, the solvability problem for orbit-finite systems of equations is decidable.*

Previously, solvability of orbit-finite systems of equations were studied mostly for specific structures. In particular, [14, Theorem 6.1] shows it to be decidable for equality atoms. Specific versions of this problem for ordered atoms were studied by [20]. Finally, [15] showed it to be decidable for ordered atoms, and also showed that decidability is preserved under taking lexicographic product. We generalise all these results to nicely orderable group actions.

6 Undecidability Results

In this section, we aim to show that the equivariant ideal membership problem is undecidable under the usual computability assumptions on the group action, when we do not assume that $(\mathrm{Mon}(\mathcal{X}), \sqsubseteq_{\mathcal{G}}^{\mathrm{div}})$ is a well-quasi-ordering. In particular, this would show that computing equivariant Gröbner bases is not possible in these settings, proving the optimality of our decidability Theorem 1.1. Beware that there are some pathological cases where the equivariant ideal membership problem is easily decidable, even when $(\mathrm{Mon}(\mathcal{X}), \sqsubseteq_{\mathcal{G}}^{\mathrm{div}})$ is not a well-quasi-ordering, as illustrated by the following Example 6.1, and it is not possible to obtain such a dichotomy result without further assumptions on the group action.

Example 6.1. Let $\mathcal{X} = \{x_1, x_2, \dots\}$ be an infinite set of indeterminates, and let $\mathcal{G}$ be trivial group acting on $\mathcal{X}$. Then, the equivariant ideal membership problem is decidable. Indeed, since the group is trivial, whenever one provides a finite set H of generators of an equivariant ideal I, one can in fact work in $\mathbb{K}[V]$, where V is the set of indeterminates that appear in H. Then, the equivariant ideal membership problem reduces to the ideal membership problem in $\mathbb{K}[V]$, which is decidable.

However, we are able to prove the undecidability of the equivariant ideal membership problem under the assumption that the set of indeterminates $\mathcal{X}$ contains an *infinite path* $P \triangleq (x_i)_{i \in \mathbb{N}} \subseteq \mathcal{X}$, that is, a set of indeterminates such that $(x_i, x_j) \in P^2$ is in the same orbit as (x_0, x_1) if and only if $|i - j| = 1$, for all $i, j \in \mathbb{N}$. We similarly define *finite paths* by considering finitely many elements. The prototypical example of a set of indeterminates containing an infinite path is $\mathcal{X} = \mathbb{Z}$ equipped with the group $\mathcal{G}$ of all shifts. The presence of an infinite path clearly prevents $(\mathrm{Mon}(\mathcal{X}), \sqsubseteq_{\mathcal{G}}^{\mathrm{div}})$ from being a well-quasi-ordering, as shown by the following Remark 6.2. Furthermore, for indeterminates obtained by considering homogeneous structures and their automorphism groups (Section 5.1), the absence of an infinite path has been conjectured to be a necessary and sufficient condition for $(\mathrm{Mon}(\mathcal{X}), \sqsubseteq_{\mathcal{G}}^{\mathrm{div}})$ to be a well-quasi-ordering: this follows from a conjecture of Schmitz restated in Conjecture 6.3.

Remark 6.2. Assume that $\mathcal{X}$ contains an infinite path $P \triangleq (x_i)_{i \in \mathbb{N}}$. Then, the set of monomials $\{x_0^3 x_1^1 \cdots x_{n-1}^1 x_n^2 \mid n \in \mathbb{N}\}$ is an infinite antichain in $(\mathrm{Mon}(\mathcal{X}), \sqsubseteq_{\mathcal{G}}^{\mathrm{div}})$. Indeed, assume that there exists $n < m$, and a group element $\pi \in \mathcal{G}$ such that $\pi \cdot \mathfrak{m}_n \sqsubseteq^{\mathrm{div}} \mathfrak{m}_m$. Then, $\pi \cdot x_0 = x_0$, because it is the only indeterminate with exponent 3 in $\mathfrak{m}_m$. Furthermore, $\pi \cdot (x_0, x_1) = (x_i, x_j)$ implies that $|i - j| = 1$, and since $\pi \cdot x_0 = x_0$, we conclude $\pi \cdot x_1 = x_1$. By an immediate induction, we conclude that $\pi \cdot x_i = x_i$ for all $0 \leq i \leq n$, but then we also have that the degree of $\pi \cdot x_n$ is less than 2 in $\mathfrak{m}_m$, which contradicts the fact that $\pi \cdot \mathfrak{m}_n \sqsubseteq^{\mathrm{div}} \mathfrak{m}_m$.

Conjecture 6.3 (Schmitz). *Let C be a class of finite relational structures. Then, the following are equivalent:*

(1) *The class of structures of C labelled with any well-quasi-ordered set $(Y, \leq)$ is itself well-quasi-ordered under the labelled-induced-substructure relation.*
(2) *For every existential formula $\varphi(x, y)$, there exists $N_\varphi \in \mathbb{N}$, such that φ does not define paths of length greater than N_φ in the structures of C.*

Where a formula defines a path of length n in a structure if there exists n distinct elements $a_0, \dots, a_{n-1}$ in the structure such that $\varphi(a_i, a_j)$ holds if and only if $|i - j| = 1$.

Monomial Reachability. The undecidability results we will present in this section regarding the equivariant ideal membership problem will use the polynomials in a very limited way: we will only need to consider *monomials*, and there will even be a bound on the maximal exponent used. Before going into the details of our reductions, let us first introduce an intermediate problem that will be easier to work with: the (equivariant) monomial reachability problem.

Definition 6.4. A *monomial rewrite system* is a finite set of pairs of the form $\{\mathfrak{m}, \mathfrak{m}'\}$ where $\mathfrak{m}, \mathfrak{m}' \in \mathrm{Mon}(\mathcal{X})$. The *monomial reachability problem* is the problem of deciding whether there exists a sequence of rewrites that transforms $\mathfrak{m}_s$ into $\mathfrak{m}_t$ using the rules of a monomial rewrite system R, where a *rewrite step* is a pair of the form

$$\mathfrak{n}(\pi \cdot \mathfrak{m}) \leftrightarrow_R \mathfrak{n}(\pi \cdot \mathfrak{m}') \text{ if } \{\mathfrak{m}, \mathfrak{m}'\} \in R \text{ and } \pi \in \mathcal{G} \quad .$$

Example 6.5. Let $\mathcal{X} = \mathbb{N}$ and $\mathcal{G}$ be the set of all bijections of $\mathcal{X}$. Then, the rewrite system $x_1^2 x_2^2 \leftrightarrow_R x_1^2$ satisfies $\mathfrak{m} \leftrightarrow_R^* x_1^2$ if and only if $\mathfrak{m}$ has all its exponents that are multiple of 2.

The following Lemma 6.6 shows that the monomial reachability problem can be reduced to the equivariant ideal membership problem, and follows the exact same reasoning as in the case of finitely many indeterminates [26]. This reduction was also noticed in [15, Theorem 64].

Lemma 6.6. *Assuming that $\mathbb{K} = \mathbb{Q}$, one can solve the monomial reachability problem provided that one can solve the equivariant ideal membership problem.*

In order to show that the equivariant ideal membership problem is undecidable, it is therefore enough to show that the monomial reachability problem is undecidable. To that end, we will encode the Halting problem of a Turing machine. There are two main obstacles to overcome: first, the reversibility of the rewriting system, which can be (partially) solved by considering a *reversible version* of a *deterministic* Turing machines, as explained in [13, Simulation by bidirected systems, p. 15]; and second, the fact that the configurations of the Turing machine cannot staightforwardly be encoded as monomials due to the commutativity of the multiplication.

