Overdetermined systems of sparse polynomial equations

OVERDETERMINED SYSTEMS OF SPARSE POLYNOMIAL EQUATIONS

FRANCESCO AMOROSO, LOUIS LEROUX, AND MARTÍN SOMBRA

Abstract. We show that, for a system of univariate polynomials given in sparse encoding, we can compute a single polynomial defining the same zero set, in time quasi-linear in the logarithm of the degree. In particular, it is possible to determine whether such a system of polynomials does have a zero in time quasi-linear in the logarithm of the degree. The underlying algorithm relies on a result of Bombieri and Zannier on multiplicatively dependent points in subvarieties of an algebraic torus.

We also present the following conditional partial extension to the higher dimensional setting. Assume that the effective Zilber conjecture holds. Then, for a system of multivariate polynomials given in sparse encoding, we can compute a finite collection of complete intersections outside hypersurfaces that defines the same zero set, in time quasi-linear in the logarithm of the degree.

1. Introduction

A system of polynomial equations

$$f_1 = \cdots = f_s = 0 \tag{1.1}$$

is "overdetermined" if the number of equations exceeds the codimension of its zero set. Our aim is to give algorithms for reducing those systems of equations to a finite number of "well-determined" systems. We focus on the case when the input polynomials are sparse in the sense that they have high degree but relatively few nonzero terms and small coefficients, and we want our algorithms to be as efficient as possible in that situation.

For univariate polynomials, the reduction of an overdetermined system as in (1.1) with $s \geq 2$, might be done by computing the greatest common divisor of the f_i's. However, this strategy does not work in our situation because the gcd of a family of sparse polynomials is not necessarily sparse, as shown by the following example due to Schinzel [Schi02]: if $a, b \geq 1$ are coprime, then

$$\gcd(x^{ab} - 1, (x^a - 1)(x^b - 1)) = \frac{(x^a - 1)(x^b - 1)}{x - 1}.$$

This polynomial has $2\min(a, b)$ nonzero terms. Hence, for $a, b \gg 0$, both $x^{ab} - 1$ and $(x^a - 1)(x^b - 1)$ are sparse, but their gcd is not.

Date: October 22, 2023.

2010 *Mathematics Subject Classification.* Primary 11Y16; Secondary 12Y05, 68W30.

Key words and phrases. Sparse polynomial, overdetermined system of equations, algebraic torus, unlikely intersections.

Amoroso and Leroux were partially supported by the CNRS research project PICS "Properties of the heights of arithmetic varieties". Amoroso was also partially supported by the ANR research project "Hauteurs, modularité, transcendance". Sombra was partially supported by the MICINN research projects MTM2009-14163-C02-01 and MTM2012-38122-C03-02.

This example suggests that one should avoid polynomials vanishing at roots of unity. Indeed, Filaseta, Granville and Schinzel have shown that, if $f, g \in \mathbb{Z}[x]$ are given in sparse encoding and either f or g do not vanish at any root of unity, then $\gcd(f,g)$ can be computed with $\widetilde{O}(\log(d))$ ops [FGS08]. Here, *ops* is an abbreviation of "bit operations", and the "soft O" notation indicates a bound with an extra factor of type $(\log\log(d))^{O(1)}$ and implicit constants depending on the size of the coefficients and number of nonzero terms of f and g. Their algorithm relies heavily on a theorem of Bombieri and Zannier on the intersection of a subvariety of the algebraic torus with subtori of dimension 1 [Schi00, Appendix], see also § 3.

Our first result is an extension of the algorithm of Filaseta, Granville and Schinzel, allowing the case when both f and g vanish at roots of unity. From now on, we fix a number field $K \subset \overline{\mathbb{Q}}$. Given $f_1, \dots, f_s \in K[x_1, \dots, x_n]$, we denote by $V(f_1, \dots, f_s)$ their set of common zeros in the affine space $\mathbb{A}^n = \overline{\mathbb{Q}}^n$. Polynomials are given in sparse encoding. Recall that the height of a polynomial is a measure of the bit size of its coefficients, see § 2.1 for details. The following statement makes the output and the complexity of our algorithm precise.

Theorem 1.1. *There is an algorithm that, given $f, g \in K[x]$, computes $p_1, p_2 \in K[x]$ such that*

$$p_1 | \gcd(f,g), \quad V(p_1) \setminus \mu_\infty = V(\gcd(f,g)) \setminus \mu_\infty, \quad \text{and} \quad V(p_2) = V(\gcd(f,g)) \cap \mu_\infty,$$

where μ_∞ denotes the subgroup of $\overline{\mathbb{Q}}^\times$ of roots of unity.

If both f and g have degree bounded by d and height and number of nonzero coefficients bounded by c, this computation is done with $\widetilde{O}(\log(d))$ ops, where the implicit constants depend only on K and c.

This result is a simplified version of Theorem 4.5, which holds for families of univariate polynomials and gives more information about the output polynomials. The underlying procedure is given by Algorithms 4.2 and 4.3. A preliminary version appears in the second author's Ph.D. thesis [Ler11].

In the notation of Theorem 1.1, we have that

$$V(p_1 p_2) = V(f,g). \tag{1.2}$$

Hence, given two univariate polynomials with bounded height and number of nonzero coefficients, we can compute a polynomial which has the same zero set as their gcd, with complexity quasi-linear in the logarithm of the degree. In particular, we deduce the following corollary.

Corollary 1.2. *Let $f, g \in K[x]$ be polynomials of degree $\leq d$ and height and number of nonzero coefficients bounded by a constant c. We can decide if*

$$\gcd(f,g) = 1$$

with $\widetilde{O}(\log(d))$ ops, where the implicit constants depend only on K and c.

A classical result of Plaisted says that computing the degree of the gcd of two univariate polynomials given in sparse encoding is an NP-hard problem [Pla77]. Using Plaisted's techniques in *loc. cit.*, it can be shown that already deciding if the degree of the gcd is zero, is an NP-hard problem. Hence, if Cook's conjecture P $\neq$ NP holds, it is not possible to decide if the degree of the gcd is zero with a complexity which is polynomial in the height, number of nonzero terms, and logarithm of the degree of the input polynomials. In contrast to this, Corollary 1.2 shows that this problem can be solved with a complexity which is quasi-linear in the logarithm of the degree although, *a priori*, not polynomial in the height and number of nonzero terms.

Our algorithms for the multivariate case rely on an effective version of the Zilber conjecture generalizing the quoted theorem of Bombieri and Zannier. For $N \geq 0$, we denote by $\mathbb{G}_{\mathrm{m}}^N = (\overline{\mathbb{Q}}^\times)^N$ the (split) algebraic torus over $\overline{\mathbb{Q}}$ of dimension N. Recall that a torsion coset of $\mathbb{G}_{\mathrm{m}}^N$ is a connected component of an algebraic subgroup or, equivalently, a translate of a subtorus by a torsion point. The effective Zilber conjecture can then be stated as follows:

> *Let W be an irreducible subvariety of $\mathbb{G}_{\mathrm{m}}^N$. There exists a finite and effectively calculable collection Ω of torsion cosets of $\mathbb{G}_{\mathrm{m}}^N$ of codimension 1 such that, if B is a torsion coset of $\mathbb{G}_{\mathrm{m}}^N$ and C an irreducible component of $B \cap W$ such that*
>
> $$\dim(C) > \dim(B) - \operatorname{codim}(W),$$
>
> *then there exists $T \in \Omega$ such that $C \subset T$.*

Zilber proposed this conjecture (under the equivalent formulation that we recall in Conjecture 3.4) in connection with the so-called "uniform Schanuel conjecture" and motivated by problems from model theory [Zil02]. It is still unproven, but several interesting cases are already known. When we restrict to $\dim(B) = 0$, the statement is equivalent to the toric case of the Manin-Mumford conjecture. This is a well-known theorem of Laurent [Lau84] and an effective proof of it can be found in Schmidt's paper [Schm96] or, more explicitly, in the second author's paper [Ler12]. The result by Bombieri and Zannier solves the case when we restrict to $\dim(B) = 1$. The case when W is a curve was proved by Maurin [Mau08], building on previous work by Bombieri, Masser and Zannier [BMZ99]. Moreover, the closely related "bounded height conjecture" has been proved by Habegger in the general case [Hab09].

The Zilber conjecture plays a central role in the study of "unlikely intersections" and has many applications in number theory, see for instance the survey [Cha12] and the book [Zan12] for accounts of this very active area of research.

A well-determined system of polynomial equations is, by definition, a complete intersection. The solution set of a system of multivariate polynomial equations cannot always be redefined by a single complete intersection, since it might have components of different codimensions and, moreover, these components might not be complete intersections either. Instead, this solution set can be described as a finite union of complete intersections on open subsets (Proposition-Definition 2.1). Such a decomposition can be understood as a sort of generalization to the multivariate setting of the polynomial p_1p_2 in (1.2) from the univariate case.

The main result of this paper is an algorithm giving a conditional partial computation of this decomposition for an arbitrary system of multivariate polynomials (Algorithm 5.5). The following statement makes the size of its output and its complexity precise.

Theorem 1.3. *Assume that the effective Zilber conjecture holds. There is an algorithm that, given $f_1, \dots, f_s \in K[x_1, \dots, x_n]$, computes a finite collection Γ whose elements are sequences $(p_1, \dots, p_r, q)$ of polynomials in $K(\omega)[x_1, \dots, x_n]$ with ω a root of unity,* *such that either* $\operatorname{codim}(V(p_1,\dots,p_r)\backslash V(q))=r$ *or* $V(p_1,\dots,p_r)\backslash V(q)=\emptyset$*, and*

$$V(f_1,\dots,f_s)=\bigcup_{(p_1,\dots,p_r,q)\in\Gamma}V(p_1,\dots,p_r)\backslash V(q). \tag{1.3}$$

If both n and s are bounded by a constant c and each f_i is of degree $\le d$ and height and number of nonzero terms bounded by c, then the cardinality of Γ is bounded by $O(1)$, the order of ω is bounded by $O(1)$, the polynomials in Γ have degree bounded by $d^{O(1)}$, height and number of nonzero coefficients bounded by $O(1)$, and the computation is done with $\widetilde{O}(\log(d))$ ops, where the implicit constants depend only on K and c.

A previous result in this direction, for systems of three polynomials in two variables, appears in the second author's Ph.D. thesis [Ler11].

From (1.3), one can derive a well-determined description of $V(f_1,\dots,f_s)$ by throwing away the empty pieces. The bounds in Theorem 1.3 imply that, if the input polynomials are sparse, then this decomposition into complete intersections outside hypersurfaces is defined by polynomials that are also sparse. The actual computation of such a decomposition from the output of Algorithm 5.5 amounts to deciding when $V(p_1,\dots,p_r)\backslash V(q)=\emptyset$ for each $(p_1,\dots,p_r,q)\in\Gamma$. Unfortunately, it is not clear yet how to perform this task with $\widetilde{O}(\log(d))$ ops, see Problem 1.5 below.

The idea for the algorithms underlying Theorems 1.1 and 1.3 is inspired by the method in [FGS08]. It can be explained as follows. First, by decomposing the affine space into a disjoint union of algebraic tori, the problem can be reduced to the analogous problem on the open subset $\mathbb{G}_{\mathrm{m}}^n\subset\mathbb{A}^n$. Write

$$f_i=\sum_{j=1}^N\alpha_{i,j}\boldsymbol{x}^{\boldsymbol{a}_j}\in K[x_1,\dots,x_n],\quad i=1,\dots,s, \tag{1.4}$$

with $\alpha_{i,j}\in K$ and $\boldsymbol{a}_j\in\mathbb{Z}^n$. Then we consider the homomorphism $\varphi\colon\mathbb{G}_{\mathrm{m}}^n\to\mathbb{G}_{\mathrm{m}}^N$ defined by the exponents $\boldsymbol{a}_j$, $j=1,\dots,s$ and the linear forms $\ell_i=\sum_{j=1}^N\alpha_{i,j}y_j$, $i=1,\dots,s$. These forms define a linear subvariety W of $\mathbb{G}_{\mathrm{m}}^N$ such that

$$\varphi^{-1}(W)=V(f_1,\dots,f_s)\cap\mathbb{G}_{\mathrm{m}}^n. \tag{1.5}$$

Roughly speaking, the next step consists of producing a stratification of W by successively intersecting this subvariety with torsion cosets of codimension 1 produced by the effective Zilber conjecture. The output of the algorithm is obtained by considering the inverse image under the homomorphism φ of some of the pieces of this stratification.

Several questions arose during our work, and we close this introduction by pointing out two of them. Both problems have interesting algorithmic consequences and seem to be related to the study of unlikely intersections in algebraic tori.

