



Sparse polynomial equations and other enumerative problems whose Galois groups are wreath products

A. Esterov¹ · L. Lang²

Accepted: 12 November 2021
© The Author(s) 2021

Abstract

We introduce a new technique to prove connectivity of subsets of covering spaces (so called inductive connectivity), and apply it to Galois theory of problems of enumerative geometry. As a model example, consider the problem of permuting the roots of a complex polynomial $f(x) = c_0 + c_1x^{d_1} + \dots + c_kx^{d_k}$ by varying its coefficients. If the GCD of the exponents is d , then the polynomial admits the change of variable $y = x^d$, and its roots split into necklaces of length d . At best we can expect to permute these necklaces, i.e. the Galois group of f equals the wreath product of the symmetric group over d_k/d elements and $\mathbb{Z}/d\mathbb{Z}$. We study the multidimensional generalization of this equality: the Galois group of a general system of polynomial equations equals the expected wreath product for a large class of systems, but in general this expected equality fails, making the problem of describing such Galois groups unexpectedly rich.

Keywords Enumerative geometry · Topological Galois theory · Galois covering · Monodromy · Newton polytope

Mathematics Subject Classification 14E20 · 14H05 · 14M25 · 14N10 · 20B20 · 52B20 · 58K10

A. Esterov: The author is partially supported by International Laboratory of Cluster Geometry NRU HSE, RF Government grant, ag. N 075-15-2021-608 dated 08.06.2021.

✉ L. Lang
lionel.lang@hig.se

A. Esterov
aesterov@hse.ru

¹ HSE University, Usacheva str., 6, Moscow 119048, Russia

² Department of Electrical Engineering, Mathematics and Science, University of Gävle, Gävle, Sweden

Contents

1	Introduction and main results	1
1.1	Sparse polynomial equations	1
1.2	Systems of sparse equations	1
1.3	Galois groups of non-reduced systems	1
1.4	Techniques and perspectives	1
2	Enumerative problems	2
2.1	Enumerative problems	2
2.2	Wreath enumerative problems	2
2.3	Powers of enumerative problems	2
3	Inductive connectivity	3
3.1	Inductive covers and solution lattices	3
3.2	Application to sparse polynomial equations	3
3.3	Lifting connectivity in covering spaces	3
3.4	Inductive connectivity	3
3.5	Proof of INDUCTIVE CONNECTIVITY THEOREM 1.14	3
3.6	Proof of Wreath product theorem 3.7	3
4	Galois groups of systems of sparse polynomial equations	4
4.1	Analogous systems of equations	4
4.2	Resultants	4
4.3	The main result	4
4.4	Preliminaries from lattice geometry	4
4.5	Preliminaries from toric geometry	4
4.6	Proof of Main Theorem 4.14.2	4
4.7	Proving inductive disconnectedness	4
	References	4

1 Introduction and main results

1.1 Sparse polynomial equations

Consider the set A of integer numbers

$$0 = a_0 < a_1 < \cdots < a_k = a$$

and the space \mathbb{C}^A of all complex polynomials of the form

$$f(x) = c_0 + c_1 x^{a_1} + \cdots + c_k x^{a_k}. \quad (1)$$

As f travels along a loop in \mathbb{C}^A , avoiding the discriminant $D = \{\text{polynomials with less than } a \text{ roots}\}$, its roots undergo a permutation. The group of all such permutations G_A is called the *monodromy group*, or the *Galois group* of the polynomial. It is naturally a subgroup of the permutation group \mathfrak{S}_a over a elements.

Remark 1.1 The latter name comes from the fact that G_A equals the Galois group of the corresponding extension of the field $\mathbb{C}(c_0, \dots, c_k)$. In this way the definition of the group G_A extends from polynomials over complex numbers to an arbitrary field. Over fields of positive characteristic, this group has been thoroughly studied especially for trinomials ($k = 2$), but the complete answer is not known so far: [5, 6,

[25,26,30]. A well known related project, originating from [1] and culminating in [2], is Abhyankar's identification of many interesting groups as Galois groups of trinomials whose coefficients are powers of the same parameter. In what follows, we restrict ourselves to the complex setting.

The following fact is widely known, see e.g. [5,6] or [15] for the algebraic and the topological proof respectively.

Observation 1.2 If a_1, \dots, a_k are mutually prime, then $G_A = \mathfrak{S}_a$.

The assumption here cannot be relaxed: if $d := \text{GCD}(a_1, \dots, a_k)$ is greater than 1, then the group G_A is strictly smaller than \mathfrak{S}_a . Indeed, the equation $f(x) = 0$ has the form $\tilde{f}(x^d) = 0$. In particular, every root y of \tilde{f} gives rise to the oriented necklace of d roots of f of the form $\sqrt[d]{y}$. At best, we can expect to permute these a/d necklaces. The group of permutations of a disjoint union of oriented necklaces is a simple example of a wreath product.

Definition 1.3 Let S be a finite set, H and G be two groups and $\varphi : G \rightarrow \mathfrak{S}(S)$ an action of G on S . The *wreath product* $H \wr_{\varphi} G$ is the semidirect product of H^S and G with respect to the action of G on H^d given by $g \cdot f = f \circ \varphi(g)$ for any element $f : S \rightarrow H$ of H^S .

Remark 1.4 We will mostly consider the case when φ is injective, that is G is a subgroup of the group of permutation $\mathfrak{S}(S)$ on S . In such case, we will simply denote the wreath product by $H \wr G$. This group can be seen as the group of all permutations σ of the set $H \times S$, satisfying the following properties:

1) σ can be included into the commutative diagram

$$\begin{array}{ccc} H \times S & \xrightarrow{\sigma} & H \times S \\ \downarrow & & \downarrow \\ S & \longrightarrow & S \end{array}$$

where the vertical arrows are the standard projection, and the bottom arrow belongs to G .

2) The restriction of σ to $H \times \{i\} \rightarrow H \times \{j\}$ for every i is the multiplication by an element of H .

In particular, if H is cyclic of order d , then $H \wr \mathfrak{S}_a$ is the group of permutations of a oriented necklaces of length d .

Proposition 1.5 For $d := \text{GCD}(a_1, \dots, a_k)$, we have $G_A = (\mathbb{Z}/d\mathbb{Z}) \wr \mathfrak{S}_{a/d}$, i.e. the monodromy group G_A includes all permutations of the roots of the Eq. (1) that preserve the necklace structure.

It was proved in [9, Theorem 2.1], motivated by the study of linear recurrent sequences over functional fields. We shall deduce it as a special case of a certain new general fact about the monodromy of enumerative problems: it is a consequence of WREATH PRODUCT THEOREM 3.7 and Lemma 3.8, see Sect. 3.2.

Remark 1.6 It would be interesting to give this fact an algebraic proof and to understand to what extent it survives the positive characteristic.

1.2 Systems of sparse equations

As we observed, the Galois group G_A of a support set $A \subset \mathbb{Z}$ obeys a simple dichotomy dictated by $\text{GCD}(A)$. We now discuss the situation of a system of several equations in several variables. The outcome will turn out to be quite different.

Identifying a point $a := (a_1, \dots, a_n) \in \mathbb{Z}^n$ with the monomial $x^a := x_1^{a_1} \dots x_n^{a_n}$, every finite set $P \subset \mathbb{Z}^n$ gives rise to the vector space $\mathbb{C}^P = \{\sum_{a \in P} c_a x^a\}$ of *Laurent polynomials supported at P* . Every such polynomial defines a function on the *complex torus* $T := (\mathbb{C}^\star)^n$.

For a tuple of finite sets $A := (A_1, \dots, A_n)$, $A_i \subset \mathbb{Z}^n$, a tuple $f := (f_1, \dots, f_n)$ from the space $\mathbb{C}^A := \mathbb{C}^{A_1} \oplus \dots \oplus \mathbb{C}^{A_n}$ can be regarded as a system of polynomial equations $f = 0$ in the torus T . According to the Kouchnirenko–Bernstein theorem [4, Theorem A], the number d of solutions of this system equals the mixed volume of the convex hulls of A_1, \dots, A_n unless the tuple f belongs to a certain proper Zariski closed subset $D \subset \mathbb{C}^A$, called the *bifurcation set*. As in the previous section, the loops in $\mathbb{C}^A \setminus D$ based at a given tuple f induce a permutation on the set of solutions of the system $f = 0$ and give rise to the monodromy/Galois group $G_A \subset \mathfrak{S}_d$.

Theorem 1.7 [15, Theorem 1.5] *The Galois group G_A equals the symmetric group \mathfrak{S}_d , if A is reduced and irreducible in the following sense.*

Definition 1.8 A tuple of finite sets $A := (A_1, \dots, A_n)$, $A_i \subset \mathbb{Z}^n$, (and the corresponding system of equations with indeterminate coefficients) is said to be *non-reduced* if all sets can be shifted to the same proper sublattice, and *reducible* if k of them can be shifted to a rank k sublattice for some $k < n$.

Example 1.9 The equation with indeterminate coefficients $c_8 x^8 + c_4 x^4 + c_0 = 0$ supported at $\{0, 4, 8\}$ is non-reduced. A system of the form $f(x) = g(x, y) = 0$ is reducible.

Remark 1.10 1) There is no loss of generality in assuming that $0 \in A_i$ for $i = 1, \dots, n$. Indeed, we can divide every equation of a system by a certain monomial so that the resulting system satisfies the above assumption. Since dividing by a monomial does not affect the roots of the system in the complex torus, the resulting system has the same monodromy group as the initial one. Therefore, we will always work under this assumption throughout this paper.

2) Under this assumption, we can interpret non-reduced systems as systems that can be simplified by a monomial change of variables, and reducible systems as systems that have a proper square subsystem of equations upon an appropriate monomial change of coordinates, as in the preceding example.

3) The most natural source of systems of sparse equations comes from the theory of Newton polytopes, when $A_1 = \dots = A_n$ is the set of lattice points of a lattice polytope P . Note that even in this case, starting from dimension 3, such systems may be non-reduced, i.e. the lattice points of the polytope P may not generate the ambient lattice. Such polytopes are called non-reduced or non-spanning, see e.g. [21] for the classification up to volume 4 (which extends to the mixed case using [3]).

4) Mind the difference between non-reduced and reducible (i.e. non-irreducible). The terms reflect the fact that discriminants and other geometric objects, related to

the system of equations $f = 0$ for the general tuple $f \in \mathbb{C}^A$, tend to be reduced and irreducible in the sense of algebraic geometry if the tuple $A = (A_1, \dots, A_n)$ has the property of the same name. See e.g. Remark 3.17 and Theorem 3.21 in [15] for details. Note that some authors use the terms “lacunary” and “triangular” instead of “non-reduced” and “reducible”.

1.3 Galois groups of non-reduced systems

The dichotomy between reduced and non-reduced systems is the multidimensional generalisation of the dichotomy given by the GCD for the one-dimensional support sets considered in Sect. 1.1. According to Remark 1.10.2), the assumptions of Theorem 1.7 are optimal, that is the Galois group G_A is not the full symmetric group if A is either reducible or non-reduced. In the present paper, we focus on non-reduced systems and assume irreducibility (because reducible systems deserve a separate study that would make use of the results of the present paper).

Let $\tilde{N} \simeq \mathbb{Z}^n$ be a lattice and $\tilde{A} := (\tilde{A}_1, \dots, \tilde{A}_n)$, $\tilde{A}_i \subset \tilde{N}$, be a non-reduced irreducible tuple. Then, there exist a lattice $N \simeq \mathbb{Z}^n$, a reduced irreducible tuple $A = (A_1, \dots, A_n)$, $A_i \subset N$, and a proper linear embedding $L : N \rightarrow \tilde{N}$ such that $\tilde{A}_i = L(A_i)$ for $i = 1, \dots, n$. We call the tuple A a *reduction* of \tilde{A} .

Remark 1.11 The reduction A of \tilde{A} is unique up to affine linear automorphism of N .

Given a reduction A of a non-reduced tuple $\tilde{A} = L(A)$, denote by $T := \text{Hom}(N, \mathbb{C}^*)$, by $\tilde{T} := \text{Hom}(\tilde{N}, \mathbb{C}^*)$ and by $\phi_L : \tilde{T} \rightarrow T$ the map of tori induced by L . In coordinates, this is a monomial change of variables that takes every $f \in \mathbb{C}^A$ to $\tilde{f}(x) := f(\phi_L(x)) \in \mathbb{C}^{\tilde{A}}$. The map assigning \tilde{f} to f is an isomorphism of vector spaces $\mathbb{C}^{\tilde{A}} \rightarrow \mathbb{C}^A$. As a consequence, we have a natural injection

$$G_{\tilde{A}} \hookrightarrow \ker \phi_L \wr \mathfrak{S}_d, \quad (2)$$

see Observation 2.5.

The main interest of this paper is to determine whether (2) is an isomorphism. In contrast to the one-dimensional case, we will see that the answer depends upon the support \tilde{A} . Already in dimension 2, there exist non-reduced supports \tilde{A} for which the inclusion (2) is proper, see Example 1.13 below. This observation turns the determination of Galois groups of the form $G_{\tilde{A}}$ into an unexpectedly rich and challenging problem that can be addressed in two steps:

- (A) *determine the irreducible non-reduced supports \tilde{A} for which (2) is an isomorphism,*
- (B) *compute the $G_{\tilde{A}}$ whenever (2) is a proper inclusion.*

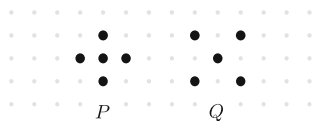
Here, we will exclusively address (A) by providing criteria ensuring that (2) is an isomorphism as well as criteria ensuring that (2) is proper. In particular, we show that (2) is an isomorphism for a large class of systems of equations. For the sake of this introduction, we state below a simplified version of our main result in dimension 2.

For a finite subset $B \in \mathbb{Z}^n$, denote the intersection of B with the boundary of its convex hull by ∂B .

Proposition 1.12 *Assume that $n = 2$, $\tilde{A}_1 = \tilde{A}_2 =: B$, and (with no loss of generality) that $0 \in \partial B$. Then, for $\tilde{A} := (\tilde{A}_1, \tilde{A}_2)$, the Galois group $G_{\tilde{A}}$ equals the expected wreath product (2) provided that ∂B generates the same sublattice of \mathbb{Z}^2 as B .*

In Sect. 4, we prove a generalization of this fact (Theorem 4.5 and its stronger version, MAIN THEOREM 4.14) for arbitrary dimension and tuples of non-equal support sets. For all tuples of the form $A_1 = \dots = A_n \subset \mathbb{Z}^n$ and more general tuples that we refer to as analogous, we achieve step (A).