Structures Containing Paths. Let us assume for the rest of this section that $\mathcal{X}$ is a set of indeterminates that contains an infinite path, let us fix a binary alphabet $\Sigma \triangleq \{a, b\}$. Given a finite path $P \triangleq (x_i)_{0 \leq i < 4n}$, we define a function $[\![\cdot]\!]_P : \Sigma^{\leq n} \to \mathrm{Mon}(\mathcal{X})$, where Σ is a finite alphabet, that *encodes a word* $u \in \Sigma^{\leq n}$ as a monomial. Namely, we define inductively $[\![\varepsilon]\!] \triangleq 1$, $[\![au]\!]_P = x_0^4 x_1^2 x_2^1 x_3^3 (\mathrm{shift}_{+4} \cdot [\![u]\!]_P)$ and $[\![bu]\!]_P = x_0^4 x_1^1 x_2^2 x_3^3 (\mathrm{shift}_{+4} \cdot [\![u]\!]_P)$ for all $u \in \Sigma^*$, where shift_{+k} acts on P by shifting the indices by k.[5] Let us remark that monomial rewriting applied on word encodings can simulate (reversible) string rewriting on words of a given size.

Lemma 6.7. *Let P, Q be two finite paths in $\mathcal{X}$, such that (p_0, p_1) is in the same orbit as (q_0, q_1). Let $u, v, w \in \Sigma^*$ be three words, such that $|u| = |v| \leq |w|$, and let $\mathfrak{n} \in \mathrm{Mon}(\mathcal{X})$ be a monomial. Assume that there exists $\pi \in \mathcal{G}$ such that $[\![w]\!]_P = \mathfrak{m}(\pi \cdot [\![u]\!]_Q)$, $\mathfrak{n} = \mathfrak{m}(\pi \cdot [\![v]\!]_Q)$, and that $[\![w]\!]_P$, $[\![u]\!]_Q$ and $[\![v]\!]_Q$ are well-defined. Then, there exists $x, y \in \Sigma^*$ such that $xuy = w$ and $[\![xvy]\!]_P = \mathfrak{n}$.* ▹ Proven p.16

Lemma 6.7 shows that all encodings using finite paths with the same initial orbit are compatible with each other for the purpose of monomial rewriting. Let us now assume that the alphabet is any finite set of letters, using a suitable unambiguous encoding of the alphabet in binary [5]. This bigger alphabet size will simplify the statement and proof of the following Lemma 6.8, which explains how to simulate a reversible Turing machine using monomial rewriting. Given a reversible Turing machine M with a finite

[5] There may be no element $\pi \in \mathcal{G}$ that acts like shift_{+1}, we only use it as a function.

set Q of states and tape alphabet Σ, we will consider the following alphabet $\Gamma \triangleq \{\triangleleft, \triangleright\} \times \{\text{pre}, \text{run}, \text{post}\} \uplus Q \uplus \Sigma \uplus \{\square, \square_1, \square_2\}$. The letter $\square$ is a blank symbol, and the letters $\triangleleft$ and $\triangleright$ are used to delimit the beginning and the end of the tape, with some extra "phase information". In a first monomial rewrite system, we will encode a run of a reversible Turing machine M on a fixed size input tape (Lemma 6.8), and in a second monomial rewrite system, we will create a tape of arbitrary size (Lemma 6.9). The union of these two monomial rewrite systems will then be used to prove the undecidability of the equivariant ideal membership problem in Theorem 1.3.

Lemma 6.8. *Let us fix (x_0, x_1) a pair of indeterminates. There exists a monomial rewrite system R_M such that the following are equivalent for every $n \geq 1$, and for any finite path P of length $4(n+2)$ such that (p_0, p_1) is in the same orbit as (x_0, x_1):*

1. $[\![\triangleright^{run} q_0 \square^{n-1} \triangleleft^{run}]\!]_P \leftrightarrow^*_{R_M} [\![\triangleright^{run} q_f \square^{n-1} \triangleleft^{run}]\!]_P$,
2. *M halts on the empty word using a tape bounded by $n-1$ cells.*

Furthermore, every monomial that is reachable from $[\![\triangleright^{run} q_0 \square^{n-1} \triangleleft^{pre}]\!]_P$ or $[\![\triangleright^{run} q_f \square^{n-1} \triangleleft^{run}]\!]_P$ is the image of a word of the form $[\![\triangleright^{run} u \triangleleft^{run}]\!]_P$ where $u \in (Q \uplus \Sigma \uplus \square)^n$. ▷ Proven p.16

Lemma 6.8 shows that one can simulate the runs, provided we know in advance the maximal size of the tape used by the reversible Turing machine. The key ingredient that remains to be explained is how one can start from a finite monomial $\mathfrak{m}$ and create a tape of arbitrary size using a monomial rewrite system. The difficulty is that we will not be able to ensure that we follow one specific finite path when creating the tape.

Lemma 6.9. *Let (x_0, x_1) be a pair of indeterminates, P be a finite path such that (p_0, p_1) is in the same orbit as (x_0, x_1). There exists a monomial rewrite system R_{pre} such that for every monomial $\mathfrak{m} \in \mathrm{Mon}(\mathcal{X})$, the following are equivalent:*

1. $[\![\triangleright^{pre} \square \square_1 \square_2 \triangleleft^{pre}]\!]_P \leftrightarrow^*_{R_{pre}} \mathfrak{m}$ *and* $[\![\triangleright^{run}]\!]_{P'} \sqsubseteq^{\mathrm{div}}_{\mathcal{G}} \mathfrak{m}$ *for some finite path P' such that (p'_0, p'_1) is in the same orbit as (x_0, x_1).*
2. *There exists $n \geq 2$ and a finite path P' such that (p'_0, p'_1) is in the same orbit as (x_0, x_1), and $\mathfrak{m} = [\![\triangleright^{run} q_0 \square^n \triangleleft^{run}]\!]_{P'}$.*

Similarly, there exists a monomial rewrite system R_{post} with analogue properties using q_f instead of q_0. ▷ Proven p.16

Theorem 1.3 (Undecidability of Equivariant Ideal Membership). *Let $\mathcal{X}$ be a totally ordered set of indeterminates equipped with a group action $\mathcal{G} \curvearrowright \mathcal{X}$, under our computability assumptions. If $\mathcal{X}$ contains an infinite path then the equivariant ideal membership problem is undecidable.*

Proof. It suffices to combine the rewriting systems R_M, R_{pre} and R_{post} by taking their union. □

Remark 6.10. The undecidability result of Theorem 1.3 can be generalised to a *relaxed* notion of infinite path. Given finitely many orbits $O_1, \ldots, O_k$ of pairs of indeterminates, a *relaxed path* is a set of indeterminates such that (x_i, x_j) is belongs to one of the orbits O_k if and only if $|i-j| = 1$ for all $i, j \in \mathbb{N}$.