Problem 1.4. *Give an algorithm for computing the degree of the gcd of two polynomials given in the sparse encoding, of degree $\le d$ and bounded height and number of coefficients, with $\widetilde{O}(\log(d))$ ops.*

An affirmative answer to Problem 1.4 would allow to test divisibility of sparse polynomials with complexity quasi-linear in the logarithm of their degree.

Problem 1.5. *In the setting of Theorem 1.3, modify the underlying algorithm to exclude the possibility that $V(p_1,\dots,p_r)\backslash V(q)=\emptyset$.*

An affirmative answer to Problem 1.5 would allow us to compute the dimension of $V(f_1,\dots,f_s)$ with $\widetilde{O}(\log(d))$ ops. In particular, we could then determine whether the zero set $V(f_1,\dots,f_s)$ is empty with $\widetilde{O}(\log(d))$ ops, extending Corollary 1.2 to the multidimensional case.

Acknowledgments. We thank Gaël Rémond and Umberto Zannier for useful discussions about unlikely intersections and the Zilber conjecture. We also thank the referees for their many remarks that helped us to improve our presentation.

Part of this work was done while the authors met at the Universitat de Barcelona, the Université de Caen and the Centro di Ricerca Matematica Ennio de Giorgi (Pisa). We thank these institutions for their hospitality.

2. Notation and auxiliary results

We fix a number field $K \subset \overline{\mathbb{Q}}$. Bold letters denote finite sets or sequences of objects, where the type and number should be clear from the context: for instance, $\boldsymbol{x}$ might denote the group of variables $\{x_1,\dots,x_n\}$, so that $K[\boldsymbol{x}^{\pm1}]$ denotes the ring of Laurent polynomials $K[x_1^{\pm1},\dots,x_n^{\pm1}]$.

Given functions $f,g\colon \mathbb{N} \to \mathbb{R}_{>0}$, the Landau symbols $f = O(g)$ and $f = \widetilde{O}(g)$ respectively mean that there are positive constants $c_1,c_2 \geq 0$ such that, for all $m \in \mathbb{N}$,

$$f(m) \leq c_1\, g(m), \quad f(m) \leq c_1\, g(m) \max(1,\log(g(m)))^{c_2}.$$

If we want to emphasize the dependence of the constants c_1 and c_2 on parameters, say N and h, we will write $f = O_{N,h}(g)$ and $f = \widetilde{O}_{N,h}(g)$, respectively. When these parameters are said to be "bounded", we omit them from the notation as we do, for instance, in Lemma 2.3.

2.1. **Integers and Laurent polynomials.**

We denote by $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{Q}$ the monoid of natural numbers with 0, the ring of integers and the field of rational numbers, respectively. At the computational level, integers are represented in bit encoding and rational numbers are represented as quotients of integers. The complexity of an algorithm will be measured in bit operations (*ops*).

A *multiplication time function* is a function

$$\mathrm{M}\colon \mathbb{N} \to \mathbb{N}$$

such that integers of bit length $\leq k$ can be multiplied using at most $\mathrm{M}(k)$ ops. We also assume that, for $k,l \in \mathbb{N}$, this function verifies $\mathrm{M}(kl) \leq k^2\mathrm{M}(l)$ and, if $k \geq l$, it also verifies $\mathrm{M}(k)/k \geq \mathrm{M}(l)/l$.

Such a function dominates the complexity of many of the basic computations on $\mathbb{Z}$. In particular, for integers of bit length $\leq k$, division with remainder can be done with $O(\mathrm{M}(k))$ ops, and their gcd can be computed with $O(\mathrm{M}(k)\log(k))$ ops [GG03]. By the Schönhage-Strassen algorithm [GG03, Theorem 8.24], we can take

$$\mathrm{M}(k) = O(k\log(k)\log(\log(k))) = \widetilde{O}(k).$$

The number field K is represented by a monic irreducible polynomial $h \in \mathbb{Q}[z]$ such that $K \simeq \mathbb{Q}[z]/(h)$. The arithmetic operations of K (sum, difference, multiplication and division by a nonzero element) can be computed in terms of this representation. We will not be concerned by their complexity, since it will be absorbed by the constants in our bounds.

For $l \geq 1$, we denote by μ_l the subgroup of $\overline{\mathbb{Q}}^{\times}$ of roots of unity of order dividing l. We also set μ_∞ for the subgroup of $\overline{\mathbb{Q}}^{\times}$ of all roots of unity. Hence,

$$\mu_\infty = \bigcup_{l \geq 1} \mu_l.$$

For $N \geq 0$, an N-tuple of roots of unity $\boldsymbol{\eta} \in \mu_l^N$ is represented as $\boldsymbol{\eta} = (\omega^{i_1}, \dots, \omega^{i_N})$ with ω a primitive l-th root of unity and $0 \leq i_j \leq l-1$. A representation of the finite extension $K(\boldsymbol{\eta})$ can be computed in terms of $\boldsymbol{\eta}$ and a representation of K. Again, the complexity of computing this representation will play no role in our results.

Laurent polynomials will be represented in sparse encoding: a Laurent polynomial $f \in K[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$ will be given by a sequence of pairs $(\boldsymbol{a}_j, \alpha_j) \in \mathbb{Z}^n \times K$, $j = 1, \dots, N$, such that

$$f = \sum_{j=1}^{N} \alpha_j \boldsymbol{x}^{\boldsymbol{a}_j}.$$

We assume that $\boldsymbol{a}_j \neq \boldsymbol{a}_k$ for $j \neq k$.

For a vector $\boldsymbol{a} = (a_1, \dots, a_n) \in \mathbb{Z}^N$, we denote its ℓ^1-norm by

$$|\boldsymbol{a}| = |a_1| + \cdots + |a_n|.$$

We respectively define the *support* and the *degree* of f as

$$\operatorname{supp}(f) = \{\boldsymbol{a}_j \mid \alpha_j \neq 0\}, \quad \deg(f) = \max_{\boldsymbol{a}_j \in \operatorname{supp}(f)} |\boldsymbol{a}_j|.$$

When f is a polynomial, this notion of degree coincides with the usual one.

We define the *height* of f, denoted $\mathrm{h}(f)$, as the Weil height of the projective point $(1 : \alpha_1 : \cdots : \alpha_N) \in \mathbb{P}^N$, see for instance [BG06, Chapter 2] or [Zan09, Chapter 3] for details. In the particular case when $f \in \mathbb{Z}[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$,

$$\mathrm{h}(f) = \max_j \log |\alpha_j|.$$

Ideals of $K[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$ are represented by finite families of generators.

2.2. Subvarieties and locally closed subsets.

For $N \geq 0$, we set $\mathbb{G}_{\mathrm{m}}^N = (\overline{\mathbb{Q}}^{\times})^N$ and $\mathbb{A}^N = \overline{\mathbb{Q}}^n$ for the algebraic torus and the affine space over $\overline{\mathbb{Q}}$ of dimension N. We will mostly work over the algebraic torus and so, for simplicity, we will define and study subvarieties and locally closed subsets in that setting. Nevertheless the notions and properties in this subsection can be easily transported to the affine space.

A *subvariety* of $\mathbb{G}_{\mathrm{m}}^N$ is the zero set of an ideal of $\overline{\mathbb{Q}}[y_1^{\pm 1}, \dots, y_N^{\pm 1}]$. Following this convention, a subvariety is not necessarily irreducible. More generally, a *locally closed subset* of $\mathbb{G}_{\mathrm{m}}^N$ is the intersection of a subvariety with a (Zariski) open subset. The *dimension* of a locally closed subset is defined as the dimension of its (Zariski) closure. A locally closed subset is *irreducible* if its closure is.

Let W be a locally closed subset of $\mathbb{G}_{\mathrm{m}}^N$. An *irreducible component* of W is an irreducible locally closed subset $C \subset W$ that is maximal with respect to inclusion. An irreducible locally closed subset $C \subset W$ is an irreducible component of W if and only if $\overline{C}$ is an irreducible component of $\overline{W}$ and $C = \overline{C} \cap W$. We denote by $\operatorname{irr}(W)$ the finite collection of the irreducible components of W. There is an irredundant decomposition

$$W = \bigcup_{C \in \operatorname{irr}(W)} C.$$

Given a family of Laurent polynomials $\boldsymbol{F} = \{F_1, \dots, F_s\} \subset \overline{\mathbb{Q}}[y_1^{\pm 1}, \dots, y_N^{\pm 1}]$, we set

$$V(\boldsymbol{F}) = V(F_1, \dots, F_s) = \{\boldsymbol{y} \in \mathbb{G}_{\mathrm{m}}^N \mid F_1(\boldsymbol{y}) = \cdots = F_s(\boldsymbol{y}) = 0\}$$

for the associated subvariety of $\mathbb{G}_{\mathrm{m}}^N$. A family of Laurent polynomials over K can be considered as a family of Laurent polynomials over $\overline{\mathbb{Q}}$ *via* the inclusion $K \hookrightarrow \overline{\mathbb{Q}}$. In particular, such a family of Laurent polynomials defines a subvariety of $\mathbb{G}_{\mathrm{m}}^N$.

We represent a subvariety W of $\mathbb{G}_{\mathrm{m}}^N$ by a finite family of Laurent polynomials $\boldsymbol{F} \subset \overline{\mathbb{Q}}[y_1^{\pm 1}, \dots, y_N^{\pm 1}]$ such that $W = V(\boldsymbol{F})$. More generally, a locally closed subset W of $\mathbb{G}_{\mathrm{m}}^N$ is represented by two finite families $\boldsymbol{F}, \boldsymbol{G} \subset \overline{\mathbb{Q}}[y_1^{\pm 1}, \dots, y_N^{\pm 1}]$ such that $W = V(\boldsymbol{F}) \setminus V(\boldsymbol{G})$. A subvariety or a locally closed subset of $\mathbb{G}_{\mathrm{m}}^N$ defined over K are represented similarly by finite families of Laurent polynomials over K.

Let W be a subvariety of $\mathbb{G}_{\mathrm{m}}^N$. If W is a hypersurface, then there exists $F \in \overline{\mathbb{Q}}[\boldsymbol{y}^{\pm 1}]$ such that $W = V(F)$ because the ring $\overline{\mathbb{Q}}[\boldsymbol{y}^{\pm 1}]$ is a unique factorization domain. If the codimension of W is higher, then W cannot always be described as a complete intersection. However, it is possible to describe a subvariety or, more generally, a locally closed subset, as a finite union of complete intersections outside hypersurfaces.

Proposition-Definition 2.1. *Let W be a locally closed subset of $\mathbb{G}_{\mathrm{m}}^N$. Then there exists a family of locally closed subsets W_j, $j = 1, \dots, t$, given as*

$$W_j = V(F_{j,1}, \dots, F_{j,\mathrm{codim}(W_j)}) \backslash V(G_j)$$

with $F_{j,l}$, $G_j \in \overline{\mathbb{Q}}[y_1^{\pm 1}, \dots, y_N^{\pm 1}]$, and satisfying the following conditions:

(1) $\mathrm{codim}(W) = \mathrm{codim}(W_1) < \cdots < \mathrm{codim}(W_t) \leq N$;

(2) $W = \bigcup_{i=1}^t W_j$.

A family of locally closed subset $(W_j)_j$ as above is called a complete intersection stratification *of W.*

If W is defined over K, then $(W_j)_j$ can be chosen to be defined over K too. In that case, the complete intersection stratification is said to be defined over *K.*

Proof. Set $c = \mathrm{codim}(W)$. We first show that there exist $F_1, \dots, F_c, G \in \overline{\mathbb{Q}}[\boldsymbol{y}^{\pm 1}]$ such that $F_1, \dots, F_c$ is a complete intersection, $V(G)$ contains no irreducible component of W of codimension c and

$$W \backslash V(G) = V(F_1, \dots, F_c) \backslash V(G). \tag{2.1}$$

Let $\boldsymbol{P}, \boldsymbol{Q} \subset \overline{\mathbb{Q}}[\boldsymbol{y}^{\pm 1}]$ such that $W = V(\boldsymbol{P}) \setminus V(\boldsymbol{Q})$ and set

$$F_l = \sum_i \lambda_{l,i} P_i, \quad l = 1, \dots, c, \quad \text{and} \quad Q = \sum_j \mu_j Q_j$$

for a choice of $\lambda_{l,i}, \mu_j \in \overline{\mathbb{Q}}$. It can be shown that if this choice is generic in the sense that the point $(\boldsymbol{\lambda}, \boldsymbol{\mu})$ does not lie in a certain hypersurface of the parameter space, then $F_1, \dots, F_c$ defines a complete intersection in the complement of $V(\boldsymbol{Q})$, and the hypersurface $V(Q)$ contains no irreducible component of W. Assume that our choice of $\lambda_{l,i}, \mu_j$ is generic in this sense. Then we have that

$$W \setminus V(Q) \subset V(\boldsymbol{F}) \setminus V(Q)$$

and, if C is an irreducible component of W of codimension c, then $C \setminus V(Q)$ is an irreducible component of both $W \setminus V(Q)$ and $V(\boldsymbol{F}) \setminus V(Q)$.