Example 1.13 Consider the non-reduced tuple (Q, Q) with reduction (P, P) where P and Q are pictured below. Since ∂Q generates a strictly smaller sublattice than Q (if the latter is shifted so that $0 \in \partial Q$), Proposition 1.12 does not ensure that the Galois group is the expected wreath product. Actually, we shall see that it is twice smaller in this particular case, although we do not know how to compute such non-expected Galois groups in general.



This can be seen as follows. The monodromy group consists of permutations of the eight roots along loops in the set $\mathbb{C}^Q \times \mathbb{C}^Q \setminus D$, where $\mathbb{C}^Q \times \mathbb{C}^Q$ is the space of systems of equations supported at $Q \subset \mathbb{Z}^2$, and D is the bifurcation set (i.e. the set of all systems with more or less than eight roots). Thus, the monodromy group is generated by permutations, whose cyclic type is the same as for permutations along small loops around the components D_i of the bifurcation set D .

Applying the description of the irreducible components of the bifurcation set (Proposition 1.11/4.10 in the arXiv/journal version of [12] respectively) to our case, we see that D consists of 5 irreducible components: one component (the discriminant D_0) consists of systems with a root of multiplicity 2 (and hence two roots of multiplicity 2, because Q generates an index 2 sublattice in \mathbb{Z}^2), and the other four components consist of systems with a root at one of the 4 one-dimensional orbits of the toric variety $\mathbb{CP}^1 \times \mathbb{CP}^1 \supset (\mathbb{C}^*)^2$. Thus, the permutation of roots along a small loop around D_0 consists of two disjoint transpositions.

The other components D_i of D correspond to the edges Q_i of the convex hull Q . By the same result from [12], a generic system of equations from D_i has several roots of multiplicity 1 in the complex torus and several roots of multiplicity h at the Q_i -orbit of the Q -toric variety, where h is the lattice distance from the line containing Q_i to $Q \setminus Q_i$. In our case, $h = 1$ for each of the four edges, so the permutations along small loops around the other four components of D are trivial.

Thus the monodromy group is contained in $A_8 \subset \mathfrak{S}_8$, while the wreath product $(\mathbb{Z}/2\mathbb{Z}) \wr \mathfrak{S}_4$ is not. Actually, one can manually check that the group $G_Q \subset \mathfrak{S}_8$ is the intersection of $(\mathbb{Z}/2\mathbb{Z}) \wr \mathfrak{S}_4$ with A_8 , i.e. the Coxeter group D_4 .

1.4 Techniques and perspectives

1.4.1 From systems of equations to enumerative geometry: wreath enumerative problems

The two main characters in the above story are the non-reduced system of polynomial equations and its reduction. The interrelation between the two is a particular instance of a general situation when an enumerative problem X is a covering of another enumerative problem Y (in a sense that we make precise in the next section). In such general framework, we call X a wreath enumerative problem, because the monodromy groups G_X and G_Y and the group of deck transformations D of the covering satisfy the relation

$$G_X \hookrightarrow D \wr G_Y \quad (3)$$

which encompasses the inclusion (2) for systems of equations.

We shall first study when the general inclusion (3) becomes an equality, and then apply the resulting criterion (WREATH PRODUCT THEOREM 3.7) to systems of equations as a special case.

1.4.2 From enumerative geometry to topology: inductive connectivity

Properties of the monodromy group of an enumerative problem can often be translated to topological properties of appropriate varieties. For instance, it is a classical fact that the k -transitivity of the monodromy group is equivalent to the connectivity of the k -incidence variety of the problem, see Sect. 2.

In the same vein, below we argue that the inclusion (3) is an isomorphism if and only if the appropriate incidence variety has the expected number of connected components, see the proof of WREATH PRODUCT THEOREM 3.7 in Sect. 3.6. It leads us to consider, yet more generally, the following topological question:

Given a covering $\pi : X \rightarrow Y$ between topological path-connected space and a subset $V \subset Y$, find general criteria for $\pi^{-1}(V)$ to be path-connected.

To that aim, we introduce the notion of (strongly) inductive coverings and prove the following fact in Sect. 3.5.

Inductive Connectivity Theorem 1.14 (light version) *Assume that $\pi : X \rightarrow Y$ is a strongly inductive covering of finite degree. The preimage of a path-connected subset $V \xrightarrow{j} Y$ is path-connected if and only if*

$$j_* H_1(V, \mathbb{Z}) + \pi_*(H_1(X, \mathbb{Z})) = H_1(Y, \mathbb{Z}).$$

1.4.3 Plan of the paper

In the context of enumerative problems, the above theorem translates to WREATH PRODUCT THEOREM 3.7, which reduces the surjectivity of the injection (3) to an equality between certain lattices in integer homology groups.

We then wish to apply this result to our target special case, when the enumerative problem is the system of equations with a prescribed tuple of support sets \tilde{A} . For this, we provide combinatorial criteria on the tuple \tilde{A} ensuring either the equality or the non-equality of the aforementioned lattices. These criteria arise after a careful study of the geometry of A-discriminants and A-resultants, see Sect. 4. The result of this study is summarized in MAIN THEOREM 4.14, whose two-dimensional version is presented above as Proposition 1.12.

1.4.4 Perspectives

From this point, one can distinguish three further key open questions in the study of Galois groups of general systems of polynomial equations.

1) If the inclusion (2) is proper, how to compute the Galois group $G_{\tilde{A}}$? The question is open even for a system of two trinomials equations of two variables.

2) It is a purely combinatorial, but open and highly non-trivial problem to decide whether the results of this paper actually allow to achieve (A) for every irreducible tuple. See Remark 4.36 for a precise combinatorial question.

3) We do not see a straightforward way to apply the technique from the present paper to the study of the Galois group for reducible tuples (such that k of the sets can be shifted to the same k -dimensional sublattice). The Galois group is unknown even for a reducible system of two trinomial equations.

Remark 1.15 We expect that our general study of monodromy groups of wreath enumerative problems will find applications beyond the special case of systems of equations, by the following reason.

It is a widely known empirical phenomenon that Galois groups of interesting enumerative problems (including the ones mentioned in Example 2.1 below, see for instance [24,27,29] and [15]) are either imprimitive or “trivial” (i.e. symmetric or alternating). On the other hand, if the Galois group of an enumerative problem is imprimitive, then, as a covering, this enumerative problem decomposes into a non-trivial composition of covering maps, which is close to being a wreath enumerative problem over a simpler one. Thus, it seems that the study of non-trivial Galois groups of enumerative problems to a large extent reduces to the case of wreath problems.

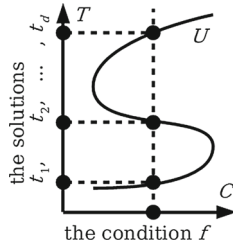
2 Enumerative problems

2.1 Enumerative problems

The general enumerative problem consists of a pair of smooth algebraic varieties T and C with C connected, together with an algebraic set $U \subset T \times C$ such that the projection $c : U \rightarrow C$ is generically finite. The sets T and C are respectively referred to as the *ambient space* and the *space of conditions* of the enumerative problem.

The set U is called the *solution space*, and the points of the fiber $c^{-1}(f)$ (as well as their images under the projection $t : U \rightarrow T$) are called the *solutions* of the enumerative problem for the condition $f \in C$.

For instance, the projection of a complex plane curve U to the horizontal axis C along the vertical axis T is the simplest example of an enumerative problem:



Here are some other important enumerative problems.

Example 2.1 1) The setting of the Sect. 1.1 can be regarded as an enumerative problem with $T = \mathbb{C}$, $C = \mathbb{C}^A$, and U defined as the set of all pairs (x, f) satisfying the equality $f(x) = 0$.

2) (Plücker). Let T be the projective plane, C be the space of degree d homogeneous polynomials on T , and U be the set of pairs (x, f) such that the plane algebraic curve $f = 0$ has a flex at x .

3) (Schubert). Let T be the space of lines in \mathbb{CP}^n , C be the space of collections (V_1, \dots, V_k) , where V_i is a linear subspace of \mathbb{CP}^n of codimension a_i , and U be the set of collections (l, V_1, \dots, V_k) such that the line l intersects every V_i . This is an enumerative problem for $\sum_i (a_i - 1) = 2n - 2$.

4) (Kouchnirenko–Bernstein) Let T be the torus $(\mathbb{C}^*)^n$, C be the space of conditions \mathbb{C}^A where $A := (A_1, \dots, A_n)$, $A_i \subset \mathbb{Z}^n$, with corresponding space of solutions $U = \{(x, f) \mid f(x) = 0\}$ in $T \times C$. This is the type of enumerative problem we will mainly focus on and will refer to it as the *A-enumerative problem*.

The first step in the study of an enumerative problem is to compute the number of solutions for a generic condition $f \in C$. This number is called the *degree* of the enumerative problem. For the problems in the preceding example, this question was addressed by the aforementioned authors.

The next natural step is to study the Galois group of the enumerative problem. More specifically, the projection $c : U \rightarrow C$ is a covering over a sufficiently small Zariski open set $C_o \subset C$, i.e. $c^{-1}(C_o) \rightarrow C_o$ is a covering. Denote its total space $c^{-1}(C_o)$ by $U_o \subset U$.

Definition 2.2 The monodromy group of the covering $U_o \rightarrow C_o$ is called the *monodromy group* or the *Galois group* of the enumerative problem $U \rightarrow C$.

Convention The Galois group of the enumerative problem $U \rightarrow C$ does not depend on the choice of C_o . Passing from the enumerative problem $U \rightarrow C$ to $U_o \rightarrow C_o$, we can and will always assume throughout the paper that every enumerative problem $U \rightarrow C$ is a covering.

Under this assumption, the variety U is smooth. Therefore, the irreducible components of U are exactly its connected components, so we shall refer to them simply as *components*.

For the last two problems in Example 2.1, the study of the Galois group was initiated in the foundational papers [19] and [31] respectively.

2.2 Wreath enumerative problems

Consider an enumerative problem $U \subset T \times C$ and a covering $\phi : \tilde{T} \rightarrow T$.

Definition 2.3 The preimage \tilde{U} of the solution space U under the covering map $(\phi, \text{id}) : \tilde{T} \times C \rightarrow T \times C$ defines the enumerative problem $\tilde{U} \rightarrow C$ that we shall call the ϕ -wreath over U .

Example 2.4 Let $\phi : (\mathbb{C}^\star) \rightarrow (\mathbb{C}^\star)$ be given by $\phi(x) = x^d$, then the ϕ -wreath over the enumerative problem of Example 2.1.1

$$T = (\mathbb{C}^\star), \quad C = \mathbb{C}^A, \quad U = \{(x, f) \mid f(x) = 0\}$$

is the enumerative problem

$$\tilde{T} = (\mathbb{C}^\star), \quad C = \mathbb{C}^{\tilde{A}}, \quad \tilde{U} = \{(\tilde{x}, \tilde{f}) \mid \tilde{f}(\tilde{x}) = 0\},$$

where $\tilde{A} = d \cdot A = \{0, da_1, \dots, da_k\}$.

Observation 2.5 Consider an enumerative problem $U \subset T \times C$ of degree d with Galois group G , and a Galois covering $\phi : \tilde{T} \rightarrow T$ with group of deck transformations D . Then the Galois group \tilde{G} of the ϕ -wreath enumerative problem \tilde{U} is contained in $W := D \wr G$.

This observation directly follows from the definitions of the wreath problem and the wreath group, and is widely known in the algebraic Galois theory (the Galois group of an iterated finite separable field extension is a subgroup of the corresponding wreath product, see e.g. [8]). A less straightforward task is to find criteria for the equality $\tilde{G} = W$. We present a criterion based on the following notions.

2.3 Powers of enumerative problems

Consider an enumerative problem $U \subset T \times C$ and let $U^{(k)}$ be the space of tuples $(x_1, \dots, x_k, f) \in T^k \times C$ such that x_1, \dots, x_k are pairwise distinct solutions in $c^{-1}(f)$. If the projection $U \rightarrow C$ is a d -fold covering, then $U^{(k)}$ is a smooth algebraic set in $T^k \times C$, and the projection $U^{(k)} \rightarrow C$ is a $\frac{d!}{(d-k)!}$ -fold covering. We need the following well known observation (the case $k = 2$ is especially important, see e.g. [19] and [27]).

Observation 2.6 1) The monodromy group of $U \rightarrow C$ is k -transitive (i.e. capable of sending any given k -tuple of solutions to any other given k -tuple) if and only if the monodromy group of $U^{(k)} \rightarrow C$ is transitive, i.e. $U^{(k)}$ is connected.

2) In particular, the monodromy group of $U \rightarrow C$ equals the symmetric group \mathfrak{S}_d if and only if the monodromy group of $U^{(d)} \rightarrow C$ is transitive, i.e. $U^{(d)}$ is connected.

3 Inductive connectivity

3.1 Inductive covers and solution lattices

In what follows, all singular homology groups are assumed to be with integer coefficients, so we omit the coefficient ring in the notation.

Definition 3.1 A covering of path-connected topological spaces $\pi : X \rightarrow Y$ is said to be *inductive*, if the natural embedding $\pi'_1(X) \rightarrow \pi'_1(Y)$ is an isomorphism (the prime stands for the commutator subgroup).

Remark 3.2 1) For an inductive covering $\pi : X \rightarrow Y$, the map $\pi_* : H_1(X) \rightarrow H_1(Y)$ is injective. Indeed, according to the diagram

$$\begin{array}{ccc} \pi_1(X) & \longrightarrow & H_1(X) \\ \downarrow & & \downarrow \pi_* \\ \pi_1(Y) & \longrightarrow & H_1(Y) \end{array}, \quad (4)$$

a non-zero element in the kernel of π_* would lift to an element in $\pi_1(X) \setminus \pi'_1(X)$ mapping to the kernel of $\pi_1(Y) \rightarrow H_1(Y)$, that is $\pi'_1(Y)$.

2) Note that the preceding implication is not an equivalence: if $X \rightarrow Y$ is the universal covering of a bouquet of circles, then the map $0 = H_1(X) \rightarrow H_1(Y)$ is injective, while $0 = \pi'_1(X) \rightarrow \pi'_1(Y)$ is not an isomorphism.

3) Every inductive covering is Galois with a commutative deck transformation group. Indeed, every subgroup H of a group G containing the commutator is normal, and the quotient G/H is commutative. Applying this fact to the image of $\pi_1(X)$ in $\pi_1(Y)$, the sought statements follow from Propositions 1.39 and 1.40 in [20].

4) Note that the preceding implication is not an equivalence: if $X \rightarrow Y$ is the non-trivial two-fold covering of the bouquet of two circles, whose restriction to one of the circles is trivial, then it is Galois with the group of deck transformations $\mathbb{Z}/2\mathbb{Z}$, but not inductive (as the map $H_1(X) \rightarrow H_1(Y)$ is not injective).

Definition 3.3 An inductive covering $\pi : X \rightarrow Y$ is said to be *strongly inductive*, if the embedding $H_1^T(X) \rightarrow H_1^T(Y)$ (see Remark 3.2.1) is an isomorphism (T stands for the torsion subgroup).