Remark 6.11. Given an oligomorphic set of indeterminates $\mathcal{X}$, it is equivalent to say that $\mathcal{X}$ contains an infinite path or to say that it contains finite paths of arbitrary length. ▷ Proven p.16

Example 6.12. The Rado graph, as introduced in Example 5.3, contains an infinite path P. Indeed, the Rado graph contains every finite graph as an induced subgraph, and in particular, it contains arbitrarily long finite paths. As a consequence of Theorem 1.3, which applies thanks to Remark 6.11, we conclude that the equivariant ideal membership problem is undecidable for the Rado graph.

Example 6.13. Let $\mathcal{X}$ be an oligomorphic infinite set of indeterminates. Then $\mathcal{X} \times \mathcal{X}$ contains a (generalised) infinite path as defined in Remark 6.10. ▷ Proven p.17

7 Concluding Remarks

We have given a sufficient condition for equivariant Gröbner bases to be computable, under natural computability assumptions, and we have shown that our sufficient condition is close to being optimal since the undecidability of the equivariant ideal membership problem can be derived for a large class of group actions that do not satisfy our condition. Let us now discuss some open questions and conjectures that arise from our work.

Total orderings on the set of indeterminates. We assumed that the indeterminates $\mathcal{X}$ were equipped with a total ordering $\leq_{\mathcal{X}}$ that is preserved by the group action. This assumption seems necessary, as the notions of leading monomials would cease to be well-defined without it. However, we do not have a clear understanding of whether this assumption is vacuous or not. Indeed, as noticed by [15, Lemma 13], and Theorem 5.11, it often suffices to extend the structures of the indeterminates to account for a total ordering. A conjecture of Pouzet [29, Problems 12] states that such an ordering always exists, and this was remarked by [15, Remark 14]. Note that in this case, one would get a complete characterisation of the group actions for which the equivariant Hilbert basis property holds [15, Property 4].

Complexity. In the present paper, we have focused on the decidability of the equivariant ideal membership problem and the computability of equivariant Gröbner bases. However, we have not addressed the complexity of such problems, and have only adapted the most basic algorithms for computing Gröbner bases. It would be interesting to know, on the theoretical side, if one can obtain complexity lower bounds for such problems, but also on the more practical side if advanced algorithms like Faugère's algorithm [12] can be adapted to the equivariant setting and yield better performance in practice.

Equivariant algebraic geometry. The development of equivariant Gröbner bases opens the door to the study of other classical results from algebraic geometry to the equivariant setting. In particular, the status of the fundamental result of algebraic geometry, *Hilbert's Nullstellensatz*, that relates ideals and *varieties* (sets of common zeros of polynomials), is still unclear in the equivariant setting. Other classical notions, such as the one of Krull dimension, also deserve to be investigated from the equivariant point of view.

References

[1] Matthias Aschenbrenner and Christopher Hillar. 2007. Finite generation of symmetric ideals. *Trans. Amer. Math. Soc.* 359.11 (2007), 5171–5192.
[2] Matthias Aschenbrenner and Christopher J. Hillar. 2008. An algorithm for finding symmetric Grobner bases in infinite dimensional rings. In *Proc. ISSAC*. ACM, 117–124.

[3] Jason P. Bell and Daniel Smertnig. 2023. Computing the linear hull: Deciding Deterministic? and Unambiguous? for weighted automata over fields. In *2023 38th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*. IEEE, 1–13. doi:10.1109/lics56636.2023.10175691

[4] Michael Benedikt, Timothy Duff, Aditya Sharad, and James Worrell. 2017. Polynomial automata: Zeroness and applications. In *2017 32nd Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*. IEEE, 1–12. doi:10.1109/lics.2017.8005101

[5] Jean Berstel, Dominique Perrin, and Christophe Reutenauer. 2009. *Codes and Automata*. Cambridge University Press. doi:10.1017/cbo9781139195768

[6] Mikołaj Bojańczyk. 2016. *Slightly infinite sets*. https://www.mimuw.edu.pl/~bojan/paper/atom-book Book draft.

[7] Mikołaj Bojańczyk. 2019. The Hilbert method for transducer equivalence. *ACM SIGLOG News* 6, 1 (Feb. 2019), 5–17. doi:10.1145/3313909.3313911

[8] Bruno Buchberger. 1976. A theoretical basis for the reduction of polynomials to canonical forms. *SIGSAM Bull.* 10, 3 (Aug. 1976), 19–29. doi:10.1145/1088216.1088219

[9] David A. Cox, John Little, and Donal O'Shea. 2015. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Springer International Publishing. doi:10.1007/978-3-319-16721-3

[10] Barbara F. Csima, Valentina S. Harizanov, Russell Miller, and Antonio Montalbán. 2011. Computability of Fraïssé Limits. *The Journal of Symbolic Logic* 76, 1 (2011), 66–93. http://www.jstor.org/stable/23043319

[11] Stéphane Demeri, Alain Finkel, Jean Goubault-Larrecq, Sylvain Schmitz, and Philippe Schnoebelen. 2017. Well-Quasi-Orders for Algorithms. (2017). https://wikimpri.dptinfo.ens-paris-saclay.fr/lib/exe/fetch.php?%20media=cours:upload:poly-2-9-1v02oct2017.pdf

[12] Jean Charles Faugère. 2002. A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation* (Lille, France) *(ISSAC '02)*. Association for Computing Machinery, New York, NY, USA, 75–83. doi:10.1145/780506.780516

[13] Moses Ganardi, Rupak Majumdar, Andreas Pavlogiannis, Lia Schütze, and Georg Zetzsche. 2022. Reachability in Bidirected Pushdown VASS. In *49th International Colloquium on Automata, Languages, and Programming (ICALP 2022) (Leibniz International Proceedings in Informatics (LIPIcs), Vol. 229)*, Mikołaj Bojańczyk, Emanuela Merelli, and David P. Woodruff (Eds.). Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl, Germany, 124:1–124:20. doi:10.4230/LIPIcs.ICALP.2022.124

[14] Arka Ghosh, Piotr Hofman, and Slawomir Lasota. 2022. Solvability of orbit-finite systems of linear equations. In *Proc. LICS'22*. ACM, 11:1–11:13.

[15] Arka Ghosh and Sławomir Lasota. 2024. Equivariant ideals of polynomials. In *Proceedings of the 39th Annual ACM/IEEE Symposium on Logic in Computer Science* (Tallinn, Estonia) *(LICS '24)*. Association for Computing Machinery, New York, NY, USA, Article 38, 14 pages. doi:10.1145/3661814.3662074

[16] Graham Higman. 1952. Ordering by divisibility in abstract algebras. *Proceedings of the London Mathematical Society* 3 (1952), 326–336. doi:10.1112/plms/s3-2.1.326

[17] David Hilbert. 1890. Ueber die Theorie der algebraischen Formen. *Math. Ann.* 36, 4 (Dec. 1890), 473–534. doi:10.1007/bf01208503

[18] Christopher J. Hillar, Robert Krone, and Anton Leykin. 2018. Equivariant Gröbner bases. *Advanced Studies in Pure Mathematics* 77 (2018), 129–154.

[19] Christopher J. Hillar and Seth Sullivant. 2012. Finite Gröbner bases in infinite dimensional polynomial rings and applications. *Advances in Mathematics* 229, 1 (2012), 1–25.