Choose $Q' \in \overline{\mathbb{Q}}[\boldsymbol{y}^{\pm 1}]$ such that the hypersurface $V(Q')$ contains the irreducible components of $W \setminus V(Q)$ of codimension $\geq c + 1$ and the irreducible components of $V(\boldsymbol{F}) \setminus V(Q)$ which are not a component of $W \setminus V(Q)$, and does not contain any of the other ones. Finally, set $G = QQ'$. It is not difficult to verify that the Laurent polynomials $F_1, \dots, F_c, G$ satisfy (2.1).

If $\boldsymbol{P}, \boldsymbol{Q} \subset K[\boldsymbol{y}^{\pm 1}]$, we can also verify that $\lambda_{l,i}, \mu_j$ and the coefficients of Q' can be chosen to lie in K, so that $F_1, \dots, F_c, G \in K[\boldsymbol{y}^{\pm 1}]$.

Now set $W_1 = V(\boldsymbol{F}) \setminus V(G)$ with $\boldsymbol{F}, G$ as in (2.1). The intersection $W \cap V(G)$ has codimension $\geq c+1$, and so we can construct $W_2, \dots, W_t$ by applying this construction iteratively. The family $(W_j)_j$ that we obtain satisfies the conditions (1) and (2). It is also clear that, if W is defined over K, then so is $(W_j)_j$. □

Given a locally closed subset W of $\mathbb{G}_{\mathrm{m}}^N$, a complete intersection stratification can be computed either by applying elimination theory or Gröbner basis algorithms. For instance, the computation of the first piece W_1 in the case when $\operatorname{codim}(W) = 2$ has been worked out in detail in the second author's Ph.D. thesis [Ler11, § 2.2.2]. The complexity of this procedure will play no role in our results.

Given a map $\phi \colon \mathbb{G}_{\mathrm{m}}^n \to \mathbb{G}_{\mathrm{m}}^N$, we denote by

$$\phi^{\#} \colon \overline{\mathbb{Q}}[y_1^{\pm 1}, \dots, y_N^{\pm 1}] \longrightarrow \overline{\mathbb{Q}}[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$$

the associated morphism of algebras. If $\psi \colon \mathbb{G}_{\mathrm{m}}^N \to \mathbb{G}_{\mathrm{m}}^M$ is a further map, then

$$(\psi \circ \phi)^{\#} = \phi^{\#} \circ \psi^{\#}. \tag{2.2}$$

Given an ideal $I \subset \overline{\mathbb{Q}}[\boldsymbol{y}^{\pm 1}]$, we denote by $\phi^{\#}(I)$ the ideal of $\overline{\mathbb{Q}}[\boldsymbol{x}^{\pm 1}]$ generated by the image of I under $\phi^{\#}$. We have that

$$V(\phi^{\#}(I)) = \phi^{-1}(V(I)). \tag{2.3}$$

2.3. **Homomorphisms and torsion cosets of algebraic tori.** We recall the basic notation and properties of homomorphisms and algebraic subgroups of tori. We refer to [BG06, § 3.2] or [Zan09, Chapter 4] for more details, including the proofs of the quoted results.

For $n, N \geq 0$, we denote by $\operatorname{Hom}(\mathbb{G}_{\mathrm{m}}^n, \mathbb{G}_{\mathrm{m}}^N)$ the set of homomorphism from $\mathbb{G}_{\mathrm{m}}^n$ to $\mathbb{G}_{\mathrm{m}}^N$, and by $\operatorname{Aut}(\mathbb{G}_{\mathrm{m}}^N)$ the group of automorphisms of $\mathbb{G}_{\mathrm{m}}^N$. We denote by $\mathrm{id}_{\mathbb{G}_{\mathrm{m}}^N}$ the identity automorphism of $\mathbb{G}_{\mathrm{m}}^N$.

Given a point $\boldsymbol{x} = (x_1, \dots, x_n) \in \mathbb{G}_{\mathrm{m}}^n$ and a vector $\boldsymbol{a} = (a_1, \dots, a_n) \in \mathbb{Z}^n$, we set $\boldsymbol{x}^{\boldsymbol{a}} = x_1^{a_1} \cdots x_n^{a_n}$. A matrix $A \in \mathbb{Z}^{N \times n}$ with rows $\boldsymbol{a}_1, \dots, \boldsymbol{a}_N \in \mathbb{Z}^n$ gives a homomorphism $\varphi_A \colon \mathbb{G}_{\mathrm{m}}^n \to \mathbb{G}_{\mathrm{m}}^N$ defined, for $\boldsymbol{x} \in \mathbb{G}_{\mathrm{m}}^n$, by

$$\varphi_A(\boldsymbol{x}) = (\boldsymbol{x}^{\boldsymbol{a}_1}, \dots, \boldsymbol{x}^{\boldsymbol{a}_N}).$$

The correspondence $A \mapsto \varphi_A$ is a bijection between $\mathbb{Z}^{N \times n}$ and $\operatorname{Hom}(\mathbb{G}_{\mathrm{m}}^n, \mathbb{G}_{\mathrm{m}}^N)$. Given matrices $A \in \mathbb{Z}^{N \times n}$ and $B \in \mathbb{Z}^{M \times N}$, we have that

$$\varphi_B \circ \varphi_A = \varphi_{BA}.$$

We define the *size* of a homomorphism $\varphi \in \operatorname{Hom}(\mathbb{G}_{\mathrm{m}}^n, \mathbb{G}_{\mathrm{m}}^N)$ as

$$\operatorname{size}(\varphi) = \max_j |\boldsymbol{a}_j|,$$

where $\boldsymbol{a}_j$, $j = 1, \dots, N$, are the rows of the matrix corresponding to φ.

We denote by $1_{\mathbb{G}_{\mathrm{m}}^N} = (1, \dots, 1)$ the neutral element of $\mathbb{G}_{\mathrm{m}}^N$. The subgroup of torsion points of $\mathbb{G}_{\mathrm{m}}^N$ agrees with μ_∞^N. A *subtorus* of $\mathbb{G}_{\mathrm{m}}^N$ is a connected algebraic subgroup or, equivalently, an algebraic subgroup which is the image of a homomorphism. A *torsion coset* of $\mathbb{G}_{\mathrm{m}}^N$ is the translate of a subtorus by a torsion point. A *torsion subvariety* of $\mathbb{G}_{\mathrm{m}}^N$ is a finite union of torsion cosets.

A submodule Λ of $\mathbb{Z}^N$ defines an algebraic subgroup of $\mathbb{G}_{\mathrm{m}}^N$ by

$$H_\Lambda = V(\{\boldsymbol{y}^{\boldsymbol{b}} - 1 \mid \boldsymbol{b} \in \Lambda\}). \tag{2.4}$$

The correspondence $\Lambda \to H_\Lambda$ is a bijection between the set of submodules of $\mathbb{Z}^N$ and that of algebraic subgroups of $\mathbb{G}_{\mathrm{m}}^N$. This correspondence reverses dimension, in the sense that

$$\operatorname{codim}(H_\Lambda) = \operatorname{rank}(\Lambda).$$

The algebraic subgroup H_Λ is a subtorus if and only if the subgroup Λ is *saturated*, that is, if and only if $\Lambda = \mathbb{R}\Lambda \cap \mathbb{Z}^N$.

For a submodule Λ of $\mathbb{Z}^N$, we denote by $\Lambda^{\mathrm{sat}} = \mathbb{R}\Lambda \cap \mathbb{Z}^N$ its *saturation.* Then $H_{\Lambda^{\mathrm{sat}}}$ is a subtorus and there is a finite subgroup $F \subset \mu_\infty^N$ of cardinality $[\Lambda^{\mathrm{sat}} : \Lambda]$ such that

$$H_\Lambda = F \cdot H_{\Lambda^{\mathrm{sat}}}. \tag{2.5}$$

Given a locally closet subset $Y \subset \mathbb{G}_{\mathrm{m}}^N$, we denote by $\langle Y \rangle$ the minimal algebraic subgroup of $\mathbb{G}_{\mathrm{m}}^N$ containing Y. Equivalently,

$$\langle Y \rangle = \bigcap_{H \supset Y} H,$$

the intersection being over all algebraic subgroups H of $\mathbb{G}_{\mathrm{m}}^N$ containing Y. The *multiplicative rank* of Y is defined as

$$\operatorname{rank}(Y) = \dim(\langle Y \rangle).$$

For instance, a point of $\mathbb{G}_{\mathrm{m}}^N$ has rank 0 if and only if it is a torsion point, and it has rank N if and only if its coordinates are multiplicatively independent.

The following lemma studies the behavior of the multiplicative rank under a homomorphism of algebraic tori.

Lemma 2.2. *Let $\varphi\colon \mathbb{G}_{\mathrm{m}}^n \to \mathbb{G}_{\mathrm{m}}^N$ be a homomorphism, $Y \subset \operatorname{im}(\varphi)$ a irreducible locally closed subset and C an irreducible component of $\varphi^{-1}(Y)$. Then*

$$\operatorname{rank}(C) - \dim(C) = \operatorname{rank}(Y) - \dim(Y).$$

Proof. For each point $\boldsymbol{\xi} \in Y$, we have that $\varphi^{-1}(\boldsymbol{\xi})$ is a translate of the kernel of φ by a point of $\mathbb{G}_{\mathrm{m}}^n$. Hence $\dim(\varphi^{-1}(\boldsymbol{\xi})) = \dim(\ker(\varphi))$ and, by the theorem of dimension of fibers,

$$\dim(\varphi^{-1}(Y)) = \dim(Y) + \dim(\ker(\varphi)) \tag{2.6}$$

Set $H = \langle \varphi^{-1}(Y) \rangle$ for the minimal algebraic subgroup of $\mathbb{G}_{\mathrm{m}}^n$ containing $\varphi^{-1}(Y)$. If $\boldsymbol{\xi}$ is any point of Y, then $\varphi^{-1}(\boldsymbol{\xi}) \subset H$. Since $\varphi^{-1}(\boldsymbol{\xi})$ is a translate of $\ker(\varphi)$ and H is a group, it follows that $\ker(\varphi) \subset H$. Moreover, we have that $\varphi(H) = \langle Y \rangle$ and so there is an exact sequence $0 \to \ker(\varphi) \to \langle \varphi^{-1}(Y) \rangle \to \langle Y \rangle \to 0$. We deduce that

$$\begin{aligned} \operatorname{rank}(\varphi^{-1}(Y)) &= \dim(\langle \varphi^{-1}(Y) \rangle) \\ &= \dim(\langle Y \rangle) + \dim(\ker(\varphi)) = \operatorname{rank}(Y) + \dim(\ker(\varphi)). \end{aligned} \tag{2.7}$$

Let $F \subset \mu_\infty^N$ be a finite subgroup and $T \subset \mathbb{G}_{\mathrm{m}}^N$ a subtorus such that $\ker(\varphi) = F \cdot T$ as in (2.5) . Let C be an irreducible component of $\varphi^{-1}(Y)$. Then the decomposition of $\varphi^{-1}(Y)$ into irreducible components is given by

$$\varphi^{-1}(Y) = \bigcup_{\boldsymbol{\eta} \in F} \boldsymbol{\eta} C.$$

Hence, $\dim(C) = \dim(\varphi^{-1}(Y))$ and $\operatorname{rank}(C) = \operatorname{rank}(\varphi^{-1}(Y))$. The statement then follows from (2.6) and (2.7). □

We represent torsion cosets as complete intersections of binomials whose coefficients are roots of unity. In precise terms, let B be a torsion coset of $\mathbb{G}_{\mathrm{m}}^N$ and write $B = \boldsymbol{\eta} H_\Lambda$ with $\boldsymbol{\eta} \in \mu_\infty$ and H_Λ a subtorus of codimension r corresponding to a saturated submodule $\Lambda \subset \mathbb{Z}^N$. Choose a basis $\boldsymbol{b}_j \in \mathbb{Z}^N$, $j = 1, \dots, r$, of Λ. Then there exist $\xi_j \in \mu_\infty$, $j = 1, \dots, r$, such that

$$B = V(\boldsymbol{y}^{\boldsymbol{b}_1} - \xi_1, \dots, \boldsymbol{y}^{\boldsymbol{b}_r} - \xi_r). \tag{2.8}$$

The following procedure allows us to compute the preimage of a torsion coset under a homomorphism.