The following sources of strongly inductive coverings will be especially important for us.

Example 3.4 1) The map $(\mathbb{C}^*) \rightarrow (\mathbb{C}^*)$, $x \mapsto x^d$, is strongly inductive.

2) If $X \rightarrow Y$ is strongly inductive, then so is $X \times Z \rightarrow Y \times Z$.

3) The composition of (strongly) inductive coverings is (strongly) inductive.

4) Conversely, if a (strongly) inductive covering $\pi : X \rightarrow Y$ decomposes into covering maps $X \rightarrow \tilde{X} \rightarrow Y$, then both of them are (strongly) inductive. Indeed, we have the factorization $\pi'_1(X) \rightarrow \pi'_1(\tilde{X}) \rightarrow \pi'_1(Y)$. Since the composition of the two arrows is an isomorphism by assumption, and each arrow is injective, it is an

isomorphism as well. Similarly, each arrow in $H_1^T(X) \rightarrow H_1^T(\tilde{X}) \rightarrow H_1^T(Y)$ is an isomorphism.

5) Every covering of a space with commutative fundamental group (in particular, every connected algebraic group covering over \mathbb{C}) is inductive. A particular instance is given by surjective morphisms $\pi : X \rightarrow Y$ between complex tori X and Y of the same dimension. Since $H_1(X)$ and $H_1(Y)$ have no torsion, the covering π is strongly inductive.

Given an enumerative problem defined by a degree d covering $c : U \rightarrow C$, choose a base point f in C , and denote the set $c^{-1}(f)$ of its d solutions by S . Consider an f -pointed loop γ in C whose induced permutation on S is the identity. Then, along this loop, every solution $s \in S$ travels a loop in T , and the homology class of this loop will be denoted by $\gamma_s \in H_1(T)$. Ordering the elements γ_s accordingly to a given ranking $\delta : S \rightarrow \{1, 2, \dots, d\}$, we obtain a vector γ_δ in $H_1(T)^d$.

Definition 3.5 For a given ranking δ , the set of all vectors of the form γ_δ is called the *solution lattice* $H_\delta \subset H_1(T)^d$.

Remark 3.6 1) The solution lattice H_δ is a subgroup in $H_1(T)^d$ since it is the image of the homomorphism $\gamma \mapsto \gamma_\delta$ defined on the kernel of the monodromy map $\pi_1(C) \rightarrow \mathfrak{S}(S)$.

2) The lattices H_δ for various δ differ by the permutations of the multipliers in $H_1(T)^d$.

Wreath Product Theorem 3.7 *In the setting of Observation 2.5, assume additionally that ϕ is strongly inductive. Then, the inclusion $\tilde{G} \subset W$ is an equality if and only if, for some ranking δ (or, equivalently, for every ranking), we have*

$$H_1(T)^d = H_\delta + \phi_* H_1(\tilde{T})^d. \quad (5)$$

The proof is given in Sect. 3.6. The importance of this theorem is that the study of (non-commutative) fundamental groups is replaced with the study of (commutative) homology groups. As an illustration of this advantage, we now prove Proposition 1.5 by constructing the solution lattice of the underlying enumerative problem.

3.2 Application to sparse polynomial equations

Proposition 1.5 is a corollary of WREATH PRODUCT THEOREM 3.7 and the following lemma.

Lemma 3.8 *In the setting of Example 2.1.1, if $\text{GCD}(A) = 1$, then the solution lattice equals $H_1(\mathbb{C}^*)^a = \mathbb{Z}^a$.*

Proof I. By Observation 1.2, the Galois group of the enumerative problem is full symmetric, thus the solution lattice is symmetric under the natural action of \mathfrak{S}_a .

II. It follows from (I) and Remark 3.6.1 that, once the solution lattice contains vectors

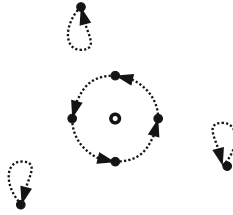
$$\underbrace{(1, \dots, 1, 0, \dots, 0)}_p \text{ and } \underbrace{(1, \dots, 1, 0, \dots, 0)}_q \in \mathbb{Z}^a,$$

it contains the vector $(\underbrace{1, \dots, 1}_{|p-q|}, 0, \dots, 0)$.

III. For every $a_j \in A$, the solution lattice contains the vector

$$(\underbrace{1, \dots, 1}_{a_j}, 0, \dots, 0) \in \mathbb{Z}^a. \quad (6)$$

To prove this, consider the trinomial $g(x) = \varepsilon + x^{a_j} + x^a$. It has a_j small roots (tending to 0 as $\varepsilon \rightarrow 0$) and $a - a_j$ other roots. As ε runs a small loop around 0, the small roots permute in a cycle around 0, and the other roots travel small loops not linked with 0:



Thus, if ε runs a_j times around 0, then the roots of g permute trivially, generating the element (6) in the solution lattice.

IV. Using (II), we can run the Euclidean algorithm on the vectors (6) for all j and conclude that the solution lattice contains the vector

$$(\underbrace{1, \dots, 1}_{\text{GCD}(A)}, 0, \dots, 0).$$

Since we are given $\text{GCD}(A) = 1$, we have proved that $(1, 0, \dots, 0) \in H_\delta$ and hence by (I) the other vectors of the standard basis are contained in the solution lattice. \square

Remark 3.9 The proof essentially consists of constructing loops in the space of conditions, generating the sought solution lattice. One could try instead to prove Proposition 1.5 by directly constructing loops generating the sought monodromy group, and observe that this task is drastically more complicated (cf. our subsequent paper [16]).

3.3 Lifting connectivity in covering spaces

WREATH PRODUCT THEOREM 3.7, which we used above to prove Proposition 1.5, will be deduced from the purely topological INDUCTIVE CONNECTIVITY THEOREM 1.14 given in the introduction, or more precisely from its finer version, INDUCTIVE CONNECTIVITY THEOREM 3.25 to follow. This finer version is necessary, because its proof is based on decomposing the covering π into a composition of cyclic covers and proving the statement by induction on the length of this decomposition (hence the name “inductive”). As is often the case, we have to strengthen the statement to be able to prove it by induction. Before making our way towards this stronger version, Theorem 3.25, let us shortly comment on the lighter version, Theorem 1.14.

Remark 3.10 1) Since irreducible components of a complex algebraic set are in one to one correspondence with the connected components of its smooth part, INDUCTIVE CONNECTIVITY THEOREM 1.14 may help to prove that the preimage of an irreducible algebraic variety $\mathcal{V} \subset Y$ under an algebraic cover $X \rightarrow Y$ is irreducible, when applied to the smooth part (or any sufficiently small Zariski open subset) of \mathcal{V} .

2) Since in what follows we apply this theorem to algebraic covers, we are fine with the assumption of finite degree. However, it would be interesting to understand to what extent one can omit assumptions on the cardinality of a fiber.

Example 3.11 The assumption of strong inductivity cannot be relaxed to inductivity in INDUCTIVE CONNECTIVITY THEOREM 1.14. For instance, consider the lens space Y defined as the quotient of $X = (\mathbb{C}^2 \setminus \{0\})$ by $(e^{2\pi i/p}, e^{2\pi i q/p})$. We have $\pi_1(X) = H_1(X) = 0$ and $\pi_1(Y) = H_1(Y) = \mathbb{Z}/p\mathbb{Z}$. For every line $V \subset \mathbb{C}^2$ through 0, its image $V \xrightarrow{j} Y$ generates the same subgroup $j_*H_1(V) \subset H_1(Y)$ for all possible choices of V , but the preimage of V may be reduced or not (and with different number of components) depending on V .

We now begin our quest for general criteria ensuring that the preimage of a connected subspace under a covering remains connected. Recall that a finite covering of connected spaces $\pi : X \rightarrow Y$ induces the natural transfer map $\pi^* : H_\bullet(Y) \rightarrow H_\bullet(X)$ (and recall that all homology groups are over \mathbb{Z} so that we drop the coefficient group from our notation). At the level of chains, this map sends every singular simplex to the sum of its preimages. We refer to [20] for more details on covering maps.

Definition 3.12 An element of an Abelian group is *primitive* if it cannot be written as the sum of $k > 1$ copies of another element modulo torsion.

Lemma 3.13 Let $\pi : X \rightarrow Y$ be a degree d covering, and $V \subset Y$ be path-connected. If V contains a singular 1-cycle c , such that $d \cdot c$ represents a primitive element in $\pi_*H_1(X)$, then the preimage $U = \pi^{-1}(V)$ is path-connected.

Remark 3.14 Since $d \cdot c = \pi_*\pi^*c$, we have:

- the 1-cycle $d \cdot c$ always represents an element in $\pi_*H_1(X)$;
- its primitivity in $\pi_*H_1(X)$ is equivalent to the primitivity of π^*c in the group $H_1(X)/\ker \pi_*$ (and actually the latter restatement will be mostly used in what follows).

Proof Since every singular 1-cycle in a path-connected space is homologous to a loop, we can assume with no loss in generality that the cycle c in V is a loop, pointed at some point y . Thus the lemma is reduced to the following special case. \square

Lemma 3.15 Let $\pi : X \rightarrow Y$ be a degree d covering, let c be a loop in Y , and denote by b the singular 1-cycle π^*c in X . If b represents a primitive element in $H_1(X)/\ker \pi_*$, then its support set $|b|$ is path-connected.

Before proving this fact, we illustrate its statement with a simple example.

Example 3.16 Let X be a genus 3 surface as pictured in Fig. 1 and Y be its (genus 2) quotient by the rotation of 180° about the central vertical axis such that the two

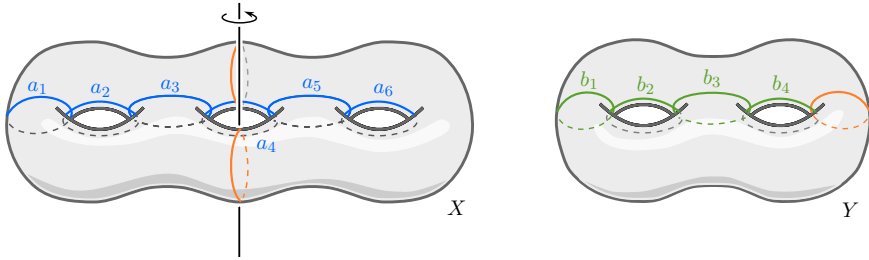


Fig. 1 Lifting connectivity in the double covering $\pi : X \rightarrow Y$

orange cycles in X are mapped to the orange cycle in Y . Let us introduce the bases a_i in $H_1(X)$ and b_j in $H_1(Y)$ as shown on the figure. Then π_* sends a_1 to b_1 , a_2 and a_6 to b_2 , a_3 and a_5 to b_3 , and a_4 to $2b_4$. So its kernel is generated by $a_2 - a_6$ and $a_3 - a_5$, and the quotient $H_1(X)/\ker \pi_*$ can be identified with the sublattice generated by b_1, b_2, b_3 and $2b_4$ in $H_1(Y)$. The class of the disconnected $\pi^*b_2 = a_2 + a_6$ in this sublattice is represented by $b_2 + b_2 = 2b_2$, which agrees with its imprimitivity (it is a non-trivial multiple of the element b_2 in the same sublattice). The class of the connected $\pi^*b_4 = a_4$ in this sublattice is represented by $2b_4$, which agrees with its primitivity in this sublattice (because b_4 is not in this sublattice). Both phenomena illustrate Lemmas 3.15 and 3.13.

Proof of Lemma 3.15 Assume towards the contradiction that b is the sum of non-zero 1-cycles b_1 and b_2 with disjoint support sets, covering the loop c with degrees k_1 and k_2 respectively. Denote $\text{GCD}(k_1, k_2)$ by k , and k_i/k by k'_i . Choose an integer decomposition $1 = n_1k'_1 + n_2k'_2$. Then, we have the identity

$$\begin{aligned} (k'_1 + k'_2) \cdot (n_1, n_2) &= (1 - n_2k'_2 + n_1k'_2, n_2k'_1 + 1 - k'_1n_1) \\ &= (1, 1) + (n_2 - n_1) \cdot (-k'_2, k'_1) = (1, 1) \bmod (-k'_2, k'_1). \end{aligned}$$

Taking the formal dot product of the vector (b_1, b_2) with the two sides of this identity, we have

$$b = b_1 + b_2 = (k'_1 + k'_2) \cdot (n_1b_1 + n_2b_2) \bmod g, \quad (7)$$

where $g = k'_2 \cdot b_1 - k'_1 \cdot b_2$. Since the projection $\pi_*(b_i)$ equals $k_i \cdot c$ as a singular 1-cycle (and all the more so as a homology 1-cycle), we have $k_2 \cdot b_1 - k_1 \cdot b_2 \in \ker \pi_*$. Dividing the latter element by k , we conclude that g is a torsion element of the group $H_1(X)/\ker \pi_*$. Thus (7) contradicts the primitivity of b in $H_1(X)/\ker \pi_*$. \square

Under few mild additional assumptions, we can strengthen the statement of Lemma 3.13 by replacing primitivity with a weaker property.

Definition 3.17 An element of an Abelian group is *weakly primitive* if it cannot be written as the sum of $k > 1$ copies of another element.

Lemma 3.18 *Let $\pi : X \rightarrow Y$ be a degree d covering, and $V \subset Y$ be path-connected. Assume additionally one of the following:*

- d is prime;
- the covering π is Galois.

If V contains a singular 1-cycle c such that $d \cdot c$ represents a weakly primitive element in $\pi_ H_1(X)$, then the preimage $U = \pi^{-1}(V)$ is path-connected.*

As well as Lemma 3.13, this one follows from the appropriate version of Lemma 3.15 below.

Lemma 3.19 *Let $\pi : X \rightarrow Y$ be a degree d covering, let c be a loop in Y and denote by b the singular 1-cycle π^*c in X . Assume additionally one of the following:*

- d is prime;
- the covering π is Galois.

If b represents a weakly primitive element in $H_1(X)/\ker \pi_$, then its support set $|b|$ is path-connected.*

Proof If d is prime, then $k = 1$ and thus $g \in \ker \pi_*$ in the proof of the original Lemma 3.15.

If π is Galois, then its group of deck transformations acts transitively. In particular, it acts transitively on the connected components s_1, \dots, s_k of $|b|$ and on the summands of the respective decomposition $b = b_1 + \dots + b_k$, $|b_i| = s_i$. Thus the push-forward $\pi_* b_i$ does not depend on i , and we have $b_i - b_j \in \ker \pi_*$ for all i and j . This implies $b = k \cdot b_1 \mod \ker \pi_*$. In particular, we have $k = 1$, because b is weakly primitive in $H_1(X)/\ker \pi_*$. \square

In the target case of algebraic groups, the observations of this section simplify as follows.