[20] Piotr Hofman and Slawomir Lasota. 2018. Linear Equations with Ordered Data. In *29th International Conference on Concurrency Theory, CONCUR 2018, Beijing, China, September 4-7, 2018 (LIPIcs, Vol. 118)*, Sven Schewe and Lijun Zhang (Eds.). Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 24:1–24:17. doi:10.4230/LIPICS.CONCUR.2018.24

[21] Itay Kaplan, Tomasz Rzepecki, and Daoud Siniora. 2021. On the automorphism Group of the Universal homogeneous Meet-Tree. *J. Symb. Log.* 86, 4 (2021), 1508–1540. doi:10.1017/JSL.2021.9

[22] J. B. Kruskal. 1960. Well-Quasi-Ordering, The Tree Theorem, and Vazsonyi's Conjecture. *Trans. Amer. Math. Soc.* 95, 2 (1960), 210–225. http://www.jstor.org/stable/1993287

[23] Serge Lang. 2002. *Algebra* (3 ed.). Springer, New York, NY.

[24] Arka Ghosh Lasota, Piotr Hofman, and Slawomir. 2025. Orbit-finite Linear Programming. *J. ACM* 72, 1 (2025), 1:1–1:39. doi:10.1145/3703909

[25] Dugald Macpherson. 2011. A survey of homogeneous structures. *Discrete Mathematics* 311, 15 (2011), 1599–1634. doi:10.1016/j.disc.2011.01.024 Infinite Graphs: Introductions, Connections, Surveys.

[26] Ernst W Mayr and Albert R Meyer. 1982. The complexity of the word problems for commutative semigroups and polynomial ideals. *Advances in Mathematics* 46, 3 (Dec. 1982), 305–329. doi:10.1016/0001-8708(82)90048-2

[27] Mikolaj Bojanczyk Moerman, Joanna Fijalkow, Bartek Klin, and Joshua. 2024. Orbit-Finite-Dimensional Vector Spaces and Weighted Register Automata. *TheoretiCS* 3 (2024). doi:10.46298/THEORETICS.24.13

[28] Markus Müller-Olm and Helmut Seidl. 2002. *Polynomial Constants Are Decidable*. Springer Berlin Heidelberg, 4–19. doi:10.1007/3-540-45789-5_4

[29] Maurice Pouzet. 2024. Well-quasi-ordering and Embeddability of Relational Structures. *Order* 41, 1 (April 2024), 183–278. doi:10.1007/s11083-024-09664-y

[30] Michal R. Przybylek. 2023. A note on encoding infinity in ZFA with applications to register automata. *CoRR* abs/2304.09986 (2023). doi:10.48550/ARXIV.2304.09986 arXiv:2304.09986

[31] Antoni Puch and Daniel Smertnig. 2024. Factoring through monomial representations: arithmetic characterizations and ambiguity of weighted automata. arXiv:2410.03444v1 [math.GR] https://arxiv.org/abs/2410.03444v1

[32] Fernando Rosa-Velardo and David de Frutos-Escrig. 2011. Decidability and complexity of Petri nets with unordered data. *Theoretical Computer Science* 412, 34 (2011), 4439–4451. doi:10.1016/j.tcs.2011.05.007

A Proofs of Section 3

Lemma 3.5 (S-polynomials). *Let p and q be two polynomials in $\mathbb{K}[\mathcal{X}]$. All the polynomials in $\mathrm{C}_{p,q}$ are obtained by multiplying a monomial with their S-polynomial $\mathrm{S}(p,q)$.*

Proof of Lemma 3.5 as stated on page 6. Let $p, q \in \mathbb{K}[\mathcal{X}]$, and let $r \in \mathrm{C}_{p,q}$. By definition, there exists $\alpha, \beta \in \mathbb{K}$ and $\mathfrak{n}, \mathfrak{m} \in \mathsf{Mon}(\mathcal{X})$ such that $r = \alpha\mathfrak{n}p + \beta\mathfrak{m}q$ and $\mathsf{LM}(r) < \max(\mathfrak{n}\,\mathsf{LM}(p), \mathfrak{m}\,\mathsf{LM}(q))$. In particular, we conclude that $\mathsf{LM}(\mathfrak{n}p) = \mathsf{LM}(\mathfrak{m}q)$, and that $\alpha\,\mathsf{LC}(\mathfrak{n}p) + \beta\,\mathsf{LC}(\mathfrak{m}q) = 0$.

Let us write $\Delta = \mathsf{LCM}(\mathsf{LM}(p), \mathsf{LM}(q))$. Because $\mathsf{LM}(\mathfrak{n}p) = \mathsf{LM}(\mathfrak{m}q)$, there exists a monomial $\mathfrak{l} \in \mathsf{Mon}(\mathcal{X})$ such that $\mathsf{LM}(\mathfrak{n}p) = \mathfrak{l}\Delta = \mathsf{LM}(\mathfrak{m}q)$. Furthermore, we know that $\mathsf{LC}(p)\beta = -\mathsf{LC}(q)\alpha$. As a consequence, one can rewrite r as follows:

$$r = \mathfrak{l}\alpha\,\mathsf{LC}(p)\left[\frac{\Delta}{\mathsf{LT}(p)} \times p - \frac{\Delta}{\mathsf{LT}(q)} \times q\right] = \mathfrak{l}\alpha\,\mathsf{LC}(p) \times \mathrm{S}(p,q)\ .$$

We have concluded. ▹ Back to p.6 □

Lemma 3.4. *Let H be an orbit finite set of polynomials, and let $p \in \mathbb{K}[\mathcal{X}]$ be a polynomial. Then $\mathsf{Rem}_H(p)$ is finite. Furthermore, this computation is equivariant. In particular, $\mathsf{Rem}_H(K)$ is a computable orbit finite set for every orbit finite set K of polynomials.*

Proof of Lemma 3.4 as stated on page 5. Let us write

$$H = \mathsf{orbit}_{\mathcal{G}}(H')\ ,$$

where H' is a finite set of polynomials. Because the relation $\to_H$ is terminating, it suffices to show that for every polynomial p, there are finitely many polynomials r such that $p \to_H r$, leveraging König's lemma. This is because $p \to_H r$ implies that $p = \alpha\mathfrak{n}(\pi{\cdot}q) + r$ for some $q \in H'$, $\alpha \in \mathbb{K}$, $\mathfrak{n} \in \mathsf{Mon}(\mathcal{X})$, and $\pi \in \mathcal{G}$. Because, $\mathsf{LM}(r) \sqsubset^{\mathrm{RevLex}} \mathsf{LM}(p)$, we conclude that $\mathsf{LM}(p) = \mathsf{LM}(\alpha\mathfrak{n}(\pi \cdot q))$, and therefore r is uniquely determined by the choice of $q \in H'$ and the choice of $\pi \in \mathcal{G}$ that maps the domain of q to the domain of p. There are finitely elements in H' and finitely many such functions from $\mathsf{dom}(q)$ to $\mathsf{dom}(p)$ because both domains are finite. ▹ Back to p.5 □

Lemma 3.7. *Assume that the action $\mathcal{G} \curvearrowright \mathcal{X}$ is ω-well-structured. Then, Algorithm 1 terminates on every orbit finite set H of polynomials.*

Proof of Lemma 3.7 as stated on page 6. Let $(H_n)_{n\in\mathbb{N}}$ be the sequence of (orbit finite) sets of polynomials computed by Algorithm 1. We associate to each set H_n the set L_n of characteristic monomials of the polynomials in H_n. Because the set of monomials is a WQO, and because the sequences are non-decreasing for inclusion, there exists an $n \in \mathbb{N}$ such that, for every $\mathfrak{m} \in L_{n+1}$, there exists $\mathfrak{n} \in L_n$, such that $\mathfrak{n} \sqsubseteq^{\mathrm{div}}_{\mathcal{G}} \mathfrak{m}$.