Algorithm 2.1 (Preimage of a torsion coset)

Input: a homomorphism $\varphi\colon \mathbb{G}_{\mathrm{m}}^n \to \mathbb{G}_{\mathrm{m}}^N$ and a torsion coset $B \subset \mathbb{G}_{\mathrm{m}}^N$.
Output: either "$\varphi^{-1}(B) = \emptyset$" or a finite collection $\boldsymbol{E} \subset \overline{\mathbb{Q}}[\boldsymbol{x}^{\pm 1}]$ of binomials with coefficients in μ_∞.

```
Let $A \in \mathbb{Z}^{N\times n}$ be the $N \times n$-matrix of $\varphi$ and write $B = V(\boldsymbol{y}^{\boldsymbol{b}_1} - \xi_1, \dots, \boldsymbol{y}^{\boldsymbol{b}_r} - \xi_r)$
  with $\boldsymbol{b}_j \in \mathbb{Z}^N$ and $\xi_j \in \mu_\infty$;
set $\boldsymbol{c}_j = \boldsymbol{b}_j A \in \mathbb{Z}^n$, $j = 1, \dots, r$;
compute a basis $\boldsymbol{e}_k \in \mathbb{Z}^n$, $k = 1, \dots, t$, of the submodule generated by the $\boldsymbol{c}_j$'s;
compute $\lambda_{k,j}, \mu_{j,k} \in \mathbb{Z}$ such that $\boldsymbol{e}_k = \sum_j \lambda_{k,j}\boldsymbol{c}_j$ and $\boldsymbol{c}_j = \sum_k \mu_{j,k}\boldsymbol{e}_k$;
set $\rho_k \leftarrow \prod_j \xi_j^{\lambda_{k,j}}$, $k = 1, \dots, t$;
if $\prod_k \rho_k^{\mu_{j,k}} = \xi_j$ for all $j$ then
    return $\boldsymbol{E} \leftarrow \{\boldsymbol{x}^{\boldsymbol{e}_k} - \rho_k\}_{1\le k\le t}$;
else
    return "$\varphi^{-1}(B) = \emptyset$".
end if
```

Lemma 2.3. *Given a homomorphism $\varphi\colon \mathbb{G}_{\mathrm{m}}^n \to \mathbb{G}_{\mathrm{m}}^N$ and a torsion coset $B \subset \mathbb{G}_{\mathrm{m}}^N$, Algorithm 2.1 decides if $\varphi^{-1}(B) \neq \emptyset$. If this is the case, it computes a finite collection $\boldsymbol{E} = \{\boldsymbol{x}^{\boldsymbol{e}_k} - \rho_k\}_{1\le k\le t}$ of binomials in $\overline{\mathbb{Q}}[\boldsymbol{x}^{\pm 1}]$ with coefficients in μ_∞ such that $t = \operatorname{codim}(\varphi^{-1}(B))$ and*

$$\varphi^{-1}(B) = V(\boldsymbol{x}^{\boldsymbol{e}_1} - \rho_1, \dots, \boldsymbol{x}^{\boldsymbol{e}_t} - \rho_t). \tag{2.9}$$

If n and N are bounded, B is given as in (2.8) with $\xi_j \in \mu_l$ with l bounded and $\operatorname{size}(\varphi) \le d$, then each coefficient ρ_k has order bounded by $O(1)$ and each binomial has degree bounded by $d^{O(1)}$ (by d in the case $n = 1$). The complexity of the algorithm is bounded by $O(\mathrm{M}(\log(d))\log(\log(d))) = \widetilde{O}(\log(d))$ ops.

Proof. Let notation be as in Algorithm 2.1. By (2.3),

$$\varphi^{-1}(B) = V(\boldsymbol{x}^{\boldsymbol{c}_1} - \xi_1, \dots, \boldsymbol{x}^{\boldsymbol{c}_r} - \xi_r). \tag{2.10}$$

Consider the ideals of $K[\boldsymbol{x}^{\pm 1}]$ given by

$$I = (\boldsymbol{x}^{\boldsymbol{c}_1} - \xi_1, \dots, \boldsymbol{x}^{\boldsymbol{c}_r} - \xi_r), \quad J = (\boldsymbol{x}^{\boldsymbol{e}_1} - \rho_1, \dots, \boldsymbol{x}^{\boldsymbol{e}_t} - \rho_t).$$

By construction, we have that $\boldsymbol{x}^{\boldsymbol{e}_k} - \rho_k \in I$ for all k and, if we set $\xi'_j = \prod_k \rho_k^{\mu_{j,k}}$, we have similarly that $\boldsymbol{x}^{\boldsymbol{c}_j} - \xi'_j \in J$ for all j. Then

$$\xi_j - \xi'_j = (\boldsymbol{x}^{\boldsymbol{c}_j} - \xi'_j) - (\boldsymbol{x}^{\boldsymbol{c}_j} - \xi_j) \in (\boldsymbol{x}^{\boldsymbol{c}_1} - \xi_1, \dots, \boldsymbol{x}^{\boldsymbol{c}_r} - \xi_r). \tag{2.11}$$

Hence, if there exists j such that $\xi'_j \neq \xi_j$, it follows from (2.10) and (2.11) that $\varphi^{-1}(B) = \emptyset$. Otherwise, we deduce that $I = J$ and so $\varphi^{-1}(B) = V(J)$, which proves

(2.9). Moreover, the binomials $\boldsymbol{x}^{\boldsymbol{e}_k} - \rho_k$, $k = 1, \dots, t$, form a complete intersection because the vectors $\boldsymbol{e}_k$, $k = 1, \dots, t$, are linearly independent. Hence $t = \operatorname{codim}(B)$, as stated.

Now suppose that n and N are bounded, B is given as in (2.8) with $\xi_j \in \mu_l$ with l bounded, and $\operatorname{size}(\varphi) \le d$. The computation of the integers $\lambda_{k,j}, \mu_{j,k}$ in line 4 can be derived from the Hermite normal form as defined in [Coh93, Definition 2.4.2], for the matrix with rows $\boldsymbol{c}_j$, $j = 1, \dots, r$. This Hermite normal form can be computed using Algorithm 2.4.5 in *loc. cit.* using a bounded number of gcd computations and multiplications of integers of size bounded by $\log(d)$. Hence, the integers $\lambda_{k,j}, \mu_{j,k}$ have size bounded by $O(\log(d))$ and the complexity of these steps is bounded by $O(\mathrm{M}(\log(d)) \log(\log(d)))$. In particular, $\deg(\boldsymbol{x}^{\boldsymbol{e}_k} - \rho_k) \le d^{O(1)}$. When $n = 1$, we have that $t = 1$ and $\boldsymbol{e}_1 = \gcd(\boldsymbol{c}_1, \dots, \boldsymbol{c}_r)$, and so $\deg(\boldsymbol{x}^{\boldsymbol{e}_1} - \rho_1) \le d$ in this case.

The computation in line 5 and the verification in line 6 can be done using repeated squaring. The overall complexity is bounded by $O(\mathrm{M}(\log(d)) \log(\log(d)))$, which completes the proof. □

Let T be a torsion coset of $\mathbb{G}_{\mathrm{m}}^N$ of codimension 1. By (2.8), there is a primitive vector $\boldsymbol{b} \in \mathbb{Z}^N$ and $\xi \in \mu_\infty$ such that

$$T = V(\boldsymbol{y}^{\boldsymbol{b}} - \xi).$$

The following simple lemma gives a monomial change of coordinates putting T into a standard position.

Lemma 2.4. *Let T be be a torsion coset of $\mathbb{G}_{\mathrm{m}}^N$ of codimension 1 given as $T = V(\boldsymbol{y}^{\boldsymbol{b}} - \xi)$ for a primitive vector $\boldsymbol{b} \in \mathbb{Z}^N$ and $\xi \in \mu_\infty$. Let $\boldsymbol{b}_j \in \mathbb{Z}^N$, $j = 1, \dots, N-1$, be a family of vectors completing $\boldsymbol{b}$ to a basis of $\mathbb{Z}^N$ and $\tau \in \operatorname{Aut}(\mathbb{G}_{\mathrm{m}}^N)$ the automorphism given, for $\boldsymbol{y} \in \mathbb{G}_{\mathrm{m}}^N$, by*

$$\tau(\boldsymbol{y}) = (\boldsymbol{y}^{\boldsymbol{b}_1}, \dots, \boldsymbol{y}^{\boldsymbol{b}_{N-1}}, \boldsymbol{y}^{\boldsymbol{b}}).$$

Then $\tau(T) = V(y_N - \xi)$.

Proof. This follows easily from the definitions. □

3. Unlikely intersections in algebraic tori

In this section, we collect the different results and conjectures on unlikely intersections in algebraic tori that we will use in the rest of the paper.

As mentioned in the introduction, the algorithm of Filaseta, Granville and Schinzel relies on a theorem of Bombieri and Zannier. We recall the statement of this result, in the refined form later obtained by these authors together with Masser in [BMZ07, Theorem 4.1].

Theorem 3.1. *Let W be an irreducible subvariety of $\mathbb{G}_{\mathrm{m}}^N$ of codimension ≥ 2. There exists a constant c_W depending only on W with the following property. Let $\boldsymbol{\zeta} \in \mu_\infty^N$, $\boldsymbol{a} \in \mathbb{Z}^N$ and $\alpha \in \overline{\mathbb{Q}}^\times$. If $(\zeta_1 \alpha^{a_1}, ..., \zeta_N \alpha^{a_N}) \in W$, then there exist $\boldsymbol{b} \in \mathbb{Z}^N \setminus \{\boldsymbol{0}\}$ such that*

$$\max_j |b_j| \le c_W \quad \text{and} \quad \prod_j (\zeta_j \alpha^{a_j})^{b_j} = 1.$$

In particular, if $\alpha \notin \mu_\infty$, then $\sum_j a_j b_j = 0$.

In the special case when $\zeta_j = 1$ for all j, the existence of the bounded non-trivial relation $\sum_j a_j b_j = 0$ was proposed by Schinzel in [Schi65, Conjecture, page 3], anticipating the Zilber conjecture thirty-seven years before its actual formulation!

Remark 3.2. The constant c_W in Theorem 3.1 is effectively calculable, as Zannier has pointed out to us in a personal communication. This is also explained in the remark following [BMZ07, Theorem 1.6]. Unfortunately, the computation of a bound for this constant has not been accomplished yet. Obtaining such a bound would enable our algorithm to be made effective in the univariate case (Algorithm 4.2) and to make explicit the dependence of its complexity on the height and number of nonzero terms of the input polynomials.

The following result is a well-known theorem of Laurent giving a positive answer to the toric case of the Manin-Mumford conjecture [Lau84]. Effective proofs of it can be found in [Schm96, Ler12].

Theorem 3.3. *Let W be a subvariety of $\mathbb{G}_{\mathrm{m}}^N$. The collection of torsion cosets contained in W which are maximal with respect to inclusion is finite. Equivalently, there exists a finite collection Θ of torsion cosets of $\mathbb{G}_{\mathrm{m}}^N$ contained in W such that, if B is a torsion coset contained in W, then there exists $T \in \Theta$ such that $B \subset T$.*

In the context of model theory, Zilber proposed in [Zil02] the following conjecture on unlikely intersections of subvarieties of $\mathbb{G}_{\mathrm{m}}^N$ with algebraic subgroups.

Conjecture 3.4 (Zilber conjecture)**.** *Let W be a subvariety of $\mathbb{G}_{\mathrm{m}}^N$. There exists a finite collection Ξ of proper algebraic subgroups of $\mathbb{G}_{\mathrm{m}}^N$ such that, if G is a proper algebraic subgroup of $\mathbb{G}_{\mathrm{m}}^N$ and Y an irreducible component of $G \cap W$ such that*

$$\dim(Y) > \dim(G) - \operatorname{codim}(W), \tag{3.1}$$

then there exists $H \in \Xi$ such that $Y \subset H$.

It is not difficult to see that Theorems 3.1 and 3.3 give this conjecture for the cases when we restrict to algebraic subgroups G with $\dim(G) = 1$ and $\dim(G) = 0$, respectively.

We will use the following reformulation for locally closed subsets of the Zilber conjecture, which we reinforce by adding the hypothesis that the collection of torsion cosets can be computed. This is crucial for our algorithmic applications.