Corollary 3.20 *Let $\pi : X \rightarrow Y$ be a covering of connected Lie groups. Let $V \subset Y$ be path-connected. If V contains a singular 1-cycle c whose preimage $\pi^*(c)$ represents a weakly primitive element in $H_1(X)$, then the preimage $U = \pi^{-1}(V)$ is path-connected.*

Proof At the level of fundamental groups, the map $\pi_1(X) \rightarrow \pi_1(Y)$ is injective for any connected covering $\pi : X \rightarrow Y$. Moreover, since the fundamental groups of Lie groups are commutative, we have $\pi_1(Y) = H_1(Y)$, and the diagram (4) ensures that $\pi_* : H_1(X) \rightarrow H_1(Y)$ is injective as well. In this case $\ker \pi_*$ is trivial, and the statement follows from Lemma 3.18, because a covering of Lie groups is Galois. \square

Remark 3.21 In the present work, X and Y will be complex tori, so the absence of torsion in their homology identifies primitivity with weak primitivity. However, for general algebraic groups, the torsion (and thus the difference between the two notions of primitivity) is non-trivial and important for their geometry.

3.4 Inductive connectivity

Our aim here is to create a context in which we could apply the results of the preceding subsection to a chain of covering maps $\dots \rightarrow X_2 \rightarrow X_1 \rightarrow Y$ to prove by induction

on k that the preimage of a certain path-connected $V \subset Y$ in X_k is path-connected. In this way we shall prove **INDUCTIVE CONNECTIVITY THEOREM 1.14**.

Proposition 3.22 *Let $\pi : X \rightarrow Y$ be an inductive covering, and let $U \subset X$ be the preimage of a subset $V \subset Y$. Then the image of $H_1(U)$ in $H_1(X)$ is the intersection of $H_1(X) \subset H_1(Y)$ with the image of $H_1(V)$ in $H_1(Y)$.*

Proof Observe first that we can treat each path-connected component of V separately and therefore assume that V is path-connected. In view of the commutative diagram

$$\begin{array}{ccc} H_1(U) & \longrightarrow & H_1(X) \\ \downarrow & & \downarrow \\ H_1(V) & \longrightarrow & H_1(Y) \end{array}$$

the image of $H_1(U)$ in $H_1(X)$ is contained in the intersection of $H_1(X) \subset H_1(Y)$ with the image of $H_1(V)$ in $H_1(Y)$. Since V is path-connected by assumption, the containment in the opposite direction is equivalent to showing that, for any loop c in X pointed at $x \in U$ such that the homology class $[\pi_*(c)]$ belongs to the image of $H_1(V)$ in $H_1(Y)$, the homology class $[c]$ belongs to the image of $H_1(U)$ in $H_1(X)$.

For c as above, the loop $\pi_*(c)$ in Y is homotopic to the product of a loop b in V (representing the same element in the image of $H_1(V)$) and a loop h representing an element of the commutator $\pi'_1(Y)$. By the inductivity of the covering, h is the image of a loop g representing an element of the commutator $\pi'_1(X)$. The homotopy between the loops $\pi_*(c)h^{-1}$ and b lifts to the homotopy between the loop cg^{-1} and a certain loop γ in U covering b . Since g belongs to $\pi'_1(X)$, it follows that $[c] = [cg^{-1}] = [\gamma]$ belongs to the image of $H_1(U)$ in $H_1(X)$. \square

In particular, for every subgroup $L \subset H_1(X)$, this proposition implies the following.

Corollary 3.23 *Let $\pi : X \rightarrow Y$ be an inductive covering, and let the subset $U \xrightarrow{i} X$ be the preimage of a subset $V \xrightarrow{j} Y$. If $j_*H_1(V) + \pi_*L$ generates $\pi_*H_1(X)$, then $i_*H_1(U) + L$ generates $H_1(X)$.*

Proof By assumption, any element $x \in \pi_*H_1(X)$ can be written as a sum $x = v + \ell$ with $v \in j_*H_1(V)$ and $\ell \in \pi_*L$. In particular, we have that $v = x - \ell$ is an element of $\pi_*H_1(X)$. By Proposition 3.22, v is an element in $\pi_*(i_*H_1(U))$. It follows that any element in $H_1(X)$ is the sum of an element in $i_*H_1(U)$ with an element in L . \square

This motivates the following notion.

Definition 3.24 A path-connected $V \subset Y$ is said to be *L -inductively connected* (or just *inductively connected* for $L = 0$) for a subgroup $L \subset H_1(Y)$, if the image of $H_1(V)$ together with L generates $H_1(Y)$.

3.5 Proof of INDUCTIVE CONNECTIVITY THEOREM 1.14

We have reached the goal stated at the beginning of the preceding subsection.

Inductive Connectivity Theorem 3.25 1) Assume that $\pi : X \rightarrow Y$ is a strongly inductive covering of finite degree, and that $V \xrightarrow{j} Y$ is (π_*L) -inductively connected for some subgroup $L \subset H_1(X)$. Then, the preimage $U := \pi^{-1}(V) \xrightarrow{i} X$ is L -inductively connected.

2) In particular, if $j_*H_1(V) + \pi_*(H_1(X)) = H_1(Y)$, then U is path-connected.

3) Conversely, if $j_*H_1(V) + \pi_*(H_1(X)) \neq H_1(Y)$, then U is path-disconnected.

Proof We first prove 1) for a covering of prime degree $p > 1$. Since $\pi_* : H_1(X) \rightarrow H_1(Y)$ is injective and restricts to an isomorphism on the torsion part, the Smith normal form for this injection provides us with two minimal sets of generators a_1, \dots, a_k and b_1, \dots, b_k of $H_1(X)$ and $H_1(Y)$ respectively such that a_1 and b_1 are not torsion elements and such that π_* is given by

$$\pi_*(a_1) = p \cdot b_1 \text{ and } \pi_*(a_j) = b_j \text{ for } j \geq 2.$$

In particular, the following conditions are equivalent for a singular 1-cycle c in V :

- $[p \cdot c]$ is a primitive element in $\pi_*H_1(X)$;
- $[c]$ is primitive in $H_1(Y)$ and not contained in $\pi_*H_1(X)$.

To see this, write $[c] = (\lambda_1, \dots, \lambda_k)$ in the coordinates provided by b_1, \dots, b_k and assume that b_1, \dots, b_ℓ are the non-torsion elements among them ($\ell \leq k$). On the one hand, the class $[c]$ is primitive and not in $\pi_*H_1(X)$ if and only if the vector $(\lambda_1, \dots, \lambda_\ell)$ is primitive and λ_1 is not divisible by p . On the other hand, the class $[p \cdot c]$ is primitive in $\pi_*H_1(X)$ if and only if the vector $(\lambda_1, p\lambda_2, \dots, p\lambda_\ell)$ is primitive. The two properties are therefore equivalent.

Since $j_*H_1(V) + \pi_*(L)$ generates $H_1(Y)$, and $\pi_*(L) \subset \pi_*(H_1(X))$, there exists at least one cycle c that satisfies one of the two equivalent conditions above. It follows from Lemma 3.13 that U is path-connected and from Corollary 3.23 that $i_*H_1(U) + L$ generates $H_1(X)$. The subspace $U \subset X$ is therefore L -inductively connected.

Now we can prove 1) for a covering of an arbitrary degree.

We first show that π can be written as a composition of strongly inductive coverings whose respective degrees are prime numbers. Indeed, the inclusion of lattices $H_1(X)/H_1^T(X) \subset H_1(Y)/H_1^T(Y)$ admits the Smith normal form and thus extends to an increasing filtration of lattices L_i , such that the index of every two consecutive lattices L_i and L_{i+1} is prime. Since path-connected coverings $\tilde{\pi} : \tilde{X} \rightarrow Y$ such that π factorizes through $\tilde{\pi}$ are in correspondence with the subgroups $G < \pi_1(Y)$ containing $\pi_*(\pi_1(X))$ (see [20, Theorem 1.38]), the filtration of lattices L_i gives rise to a decomposition of the covering π into a sequence of spaces X_i and covering spaces between them. These are strongly inductive by Example 3.4.4. The degrees of these coverings are prime, because the degree of a strongly inductive $\tilde{\pi}$, which is given by the index of $\pi_*(\pi_1(X))$ in $\pi_1(Y)$, equals the index of $H_1(X)$ in $H_1(Y)$, and further the index of $H_1(X)/H_1^T(X)$ in $H_1(Y)/H_1^T(Y)$.

Now, for every intermediate covering $X \xrightarrow{\pi_i} X_i \xrightarrow{\tilde{\pi}_i} Y$ we can deduce by induction on i that the set $\tilde{\pi}_i^{-1}(V) \subset X_i$ is $\pi_{i*}(L)$ -inductively connected. The step of the induction is the statement 1) of the theorem for the prime degree covering $X_{i+1} \rightarrow X_i$, which we have already proved.

The statement 2) is a special case of 1) with $L = H_1(X)$. For the statement 3), the subgroup $j_*H_1(V) + \pi_*(H_1(X))$ is contained in a strict subgroup of $H_1(Y)$. In particular, the subgroup generated by $\pi_1(V)$ and $\pi_*(\pi_1(X))$ in $\pi_1(Y)$ is contained in a strict subgroup $G \subset \pi_1(Y)$. Therefore, the covering π factors through the strongly inductive covering $\tilde{\pi} : \tilde{X} \rightarrow Y$ associated to G with the property that $j_*H_1(V) + \pi_*(H_1(X)) \subset \tilde{\pi}_*(H_1(\tilde{X}))$.

Assuming to the contradiction that $\tilde{U} := \tilde{\pi}^{-1}(V)$ is path-connected, we can connect two of the preimages of $y \in V$ through \tilde{U} with a path γ . We claim that the loop $\tilde{\pi}(\gamma)$ represents a cycle in $H_1(V)$ outside $\tilde{\pi}_*(H_1(\tilde{X}))$, leading to a contradiction. Thus, the set $\tilde{\pi}^{-1}(V)$ is not path-connected and so is $\pi^{-1}(V)$, as π factors through $\tilde{\pi}$.

It remains to prove the above claim. Assume to the contradiction that $\tilde{\pi}(\gamma)$ represents a cycle in $\tilde{\pi}_*(H_1(\tilde{X}))$. Then, the loop $\tilde{\pi}(\gamma)$ is homotopic to the product $a \cdot b$ of a loop $a \in \tilde{\pi}(\pi_1(X))$ with a commutator $b \in \pi'_1(Y)$, both based at y . Since $a \in \tilde{\pi}(\pi_1(X))$ and $\tilde{\pi}$ is inductive, we can lift a and b to loops c and d based at the starting point x of γ . Therefore, the homotopy between $a \cdot b$ and $\tilde{\pi}(\gamma)$ lifts to an homotopy between $c \cdot d$ and a loop based at x and covering $\tilde{\pi}(\gamma)$ once. Since there is only one lift of $\tilde{\pi}(\gamma)$ starting at x , it follows that γ is a loop. This is a contradiction. \square

3.6 Proof of Wreath product theorem 3.7

The inclusion $\tilde{G} \subset D \wr G$ makes the sought equality $\tilde{G} = D \wr G$ equivalent to the numerical one $|\tilde{G}| = |D \wr G|$ and, furthermore to

$$|(D \wr \mathfrak{S}_d)/\tilde{G}| = |\mathfrak{S}_d/G|, \quad (8)$$

since the right hand side equals $|(D \wr \mathfrak{S}_d)/(D \wr G)|$.

In order to prove (8), we will interpret the two sides of this equality as the numbers of connected components of certain enumerative problems, derived from the initial one. Namely, denote the projections of $U \subset T \times C$ to T and C by t and c respectively, and consider the following objects:

- the smooth algebraic set $V := U^{(d)} \subset T^d \times C$, that is the set of all tuples (x_1, \dots, x_d, f) such that x_1, \dots, x_d are the (arbitrarily ordered) points of the fiber $c^{-1}(f)$.
- the covering $\pi : \tilde{T}^d \times C \rightarrow T^d \times C$;
- the preimage $\tilde{V} = \pi^{-1}(V)$, that is the set of all tuples (y_1, \dots, y_d, f) such that y_1, \dots, y_d are d points of the fiber $\phi^{-1} \circ c^{-1}(f)$ such that $\phi(y_1), \dots, \phi(y_d)$ are pairwise distinct.

Choosing a base point $f \in C$ with fiber $S := c^{-1}(f)$, a ranking of this fiber $\delta : S \rightarrow \{1, 2, \dots, d\}$ defines

- the base point $f_\delta := (\delta^{-1}(1), \dots, \delta^{-1}(d), f)$ in V ,
- the component of V containing f_δ (we denote it by V_δ),

– the natural action of the symmetric group \mathfrak{S}_d on S , its induced action on the fiber of the covering $V \rightarrow C$, and the induced embedding of the monodromy group $G \subset \mathfrak{S}_d$.

The regular action of the group \mathfrak{S}_d on a fiber of the covering $V \rightarrow C$ restricts to the natural action of the monodromy group $G \subset \mathfrak{S}_d$ and the orbits of G are in correspondence with the components of V . This is because, by the definition of the action, two points of the fiber are in the same orbit if and only if they can be connected with a path in V . In particular, V has $|\mathfrak{S}_d/G|$ components.

Similarly, the regular action of $D \wr \mathfrak{S}_d$ on a fiber of the covering $\tilde{V} \rightarrow C$ restricts to the natural action of the monodromy group $\tilde{G} \subset D \wr \mathfrak{S}_d$, and the orbits of the latter are in correspondence with the components of \tilde{V} . In particular, \tilde{V} has $|(D \wr \mathfrak{S}_d)/\tilde{G}|$ components.

As a result, the equality (8) is equivalent to the fact that every component V_δ of V is covered with a unique component of \tilde{V} . The latter is equivalent to (5) by INDUCTIVE CONNECTIVITY THEOREM 3.25, applied to the covering π and the set V_δ . This application is justified by the following observations:

- The covering π is (strongly) inductive if and only if the covering ϕ is;
- Denoting the projections of V to T^d and C by t and c respectively, c_* surjectively maps $\pi_1(V_\delta, f_\delta)$ to the kernel of the monodromy map $\pi_1(C) \rightarrow \mathfrak{S}(S)$. Thus the map $\gamma \mapsto \gamma_\delta$ from the definition of the solution lattice decomposes into lifting the loop γ to $\pi_1(V_\delta, f_\delta)$ and then mapping the homology class of the lifted loop with $t_* : H_1(V_\delta) \rightarrow H_1(T^d)$. In particular, the solution lattice equals $t_* H_1(V_\delta)$.

As a result, the equality (5) is equivalent to the equality

$$H_1(T^d \times C)^d = H_1(V_\delta) + \pi_* H_1(\tilde{T}^d \times C)$$

that appears in INDUCTIVE CONNECTIVITY THEOREM 3.25.