We will prove that $H_{n+1} = H_n$ by contradiction. Assume towards this contradiction that there exists some $r \in H_{n+1} \setminus H_n$. By definition of H_{n+1}, there exists $p, q \in H_n$ such that $r \in \mathsf{Rem}_{H_n}(\mathrm{S}(p,q))$. In particular, r is normalised with respect to H_n. However, because $r \in H_{n+1}$, $\mathsf{CM}(r) \in L_{n+1}$, and therefore there exists $\mathfrak{n} \in L_n$ such that $\mathfrak{n} \sqsubseteq^{\mathrm{div}}_{\mathcal{G}} \mathsf{CM}(r)$. This provides us with a polynomial $t \in H_n$ and an element $\pi \in \mathcal{G}$ such that $\mathsf{CM}(t) \sqsubseteq^{\mathrm{div}} \pi \cdot \mathsf{CM}(r)$. Because H_n is equivariant, we can assume that π is the identity. Hence, there exists $\mathfrak{n} \in \mathsf{Mon}(\mathcal{X})$ such that $\mathsf{CM}(t) \times \mathfrak{n} = \mathsf{CM}(r)$. This means that for every indeterminate $x \in \mathsf{dom}(t)$ we have $x \in \mathsf{dom}(r)$, and then that $\mathsf{LM}(t) \sqsubseteq^{\mathrm{div}} \mathsf{LM}(r)$ by definition of the characteristic monomial. Therefore, one can find some $\alpha \in \mathbb{K}$ such that the polynomial $r' \triangleq r - \alpha\mathfrak{n}t$ satisfies $r' \prec r$, and in particular, $r \to_{H_n} r'$. This contradicts the fact that r is normalised with respect to H_n. ▹ Back to p.6 □

B Proofs of Section 4

Lemma 4.1. *Assume that $\mathcal{G} \curvearrowright \mathcal{X}$ is is effectively oligomorphic, and that $(\mathsf{Mon}_{\mathbb{N}\times\mathbb{N}}(\mathcal{X}), \sqsubseteq^{\mathrm{div}}_{\mathcal{G}})$ is a well-quasi-order. Then* `egb` *is a computable function, and the function* `weakgb` *is called on correct inputs.*

Proof of Lemma 4.1 as stated on page 7. We need to prove that the set $\mathsf{freecol}(H)$ is computable and orbit finite, that $\mathbb{K}[\mathcal{Y}]$ satistfies the computability assumptions of `weakgb`, and that the set $(\mathsf{Mon}(\mathcal{Y}), \sqsubseteq^{\mathrm{div}}_{\mathcal{G}})$ is a well-quasi-ordered set. Finally, we also need to prove that if H is orbit finite, $\mathsf{forget}(H)$ is computable and orbit finite.

Let us start by proving that $\mathsf{freecol}(H)$ is computable and orbit finite. Because H is orbit finite, there exists a finite set $H_0 \subseteq H$ of polynomials such that $\mathsf{orbit}(H_0) = \mathsf{orbit}(H)$. Then, let us remark that $\mathsf{freecol}(H_0)$ can be obtained by considering all finite subsets V of variables that appear in H_0, which is a computable finite set. As a consequence, $\mathsf{freecol}(H_0)$ is computable, and since $\mathsf{freecol}$ is equivariant, $\mathsf{orbit}(\mathsf{freecol}(H_0)) = \mathsf{freecol}(\mathsf{orbit}(H_0)) = \mathsf{freecol}(H)$.

Let us now focus on the set $\mathbb{K}[\mathcal{Y}]$. First, it is clear that $\mathcal{G}$ is compatible with the ordering on $\mathcal{Y}$ by definition of the action, and because $\mathcal{G}$ was compatible with the ordering on $\mathcal{X}$. Then, the action of $\mathcal{G}$ on $\mathcal{Y}$ is effectively oligomorphic since orbits of tuples of $\mathcal{Y}$ can be identified with orbits of tuples of $\mathcal{X}$ together with a coloring in two colors, which is a finite amount of extra information.

Let us now prove that $(\mathsf{Mon}(\mathcal{Y}), \sqsubseteq^{\mathrm{div}}_{\mathcal{G}})$ is a well-quasi-ordered set. A monomial in $\mathsf{Mon}(\mathcal{Y})$ naturally corresponds to a monomial in $\mathsf{Mon}_{\mathbb{N}\times\mathbb{N}}(\mathcal{X})$, where the two exponents are respectively the one of the lower copy and the one of the upper copy of the variable. Because $(\mathsf{Mon}_{\mathbb{N}\times\mathbb{N}}(\mathcal{X}), \sqsubseteq^{\mathrm{div}}_{\mathcal{G}})$ is a well-quasi-ordered set, we immediately conclude that $(\mathsf{Mon}(\mathcal{Y}), \sqsubseteq^{\mathrm{div}}_{\mathcal{G}})$ is a well-quasi-ordered set.

Finally, let us prove that $\mathsf{forget}(H)$ is computable and orbit finite. This is clear because forget simply consists in forgetting the color of the variables. ▹ Back to p.7 □

Lemma 4.2. *Let $H \subseteq \mathbb{K}[\mathcal{X}]$, then $\mathsf{egb}(H)$ generates $\langle H \rangle_{\mathcal{G}}$.*

Proof of Lemma 4.2 as stated on page 7. Let us remark that

$$\mathsf{forget}(\mathsf{freecol}(H)) = H \quad . \tag{8}$$

Since $\mathsf{weakgb}(\mathsf{freecol}(H))$ generates the same ideal as $\mathsf{freecol}(H)$, and since forget is a morphism, we conclude that the set of polynomials $\mathsf{forget}(\mathsf{weakgb}(\mathsf{freecol}(H)))$ generates the same ideal as $\mathsf{forget}(\mathsf{freecol}(H)) = H$. ▹ Back to p.7 □

Corollary 1.2. *Assume that $\mathcal{G} \curvearrowright \mathcal{X}$ is effectively oligomorphic and well-structured. Then one has an* effective representation *of the equivariant ideals of $\mathbb{K}[\mathcal{X}]$, such that:*

(1) *One can obtain a representation from an orbit-finite set of generators,*

(2) *One can effectively decide the equivariant ideal membership problem given a representation,*
(3) *The following operations are computable at the level of representations: the union of two equivariant ideals, the product of two equivariant ideals, the intersection of two equivariant ideals, and checking whether two equivariant ideals are equal.*

Proof of Corollary 1.2 as stated on page 2. Most of this statement follows from Theorem 1.1, using equivariant Gröbner bases as a representation of equivariant ideals. Indeed, because $\mathbb{N} \times \mathbb{N}$ is a well-quasi-ordered set, we conclude $(\mathrm{Mon}_{\mathbb{N}\times\mathbb{N}}(\mathcal{X}), \sqsubseteq_{\mathcal{G}}^{\mathrm{div}})$ is a well-quasi-ordered set too. The only non-trivial part is the fact that one can compute an equivariant Gröbner basis of the *intersection* of two equivariant ideals. To that end, we will adapt the classical argument using Gröbner bases to the case of equivariant Gröbner bases [9, Chapter 4, Theorem 11].