Conjecture 3.5. *Let W be a locally closed subset of $\mathbb{G}_{\mathrm{m}}^N$. There exists a finite and effectively calculable collection Ω of torsion cosets $\mathbb{G}_{\mathrm{m}}^N$ of codimension 1 such that, if B is a torsion coset, C an irreducible component of W and $Y \subset B \cap C$ an irreducible locally closed subset such that*

$$\dim(Y) > \dim(B) - \operatorname{codim}(C), \tag{3.2}$$

then there exists $T \in \Omega$ such that $Y \subset T$.

Proposition 3.6. *Conjecture 3.4 is equivalent to the non-effective version of Conjecture 3.5.*

Proof. Suppose that the Zilber conjecture 3.4 holds. Let $W \subset \mathbb{G}_{\mathrm{m}}^N$ be a locally closed subset and, for each irreducible component C_j of W, let Ξ_j the finite collection given by this conjecture applied to the subvariety $\overline{C_j}$. We can assume without loss of generality that each proper algebraic subgroup in Ξ_j has codimension 1. Consider then the finite collection Ω of torsion cosets of codimension 1 made of the irreducible components of the algebraic subgroups in the collections Ξ_j.

Let B be a torsion coset of $\mathbb{G}_{\mathrm{m}}^N$ and $\langle B\rangle$ the minimal algebraic subgroup containing it. Let $C = C_{j_0}$ be an irreducible component of W and $Y \subset B \cap C$ an irreducible locally closed subset such that (3.2) holds. Let Z be an irreducible component of $\langle B\rangle \cap \overline{C}$ containing Y. Then

$$\dim(Z) \geq \dim(Y) > \dim(B) - \operatorname{codim}(C) = \dim(\langle B\rangle) - \operatorname{codim}(\overline{C}).$$

It follows that there exists $H \in \Xi_{j_0}$ such that $Z \subset H$. Since Z is irreducible, there exists $T \in \Omega$ such that $Z \subset T$ and, *a fortiori*, $Y \subset T$. Hence, the non-effective version of Conjecture 3.5 holds with this choice of Ω.

Conversely, suppose that the non-effective version of Conjecture 3.5 holds. Let W be a subvariety of $\mathbb{G}_{\mathrm{m}}^N$ and Ω the collection of torsion cosets of codimension 1 given by this conjecture. Then $\Xi = \{\langle T\rangle\}_{T\in\Omega}$ is a finite collection of algebraic subgroups of codimension 1, and it is easy to verify that it satisfies the conditions of the Zilber conjecture 3.4. □

Definition 3.7. Let W be a locally closed subset of $\mathbb{G}_{\mathrm{m}}^N$. An irreducible locally closed subset Y of W is called *atypical* if there is a torsion coset B of $\mathbb{G}_{\mathrm{m}}^N$ and an irreducible component C of W such that $Y \subset B \cap C$ and $\dim(Y) > \dim(B) - \operatorname{codim}(C)$. The *exceptional subset* of W is defined as

$$W^{\mathrm{exc}} = \bigcup_{Y \text{atypical}} Y.$$

Notation 3.8. Suppose that Conjecture 3.5 holds. Given a locally closed subset W of $\mathbb{G}_{\mathrm{m}}^N$, we denote by Ω_W a choice of a finite and effectively calculable collection of torsion cosets of codimension 1 satisfying the conditions of this conjecture. We also write

$$\bigcup \Omega_W = \bigcup_{T\in\Omega_W} T.$$

Conjecture 3.5 implies that the exceptional set of a locally closed subset W is contained in the torsion subvariety $\bigcup \Omega_W$. In particular, if W is not contained in a proper torsion subvariety of $\mathbb{G}_{\mathrm{m}}^N$, then W^{exc} is a proper subset of W.

4. The univariate case

In this section, we present an algorithm that, given a system of univariate polynomials with coefficients in the number field K, of degree bounded by d and bounded height and number of nonzero coefficients, computes a single polynomial defining the same zero set with $\widetilde{O}(\log(d))$ ops. Our approach is inspired by the one in [FGS08], but it is simpler and more geometric.

The following subroutine is one of the main components of the algorithm. It tests whether a subtorus of codimension 1 contains the image of a homomorphism and, if this is the case, reduces the dimension of the problem by intersecting the variety under consideration with that subtorus.

Lemma 4.1. *For a given input $(\varphi, T, \boldsymbol{F})$, Algorithm 4.1 stops after a finite number of steps. It decides if* $\operatorname{im}(\varphi) \subset T$ *and, if this is the case, its output $(\widetilde{\varphi}, \boldsymbol{F})$ satisfies*

$$\widetilde{\varphi}^{\#}(\widetilde{\boldsymbol{F}}) = \varphi^{\#}(\boldsymbol{F}). \tag{4.1}$$

In particular, $\widetilde{\varphi}^{-1}(V(\widetilde{\boldsymbol{F}})) = \varphi^{-1}(V(\boldsymbol{F}))$.

If $\operatorname{size}(\varphi) \leq d$, *then* $\operatorname{size}(\widetilde{\varphi}) \leq O_T(d)$ *and each $\widetilde{F}_i$ has degree, height and number of nonzero coefficients bounded by $O_{T,\boldsymbol{F}}(1)$. The complexity of the algorithm is bounded by $O_T(\log(d)) + O_{T,\boldsymbol{F}}(1)$ ops.*

Algorithm 4.1 (Reduction of dimension for ideals)

```
Input: a homomorphism $\varphi \in \mathrm{Hom}(\mathbb{G}_{\mathrm{m}}^n, \mathbb{G}_{\mathrm{m}}^N)$, a subtorus $T \subset \mathbb{G}_{\mathrm{m}}^N$ of codimension 1,
    and a family of Laurent polynomials $F_i \in K[y_1^{\pm 1}, \dots, y_N^{\pm 1}]$, $i = 1, \dots, s$.
Output: either "$\mathrm{im}(\varphi) \not\subset T$", or a homomorphism $\widetilde{\varphi} \in \mathrm{Hom}(\mathbb{G}_{\mathrm{m}}^n, \mathbb{G}_{\mathrm{m}}^{N-1})$ and a family
    of Laurent polynomials $\widetilde{F}_i \in K[y_1^{\pm 1}, \dots, y_{N-1}^{\pm 1}]$, $i = 1, \dots, s$.
1. Let $A \in \mathbb{Z}^{N \times n}$ be the $N \times n$-matrix associated to $\varphi$ and $\boldsymbol{b} \in \mathbb{Z}^N$ a primitive vector
   such that $T = V(\boldsymbol{y}^{\boldsymbol{b}} - 1)$;
2. if $\boldsymbol{b}A = \boldsymbol{0}$ then
3.     choose $\tau \in \mathrm{Aut}(\mathbb{G}_{\mathrm{m}}^N)$ such that $\tau(T) = V(y_N - 1)$ as in Lemma 2.4;
4.     let $\iota \colon \mathbb{G}_{\mathrm{m}}^{N-1} \to \mathbb{G}_{\mathrm{m}}^N$ be the standard inclusion identifying $\mathbb{G}_{\mathrm{m}}^{N-1}$ with the hyperplane
       $V(y_N - 1)$, and $\pi \colon \mathbb{G}_{\mathrm{m}}^N \to \mathbb{G}_{\mathrm{m}}^{N-1}$ the projection onto the first $N - 1$
       coordinates;
5.     return $\widetilde{\varphi} \leftarrow \pi \circ \tau \circ \varphi$ and $\widetilde{F}_i \leftarrow (\tau^{-1} \circ \iota)^{\#}(F_i)$, $i = 1, \dots, s$;
6. else
7.     return "$\mathrm{im}(\varphi) \not\subset T$";
8. end if
```

Proof. Let notation be as in Algorithm 4.1. Under the correspondence in (2.4), the subtorus $\mathrm{im}(\varphi)$ is associated to the kernel of the linear map $A^{\mathrm{t}} \colon \mathbb{Z}^N \to \mathbb{Z}^n$, for the matrix A in line 1 of the algorithm. Then $T = V(\boldsymbol{y}^{\boldsymbol{b}} - 1)$ contains the image of φ if and only if $\boldsymbol{b} \in \ker(A^{\mathrm{t}})$ or, equivalently, if $\boldsymbol{b}A = \boldsymbol{0}$. Hence, the algorithm decides correctly whether this holds.

To prove (4.1), assume that $\mathrm{im}(\varphi) \subset T$. Consider the diagram

$$\begin{tikzcd}
\mathbb{G}_{\mathrm{m}}^N \arrow[r, bend left, "\tau"] & \mathbb{G}_{\mathrm{m}}^N \arrow[l, bend left, "\tau^{-1}"] \arrow[r, bend left, "\pi"] & \mathbb{G}_{\mathrm{m}}^{N-1} \arrow[l, bend left, "\iota"] \arrow[d, equal] \\
T \arrow[u, hook] \arrow[r, bend left] & V(y_N - 1) \arrow[u, hook] \arrow[l, bend left] \arrow[r, bend left] & \mathbb{G}_{\mathrm{m}}^{N-1} \arrow[l, bend left]
\end{tikzcd}$$

where the maps in the second line are induced by the ones in the first line. These maps in the second line are isomorphisms. Considering the corresponding maps of K-algebras, we deduce that

$$(\boldsymbol{F}) + (\boldsymbol{y}^{\boldsymbol{b}} - 1) = (\pi \circ \tau)^{\#}((\tau^{-1} \circ \iota)^{\#}((\boldsymbol{F}) + (\boldsymbol{y}^{\boldsymbol{b}} - 1)) = (\pi \circ \tau)^{\#}(\widetilde{\boldsymbol{F}})$$

because $(\tau^{-1} \circ \iota)^{\#}(\boldsymbol{y}^{\boldsymbol{b}} - 1) = \iota^{\#}(y_N - 1) = 0$. We also have that $\varphi^{\#}(\boldsymbol{y}^{\boldsymbol{b}} - 1) = 0$ because $\mathrm{im}(\varphi) \subset T$. Using the functoriality (2.2), it follows that

$$\varphi^{\#}(\boldsymbol{F}) = \varphi^{\#}((\boldsymbol{F}) + (\boldsymbol{y}^{\boldsymbol{b}} - 1)) = \varphi^{\#}((\pi \circ \tau)^{\#}(\widetilde{\boldsymbol{F}})) = \widetilde{\varphi}^{\#}(\widetilde{\boldsymbol{F}}),$$

as stated. Clearly, this implies that $\widetilde{\varphi}^{-1}(V(\widetilde{\boldsymbol{F}})) = \varphi^{-1}(V(\boldsymbol{F}))$.

Now suppose that $\mathrm{size}(\varphi) \leq d$. The automorphism τ in line 3 depends only on T. Hence, the construction of $\widetilde{\varphi}$ in line 5 implies that $\mathrm{size}(\widetilde{\varphi}) \leq O_T(d)$. The construction of each $\widetilde{F}_i$, also in line 5, consists of composing F_i with a homomorphism depending only on T. Hence, the number of nonzero coefficients of $\widetilde{F}_i$ is bounded by that of F_i, and its degree and height are bounded by $O_{T,\boldsymbol{F}}(1)$.

The verification $\boldsymbol{b}A = \boldsymbol{0}$ in line 2 costs $O_T(\log(d))$ ops using classical multiplication of integers. The construction of τ in line 3 uses $O_T(1)$ ops. The computations in line 5 of $\widetilde{\varphi}$ and $\widetilde{F}_i$, $i = 1, \dots, s$, take $O_T(\log(d))$ ops and $O_{T,\boldsymbol{F}}(1)$ ops, respectively, using classical multiplication. Hence, the overall complexity of the algorithm is bounded by $O_T(\log(d)) + O_{T,\boldsymbol{F}}(1)$ ops. □

Remark 4.2. The Laurent polynomials $\widetilde{F}_i$, $i = 1, \dots, s$, in Algorithm 4.1, line 5, can be written down, in more explicit terms, as

$$\widetilde{F}_i = F_i \circ \tau^{-1}(y_1, \dots, y_{N-1}, 1).$$

The following procedure computes the non-torsion points in the zero set of a system of univariate polynomials, and gives the first half of the algorithm. It is based on the strategy described in (1.5). In the univariate setting, we apply Theorem 3.1 to successively intersect the linear subvariety W until all non-torsion points lie in a hypersurface (while loop between lines 4 and 14 in Algorithm 4.2 below). Once this is achieved, the hypersurface is described by a single polynomial that we obtain through a gcd computation, and the non-torsion points are obtained as the inverse image under a homomorphism of this hypersurface (lines 15 and 16).

For a Laurent polynomial $p \in K[x^{\pm 1}] \setminus \{0\}$, we denote by $\mathrm{ord}(p)$ the maximal integer m such that $x^{-m}p \in K[x]$.