4 Galois groups of systems of sparse polynomial equations

In this section, we state and prove a generalization of Proposition 1.12 that in particular

- completely characterizes tuples $A_1 = \dots = A_n \subset \mathbb{Z}^n$ such that the Galois group G_A of the corresponding system of sparse equations equals the expected wreath product;
- extends this result to tuples of support sets that are not equal but similar in a sense (see the notion of analogous sets below).

As in Sect. 1.2, the tuple of finite sets $A := (A_1, \dots, A_n)$ in the character lattice \mathbb{Z}^n of the complex torus $T := (\mathbb{C}^*)^n$ is assumed to be reduced and irreducible, see Definition 1.8. The mixed volume of the convex hulls of A_1, \dots, A_n is denoted by d .

4.1 Analogous systems of equations

For a linear function $\gamma : \mathbb{Z}^n \rightarrow \mathbb{Z}$ and a finite set $P \subset \mathbb{Z}^n$, let $P^\gamma \subset P$ be the set of all points where γ attains its maximal value on P .

Definition 4.1 We say that the sets A_1, \dots, A_n are *analogous* if, for every $\gamma \in (\mathbb{Z}^n)^*$, there exists a vector subspace $V_\gamma \subset \mathbb{R}^n$ such that for all $i = 1, \dots, n$, the minimal affine subspace containing A_i^γ is a shifted copy of V_γ .

Equivalently, the sets A_1, \dots, A_n are analogous if the convex hulls of A_1, \dots, A_n share the same dual fan, see [17, Section 1.5].

Example 4.2 If the convex hulls of A_1, \dots, A_n are equal, or more generally homothetic, then A_1, \dots, A_n are analogous.

Remark 4.3 A tuple of analogous sets of full dimension is always irreducible. A tuple is analogous if and only if its reduction is analogous, see Remark 1.11.

Let $\mathcal{G}_A \subset (\mathbb{Z}^n)^*$ be the (finite) set of all primitive γ such that V_γ is a hyperplane, and let d_γ be the index in V_γ of the minimal sublattice to which each of $A_1^\gamma, \dots, A_n^\gamma$ can be shifted.

Definition 4.4 Let \tilde{A} be an analogous tuple in a lattice \tilde{N} with reduction A (see Sect. 1.3) given by a linear embedding $L : N \rightarrow \tilde{N}$ and denote by L^* the dual embedding. We say that \tilde{A} is *ample* if the vectors $d_\gamma \cdot \gamma \in N^*$, $\gamma \in \mathcal{G}_A$, together with the lattice $\text{im}(L^*)$ generate N^* .

In particular, a reduced analogous tuple A is always ample, since $\text{im}(L^*) = N^*$. Note that the property of being ample does not depend on the choice of the reduction.

Main Theorem 4.5 (light version) *Let $\tilde{A} := (\tilde{A}_1, \dots, \tilde{A}_n)$ be a tuple of finite sets in a lattice \tilde{N} such that $0 \in A_i$ and denote by $\Lambda \subset \tilde{N}$ the sublattice generated by the sets \tilde{A}_i . Denote also by \tilde{d} the mixed volume of the convex hulls of these sets and let $d := \tilde{d}/|\mathbb{Z}^n/\Lambda|$.*

1) Assume that $\tilde{A}_1, \dots, \tilde{A}_n$ are analogous. Then, the monodromy group $G_{\tilde{A}}$ of the system of equations with indeterminate coefficients supported at \tilde{A} is isomorphic to $(\tilde{N}/\Lambda) \wr \mathfrak{S}_d$ if \tilde{A} is ample, and is strictly smaller otherwise.

2) Assume that \tilde{A} has a reduction $A := (A_1, \dots, A_n)$ such that every A_i is contained in the positive quadrant $\mathbb{Z}_{\geq 0}^n$ of $N \simeq \mathbb{Z}^n$ and contains the vertices of the standard simplex (i.e. \mathbb{C}^{A_i} consists of non-Laurent polynomials and contains the space of affine linear functions). Then, the monodromy group $G_{\tilde{A}}$ is isomorphic to $(\tilde{N}/\Lambda) \wr \mathfrak{S}_d$.

Proof (modulo the subsequent Theorem 4.14) essentially repeats Proposition 1.5: we prove the multidimensional version of Lemma 3.8 (Theorem 4.14 below) claiming that the solution lattice of the A -enumerative problem is sufficiently large, notice that the assumptions of both parts of MAIN THEOREM 4.5 ensure applicability of Theorem 4.14 (which is actually applicable to a much wider class of systems), and then apply WREATH PRODUCT THEOREM 3.7. \square

It remains to prove Theorem 4.14. However, the trinomial deformation of a given polynomial equation from the proof of Lemma 3.8 becomes drastically more complicated in this multidimensional setting, and its construction occupies most of this section. It is based on geometry of A -resultants and A -discriminants.

4.2 Resultants

The first homology group $H := H_1(T)$ is the lattice dual to \mathbb{Z}^n : the composition of a loop $S^1 \rightarrow (\mathbb{C}^\star)^n$ representing a cycle $\gamma \in H$ and a monomial $m : (\mathbb{C}^\star)^n \rightarrow (\mathbb{C}^\star)^1$ is a map $S^1 \rightarrow (\mathbb{C}^\star)^1$, and its class $r \in \pi_1(\mathbb{C}^\star)^1 = \mathbb{Z}$ defines the natural non-degenerate pairing $H \times \mathbb{Z}^n \rightarrow \mathbb{Z}$, $(\gamma, m) \mapsto \gamma \cdot m = r$.

Every $\gamma \in H$, considered as a linear function on \mathbb{Z}^n attains its maximum on A_i at some subset that we denote by A_i^γ . For short, the tuples (A_1, \dots, A_n) and $(A_1^\gamma, \dots, A_n^\gamma)$ will be denoted by A and A^γ respectively, and the spaces of systems of equations $\mathbb{C}^{A_1} \oplus \dots \oplus \mathbb{C}^{A_n}$ and $\mathbb{C}^{A_1^\gamma} \oplus \dots \oplus \mathbb{C}^{A_n^\gamma}$ supported at these tuples – by \mathbb{C}^A and \mathbb{C}^{A^γ} .

The *reduced resultant* $R_{A^\gamma}^{red}$ is the closure of the set of all tuples $g = (g_1, \dots, g_n) \in \mathbb{C}^{A^\gamma}$ such that the system $g_1(x) = \dots = g_n(x) = 0$ has a root $x \in (\mathbb{C}^\star)^n$. All A_i^γ by definition can be shifted to the hyperplane $\ker \gamma$ (where γ is considered as a linear function on \mathbb{Z}^n), so the set of solutions of $g_j = 0$ is invariant under the action of the 1-dimensional subtorus $T_\gamma \subset (\mathbb{C}^\star)^n$ whose homology embeds in H as $\mathbb{Z} \cdot \gamma$.

Definition 4.6 A primitive vector $\gamma \in H$ is said to be *essential*, if the tuple A^γ does not contain $k \geq 2$ sets that can be shifted to the same $(k - 2)$ -dimensional plane. The set of essential vectors will be denoted by \mathcal{G} .

Remark 4.7 The set \mathcal{G} is finite: in particular, it is contained in the set of all primitive exterior normal vectors to the facets of the convex hull of $A_1 + \dots + A_n$.

The resultant $R_{A^\gamma}^{red}$ is an irreducible hypersurface (see [28]) if and only if γ is proportional to an essential vector. Then the dimension count shows that, for a generic tuple $g \in R_{A^\gamma}^{red}$, the zero locus $\{g = 0\}$ is one-dimensional. Thus its quotient by the torus T_γ is a finite set, whose cardinality will be denoted by d_γ . This number should be regarded as a natural multiplicity of the resultant $R_{A^\gamma}^{red}$, and will be explicitly computed in Theorem 4.9 below.

Definition 4.8 [11] 1) If γ is essential, then the *algebraic resultant* R_{A^γ} is defined as F^{d_γ} , where F is the irreducible polynomial defining the hypersurface $R_{A^\gamma}^{red}$, and the number d_γ is the *resultant multiplicity*, defined above.

2) If γ is not proportional to an essential vector, then by definition the algebraic resultant R_{A^γ} is 1, and its multiplicity d_γ equals 0.

The computation of the resultant multiplicity d_γ for an essential vector γ is based on the following observation from [28]. The set I of subsets $K \subset \{1, \dots, n\}$ such that all A_i^γ , $i \in K$, can be shifted to the same $(|K| - 1)$ -dimensional sublattice, has a unique element which is minimal with respect to inclusion. Indeed, the set I is not empty since it contains $\{1, \dots, n\}$, and the intersection of two elements of I necessarily belongs to I , otherwise their union would certify that γ is not essential (see [28] for details). The minimal element in I will be denoted by K_γ , and the minimal sublattice to which all A_i^γ , $i \in K_\gamma$, can be shifted, will be denoted by $L_\gamma \subset \mathbb{Z}^n$.

Let d'_γ be the index of the lattice L_γ in its saturation \tilde{L}_γ . The images of the sets A_i^γ , $i \notin K_\gamma$, under the projection $\mathbb{Z}^n \rightarrow \mathbb{Z}^n / \tilde{L}_\gamma$ are $n - |K_\gamma| + 1$ sets in a lattice of

dimension $n - |K_\gamma| + 1$. Thus, the lattice mixed volume of the convex hulls of these images makes sense and is denoted by d''_γ .

Theorem 4.9 (Theorem 2.23 in [10]) 1) The resultant multiplicity d_γ equals $d'_\gamma \cdot d''_\gamma$.

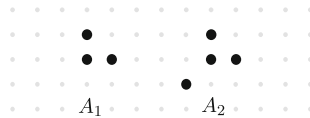
2) For a generic tuple $g \in R_{A^\gamma}^{red}$, among the differentials dg_1, \dots, dg_n at a point of the zero locus $\{g = 0\}$, the only linearly dependent subtuple is $dg_i, i \in K_\gamma$, and its corank is 1 (i.e. they satisfy a unique non-trivial linear relation).

Definition 4.10 The tuple (E_1, \dots, E_n) such that $E_k := \emptyset$ for $k \notin K_\gamma$ and $E_k := A_k^\gamma$ otherwise, is said to be the *essential tuple* defined by an essential vector γ .

We denote by A_{ess}^γ the essential tuple defined by $\gamma \in \mathcal{G}$, denote the set of all essential tuples by \mathcal{E} , and denote by $\mathcal{E}_0 \subset \mathcal{E}$ the set of tuples $(E_1, \dots, E_n) \in \mathcal{E}$ such that the convex hull of every E_i has dimension $(n - 1)$.

Note that different vectors $\gamma \in \mathcal{G}$ may give rise to the same essential tuple.

Example 4.11 For A_1 and A_2 as on the picture below, both $(-1, 0)$ and $(0, -1)$ belong to \mathcal{G} and give the same essential tuple $(\emptyset, \text{the bottom-left point of } A_2)$.



Remark 4.12 1) A vector $\gamma \in \mathcal{G}$ satisfies $A_{ess}^\gamma \in \mathcal{E}_0$ if and only if there exists a facet in every A_i whose primitive normal exterior vector is γ .

2) The map $\mathcal{G} \rightarrow \mathcal{E}, \gamma \mapsto A_{ess}^\gamma$, is one to one over \mathcal{E}_0 , i.e. every essential tuple $E \in \mathcal{E}_0$ is defined by a unique $\gamma \in \mathcal{G}$, which we denote by γ_E .

3) If A_1, \dots, A_n are analogous (Definition 4.1), then $\mathcal{E}_0 = \mathcal{E}$, and $A_{ess}^\gamma = A^\gamma$. As a consequence, \mathcal{G} and \mathcal{E} are in one to one correspondence.

By a harmless abuse of notation, we denote the lift of the algebraic discriminant R_{A^γ} under the natural forgetful projection $\mathbb{C}^A \rightarrow \mathbb{C}^{A^\gamma}$ by the same symbol R_{A^γ} . Let \mathcal{R} be the set of all hypersurfaces of the form $R_{A^\gamma} = 0$ in \mathbb{C}^A .

Remark 4.13 The terminology “essential tuple” is motivated by the fact that, by construction, two equations $R_{A^\gamma} = 0$ and $R_{A^{\gamma'}} = 0$ define the same set in \mathbb{C}^A if and only if γ and γ' define the same essential tuple. Thus, \mathcal{R} is in one to one correspondence with the set of essential tuples \mathcal{E} (and, by Remark 4.12, also with \mathcal{G} when A is analogous). For $E \in \mathcal{E}$, denote the corresponding resultant set in \mathbb{C}^A by $R_E^{red} \in \mathcal{R}$.

4.3 The main result

We consider a reduced irreducible tuple $A := (A_1, \dots, A_n)$ of finite sets in \mathbb{Z}^n . According to Theorem 1.7, the general system of equations supported at this tuple has Galois group \mathfrak{S}_d (where d is the generic number of roots of the system, i.e. the lattice mixed volume of the convex hulls of A_i).

However, if this system of equations undergoes a monomial change of coordinates corresponding to a proper sublattice $L \subset H$, then the Galois group of the resulting non-reduced system is not symmetric. In order to analyse this Galois group $G_{L,A}$ using WREATH PRODUCT THEOREM 3.7, we should check whether

$$H^{\oplus d} = L^{\oplus d} + H_\delta, \quad (9)$$

or, in other words, whether the solution space of the initial system of equations is $L^{\oplus d}$ -inductively connected.

Recall the definition of the solution lattice H_δ in this context. Pick a generic system of equations f_\circ in the space \mathbb{C}^A , and order its roots: $\delta : \{x \mid f_\circ(x) = 0\} \rightarrow \{1, \dots, d\}$. Every loop α in \mathbb{C}^A pointed at f_\circ defines a permutation of the roots. If this permutation is trivial, then, as the system of equations travels along the loop, its i -th root (with respect to the order δ) travels along a loop α_i in the torus T , and the homology classes $\tilde{\alpha}_i$ of these loops define an element $\tilde{\alpha}_\delta \in H^{\oplus d}$. The set of all such elements is the solution lattice H_δ .

We shall prove the following criterion of whether the equality (9) holds for given A and L . For an essential tuple $B \in \mathcal{E}$, define \mathcal{G}_B to be the set of all vectors $\gamma \in \mathcal{G}$ supporting this essential tuple: $A_{ess}^\gamma = B$.

Main Theorem 4.14 1) Assume that the vectors $\sum_{\gamma \in \mathcal{G}_B} d_\gamma \cdot \gamma$ over all $B \in \mathcal{E}$ together with L do not generate the lattice H . Then (9) is not satisfied, and the Galois group $G_{L,A}$ is strictly smaller than the wreath product $(H/L) \wr \mathfrak{S}_d$.