Let I and J be two equivariant ideals of $\mathbb{K}[\mathcal{X}]$, respectively represented by equivariant Gröbner bases $\mathcal{B}_I$ and $\mathcal{B}_J$. Let t be a fresh indeterminate, and let us consider $\mathcal{Y} \triangleq \mathcal{X} + \{t\}$, that is, the disjoint union of $\mathcal{X}$ and $\{t\}$, where t is greater than all the variables in $\mathcal{X}$.

We construct the equivariant ideal T of $\mathbb{K}[\mathcal{Y}]$, generated by all the polynomials $t \times h_i$, and $(1-t) \times h_j$, where h_i ranges over $\mathcal{B}_I$ and h_j ranges over $\mathcal{B}_J$. It is clear that $T \cap \mathbb{K}[\mathcal{X}] = I \cap J$. Now, because of the hypotheses on $\mathcal{X}$, we know that one can compute the equivariant Gröbner basis $\mathcal{B}_T$ of T by applying egb to the generating set of T. Finally, we can obtain the equivariant Gröbner basis of $I \cap J$ by considering $\mathcal{B}_T \cap \mathbb{K}[\mathcal{X}]$, that is, selecting the polynomials of $\mathcal{B}_T$ that do not contain the indeterminate t, which is possible because $\mathcal{B}_T$ is an orbit-finite set and $\mathbb{K}[\mathcal{Y}]$ is effectively oligomorphic. ▹ Back to p.2 □

C Proof of Section 5

C.1 Homogenous ordered meet-tree

Arka: Check the proof and replace "meet-tree" with "ordered meet-tree"

A *meet-tree* is a structure $(T, \prec_T, \wedge_T)$ where

(1) $\prec_T$ is a partial order (called *ancestry*),
(2) for every $a \in T$ the set $\{x \in T \mid x \preceq_T a\}$ is linearly ordered,
(3) T has a smallest element with respect to $\prec$ which is called the *root* of T (written as $\textsc{root}(T)$),
(4) $\wedge_T$ is a binary operation computing the *greatest common lower bound* operation of its inputs.

An *ordered meet-tree* is a structure $(T, \prec_T, \wedge_T, <_T)$ where $(T, \prec_T)$ is a *meet-tree* and $<_T$ is a linear order extending $\prec$ such that for every $a \leq_T b$, $a \preceq_T a'$ and $b \preceq_T b'$, we have $a' \leq_T b'$. Essentially, $<_T$ is induced by a *depth first search*.

To show existence of a *homogenous ordered meet-tree* we show that the class of such trees are closed under *amalgamation*, i.e., for every pair of embeddings $(f : A \to B, g : A \to C)$ there exists another pair of embeddings $(f' : B \to D, g' : C \to D)$ such that $f' \circ f = g' \circ g$.

We build D by extending A. This extension is done in three steps.

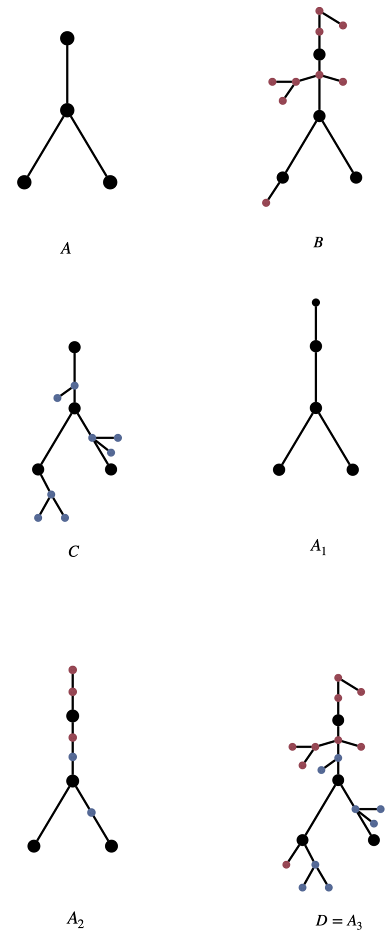

Figure 2: Amalgamation of finite ordered meet-tree

Step 1: Add an element r to A that is smaller than $\textsc{root}(A)$. Observe that r is the root of the resulting tree. Call this is tree A_1. At this point f' and g' is defined only on $f(A)$ and $g(B)$, respectively.

Definition C.1. For two nodes $x \preceq_T y$ in a meet-tree T, we use $I(x, y)$ to denote the *interval* between x and y

$$I(x, y) \stackrel{\text{def}}{=} \{z \in T \mid x \preceq_T z \preceq_T y\} .$$

Step 2: Let R_B (resp. R_C) be the set of nodes of B (resp. C) that belong to some interval between nodes in $f(B) \cup \{\textsc{root}(B)\}$ (resp. $g(C) \cup \{\textsc{root}(C)\}$). Add enough nodes in the intervals between nodes in A_1 such that f' (resp. g') can be extended to R_B (resp. R_C). Call this is tree A_2.

Step 3: Extend A_2 by adding enough subtrees to its nodes such that f' (resp. g') can be extended to subtrees rooted at R_B (resp. R_C). Call this tree $A_3 = D$.

We leave it to the reader to check the correctness of this construction.

D Proofs of Section 6

Lemma 6.7. *Let P, Q be two finite paths in $\mathcal{X}$, such that (p_0, p_1) is in the same orbit as (q_0, q_1). Let $u, v, w \in \Sigma^*$ be three words, such that $|u| = |v| \leq |w|$, and let $\mathfrak{n} \in \mathrm{Mon}(\mathcal{X})$ be a monomial. Assume that there exists $\pi \in \mathcal{G}$ such that $\llbracket w \rrbracket_P = \mathfrak{m}(\pi \cdot \llbracket u \rrbracket_Q)$, $\mathfrak{n} = \mathfrak{m}(\pi \cdot \llbracket v \rrbracket_Q)$, and that $\llbracket w \rrbracket_P$, $\llbracket u \rrbracket_Q$ and $\llbracket v \rrbracket_Q$ are well-defined. Then, there exists $x, y \in \Sigma^*$ such that $xuy = w$ and $\llbracket xvy \rrbracket_P = \mathfrak{n}$.*

Proof of Lemma 6.7 as stated on page 11. Let us write $\pi \cdot q_0 = p_k$ for some $k \in \mathbb{N}$. Because the only indeterminates with degree 4 in $\llbracket w \rrbracket_P$ are the ones of the form p_{4i}, we have that k is a multiple of 4 (i.e. at the start of a letter block). Since (q_0, q_1) is in the same orbit as (p_0, p_1), and both P and Q are finite paths, we conclude that $\pi \cdot (q_0, q_1) = (p_{4i}, p_{4i+1})$ or $\pi \cdot (q_0, q_1) = (p_{4i+1}, p_{4i-1})$. Applying the same reasoning, thrice, we have either $\pi \cdot (q_0, q_1, q_2, q_3) = (p_{4i}, p_{4i+1}, p_{4i+2}, p_{4i+3})$ or $\pi \cdot (q_0, q_1, q_2, q_3) = (p_{4i}, p_{4i-1}, p_{4i-2}, p_{4i-3})$. However, in the second case, the exponent of p_{4i-3} in $\llbracket w \rrbracket_P$ is at most 2, which is incompatible with the fact that the one of q_3 in $\llbracket u \rrbracket_Q$ is 3. By induction on the length of u, we immediately obtain that $\pi \cdot \llbracket u \rrbracket_Q = \mathrm{shift}_{+4i} \cdot \llbracket u \rrbracket_P$ and therefore that $w = xuy$ for some $x, y \in \Sigma^*$. Finally, because $\llbracket v \rrbracket_Q$ uses exactly the same indeterminates as $\llbracket u \rrbracket_Q$, we can also conclude that $\llbracket xvy \rrbracket_P = \mathfrak{n}$. ▹ Back to p.11 □