Algorithm 4.2 (Non-torsion points)

Input: a family of polynomials $f_i \in K[x]$, $i = 1, \dots, s$.
Output: a polynomial $p_1 \in K[x]$.

```
1.  Write $f_i = \sum_{j=1}^{N} \alpha_{i,j} x^{a_j}$ with $\alpha_{i,j} \in K$ and $a_j \in \bigcup_i \mathrm{supp}(f_i)$;
2.  set $F_i \leftarrow \sum_{j=1}^{N} \alpha_{i,j} y_j$, $i = 1, \dots, s$ and $\boldsymbol{F} \leftarrow (F_1, \dots, F_s)$;
3.  set $k \leftarrow 0$ and let $\varphi \in \mathrm{Hom}(\mathbb{G}_{\mathrm{m}}, \mathbb{G}_{\mathrm{m}}^N)$ be the homomorphism corresponding to the
    exponents $a_j \in \mathbb{N}$, $j = 1, \dots, N$;
4.  while $k < N$ do
5.    for each irreducible component $W$ of $V(\boldsymbol{F})$ of codimension $\geq 2$, compute $c_W$ as in
      Theorem 3.1 and set $\Phi \leftarrow \{V(\boldsymbol{y}^b - 1) \mid \boldsymbol{b} \in \mathbb{Z}^N$ primitive such that $\max_j |b_j| \leq$
      $\max_W c_W\}$;
6.    while $\Phi \neq \emptyset$ do
7.      choose $T \in \Phi$ and apply Algorithm 4.1 to $(\varphi, T, \boldsymbol{F})$;
8.      if $\mathrm{im}(\varphi) \subset T$ then
9.        set $\boldsymbol{F} \leftarrow \widetilde{\boldsymbol{F}}$, $\varphi \leftarrow \widetilde{\varphi}$, $k \leftarrow k+1$, $\Phi \leftarrow \emptyset$;
10.     else
11.       set $\Phi \leftarrow \Phi \setminus \{T\}$;
12.     end if
13.   end while
14. end while
15. set $p \leftarrow \varphi^{\#}(\gcd(F_1, \dots, F_s))$;
16. return $p_1 \leftarrow x^{-\mathrm{ord}(p)} p$.
```

Theorem 4.3. *Given $f_i \in K[x]$, $i = 1, \dots, s$, Algorithm 4.2 stops after a finite number of steps and computes $p_1 \in K[x]$ such that*

$$p_1 \,|\, \gcd(f_1, \dots, f_s) \quad \text{and} \quad V\Big(\frac{\gcd(f_1, \dots, f_s)}{p_1}\Big) \subset \mu_\infty.$$

If s is bounded and each f_i has degree bounded by d and bounded height and number of nonzero coefficients, then p_1 has degree bounded by d, and height and number of *nonzero coefficients bounded by $O(1)$. The complexity of the algorithm is bounded by $O(\log(d))$ ops.*

Proof. For $i = 0, \dots, s$, the initial value of F_i at line 2 satisfies

$$\varphi^{\#}(F_i) = f_i. \tag{4.2}$$

By Lemma 4.1, this holds also for the updated values of F_i and φ in line 9. Hence, the equality (4.2) holds for the final value of F_i as in line 15. For the rest of this proof, we denote by F_i this final value.

Set $P = \gcd(F_1, \dots, F_s)$. We have that $(F_1, \dots, F_s) \subset (P) \subset K[y_1^{\pm 1}, \dots, y_{N-k}^{\pm 1}]$, The equality (4.2) implies that $(f_1, \dots, f_s) \subset (p) \subset K[x^{\pm 1}]$ and so

$$p_1 | \gcd(f_1, \dots, f_s) \quad \text{in } K[x].$$

Set $\boldsymbol{f} = \{f_1, \dots, f_s\}$ and $\boldsymbol{F} = \{F_1, \dots, F_s\}$ for short. Let $\alpha \in V(\boldsymbol{f}) \setminus \mu_\infty$, so that $\varphi(\alpha) \in V(\boldsymbol{F})$. Let W an irreducible component of $V(\boldsymbol{F})$ such that

$$\varphi(\alpha) = (\alpha^{a_1}, \dots, \alpha^{a_N}) \in W.$$

By Theorem 3.1, W is necessarily of codimension 1. Otherwise, there would exist $T \in \Phi$ such that $\mathrm{im}(\varphi) \subset T$ but, by construction, this is not possible.

This discussion implies that the ideal $(\boldsymbol{F}) \subset K[y_1^{\pm 1}, \dots, y_{N-k}^{\pm 1}]$ becomes principal when restricted to a suitable neighborhood $U \subset \mathbb{G}_{\mathrm{m}}^{N-k}$ of $\varphi(V(\boldsymbol{f}) \setminus \mu_\infty)$. Hence, $(\boldsymbol{F}) = (P)$ on that neighborhood. We deduce that $\varphi^{-1}(U)$ is a neighborhood of $V(\boldsymbol{f}) \setminus \mu_\infty$ and $(\boldsymbol{f}) = \varphi^{\#}(p)$ on $\varphi^{-1}(U)$. Thus, $V(\gcd(f_1, \dots, f_s)/p_1) \cap \varphi^{-1}(U) = \emptyset$ or, equivalently,

$$V\Big(\frac{\gcd(f_1, \dots, f_s)}{p_1}\Big) \subset \mu_\infty.$$

This completes the proof of the first part of the statement.

For the second, part, assume that s is bounded and that the f_i's have degree bounded by d, and bounded height and number of nonzero coefficients. The construction of $P = \gcd(F_1, \dots, F_s)$ does not depend on the exponents a_j. Hence, the height and number of nonzero coefficients of P is bounded, and so this also holds for p_1. The fact that p_1 divides $\gcd(f_1, \dots, f_s)$ implies that $\deg(p_1) \le d$. The list of linear forms $\boldsymbol{F}$ in line 2 does not depend on the exponents a_j and so, *a fortiori*, it is independent on the degree of the input polynomials f_i. Therefore, the computations in lines 5 and 15 cost $O(1)$ ops. By Lemma 4.1, the computation in line 7 costs $O(\log(d))$ ops. Since the number of iterations in the while loop between lines 4 and 14 is bounded, we conclude that the overall complexity of the algorithm is bounded by $O(\log(d))$, as stated. □

The following procedure computes the torsion points in the zero set of a system of univariate polynomials, and completes the algorithm. It consists in considering the finite collection of maximal torsion cosets given by Theorem 3.3 for the linear subvariety W as in (1.5), and compute with Algorithm 2.1 its inverse image with respect to the homomorphism φ.

Theorem 4.4. *Given $f_i \in K[x]$, $i = 1, \dots, s$, Algorithm 4.3 stops after a finite number of steps and computes $p_2 \in K[x]$ such that*

$$V(p_2) = V(f_1, \dots, f_s) \cap \mu_\infty.$$

If s is bounded and each f_i has degree bounded by d and bounded height and number of nonzero coefficients, then p_2 has degree bounded by $O(d)$ and height and number of nonzero coefficients bounded by $O(1)$. The complexity of the algorithm is bounded by $O(\mathrm{M}(\log(d)) \log(\log(d))) = \widetilde{O}(\log(d))$ ops.

Algorithm 4.3 (Torsion points)

```
Input: a family of polynomials $f_j \in K[x]$, $j = 1, \dots, s$.
Output: a polynomial $p_2 \in K[x]$.
1. Write $f_i = \sum_{j=1}^{N} \alpha_{i,j} x^{a_j}$ with $\alpha_{i,j} \in K$ and $a_j \in \bigcup_i \operatorname{supp}(f_i)$;
2. set $F_i \leftarrow \sum_{j=1}^{N} \alpha_{i,j} y_j$, $i = 1, \dots, s$;
3. set $W \leftarrow V(F_1, \dots, F_s) \subset \mathbb{G}_{\mathrm{m}}^N$, $\varphi \in \operatorname{Hom}(\mathbb{G}_{\mathrm{m}}, \mathbb{G}_{\mathrm{m}}^N)$ the homomorphism corresponding to the exponents $a_j \in \mathbb{N}$, $j = 1, \dots, N$, and $\Lambda \leftarrow \emptyset$;
4. compute the collection $\Theta$ of maximal torsion cosets of $W$ from Theorem 3.3;
5. for $B \in \Theta$ do
6.    apply Algorithm 2.1 to the pair $(\varphi, B)$;
7.    if $\varphi^{-1}(B) \neq \emptyset$ then
8.       let $\boldsymbol{E}$ be the output of Algorithm 2.1, write $\boldsymbol{E} = \{x^b - \xi\}$ with $b \in \mathbb{N}$ and $\xi \in \mu_\infty$, and add the binomial $x^b - \xi$ to $\Lambda$;
9.    end if
10. end for
11. return $p_2 \leftarrow \prod_{g \in \Lambda} g$.
```

Proof. Write $\boldsymbol{f} = (f_1, \dots, f_s)$ for short and let Θ be as in line 4 of the algorithm. Then

$$V(\boldsymbol{f}) \cap \mu_\infty = \bigcup_{B \in \Theta} \varphi^{-1}(B).$$

With notation as in line 8, we have that $\varphi^{-1}(B) = V(x^b - \xi)$ because of (2.9). It follows that

$$V(\boldsymbol{f}) \cap \mu_\infty = \bigcup_{g \in \Lambda} V(g) = V(p_2).$$

The collection Θ is invariant under K-automorphisms of $\overline{\mathbb{Q}}$ and so is p_2. It follows that $p_2 \in K[x]$, completing the proof of the first part of the statement.

The construction of W in line 3 and, *a fortiori*, that of Θ, do not depend on the exponents a_j. Hence, the size of Θ is bounded by $O(1)$ and its computation costs $O(1)$ ops. Hence, the number of steps in the for loop between lines 5 and 10 is bounded by $O(1)$. The second part of the statement then follows easily from Lemma 2.3. □

Putting together Theorems 4.3 and 4.4, we obtain the following more general and precise version of Theorem 1.1 in the introduction.

Theorem 4.5. *Given $f_i \in K[x]$, $i = 1, \dots, s$, Algorithms 4.2 and 4.3 compute $p_1, p_2 \in K[x]$ such that $p_1 | \gcd(f_1, \dots, f_s)$,*

$$V(p_1) \setminus \mu_\infty = V(\gcd(f_1, \dots, f_s)) \setminus \mu_\infty \quad \text{and} \quad V(p_2) = V(\gcd(f_1, \dots, f_s)) \cap \mu_\infty.$$

If s is bounded and each f_i has degree bounded by d, bounded height and number of nonzero coefficients, then $\deg(p_1) \leq d$ and $\deg(p_2) \leq O(d)$, and the height and number of nonzero coefficients of both p_1 and p_2 are bounded by $O(1)$. The complexity of the procedure is bounded by $O(\mathrm{M}(\log(d)) \log(\log(d))) = \widetilde{O}(\log(d))$ ops.

5. The multivariate case

In this section, we present the procedure for the reduction of overdetermined systems of multivariate polynomial equations. We first give a simple algorithm which allows us to treat the components of top multiplicative rank. Strictly speaking, this procedure is not needed to treat the general case, but it is considerably simpler and serves as a first approach. After this, we give the main procedure (Algorithm 5.5) and prove Theorem 1.3 in the introduction.

We will express our algorithms in terms of geometrical objects to avoid the burden of their syntactical treatment in terms of families of Laurent polynomials. As before, we denote by K a number field together with an inclusion into $\overline{\mathbb{Q}}$.

5.1. **The weakly transverse case.** The following is a reformulation of Algorithm 4.1 in terms of locally closed subsets.