2) Assume that the vectors $d_{\gamma_B} \cdot \gamma_B$ over all $B \in \mathcal{E}_0$ together with L generate the lattice H . Then (9) is satisfied, and the Galois group $G_{L,A}$ is isomorphic to the wreath product $(H/L) \wr \mathfrak{S}_d$.

Remark 4.15 1) If the tuple A is analogous, then Remark 4.12 ensures that the set of vectors from MAIN THEOREM 4.14.1) coincides with that of MAIN THEOREM 4.14.2), i.e. $\sum_{\gamma \in \mathcal{G}_B} d_\gamma \cdot \gamma = d_{\gamma_B} \cdot \gamma_B$. Thus, the theorem completely characterizes analogous tuples satisfying the equality (9).

2) In general, we have the following three increasing classes of tuples, which coincide for analogous tuples:

- (a) Tuples A , such that the vectors $d_{\gamma_B} \cdot \gamma_B$ over all $B \in \mathcal{E}_0$, generate the lattice;
- (b) Tuples satisfying the equality (9);
- (c) Tuples A , such that the vectors $\sum_{\gamma \in \mathcal{G}_B} d_\gamma \cdot \gamma$ over all $B \in \mathcal{E}$ generate the lattice.

We expect that, for general reduced irreducible tuples, (b) is strictly larger than (a). Regarding the comparison of (b) and (c), see the subsequent Remark 4.36.

4.4 Preliminaries from lattice geometry

In order to prove MAIN THEOREM 4.14.2, we aim at constructing enough loops α to generate $H^{\oplus d}/L^{\oplus d}$ with the respective elements $\tilde{\alpha}_\sigma$. For this purpose, the following obvious combinatorial fact will be useful.

Definition 4.16 For an element $u = (u_1, \dots, u_d) \in H^{\oplus d}$, the sum $u_1 + \dots + u_d \in H$ is denoted by $\sum u$. The element u is said to be *homogeneous* if all of its non-zero entries are equal to each other.

Lemma 4.17 *I. Let $U \subset H^{\oplus d}$ be a subset of homogeneous elements such that the vectors $\sum u$ over all $u \in U$ do not generate H/L . Then, the set $\mathfrak{S}_d \cdot U$ (in the sense of the natural action of the permutation group \mathfrak{S}_d on the d direct summands of $H^{\oplus d}$) does not generate the space $H^{\oplus d}/L^{\oplus d}$.*

II. Let $U \subset H^{\oplus d}$ be a subset of homogeneous elements satisfying the following:

1) for any $u := (u_1, \dots, u_d) \in U$ with a non-zero entry u_i , there exists $\tilde{u} := (\tilde{u}_1, \dots, \tilde{u}_d) \in U$

such that $\tilde{u}_j = u_i$ and $\tilde{u}_k = 0$ for some indices j and k , and

2) the vectors $\sum u$ over all $u \in U$ generate H/L .

Then, the set $\mathfrak{S}_d \cdot U$ generates the space $H^{\oplus d}/L^{\oplus d}$.

Proof In the setting of part I, the map \sum sends $\mathfrak{S}_d \cdot U$ and $L^{\oplus d}$ to the proper sublattice of H generated by $\sum u$, $u \in U$, and L , thus $\mathfrak{S}_d \cdot U$ and $L^{\oplus d}$ also generate a proper sublattice of $H^{\oplus d}$.

In the setting of Part II, the assumption 1) allows to obtain, starting from a homogeneous element $u \in U$ with the nonzero entry δ , the element in $\mathfrak{S}_d \cdot U$ of the form $(\delta, \dots, \delta, 0, \dots, 0)$ with at least one zero, then the element $(\delta, \dots, \delta, 0, \delta, 0, \dots, 0)$ with the same number of zeroes, then, by permuting the difference of the preceding two vectors, the element $(0, \dots, 0, \delta, 0, \dots, 0, -\delta, 0, \dots, 0)$ with δ and $-\delta$ at arbitrary positions, and finally, adding such elements to the initial u , the vector $(0, \dots, 0, \sum u, 0, \dots, 0)$ with $\sum u$ at an arbitrary position. By the assumption 2), such vectors together with $L^{\oplus d}$ generate $H^{\oplus d}$. \square

Note that Part II does not hold without the assumption 1. Eventually, for this reason, we shall need the following elementary geometric fact.

Lemma 4.18 *Under the assumptions of MAIN THEOREM 4.14.2, assume that for some $B \in \mathcal{E}_0$ and the corresponding $\gamma := \gamma_B$, every $j = 1, \dots, n$, and every point $a \in A_j \setminus A_j^\gamma$, we have $V(A) = h_a \cdot d_\gamma$ where $h_a := |\gamma(a) - \gamma(A_j^\gamma)|$ is the lattice distance from a to the hyperplane $A_j^\gamma + \ker \gamma$. Then the lattice mixed volume of A_1, \dots, A_n equals 1. In particular, by [13], all A_i are equal to subsets of the set of vertices of the same elementary lattice simplex up to a shift.*

Proof By monotonicity of the mixed volume, we have $V(A) \geq V(a \cup B_j, \{B_i\}_{i \neq j}) = h_a V_j$, where V_j is the $(n-1)$ -dimensional lattice mixed volume of the convex hulls of $B_i = A_i^\gamma$, $i \neq j$. Since all of these convex hulls are $(n-1)$ -dimensional (by definition of \mathcal{E}_0), the mixed volume V_j is a positive multiple of d_γ . Thus, for every j and a , we have $V_j = d_\gamma$, and $h_a = h$ does not depend on a (and j). In particular, in the minimal lattice L' containing every B_i up to a shift, there exists an elementary simplex S containing every B_i up to a shift. Thus, up to a shift, every A_i consists of a subset of the set of vertices of S together with some (possibly none) points at lattice distance h from L' (on the same side from it). In this case, the equality $V(A) = h_a \cdot d_\gamma = h \cdot \text{Vol } S$ and the monotonicity of the mixed volume imply the existence of a point a_0 such that every A_i consists of a subset of the union of the set vertices of S with a_0 . This implies that $\text{Vol } S = h = 1$, otherwise A would not be reduced. \square

4.5 Preliminaries from toric geometry

In order to prove MAIN THEOREM 4.14.2, we shall need to construct a certain deformation of the system of equations $f_o = 0$, which is (slightly) degenerate in the sense of the theory of Newton polyhedra.

In order to prove the existence of a sought deformation, we briefly recall how to construct toric compactifications of non-degenerate complete intersections, and how they degenerate.

Definition 4.19 For a system of polynomial equations $f_1 = \cdots = f_k = 0$, we denote the set of its solutions by $Z(f)$, say that it is a *complete intersection* if its codimension equals k , and say that it is *regular* if 0 is a regular value of the polynomial map $f = (f_1, \dots, f_k)$.

Remark 4.20 1) Adopting a standard harmless abuse of terminology, we characterize the aforementioned property of the tuple f (not of $Z(f)$ itself) by saying that $Z(f)$ is regular.

2) In what follows, f_i are Laurent polynomials, and $Z(f)$ belongs to the complex torus T .

We consider the character lattice \mathbb{Z}^n of the complex torus $T = (\mathbb{C}^*)^n$ and its dual lattice $H = H_1(T)$. Given a finite set $B \subset \mathbb{Z}^n$, a polynomial $g \in \mathbb{C}^B$, and a vector $\gamma \in H$, we define the γ -leading term of $g = \sum_{b \in B} c_b x^b$ as $g = \sum_{b \in B^\gamma} c_b x^b$; for generic $g \in \mathbb{C}^B$, this is the highest non-zero homogeneous component of g with respect to the degree $\deg x^b := \gamma(b)$.

Similarly, given a tuple of finite sets $A = (A_1, \dots, A_m)$ in \mathbb{Z}^n and a tuple of polynomials $f = (f_1, \dots, f_m) \in \mathbb{C}^A$, we define $f^\gamma := (f_1^\gamma, \dots, f_m^\gamma)$. For a generic tuple $f \in \mathbb{C}^A$, the system of equations $f^\gamma = 0$ defines the regular zero locus $Z(f^\gamma)$.

Let us briefly recall how the sets $Z(f^\gamma)$ (over all γ) can be used to construct a smooth compactification of $Z(f)$. We refer to [22] and [23] for terminology and facts on toric compactifications.

If a collection of vectors $V \subset H$ can be completed to a lattice basis, then the set of all strictly positive integer combinations of these vectors is called *the simple cone* generated by V , and its *faces* are defined as the cones generated by the subcollections of V . A cone $C \subset H$ is said to be *compatible* with a set $A \subset \mathbb{Z}^n$, if the support set A^γ does not depend on the choice of $\gamma \in C$. A *simple fan* Σ in H is a finite collection of non-intersecting simple cones covering H and closed with respect to taking faces.

Remark 4.21 Note that, for the sake of brevity, by a simple cone we mean the set of lattice points in a relatively open simple cone, and by a simple fan we mean a complete simple fan.

Every simple fan Σ gives rise to a smooth n -dimensional *toric variety* X_Σ with an action of the torus T . Orbits of this action are in correspondence with cones of Σ . This correspondence reverses the dimensions and adjacencies and sends the 0-dimensional cone $\{0\} \in \Sigma$ to the dense orbit identified with the torus T , so that T can be regarded as a subset of X_Σ .

Theorem 4.22 [22] *For every tuple of finite sets $A = (A_1, \dots, A_m)$ in \mathbb{Z}^n , there exists a simple fan Σ compatible with each of them (i.e. such that every cone in Σ is compatible with each of the sets A_i). Moreover, given a simple cone C compatible with every A_i , the fan Σ can be chosen to contain C .*

If the simple fan Σ is compatible with A , then, for a generic tuple of polynomials $f = (f_1, \dots, f_m) \in \mathbb{C}^A$, the closure of the algebraic set $Z(f) \subset T$ in the toric compactification X_Σ is a smooth compact algebraic variety $\overline{Z(f)}$. This smooth compactification splits into its intersections with the toric orbits, and each of these intersections can be explicitly described by polynomial equations.

Namely, let O be the orbit of X_Σ , corresponding to a cone $C \in \Sigma$. This orbit is the quotient of the torus T by the subtorus T_C , whose homology is the vector span of $C \subset H$. Since the fan is compatible, the tuple f^γ does not depend on the choice of $\gamma \in C$, so we denote it by f^C .

Theorem 4.23 [23] *Let Σ be a simple fan compatible with a tuple A , $f \in \mathbb{C}^A$ be a generic system of equations, and C be any cone in Σ . Then the zero locus $Z(f^C)$ is regular and the intersection of the closure $\overline{Z(f)} \subset X_\Sigma$ with the corresponding orbit $O \subset X_\Sigma$ is transversal. In particular, $\overline{Z(f)}$ is smooth and splits into smooth strata $Z(f^C)/T_C$ over all cones $C \in \Sigma$.*

In what follows, we shall have to deal with generic systems of equations that do not satisfy the assumption of this theorem. The set of all such systems of equations is called the *A-bifurcation set*.

Remark 4.24 In other words, f is in the *A-bifurcation set* if $Z(f^\gamma)$ is not regular for some γ . In particular, the definition of the *A-bifurcation set* does not depend on the choice of the fan Σ compatible with A .

For $m = n$, the *A-bifurcation set* is the union of the resultant sets $R_B^{red} \subset \mathbb{C}^A$ over all essential tuples $B \in \mathcal{E}$, as described in Sect. 4.2, and the *A-discriminant* (the closure of all $f \in \mathbb{C}^A$ such that $Z(f)$ is not regular). We now formulate a similar description for arbitrary $m < n$, given in [12] (in what follows, we shall particularly need the case $n = m + 1$).

Definition 4.25 For a tuple A of finite sets $A_1, \dots, A_m \in \mathbb{Z}^n$, its *Cayley configuration* $\mathcal{A} \subset \mathbb{Z}^n \times \mathbb{Z}^m$ is the set $\cup_{i=1}^m A_i \times \{e_i\}$, where e_1, \dots, e_m is the standard basis in \mathbb{Z}_m .

The spaces \mathbb{C}^A and $\mathbb{C}^{\mathcal{A}}$ can be identified by sending a tuple $f = (f_1, \dots, f_m) \in \mathbb{C}^A$ to the Laurent polynomial $F = \sum_{i=1}^m \lambda_i f_i(x)$ of the variables λ and x .

Definition 4.26 1) The Cayley discriminant $D_A^C \subset \mathbb{C}^A \simeq \mathbb{C}^{\mathcal{A}}$ is the *A-discriminant*, i.e. the closure of all $F \in \mathbb{C}^{\mathcal{A}}$ for which 0 is a critical value.

2) The tuple A is said to be *Cayley-effective*, if its Cayley discriminant has codimension 1, and *Cayley-defective* otherwise.

Remark 4.27 1) The latter condition makes sense, because the *A-discriminant* is a proper irreducible algebraic set in $\mathbb{C}^{\mathcal{A}}$ (see [18]).

2) Assume that the dimension of the affine span of $A_1 + \dots + A_m$ is smaller than m , then the results of Section 1 in [28] can be rephrased as follows. The tuple A is

Cayley-effective if and only if no k sets in the tuple A can be shifted to the same $(k - 1)$ -dimensional space for $0 < k < m$. Under this assumption, the dimension of the affine span of $A_1 + \dots + A_m$ equals $m - 1$, and the Cayley discriminant D_A^C is the A -resultant R_A^{red} .

A tuple B is said to be a *facing* of a tuple $A = (A_1, \dots, A_m)$ of finite sets in \mathbb{Z}^n , if there exists a vector γ such that B_i is either empty or equal to A_i^γ for every $i = 1, \dots, m$. For every facing B , the forgetful projection $\mathbb{C}^A \rightarrow \mathbb{C}^B$ is defined by sending the tuple f of polynomials $\sum_{a \in A_i} c_{a,i} x^a$ to the tuple $f|_B$ of polynomials $\sum_{a \in B_i} c_{a,i} x^a$. The preimage of the Cayley discriminant D_B^C under this projection will be called and denoted in the same way.

Proposition 4.28 1) For all effective facings B of a tuple A , the irreducible hypersurfaces $D_B^C \subset \mathbb{C}^A$ are pairwise distinct.

2) Every codimension 1 irreducible component of the regular A -discriminant coincides with the Cayley discriminant D_B^C for some effective subtuple B .

3) Every codimension 1 irreducible component of the A -bifurcation set coincides with the Cayley discriminant D_B^C for some effective facing B .