Lemma 6.8. *Let us fix (x_0, x_1) a pair of indeterminates. There exists a monomial rewrite system R_M such that the following are equivalent for every $n \geq 1$, and for any finite path P of length $4(n+2)$ such that (p_0, p_1) is in the same orbit as (x_0, x_1):*

1. $\llbracket \triangleright^{run} q_0 \square^{n-1} \triangleleft^{run} \rrbracket_P \leftrightarrow^*_{R_M} \llbracket \triangleright^{run} q_f \square^{n-1} \triangleleft^{run} \rrbracket_P$,
2. *M halts on the empty word using a tape bounded by $n-1$ cells.*

Furthermore, every monomial that is reachable from $\llbracket \triangleright^{run} q_0 \square^{n-1} \triangleleft^{pre} \rrbracket_P$ or $\llbracket \triangleright^{run} q_f \square^{n-1} \triangleleft^{run} \rrbracket_P$ is the image of a word of the form $\llbracket \triangleright^{run} u \triangleleft^{run} \rrbracket_P$ where $u \in (Q \uplus \Sigma \uplus \square)^n$.

Proof of Lemma 6.8 as stated on page 12. Transitions of the deterministic reversible Turing machine using bounded tape size can be modelled as a reversible string rewriting system using finitely many rules of the form $u \leftrightarrow v$, where u and v are words over $(Q \uplus \Sigma \uplus \square)$ having the same length ℓ. For each rule $u \leftrightarrow v$, we create rules $\llbracket u \rrbracket_P \leftrightarrow_{R_M} \llbracket v \rrbracket_P$ for every finite path P of length 4ℓ. Note that there are only orbit finitely many such finite paths P, and one can effectively list some representatives, because $\mathcal{X}$ is effectively oligomorphic. This system is clearly complete, in the sense that one can perform a substitution by applying a monomial rewriting rule, but Lemma 6.7 also tells us it is correct, in the sense that it cannot perform anything else than string substitutions. Furthermore, we can assume that the reversible Turing machine starts with a clean tape and ends with a clean tape. ▹ Back to p.12 □

Lemma 6.9. *Let (x_0, x_1) be a pair of indeterminates, P be a finite path such that (p_0, p_1) is in the same orbit as (x_0, x_1). There exists a monomial rewrite system R_{pre} such that for every monomial $\mathfrak{m} \in \mathrm{Mon}(\mathcal{X})$, the following are equivalent:*

1. $\llbracket \triangleright^{pre} \square \square_1 \square_2 \triangleleft^{pre} \rrbracket_P \leftrightarrow^*_{R_{pre}} \mathfrak{m}$ *and* $\llbracket \triangleright^{run} \rrbracket_{P'} \sqsubseteq^{\mathrm{div}}_{\mathcal{G}} \mathfrak{m}$ *for some finite path P' such that (p'_0, p'_1) is in the same orbit as (x_0, x_1).*
2. *There exists $n \geq 2$ and a finite path P' such that (p'_0, p'_1) is in the same orbit as (x_0, x_1), and $\mathfrak{m} = \llbracket \triangleright^{run} q_0 \square^n \triangleleft^{run} \rrbracket_{P'}$.*

Similarly, there exists a monomial rewrite system R_{post} with analogue properties using q_f instead of q_0.

Proof of Lemma 6.9 as stated on page 12. We create the following rules, where P_1 and P_2 range over finite paths such that their first two elements are in the same orbit as (x_0, x_1), and assuming that the indeterminates of P_1 and P_2 are disjoint:

1. Cell creation:
$$\llbracket \triangleright^{\mathrm{pre}} \square \rrbracket_{P_1} \llbracket \square_1 \square_2 \triangleleft^{\mathrm{pre}} \rrbracket_{P_2} \leftrightarrow_{R_{\mathrm{pre}}} \llbracket \triangleright^{\mathrm{pre}} \square_1 \rrbracket_{P_1} \llbracket \square\square\square_2 \triangleleft^{\mathrm{pre}} \rrbracket_{P_2}$$
2. Linearity checking:
$$\llbracket \square_1 \square \rrbracket_{P_1} \llbracket \square_2 \triangleleft^{\mathrm{pre}} \rrbracket_{P_2} \leftrightarrow_{R_{\mathrm{pre}}} \llbracket \square\square_1 \rrbracket_{P_1} \llbracket \square_2 \triangleleft^{\mathrm{pre}} \rrbracket_{P_2}$$
3. Phase transition:
$$\llbracket \triangleright^{\mathrm{pre}} \square \rrbracket_{P_1} \llbracket \square_1 \square_2 \triangleleft^{\mathrm{pre}} \rrbracket_{P_2} \leftrightarrow_{R_{\mathrm{pre}}} \llbracket \triangleright^{\mathrm{run}} q_0 \rrbracket_{P_1} \llbracket \square\square \triangleleft^{\mathrm{run}} \rrbracket_{P_2}$$

Note that there are only orbit finitely many such pairs of monomials, and that we can enumerate representative of these orbits because $\mathcal{X}$ is effectively oligomorphic.

Let us first argue that this system is complete. Because there exists an infinite path P_∞, it is indeed possible to reach $\llbracket \triangleright^{\mathrm{run}} q_0 \square^n \triangleleft^{\mathrm{run}} \rrbracket_{P_\infty}$ by repeatedly applying the first rule, and then the second rule until $\square_1$ reaches the end of the tape, and continuing so until one decides to apply the third rule to reach the desired tape configuration.

We now claim that the system is correct, in the sense that it can only reach valid tape encodings. First, let us observe that in a rewrite sequence, one can always assume that the rewriting takes the form of applying the first rule, then the second rule until one cannot apply it anymore, and repeating this process until one applies the third rule. Because rule (2) ensures that when we add new indeterminates using rule (1), they were not already present in the monomial, and because rule (1) ensures that locally the structure of the indeterminates remains a finite path, we can conclude that the whole set of indeterminates used come from a finite path P'. As a consequence, if one can reach a state where (2) or (3) are applicable, then the tape is of the form $\llbracket \triangleright^{\mathrm{pre}} \square^n \square_1 \square_2 \triangleleft^{\mathrm{pre}} \rrbracket_{P'}$, with $n \geq 1$. It follows that when one can apply rule (3), the monomial obtained is of the form $\llbracket \triangleright^{\mathrm{run}} q_0 \square^n \triangleleft^{\mathrm{run}} \rrbracket_{P'}$, where P' is a finite path such that (p'_0, p'_1) is in the same orbit as (x_0, x_1). ▹ Back to p.12 □

Remark 6.11. Given an oligomorphic set of indeterminates $\mathcal{X}$, it is equivalent to say that $\mathcal{X}$ contains an infinite path or to say that it contains finite paths of arbitrary length.