Algorithm 5.1 (Reduction of dimension for locally closed subsets)

```
Input: $(n, N, \varphi, T, W)$ where $n$ and $N$ are positive integers, $\varphi \in \mathrm{Hom}(\mathbb{G}_{\mathrm{m}}^n, \mathbb{G}_{\mathrm{m}}^N)$ is a
    homomorphism, $T \subset \mathbb{G}_{\mathrm{m}}^N$ is a subtorus of codimension 1, and $W \subset \mathbb{G}_{\mathrm{m}}^N$ is a locally
    closed subset.
Output: either "$\mathrm{im}(\varphi) \not\subset T$", or a homomorphism $\widetilde{\varphi} \in \mathrm{Hom}(\mathbb{G}_{\mathrm{m}}^n, \mathbb{G}_{\mathrm{m}}^{N-1})$ and a locally
    closed subset $\widetilde{W} \subset \mathbb{G}_{\mathrm{m}}^{N-1}$.
  1. Take $\boldsymbol{F}, \boldsymbol{G} \subset \overline{\mathbb{Q}}[y_1^{\pm 1}, \dots, y_N^{\pm 1}]$ such that $W = V(\boldsymbol{F}) \setminus V(\boldsymbol{G})$;
  2. apply Algorithm 4.1 to $(\varphi, T, \boldsymbol{F})$ and to $(\varphi, T, \boldsymbol{G})$ and, if $\mathrm{im}(\varphi) \subset T$, set $(\widetilde{\varphi}, \widetilde{\boldsymbol{F}})$
     and $(\widetilde{\varphi}, \widetilde{\boldsymbol{G}})$ for its output;
  3. return $\widetilde{W} \leftarrow V(\widetilde{\boldsymbol{F}}) \setminus V(\widetilde{\boldsymbol{G}})$.
```

Lemma 5.1. *For a given input (φ, T, W), Algorithm 5.1 stops after a finite number of steps. It decides whether* $\mathrm{im}(\varphi) \subset T$ *and, if this is the case, its output satisfies*

$$\widetilde{\varphi}^{-1}(\widetilde{W}) = \varphi^{-1}(W). \tag{5.1}$$

If $\mathrm{size}(\varphi) \le d$*, then* $\mathrm{size}(\widetilde{\varphi}) \le O_T(d)$ *and the Laurent polynomials defining $\widetilde{W}$ have degree, height and number of nonzero coefficients bounded by $O_{T,\boldsymbol{F}}(1)$. The complexity of the algorithm is bounded by $O_{T,W}(\log(d))$ ops.*

Proof. This follows readily from Lemma 4.1. □

Definition 5.2. Let X be an irreducible locally closed subset of $\mathbb{G}_{\mathrm{m}}^n$. Following Viada [Via08], we say that X is *weakly transverse* if it is not contained in any proper torsion coset or, equivalently, if $\mathrm{rank}(X) = n$.

Remark 5.3. An irreducible locally closed subset $X \subset \mathbb{G}_{\mathrm{m}}^n$ is weakly transverse if and only if it is not atypical as a subset of itself. If Ω_X denotes a finite collection of torsion cosets of $\mathbb{G}_{\mathrm{m}}^n$ of codimension 1 as in Notation 3.8, this is equivalent to the condition that $X \not\subset \bigcup \Omega_X$.

The following procedure is the natural generalization of Algorithm 4.2 to the multivariate case.

Theorem 5.4. *Assume that Conjecture 3.5 holds. Given a subvariety $V \subset \mathbb{G}_{\mathrm{m}}^n$, Algorithm 5.2 stops after a finite number of steps and its output satisfies:*

(1)

$$V = \bigcup_{Z \in \Gamma} Z;$$

(2) each $Z \in \Gamma$ is given as the zero set of l_Z Laurent polynomials in the complement of the zero set of a further Laurent polynomial. Moreover, if C is an irreducible component of Z that is weakly transverse, then $\mathrm{codim}(C) = l_Z$.

Algorithm 5.2 (Reduction of weakly transverse components)

```
Input: a subvariety $V \subset \mathbb{G}_{\mathrm{m}}^n$ defined by a linearly independent family of Laurent
    polynomials in $\overline{\mathbb{Q}}[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$;
Output: a finite collection $\Gamma$ of locally closed subsets of $\mathbb{G}_{\mathrm{m}}^n$.
 1. Let $f_i$, $i = 1, \dots, s$, be the Laurent polynomials defining $V$ and write $f_i = \sum_{j=1}^{N} \alpha_{i,j} \boldsymbol{x}^{\boldsymbol{a}_j}$ with $\alpha_{i,j} \in \overline{\mathbb{Q}}$ and $\boldsymbol{a}_j \in \bigcup_i \mathrm{supp}(f_i)$;
 2. set $k \leftarrow 0$, $W \leftarrow V(\sum_{j=1}^{N} \alpha_{1,j} y_j, \dots, \sum_{j=1}^{N} \alpha_{s,j} y_j) \subset \mathbb{G}_{\mathrm{m}}^N$, $t \leftarrow 1$, $W_1 \leftarrow W$, and
    $\varphi \in \mathrm{Hom}(\mathbb{G}_{\mathrm{m}}^n, \mathbb{G}_{\mathrm{m}}^N)$ the homomorphism corresponding to the exponents $\boldsymbol{a}_j \in \mathbb{Z}^n$,
    $j = 1, \dots, N$;
 3. compute the collection $\Omega_{W_1}$ of torsion cosets of codimension 1 (Notation 3.8) and
    set $\Phi \leftarrow \{T \in \Omega_{W_1} \mid T \text{ is a subtorus}\}$;
 4. while $\exists\, T \in \Phi$ such that $\mathrm{im}(\varphi) \subset T$ do
 5.     apply Algorithm 5.1 with input $(n, N-k, \varphi, T, W)$ and denote by $(\widetilde{\varphi}, \widetilde{W})$ its
        output;
 6.     set $W \leftarrow \widetilde{W}$, $\varphi \leftarrow \widetilde{\varphi}$, $k \leftarrow k + 1$;
 7.     compute a complete intersection stratification $(W_j)_{1 \le j \le t}$ of $W$ (Proposition-
        Definition 2.1);
 8.     compute the collections $\Omega_{W_j}$, $j = 1, \dots, t$;
 9.     set $\Phi \leftarrow \bigcup_{j=1}^{t} \{T \in \Omega_{W_j} \mid T \text{ is a subtorus}\}$;
10. end while
11. return $\Gamma \leftarrow \{\varphi^{-1}(W_j)\}_{1 \le j \le t}$.
```

If n is bounded and V is defined over K by a bounded number of Laurent polynomials of degree $\le d$, of bounded height and number of nonzero coefficients, then the cardinality of Γ is bounded by $O(1)$, the Laurent polynomials defining each $Z \in \Gamma$ have coefficients in K, degree bounded by $O(d)$, and height and number of nonzero coefficients bounded by $O(1)$. The complexity of the algorithm is bounded by $O(\log(d))$ ops.

Proof. If Conjecture 3.5 holds, then the computation of the collections Ω_{W_j} in lines 3 and 8 can be done and the algorithm makes sense. At each while loop (lines 4 to 10), the value of the variable k in line 6 increases by one. Hence, this while loop cannot be repeated more than N times since when $k = N$, the collection Φ in line 9 is empty. Hence, the algorithm stops after a finite number of steps.

To prove (1), we first show that, after each while loop, the subvariety $W \subset \mathbb{G}_{\mathrm{m}}^{N-k}$ and the homomorphism $\varphi \in \mathrm{Hom}(\mathbb{G}_{\mathrm{m}}^n, \mathbb{G}_{\mathrm{m}}^{N-k})$ satisfy

$$V = \varphi^{-1}(W). \tag{5.2}$$

By construction, this is clear for the initial values of W and φ in line 2. Now suppose that (5.2) holds at the start of the while loop. If this loop is actually executed, then there exists a subtorus $T \in \Phi$ such that $\mathrm{im}(\varphi) \subset T$. With notation as in line 5, by (5.1) it follows that $\varphi^{-1}(W) = \widetilde{\varphi}^{-1}(\widetilde{W})$. We conclude that (5.2) also holds for the updated values of W and φ in line 6.

For the rest of this proof, we denote by $W \subset \mathbb{G}_{\mathrm{m}}^{N-k}$ the final value of this variable after the last execution of the while loop, and $(W_j)_j$ its corresponding complete intersection stratification. Then $W = \bigcup_j W_j$ and so

$$V = \bigcup_j \varphi^{-1}(W_j) = \bigcup_{Z \in \Gamma} Z.$$

The first part of (2) follows from the definition of a complete intersection stratification and the construction of Γ in line 11. We now prove the second part. Let C be an irreducible component of $Z \in \Gamma$ that is weakly transverse and suppose that $\operatorname{codim}(C) < l_Z$. Let W_j be a stratum in the complete intersection stratification of W of codimension l_Z and such that $Z = \varphi^{-1}(W_j)$. Let Y be an irreducible component of $W_j \cap \operatorname{im}(\varphi)$ such that C is an irreducible component of $\varphi^{-1}(Y)$. Applying Lemma 2.2 and the fact that C is weakly transverse, we obtain that

$$\operatorname{codim}(C) = \operatorname{rank}(C) - \dim(C) = \operatorname{rank}(Y) - \dim(Y). \tag{5.3}$$

The fact that C is weakly transverse also implies that $\langle Y \rangle = \operatorname{im}(\varphi)$ and so $\operatorname{rank}(Y) = \dim(\operatorname{im}(\varphi))$. Let $\widetilde{C}$ be an irreducible component of W_j containing Y, so that $Y \subset \operatorname{im}(\varphi) \cap \widetilde{C}$. From (5.3), we deduce that

$$\dim(Y) > \dim(\operatorname{im}(\varphi)) - \operatorname{codim}(\widetilde{C}).$$

Conjecture 3.5 then implies that there exists $T \in \Omega_{W_j}$ such that $Y \subset T$. It follows that $\operatorname{im}(\varphi) \subset T$ and that T is a subtorus. But this cannot happen since, otherwise, the while loop would not been terminated. We deduce that $\operatorname{codim}(C) \geq l_Z$.

On the other hand, since Z is defined by l_Z equations in the complement of a hypersurface, it follows that $\operatorname{codim}(C) = l_Z$, proving the second part of (2).

The subvariety W in line 2 does not depend on the exponents a_j and so, *a fortiori*, is independent on the bound d for the degrees of the polynomials defining V. The bounds for the size of the output and the complexity of the algorithm then follow easily from Lemma 4.1. □

With notation and assumptions as in Theorem 5.4, denote by $\Gamma_{\max}$ the subset of Γ consisting of the locally closed subsets $Z \in \Gamma$ such that $\overline{Z}$ is maximal with respect to inclusion. Clearly,

$$V = \bigcup_{Z \in \Gamma_{\max}} \overline{Z}.$$

Hence, given an irreducible component C of V that is weakly transverse, there exists $Z \in \Gamma_{\max}$ such that C is an irreducible component of the closure $\overline{Z}$. By Theorem 5.4(2), the equations defining Z form a complete intersection in a suitable neighborhood of C. This observation is clear in the case when all the irreducible components of V are weakly transverse.

Corollary 5.5. *Let notation and assumptions be as in Theorem 5.4. Suppose that all the irreducible components of V are weakly transverse. Then Algorithm 5.2 gives every locally closed subset $Z \in \Gamma_{\max}$ as a complete intersection outside a hypersurface.*

Proof. Let $Z \in \Gamma_{\max}$ and C an irreducible component of $\overline{Z}$. Then C is an irreducible component of V, and so it is weakly transverse. By Theorem 5.4(2), the equations defining Z form a complete intersection in a neighborhood of C. Since this holds for all the components of Z, it follows that this locally closed subset is given as a complete intersection outside a hypersurface. □

For instance, if we know *a priori* that $\dim(V) = 0$ and all points in V have multiplicatively independent coordinates, then

$$V = \bigcup_{Z} Z,$$

where the union is over the locally closed subsets produced by Algorithm 5.2 and given as the zero set of n equations outside a hypersurface. Each of these locally closed subsets are either of dimension 0, or the empty set.

5.2. **The general case.** We devote the rest of this section to the general multivariate case. We first give a simple subroutine which, given a locally closed subset W of an algebraic torus and a torsion coset of codimension 1, computes their intersection as a locally closed subset of an algebraic torus of lower dimension.