Proof Part 1 follows from the fact (noticed in [11]) that the defining equation of the hypersurface D_B^C non-trivially depends on every coordinate in the space \mathbb{C}^B . Part 2 follows from Theorem 2.31 in [11] (which moreover explicitly describes all such subtuples). Part 3 follows from Proposition 1.11/4.10 in the arxiv/journal version of [12] (which moreover explicitly describes all such facings). \square

Corollary 4.29 Let $A := (A_1, \dots, A_m)$ be a tuple of finite sets in \mathbb{Z}^n and A^γ be an effective facing. Then, for a generic system of equations f in the Cayley discriminant $D_{A^\gamma}^C \subset \mathbb{C}^A$ and any other facing B , the zero locus $Z(f|_B)$ is regular. In particular, in a toric compactification $X_\Sigma \supset T$ whose fan Σ is compatible with A , the closure of the zero locus $Z(f)$ is smooth outside the orbit whose cone contains γ , and the closure of the zero locus $Z(\hat{f})$ for any proper subtuple \hat{f} of the tuple f is smooth everywhere.

Proof The regularity of $Z(f|_B)$ follows from Proposition 4.28, the smoothness of the closure follows from Theorem 4.23. \square

4.6 Proof of Main Theorem 4.14.2

From the start, we assume that A does not satisfy the assumption of Lemma 4.18, otherwise $d = 1$ by this lemma and (9) is satisfied by assumption. The statement follows then from WREATH PRODUCT THEOREM 3.7.

According to Lemma 4.17, it is enough to construct loops α in $\mathbb{C}^A \setminus \{\text{bifurcation set}\}$ such that the corresponding elements $\tilde{\alpha}_\sigma \in H^{\oplus d}$ are homogeneous, and the vectors $\sum \tilde{\alpha}_\sigma$ generate H/L . In this section, we shall construct such loops explicitly, starting from the primitive covector $\gamma = \gamma_B$, corresponding to an arbitrary essential tuple $B = A^\gamma \in \mathcal{E}_0$, an arbitrary integer $j \in \{1, \dots, n\}$ and an arbitrary point $a \in A_j \setminus B_j$.

With no loss of generality, we assume that $0 \in B_i$ for every $i = 1, \dots, n$ (otherwise we can shift A_i accordingly). We should now make some consecutive choices to

construct the sought loop. For a given $j \in \{1, \dots, n\}$, a given $a \in A_j \setminus B_j$ and given $g = (g_1, \dots, g_n) \in \mathbb{C}^B$ and $\tilde{g} = (\tilde{g}_1, \dots, \tilde{g}_n) \in \mathbb{C}^A$, define the tuple

$$f_{j,t,g}(x) := x^a + g_j(x) + t \cdot \tilde{g}_j(x) \quad \text{and} \quad f_{i,t,g}(x) := g_i(x) + t \cdot \tilde{g}_i(x)$$

for any $i \in \{1, \dots, n\} \setminus \{j\}$. We will occasionally denote $f_{j,t,g}(x) =: F_{j,g}(x, t) =: F_j(x, t)$ when the dependence in the parameters t and g is clear from the context.

From now on and until the end of this section, we choose generic tuples $g = (g_1, \dots, g_n)$ in R_B^{red} and $\tilde{g} = (\tilde{g}_1, \dots, \tilde{g}_n)$ in \mathbb{C}^A (which means that subsequently we shall use certain properties of g and \tilde{g} that are satisfied for all pairs $(g, \tilde{g}) \in R_B^{\text{red}} \times \mathbb{C}^A$ outside a certain proper Zariski closed subset), and call $f_{1,t_0,g} = \dots = f_{n,t_0,g} = 0$ for small $t_0 \neq 0$ the *central system of equations*. The name is explained by the following key lemma that, together with Lemma 4.17, proves MAIN THEOREM 4.14.2.

Lemma 4.30 *Let $G : (\mathbb{C}, 0) \rightarrow (\mathbb{C}^B, g)$ be a germ of an analytic curve transversal to the resultant R_B^{red} at its smooth point g and choose sufficiently small $|t_0| \ll \varepsilon \ll 1$. As the argument of G travels $-\gamma(a)$ times along the loop $\varepsilon \exp(2\pi i s)$, $s \in [0, 1]$, the roots of the corresponding system of equations*

$$f_{\bullet, t_0, G(\varepsilon \exp(2\pi i s))} = 0 \tag{10}$$

permute trivially. Moreover, $-d_\gamma \cdot \gamma(a)$ of the roots of this system travel a loop in T whose homology class equals $\gamma \in H$ and the other roots travel a contractible loop.

Remark 4.31 The roots of the family of systems of equations (10) split into “travelling” roots and “still” ones. If t_0 vanishes, the “still” roots hide at infinity, but “travelling” roots of the resulting family $f_{\bullet, 0, G(\varepsilon \exp(2\pi i s))} = 0$ keep traveling as described in the lemma. So the only purpose of including monomials with t in the definition of $f_{j,t,g}$ (and setting this t to be non-zero albeit small) is to drive the “still” roots back from infinity, while not affecting the itinerary of the travelling roots.

The rest of this subsection is devoted to the proof of this lemma. This is actually the multidimensional version of step (III) in the proof of Lemma 3.8, but the statement and the proof are significantly more technical.

I: describing the roots of the central system of equations as $t_0 \rightarrow 0$. The polynomials $F_j := F_{j,g}$ are defined on the complex torus $T' = (\mathbb{C}^*)^n \times (\mathbb{C}^*)^1$ with the standard coordinates (x, t) , and their respective Newton polytopes Δ_j are contained in the character lattice $\mathbb{Z}^n \times \mathbb{Z}^1$ of T' , see Fig. 2 for an example.

Note that every strictly positive linear combination δ of the covectors $(0, -1)$ and $(\gamma, 0) \in (\mathbb{Z}^n \times \mathbb{Z}^1)^*$ supports the same face Δ_i^δ : this face is the convex hull of $B_i \times \{0\} \subset \mathbb{Z}^n \times \mathbb{Z}^1$. Thus, by Theorem 4.22, the simple cone C generated by $(0, -1)$ and $(\gamma, 0)$ can be extended to a simple fan Σ compatible with the polytopes Δ_i . Let X be the corresponding smooth toric compactification of T' . Denote its orbit corresponding to C by O , and the adjacent codimension 1 orbits corresponding to the vectors $(0, -1)$ and $(\gamma, 0)$ by $O_{(0,-1)}$ and $O_{(\gamma,0)}$ respectively, see Fig. 2 for an example.

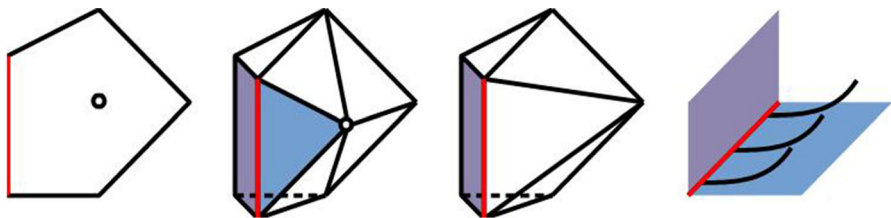


Fig. 2 An example of the toric compactification X in the case $n = 2$. On the left, we represent the convex hull of $A_1 = A_2$ with the red edge $B := B_1 = B_2$ and the point a . The two figures in the middle represent the polytopes Δ_i and Δ_j , $j \neq i$, with the red edge $B \times \{0\}$: the blue facet supports the covector $(0, -1)$ and the purple ones the covector $(\gamma, 0)$. On the right, we picture the (real part of the) orbits O , $O_{(0,-1)}$ and $O_{(\gamma,0)}$ in X corresponding to the faces of the polytopes Δ_j of the respective colors, and the black curve $F_1 = F_2 = 0$ near O

Denoting by \tilde{O} the union of O , T' and the two aforementioned codimension 1 orbits, we notice that the polynomials F_1, \dots, F_n and t define regular functions on the open set \tilde{O} , because $0 \in B_i$. We denote these regular functions on \tilde{O} by the same letters.

Lemma 4.32 *Let Z_i be the closure of the zero locus $Z(F_i)$ in the toric variety X . Then, for generic choice of $(g, \tilde{g}) \in R_B^{\text{red}} \times \mathbb{C}^A$, the following transversality conditions take place.*

1) *The intersection of Z_1, \dots, Z_n and the orbit O consists of d_γ points (see Sect. 4.1 for the resultant multiplicity d_γ). Near each of these points x_0 , the hypersurfaces Z_1, \dots, Z_n are smooth and intersect each other transversally along a smooth curve. This curve is transversal to the closure of $O_{(\gamma,0)}$ and tangent of order $-\gamma(a)$ to the closure of the orbit $O_{(0,-1)}$.*

2) *If a point $x_0 \in X$ belongs to the hypersurfaces Z_{i_1}, \dots, Z_{i_k} and the closures of the codimension 1 orbits C_1, \dots, C_m , then these $k + m$ hypersurfaces are smooth and mutually transversal at x_0 , except for the setting of part (1), i.e. unless $x_0 \in O$, the closure of $O_{(0,-1)}$ is among C_1, \dots, C_m , and $k = n$.*

Remark 4.33 As we shall see from the proof, part 1 is valid for a generic choice of $g \in R_B^{\text{red}}$ and $\tilde{g}_{j'} \in \mathbb{C}^{B_{j'}}$ for some j' , even if \tilde{g}_i are chosen to be 0 for $i \neq j'$.

Proof Part 2 is a special case of Corollary 4.29, because the resultant R_B^{red} coincides with the Cayley discriminant D_B^C by Remark 4.27.2.

Transversality of Z_1, \dots, Z_n and $O_{(\gamma,0)}$. By Theorem 4.9.2, the differentials of g_i , $i \in \{1, \dots, n\}$, at x_0 satisfy a unique linear relation, thus the differentials of $g_i + t\tilde{g}_i^\gamma$ are linearly independent for generic choice of \tilde{g}_i . Since $g_i + t\tilde{g}_i^\gamma$ is the restriction of F_i to the orbit $O_{(\gamma,0)}$, this implies transversality of Z_1, \dots, Z_n and the closure of $O_{(\gamma,0)}$.

Order of tangency of the sought curve with $O_{(0,-1)}$. This order equals the order of tangency of the hypersurface $Z_j = \{F_j = 0\}$ with the intersection of the hypersurfaces Z_i , $i \neq j$, and the closure of $O_{(0,-1)}$. Part 2 ensures that the latter intersection is transversal and defines a smooth curve. By the definition of its defining equations, this smooth curve is a shifted one-dimensional torus $T_\gamma \subset O_{(0,-1)} \simeq T$, and the restriction of F_j to it equals x^a , thus the sought order of tangency equals $-\gamma(a)$. \square

Recall that we are interested in the roots of the central system of equations. Identifying the subtorus $t = t_0$ in T' with T , the roots of the central system are the intersection points of the curve $F_1 = \cdots = F_n = 0$ and the subtorus $t = t_0$. Consider the closure C of this curve in the toric variety X . Lemma 4.32 ensures that C is smooth.

The coordinate function t on the torus T' extends to a meromorphic function on X , and the equation $t = 0$ defines a normal crossing divisor supported at the closure of certain codimension 1 orbits $O_m \subset X$, $m = 1, \dots, M$. By Lemma 4.32, the restriction of t to the smooth curve C has the following (and no other) roots:

- finitely many (possibly multiple) roots $x_{m,k}$ in the codimension 1 orbits O_m ;
- d_γ roots x_k of multiplicity $-\gamma(a)$ in the codimension 2 orbit O .

The roots of the central system of equations tend to $x_{m,k}$ and x_k as t_0 tends to 0, so we need a convenient coordinate system around every $x_{m,k}$ and x_k to analyze the roots of the central system for small t_0 .

II: describing a good neighborhood of a root $x_{m,k} \in O_m$. By Lemma 4.32, every root $x_{m,k}$ admits an open neighborhood $U_{m,k} \subset X$ with an analytic coordinate system (y_1, \dots, y_n, τ) such that:

- the coordinate y_i is given by F_i for any $i \in \{1, \dots, n\}$;
- the coordinate t is given by τ^μ for some positive integer μ ;
- $U_{m,k}$ does not intersect orbits of X outside $T' \cup O_m$;
- the intersection of $U_{m,k}$ with the plane $\tau = \tau_0$ for every sufficiently small τ_0 is a topological disc.

This implies the existence of neighbourhoods $V_{m,k} \subset \mathbb{C}^B$ of g and $W_{m,k} \subset \mathbb{C}$ of 0 such that, for every τ_0 , $\tau_0^\mu \in W_{m,k}$, and every $g' \in V_{m,k}$, the curve $F_{1,g'} = \cdots = F_{n,g'} = 0$ transversely intersects the disc $U_{m,k} \cap \{\tau = \tau_0\}$ at one point.

Lemma 4.34 *Assume that, in the setting of Lemma 4.30, ε is so small that the loop $G(\varepsilon \exp(2\pi i s))$, $s \in [0, 1]$, is contained in $V_{m,k}$, and $t_0 \in W_{m,k}$. As the system $f_{\bullet, t_0, G(\varepsilon \exp(2\pi i s))} = 0$ travels along this loop, its roots in $\{t = t_0\} \cap U_{m,k}$ permute trivially, and each of them travels a contractible loop in the torus $\{t = t_0\} \simeq T$.*

Proof By the choice of the neighborhoods $U_{m,k}$, $V_{m,k}$, $W_{m,k}$, the intersection $\{t = t_0\} \cap U_{m,k}$ consists of μ disjoint discs in T , and exactly one of the roots varies in each of these discs. Thus the roots do not permute and travel contractible loops. \square

III: describing a good neighborhood of a root $x_k \in O$.

for every root x_k and every choice of $j' \in \{1, \dots, n\}$, there exists an open neighborhood $U_k \ni x_k$ with an analytic coordinate system such that:

- t and F_i , $i \neq j'$, are n of the $n + 1$ coordinate functions;
- if ℓ is the coordinate line defined by them, and φ is the remaining coordinate function, then the restriction of $F_{j'}$ to ℓ equals $\varphi^{-\gamma(a)}$;
- U_k does not intersect orbits of X outside \tilde{O} ;
- the intersection of U_k with the plane $t = t_0$ for every sufficiently small t_0 is a topological disc.

This implies the existence of neighbourhoods $V_k \subset \mathbb{C}^B$ of g and $W_k \subset \mathbb{C}$ of 0 such that, for every non-zero $t_0 \in W_k$ and $g' \in V_k$, the curve $F_{1,g'} = \cdots = F_{n,g'} = 0$ transversally intersects the disc $U_k \cap \{t = t_0\}$ at $-\gamma(a)$ points.