Proof of Remark 6.11 as stated on page 12. Assume that there are arbitrarily long finite paths in $\mathcal{X}$. Then, one can create an infinite tree whose nodes are representatives of (distinct) orbits of finite paths, whose root is the empty path, and where the ancestor relation is obtained by projecting on a subset of indeterminates. Because $\mathcal{X}$ is oligomorphic, there are finitely many nodes at each depth in the tree (i.e. at each length of the finite path). Hence, there exists an infinite branch in the tree due to König's lemma, and this branch is a witness for the existence of an infinite path in $\mathcal{X}$. ▹ Back to p.12 □

Example 6.13. Let $\mathcal{X}$ be an oligomorphic infinite set of indeterminates. Then $\mathcal{X} \times \mathcal{X}$ contains a (generalised) infinite path as defined in Remark 6.10.

Proof of Example 6.13 as stated on page 12. Let $(x_i)_{i\in\mathbb{N}}$ and $(y_i)_{i\in\mathbb{N}}$ be two infinite sets of distinct indeterminates in $\mathcal{X}$. Let us define $P \triangleq (x_0, y_0), (x_1, y_0), (x_1, y_1), (x_2, y_1), \ldots$. The orbits of pairs that define the successor relation are the orbits of $((x_i, y_j), (x_k, y_l))$, where $x_i = x_k$ and $y_j \neq y_l$, or where $x_i \neq x_k$ and $y_j = y_l$. Because $\mathcal{X}$ is oligomorphic, there are finitely many such orbits. Let us sketch the fact that this defines a generalised path. Consider that $((x_i, y_j), (x_k, y_l))$ is in the same orbit as $((x_0, y_0), (x_1, y_0))$, then there exists $\pi \in \mathcal{G}$ such that $\pi \cdot (x_i, y_j) = (x_0, y_0)$ and $\pi \cdot (x_k, y_l) = (x_1, y_0)$, but then $\pi \cdot y_j = \pi \cdot y_l = y_0$, and because π is invertible, $y_j = y_l$. Similarly, we conclude that $x_i \neq x_k$. The same reasoning shows that if $((x_i, y_j), (x_k, y_l))$ is in the same orbit as $((x_0, y_0), (x_0, y_1))$, then $y_j \neq y_l$ and $x_i = x_k$. ▹ Back to p.12 □

E Proofs of Section 5.3

Proof of Theorem 5.13 as stated on page 10. Let us consider an orbit finite polynomial automaton $A = (Q, \delta, q_0, F)$. Following the classical *backward procedure* for such systems, we will compute a sequence of sets $E_0 \triangleq \{q \in Q \mid F(q) = 0\}$, and $E_{i+1} \triangleq \mathrm{pre}^{\forall}(E_i) \cap E_i$, where $\mathrm{pre}^{\forall}(E)$ is the set of states $q \in Q$ such that for every $a \in \Sigma$, $\delta^*(q, a) \in E$. We will prove that the sequence of sets E_i stabilises, and that it is computable. As an immediate consequence, it suffices to check that $q_0 \in E_\infty$, where E_∞ is the limit of the sequence $(E_i)_{i\in\mathbb{N}}$, to decide the zeroness problem.

The only idea of the proof is to notice that all the sets E_i are representable as zero-sets of equivariant ideals in $\mathbb{K}[\mathcal{X}]$, allowing us to leverage the effective computations of Corollary 1.2. Given a set H of polynomials, we write $\mathcal{V}(H)$ the collections of states $q \in Q$ such that $p(q) = 0$ for all $p \in H$. It is easy to see that $E_0 = \mathcal{V}(\{F\}) = \mathcal{V}(\mathcal{I}_0)$, where $\mathcal{I}_0$ is the equivariant ideal generated by F, since $F \in \mathbb{K}[V]$ and V is invariant under the action of $\mathcal{G}$. Furthermore, assuming that $E_i = \mathcal{V}(\mathcal{I}_i)$, we can see that

$$\begin{aligned}
\mathrm{pre}^{\forall}(E_i) &= \{q \in Q \mid \forall a \in \mathcal{X}, \delta^*(a, q) \in E_i\} \\
&= \{q \in Q \mid \forall a \in \mathcal{X}, \forall p \in \mathcal{I}_i, p(\delta^*(a, q)) = 0\} \\
&= \{q \in Q \mid \forall p' \in \mathcal{J}, p'(q) = 0\}
\end{aligned}$$

Where, the equivariant ideal $\mathcal{J}$ is generated by the polynomials $\mathrm{pullback}(p, a) \triangleq p[x \mapsto \delta(a, x)]$ for every pair $(p, a) \in \mathcal{I}_i \times \mathcal{X}$. As a consequence, we have $E_{i+1} = \mathcal{V}(\mathcal{I}_{i+1})$, where $\mathcal{I}_{i+1} = \mathcal{I}_i + \mathcal{J}$. Because the sequence $(\mathcal{I}_i)_{i\in\mathbb{N}}$ is increasing, and thanks to the equivariant Hilbert basis property of $\mathbb{K}[\mathcal{X}]$, there exists an $n_0 \in \mathbb{N}$ such that $\mathcal{I}_{n_0} = \mathcal{I}_{n_0+1} = \mathcal{I}_{n_0+2} = \cdots$. In particular, we do have $E_{n_0} = E_{n_0+1} = E_{n_0+2} = \cdots$.

Let us argue that we can compute the sequence $\mathcal{I}_i$. First, $\mathcal{I}_0 = \langle F \rangle_{\mathcal{G}}$ is finitely represented. Now, given an equivariant ideal $\mathcal{I}$, represented by an orbit finite set of generators H, we can compute the equivariant ideal $\mathcal{J}$ generated by the polynomials $\mathrm{pullback}(p, a) \triangleq p[x_i \mapsto \delta(a)(x_i)]$ for every pair $(p, a) \in H \times \mathcal{X}$. Indeed, $H \times \mathcal{X}$ is orbit finite, and the function pullback is computable and equivariant: given $\pi \in \mathcal{G}$, we can show that

$$\begin{aligned}
&\pi \cdot \mathrm{pullback}(p, a) \\
&= \pi \cdot (p[x_i \mapsto \delta(a, x_i)]) && \text{by definition} \\
&= p[x_i \mapsto (\pi \cdot \delta(a, x_i))] && \pi \text{ acts as a morphism} \\
&= p[x_i \mapsto \delta(\pi \cdot a, \pi \cdot x_i))] && \delta \text{ is equivariant} \\
&= (\pi \cdot p)[x_i \mapsto \delta(\pi \cdot a, x_i)] && \text{definition of substitution} \\
&= \mathrm{pullback}(\pi \cdot p, \pi \cdot a). && \text{by definition.}
\end{aligned}$$

Finally, one can detect when the sequence stabilises, by checking whether $\mathcal{I}_i = \mathcal{I}_{i+1}$, which is decidable because the equivariant ideal membership problem is decidable by Theorem 1.1.

To conclude, it remains to check whether $q_0 \in E_\infty$, which amounts to check that $q_0 \in \mathcal{V}(\mathcal{I}_\infty)$. This is equivalent to checking whether for every element $p \in \mathcal{B}$ where $\mathcal{B}$ is an equivariant Gröbner basis of $\mathcal{I}_\infty$, we have $p(q_0) = 0$, which can be done by enumerating relevant orbits. ▹ Back to p.10 □

Received 20 February 2007; revised 12 March 2009; accepted 5 June 2009