Lemma 4.35 *Assume that, in the setting of Lemma 4.30, ε is so small that the loop $G(\varepsilon \exp(2\pi i s))$, $s \in [0, 1]$, is contained in V_k , and $|t_0| \ll \varepsilon$. As the system $f_{\bullet, t_0, G(\varepsilon \exp(2\pi i s))} = 0$ travels along this loop, all of its $-\gamma(a)$ roots in $U_k \cap \{t = t_0\}$ permute cyclically, and their paths form a loop in $\{t = t_0\} \simeq T$, whose homology class equals $\gamma \in H$.*

Proof First, we assume with no loss of generality that $t_0 = 0$, because the statement is invariant under perturbations of t_0 . Second, we assume without loss of generality that G is given by $G_{j'}(\epsilon) = g_{j'} + \epsilon \tilde{g}_{j'}$ for generic $g_{j'} \in \mathbb{C}^{B_{j'}}$ and $G_i(\epsilon) = g_i$ for $i \neq j'$, because all small loops around the resultant R_B^{reg} near its smooth point g are homotopy equivalent.

Under these additional assumptions, the sought statement turns into the following question: given the curve $C' \subset T'$ defined by the system of equations $f_{\bullet, 0, G(t)}(x) = 0$, and the point x_k in its closure, what happens to the points of the intersection $C' \cap \{t = t_0\}$ near x_k as t_0 runs once around 0?

The answer is the expected one: the paths of the intersection points form a loop in $\{t = t_0\} \simeq T$, whose homology class equals $\gamma \in H$. This is because, by Lemma 4.32.1 (which is applicable to the equations $f_{\bullet, 0, G(t)}(x) = 0$ according to Remark 4.33), the point x_k is a smooth point of the closure of C' , and the restriction of t to this closure has a root of multiplicity $-\gamma(a)$ at x_k . \square

Proof For ε and $|t_0|$ small enough, all roots of the system of equations $(*)$ belong to the neighborhoods $U_{m,k} \cap \{t = t_0\}$ and $U_k \cap \{t = t_0\}$, because all intersections of the hyperplane $t = t_0$ with the curve $F_{1,g'} = \dots = F_{n,g'} = 0$ tend to the points $x_{m,k}$ and x_k as $t_0 \rightarrow 0$ and $g' \rightarrow g$. In these neighborhoods, for $|t_0| \ll \varepsilon$, the roots permute as desired according to Lemmas 4.34 and 4.35. \square

Proof of MAIN THEOREM 4.14.2.

Given a number $j \in \{1, \dots, d\}$, a vector $\gamma := \gamma_B$, $B \in \mathcal{E}_0$, and a point $a \in A_j \setminus B_j$, choose any path β from f_\circ to the base point of the loop constructed in Lemma 4.30. Conjugating the latter loop with β , we obtain a loop $\alpha_{\beta, \gamma, j, a}$ based at f_\circ .

Choosing an ordering $\delta : \{\text{roots of the base system } f_\circ = 0\} \rightarrow \{1, \dots, d\}$, the loop $\alpha_{\beta, \gamma, j, a}$ gives rise to the corresponding vector $\tilde{\alpha}_{\delta, \beta, \gamma, j, a}$ in the solution lattice $H_\delta \subset H^{\oplus d}$ (recall that its i -th component equals the homology class of loop run by the i -th root of $f_\circ = 0$ as f_\circ travels along $\alpha_{\beta, \gamma, j, a}$).

According to Lemma 4.30, all non-zero components of this vector are equal to $\gamma \in H$, and the number of them equals $(\gamma(B_j) - \gamma(a)) \cdot d_\gamma$. Moreover, every vector of this form equals $\tilde{\alpha}_{\delta, \beta, \gamma, j, a}$ for suitable β , since the monodromy group of the general reduced irreducible system of equations equals \mathfrak{S}_d (by Theorem 1.7).

We conclude that, for every γ, j, a as above, every vector with $(\gamma(B_j) - \gamma(a)) \cdot d_\gamma$ components equal to γ and other components equal to 0 is contained in the solution lattice H_δ .

Note that, for a given γ , the numbers $\gamma(B_j) - \gamma(a)$ over all j and a are mutually prime (otherwise, if GCD equals $k > 1$, then the sets of tuple A can be shifted to the proper sublattice $\gamma^{-1}(k\mathbb{Z})$, so A is not reduced). Thus the Euclidean algorithm ensures that every vector with d_γ components equal to γ and other components equal to 0 is contained in the solution lattice H_δ .

By the assumption of MAIN THEOREM 4.14, the sums of components of such vectors generate H/L , thus by Lemma 4.17.II the vectors themselves generate $H^{\oplus d}/L^{\oplus d}$ (the condition (1) of this lemma satisfied by Lemma 4.18). \square

Remark 4.36 Actually, the construction from the preceding proof is applicable to $B \in \mathcal{E}$ even if $B \notin \mathcal{E}_0$. Choose an arbitrary tuple $C = (C_1, \dots, C_n)$, $C_i \subset A_i$, generic $\tilde{f} = (\tilde{f}_1, \dots, \tilde{f}_n) \in \mathbb{C}^C$ and a small loop $g_s \in \mathbb{C}^B$, $s \in S^1$, around the resultant R_B^{red} . For every linear function $\gamma \in \mathcal{G}_B$, let h_γ be $\max_i (\max \gamma|_{A_i} - \max \gamma|_{C_i})$. Set $f_{i,t,s}(x) = g_{i,s}(x) + \tilde{f}_i(x) + t \cdot \tilde{g}_i(x)$ and let $s \in S^1$ run a loop for a small $t \neq 0$. Then, as in the preceding proof, the roots of the system $f_{\bullet,t,s} = 0$ permute so that (cf. Proposition 5.2 in [14]):

- 1) among the disjoint cycles of the permutation of the roots, we have d_γ cycles of length h_γ for every $\gamma \in \mathcal{G}_B$;
- 2) the paths of the roots from one cycle constitute a loop whose class in the homology H equals γ .

As $s \in S^1$ runs around the circle sufficiently many times (more specifically, $M = \text{LCM}\{h_\gamma \mid \gamma \in \mathcal{G}_B\}$ times), we obtain a certain element $\tilde{\gamma}_B \in H^{\oplus d}$ in the homology of the solution space. According to 1) and 2), this element $\tilde{\gamma}_B$ has d_γ entries equal to $\frac{M}{h_\gamma} \gamma$ for every $\gamma \in \mathcal{G}_B$, and the other entries are equal to 0. As in the preceding proof, we now have four increasing classes, extending Remark 4.15.2:

- a) Tuples A , such that the vectors $d_{\gamma_B} \cdot \gamma_B$ over all $B \in \mathcal{E}_0$ generate the lattice H ;
- b) Tuples A , such that the vectors $\tilde{\gamma}_B$ over all $B \in \mathcal{E}$ generate the lattice $H^{\oplus d}$;
- c) Tuples with inductively connected solution spaces;
- d) Tuples A , such that the vectors $\sum_{\gamma \in \mathcal{G}_B} d_\gamma \cdot \gamma$ over all $B \in \mathcal{E}$ generate the lattice H .

It is now a purely combinatorial (although highly non-trivial) problem to understand whether the classes (b) and (d) coincide for all reduced irreducible tuples A . If the answer is “yes” (and this is what we expect at least for $n = 2$), then we have (b)=(c)=(d), so MAIN THEOREM 4.14.1 actually provides a criterion of whether the Galois group of a given tuple equals the expected wreath product. If the answer is “no”, then a more subtle study of solution spaces is required to answer this question.

4.7 Proving inductive disconnectedness

In order to prove that a given tuple A is not inductively connected, we need the following Poisson-type formula for the product of roots of a system of polynomial equations. It is the special case of the Poisson–Pedersen–Sturmfels–D’Andrea–Sombra formula [7, Theorem 1.1], when one of the $n + 1$ polynomials involved is a monomial x^b .

Theorem 4.37 *For a generic system of equations $f = (f_1, \dots, f_n) \in \mathbb{C}^A$, the product of the values of the monomial x^b over the roots of $f_1 = \dots = f_n = 0$ equals $\prod_{\gamma \in \mathcal{G}} [R_{A^\gamma}(f)]^{\gamma \cdot b}$.*

Proof of MAIN THEOREM 4.14. 1. Under the assumptions of MAIN THEOREM 4.14.1, we can choose $b \in \mathbb{Z}^n$ and $p > 1$ that divides $d_\gamma \cdot (\gamma \cdot b)$ and $l \cdot b$ for all $\gamma \in \mathcal{G}$ and all $l \in L$. Recall that the polynomial R_{A^γ} is equal to F^{d_γ} for some polynomial

F on \mathbb{C}^A . In this case, the preceding Poisson-type formula implies that the product of the monomial x^b over the roots of f equals G^p for some polynomial G on \mathbb{C}^A . Moreover, the polynomial G does not vanish at systems of equations f that have d distinct roots in the torus since the irreducible factors of G describe systems f with roots at infinity. Thus, for any loop α in the space of systems with d distinct roots, the composition $G^p \circ \alpha$ is a loop in \mathbb{C}^* whose homology class is divisible by p . The latter homology class is given by $(\sum \tilde{\alpha}_\sigma) \cdot b$, since $G^p(\alpha(s))$ is the product of the monomials x^b over the roots of the system $\alpha(s)$. We deduce that $(\sum \tilde{\alpha}_\sigma) \cdot b$ is divisible by p . All such elements together with the sublattice $L^{\oplus d}$ generate a proper sublattice in $H^{\oplus d}$, because it is contained in the proper sublattice of all $u \in H^{\oplus d}$ such that $b \cdot \sum u$ is divisible by p . Therefore $L^{\oplus d}$ and the solution lattice H_δ do not generate $H^{\oplus d}$. \square

Acknowledgements The two authors met during the program “Tropical Geometry, Amoebas and Polytopes” held at the Institute Mittag-Leffler in spring 2018. The authors would like to express their gratitude to the organizers J. Draisma, A. Jensen, H. Markwig, B. Nill and to the institute for providing inspiring working conditions.

Funding Open access funding provided by University of Gävle

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article’s Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article’s Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

1. Abhyankar, S.S.: Coverings of algebraic curves. *Am. J. Math.* **79**, 825–856 (1957)
2. Abhyankar, S.S., Seiler, W.K., Popp, H.: Mathieu group coverings of the affine line. *Duke Math. J.* **68**(2), 301–311 (1992)
3. Averkov, G., Borger, C., Soprunov, I.: Classification of triples of lattice polytopes with a given mixed volume. *Discrete Comput. Geom.* **66**, 165–202 (2021). [arXiv:1902.00891](https://arxiv.org/abs/1902.00891)
4. Bernstein, D.N.: The number of roots of a system of equations. *Funct. Anal. Appl.* **9**, 183–185 (1975)
5. Cohen, S.D.: The Galois group of a polynomial with two indeterminate coefficients. *Pac. J. Math.* **90**, 63–76 (1980)
6. Cohen, S.D.: The Galois group of a polynomial with two indeterminate coefficients. *Pac. J. Math.* **97**, 483–486 (1981)
7. D’Andrea, C., Sombra, M.: A Poisson formula for the sparse resultant. *Proc. Lond. Math. Soc.* **110**, 932–964 (2015). [arXiv:1310.6617](https://arxiv.org/abs/1310.6617)
8. de Smit, B.: Galois groups and wreath products (2007). <http://www.math.leidenuniv.nl/~desmit/notes/krans.pdf>
9. Dvornicich, R., Zannier, U.: Newton functions generating symmetric fields and irreducibility of Schur polynomials. *Adv. Math.* **222**, 1982–2003 (2009)
10. Esterov, A.: Determinantal singularities and Newton polyhedra. *Proc. Steklov Inst. Math.* **259**, 16–34 (2007)
11. Esterov, A.: Newton polyhedra of discriminants of projections. *Discrete Comput. Geom.* **44**, 96–148 (2010). [arXiv:0810.4996](https://arxiv.org/abs/0810.4996)
12. Esterov, A.: The discriminant of a system of equations. *Adv. Math.* **245**, 534–572 (2013). [arXiv:1110.4060](https://arxiv.org/abs/1110.4060)

13. Esterov, A., Gusev, G.: Systems of equations with a single solution. *J. Symb. Comput.* **68**, 116–130 (2015). [arXiv:1211.6763](#)
14. Esterov, A., Gusev, G.: Multivariate Abel–Ruffini. *Math. Ann.* **365**, 1091–1110 (2016). [arXiv:1405.1252](#)
15. Esterov, A.: Galois theory for general systems of polynomial equations. *Compos. Math.* **155**, 229–245 (2019). [arXiv:1801.08260](#)
16. Esterov, A., Lang, L.: Braid monodromy of univariate fewnomials. *Geom. Topol.* **25**(6), 3053–3077. <https://doi.org/10.2140/gt.2020.25.3053>
17. Fulton, W.: *Introduction to Toric Varieties*. The William H. Roever Lectures in Geometry, Annals of Mathematics Studies, Princeton University Press, Princeton (1993)
18. Gelfand, I.M., Kapranov, M.M., Zelevinsky, A.V.: *Discriminants, Resultants, and Multidimensional Determinants*. Springer, Berlin (1994)
19. Harris, J.: Galois groups of enumerative problems. *Duke Math. J.* **46**, 685–724 (1979)
20. Hatcher, A.: *Algebraic Topology*, pp. 1–544. Cambridge University Press, Cambridge (2002)
21. Hibi, T., Tsuchiya, A.: Classification of lattice polytopes with small volumes. *J. Combin.* **11**, 495–509 (2020). [arXiv:1708.00413](#)
22. Kempf, G., Knudsen, F., Mumford, D., Saint-Donat, B.: *Toroidal Embeddings I*. Lecture Notes in Mathematics, 339. Springer, Berlin (1973)
23. Khovanskii, A.G.: Newton polyhedra and toroidal varieties. *Funct. Anal. Appl.* **11**, 289–296 (1977)
24. Lang, L.: Monodromy of rational curves on toric surfaces. *J. Topol.* **13**, 1658–1681 (2020). [arXiv:1902.08099](#)
25. Smith, J.H.: General trinomials having symmetric Galois group. *Proc. Am. Math. Soc.* **63**, 208–212 (1977)
26. Smith, J.H.: Sur le groupe de Galois d’un polynome dont les coefficients sont indépendants. *Sem. Théor. Nombres Bordeaux*, 1–11 (1984)
27. Sottile, F., White, J.: Double transitivity of Galois groups in Schubert calculus of Grassmannians. *Algebr. Geom.* **2**, 422–445 (2015). [arXiv:1312.5987](#)
28. Sturmfels, B.: On the Newton polytope of the resultant. *J. Algebr. Combin.* **3**(2), 207–236 (1994)
29. Tyomkin, I.: An example of a reducible Severi variety. *Proceedings of the 20th Gökova Geometry-Topology Conference, Gökova, Turkey*, 33–40 (2014). [arXiv:1311.6124](#)
30. Uchida, K.: Galois group of an equation $X^n - aX + b = 0$. *Tohoku Math. J.* **22**, 670–678 (1970)
31. Vakil, R.: Schubert induction. *Ann. Math.* **164**, 489–512 (2006). [arXiv:math/0302296](#)