Algorithm 5.3 (Intersecting with a torsion coset)

```
Input: $N, k \in \mathbb{N}$ such that $N > k$ and a quadruple $(\boldsymbol{\eta}, W, T, \delta)$ with $\boldsymbol{\eta} \in \mu_\infty^k$, $W \subset \mathbb{G}_{\mathrm{m}}^{N-k}$ a locally closed subset defined over $K(\boldsymbol{\eta})$, $T \subset \mathbb{G}_{\mathrm{m}}^{N-k}$ a torsion coset of codimension 1, and $\delta \in \mathrm{Aut}(\mathbb{G}_{\mathrm{m}}^N)$.
Output: a triple $(\widetilde{\boldsymbol{\eta}}, \widetilde{W}, \widetilde{\delta})$ with $\widetilde{\boldsymbol{\eta}} \in \mu_\infty^{k+1}$, $\widetilde{W} \subset \mathbb{G}_{\mathrm{m}}^{N-k-1}$ a locally closed subset defined over $K(\widetilde{\boldsymbol{\eta}})$, and $\widetilde{\delta} \in \mathrm{Aut}(\mathbb{G}_{\mathrm{m}}^N)$.
1. Write $T = V(\boldsymbol{y}^{\boldsymbol{b}} - \xi)$ for a primitive vector $\boldsymbol{b} \in \mathbb{Z}^{N-k}$ and $\xi \in \mu_\infty$;
2. choose $\tau \in \mathrm{Aut}(\mathbb{G}_{\mathrm{m}}^{N-k})$ such that $\tau(T) = V(y_{N-k} - \xi)$ as in Lemma 2.4 and let $\pi\colon \mathbb{G}_{\mathrm{m}}^{N-k} \to \mathbb{G}_{\mathrm{m}}^{N-k-1}$ be the projection onto the first $N-k-1$ coordinates;
3. return $\widetilde{\boldsymbol{\eta}} \leftarrow \xi \times \boldsymbol{\eta}$, $\widetilde{W} \leftarrow \pi(\tau(W) \cap V(y_{N-k} - \xi))$ and $\widetilde{\delta} \leftarrow (\tau \times \mathrm{id}_{\mathbb{G}_{\mathrm{m}}^k}) \circ \delta$;
```

Lemma 5.6. *For a given input $(\boldsymbol{\eta}, W, T, \delta)$, the output of Algorithm 5.3 satisfies*

$$\delta^{-1}((W \cap T) \times \{\boldsymbol{\eta}\}) = \widetilde{\delta}^{-1}(\widetilde{W} \times \{\widetilde{\boldsymbol{\eta}}\}).$$

Proof. With notation as in the algorithm, we verify that $\tau(W \cap T) = \widetilde{W} \times \{\xi\}$. We deduce that

$$\delta^{-1}((W \cap T) \times \{\boldsymbol{\eta}\}) = (\delta^{-1} \circ (\tau \times \mathrm{id}_{\mathbb{G}_{\mathrm{m}}^k})^{-1})(\widetilde{W} \times \{\widetilde{\boldsymbol{\eta}}\}) = \widetilde{\delta}^{-1}(\widetilde{W} \times \{\widetilde{\boldsymbol{\eta}}\}),$$

as stated. □

Remark 5.7. The locally closed subset $\widetilde{W}$ in Algorithm 5.3, line 3, can be represented as follows. Write $W = V(\boldsymbol{F}) \setminus V(\boldsymbol{G})$ with $F_j, G_l \in \mathbb{Q}[y_1^{\pm 1}, \dots, y_{N-k}^{\pm 1}]$. Then

$$\widetilde{W} = V(\widetilde{\boldsymbol{F}}) \setminus V(\widetilde{\boldsymbol{G}})$$

with $\widetilde{F}_j = F_j \circ \tau^{-1}(y_1, \dots, y_{N-k-1}, \xi)$ and $\widetilde{G}_l = G_l \circ \tau^{-1}(y_1, \dots, y_{N-k-1}, \xi)$.

In Algorithm 5.4 below, we apply the previous procedure to a subvariety W_0 of $\mathbb{G}_{\mathrm{m}}^N$ and the torsion cosets successively produced by Conjecture 3.5. We thus obtain a decomposition of W_0 as a union of a finite collection of complete intersections outside hypersurfaces with empty exceptional subset (Definition 3.7).

Lemma 5.8. *Assume that Conjecture 3.5 holds. Given a subvariety $W_0 \subset \mathbb{G}_{\mathrm{m}}^N$ defined over K, Algorithm 5.4 stops after a finite number of steps and its output has the following properties:*

(1)

$$W_0 = \bigcup_{k=0}^{N} \bigcup_{(W,\boldsymbol{\eta},\delta) \in \Lambda_k} \delta^{-1}(W \times \{\boldsymbol{\eta}\});$$

(2) the locally closed subset W in a triple $(\boldsymbol{\eta}, W, \delta) \in \Lambda_k$ is given by a collection of Laurent polynomials over $K(\boldsymbol{\eta})$ defining a complete intersection in the complement of a hypersurface;

Algorithm 5.4 (Descent)

```
Input: a subvariety $W_0 \subset \mathbb{G}_{\mathrm{m}}^N$ defined over $K$.
Output: for $k = 0, \dots, N$, a finite collection $\Lambda_k$ of triples $(\boldsymbol{\eta}, W, \delta)$ with $\boldsymbol{\eta} \in \mu_\infty^k$,
    $W \subset \mathbb{G}_{\mathrm{m}}^{N-k}$ a locally closed subset and $\delta \in \mathrm{Aut}(\mathbb{G}_{\mathrm{m}}^N)$.
 1. Set $\Sigma_0 \leftarrow \{(1_{\mathbb{G}_{\mathrm{m}}^0}, W_0, \mathrm{id}_{\mathbb{G}_{\mathrm{m}}^N})\}$, where $1_{\mathbb{G}_{\mathrm{m}}^0}$ denotes the neutral element of $\mathbb{G}_{\mathrm{m}}^0$;
 2. for $k$ from 0 to $N$ do
 3.   set $\Lambda_k \leftarrow \emptyset$ and $\Sigma_{k+1} \leftarrow \emptyset$;
 4.   for $(\boldsymbol{\eta}, W, \delta) \in \Sigma_k$ do
 5.     compute a complete intersection stratification $(W_j)_j$ of $W$ defined over $K$;
 6.     compute the collections $\Omega_{W_j}$ for all $j$;
 7.     if $W_j \not\subset \bigcup \Omega_{W_j}$, then add $(\boldsymbol{\eta}, W_j \setminus \bigcup \Omega_{W_j}, \delta)$ to $\Lambda_k$;
 8.     for each $j$ and $T \in \Omega_{W_j}$ do
 9.       apply Algorithm 5.3 to $(\boldsymbol{\eta}, W_j, T, \delta)$ and add its output to $\Sigma_{k+1}$;
10.     end for
11.   end for
12. end for
```

(3) if $(\boldsymbol{\eta}, W, \delta) \in \Lambda_k$ for some k and $Z \subset \mathbb{G}_{\mathrm{m}}^N$ is an irreducible locally closed subset contained in $\delta^{-1}(W \times \{\boldsymbol{\eta}\})$, then

$$\mathrm{rank}(Z) - \dim(Z) \geq \mathrm{codim}(W).$$

Proof. If Conjecture 3.5 holds, the computation of the collections Ω_{W_j} in line 6 of the algorithm can be performed and so Algorithm 5.4 stops after a finite number of steps.

We first show that, for $k = 0, \dots, N+1$,

$$W_0 = \Big(\bigcup_{l=0}^{k-1} \bigcup_{(\boldsymbol{\eta},W,\delta)\in\Lambda_l} \delta^{-1}(W \times \{\boldsymbol{\eta}\}) \Big) \cup \Big(\bigcup_{(\boldsymbol{\eta},W,\delta)\in\Sigma_k} \delta^{-1}(W \times \{\boldsymbol{\eta}\}) \Big). \tag{5.4}$$

This is clear for $k = 0$, because of the definition of Σ_0 in line 1 and the fact that the first union in the right-hand side is empty. For $k \geq 1$, the construction of the collections Λ_k and Σ_{k+1} in lines 7 and 9 together with Lemma 5.6 implies that

$$\bigcup_{(\boldsymbol{\eta},W,\delta)\in\Sigma_k} \delta^{-1}(W \times \{\boldsymbol{\eta}\}) = \Big(\bigcup_{(\boldsymbol{\eta},W,\delta)\in\Lambda_k} \delta^{-1}(W \times \{\boldsymbol{\eta}\}) \Big) \cup \Big(\bigcup_{(\boldsymbol{\eta},W,\delta)\in\Sigma_{k+1}} \delta^{-1}(W \times \{\boldsymbol{\eta}\}) \Big).$$

Then (5.4) follows from the inductive hypothesis. For $(\boldsymbol{\eta}, W, \delta) \in \Sigma_N$, the collections Ω_{W_j} are empty. Hence, $\Sigma_{N+1} = \emptyset$. The statement (1) then follows from the case $k = N+1$ of (5.4).

Statement (2) is clear from the construction of Λ_k in line 7.

To prove (3), let Z' be the locally closed subset of W such that $Z = \delta^{-1}(Z' \times \{\boldsymbol{\eta}\})$. The locally closed subset W is equidimensional and has empty exceptional subset, since it is the complement in W_j of the collection Ω_{W_j}. Hence Z' is not atypical (Definition 3.7), which implies that

$$\mathrm{rank}(Z') - \dim(Z') = \mathrm{codim}(W).$$

In turn, this implies (3) since $\mathrm{rank}(Z) = \mathrm{rank}(Z')$ and $\dim(Z) = \dim(Z')$. □

Remark 5.9. The condition $W_j \not\subset \bigcup \Omega_{W_j}$ in line 7 is equivalent to the fact that W_j has at least one irreducible component that is weakly transverse, see Remark 5.3. This test avoids adding to the collection Λ_k a triple with an empty locally closed set.

Algorithm 5.5 below gives the procedure for the reduction of overdetermined systems. First, it applies Algorithm 5.4 to decompose the linear subvariety $W \subset \mathbb{G}_{\mathrm{m}}^N$ into pieces without exceptional subset. Then, it produces the sought decomposition of the zero set of the given system of equations as the inverse image of these pieces with respect to the homomorphism φ.

Algorithm 5.5 (Reduction of overdetermined systems)

```
Input: a subvariety $V \subset \mathbb{G}_{\mathrm{m}}^n$ defined over $K$.
Output: a finite collection $\Gamma$ of locally closed subsets $Y \subset \mathbb{G}_{\mathrm{m}}^n$ defined over a cyclotomic extension of $K$.
1.  Let $f_i$, $i = 1, \dots, s$, be the Laurent polynomials defining $V$ and write $f_i = \sum_{j=1}^N \alpha_{i,j} \boldsymbol{x}^{\boldsymbol{a}_j}$ with $\alpha_{i,j} \in K$ and $\boldsymbol{a}_j \in \bigcup_i \mathrm{supp}(f_i)$;
2.  set $W \leftarrow V(\sum_{j=1}^N \alpha_{1,j} y_j, \dots, \sum_{j=1}^N \alpha_{s,j} y_j) \subset \mathbb{G}_{\mathrm{m}}^N$;
3.  apply Algorithm 5.4 to $W$ and set $(\Lambda_k)_{0 \le k \le N}$ for its output;
4.  let $\varphi \in \mathrm{Hom}(\mathbb{G}_{\mathrm{m}}^n, \mathbb{G}_{\mathrm{m}}^N)$ be the homomorphism corresponding to the exponents $\boldsymbol{a}_j \in \mathbb{Z}^n$, $j = 1, \dots, N$;
5.  for $k$ from 0 to $N$ do
6.    set $\pi_1 \colon \mathbb{G}_{\mathrm{m}}^N \to \mathbb{G}_{\mathrm{m}}^{N-k}$ and $\pi_2 \colon \mathbb{G}_{\mathrm{m}}^N \to \mathbb{G}_{\mathrm{m}}^k$ for the projections onto the first $N-k$ coordinates and the last $k$ coordinates, respectively;
7.    for $(\boldsymbol{\eta}, W, \delta) \in \Lambda_k$ do
8.      apply Algorithm 2.1 to the homomorphism $\pi_2 \circ \delta \circ \varphi \colon \mathbb{G}_{\mathrm{m}}^n \to \mathbb{G}_{\mathrm{m}}^k$ and the torsion coset $\{\boldsymbol{\eta}\} \subset \mathbb{G}_{\mathrm{m}}^k$;
9.      if $\varphi^{-1}(\boldsymbol{\eta}) \neq \emptyset$ then
10.       let $\boldsymbol{E} = \{p_j\}_{1 \le j \le t}$ be the output of Algorithm 2.1;
11.       let $F_j$, $j = 1, \dots, l$, and $G$ be the Laurent polynomials over $K(\boldsymbol{\eta})$ defining $W$;
12.       set $p_{t+j} \leftarrow F_j \circ \pi_1 \circ \delta \circ \varphi$, $j = 1, \dots, l$, and $q \leftarrow G \circ \pi_1 \circ \delta \circ \varphi$;
13.       set $Y \leftarrow V(p_1, \dots, p_{t+l}) \setminus V(q)$ and add $Y$ to $\Gamma$;
14.     end if
15.   end for
16. end for
```

Theorem 5.10. *Assume that Conjecture 3.5 holds. Given a subvariety $V \subset \mathbb{G}_{\mathrm{m}}^n$ defined over K, Algorithm 5.5 stops after a finite number of steps and its output satisfies:*

(1)
$$V = \bigcup_{Y \in \Gamma} Y;$$

(2) each locally closed subset $Y \in \Gamma$ is either given as a complete intersection in the complement of a hypersurface, or it is the empty set.

If n is bounded and V is defined by a bounded number of Laurent polynomials of degree $\le d$, bounded height and number of nonzero coefficients, then the cardinality of Γ is bounded by $O(1)$, the Laurent polynomials defining each $Y \in \Gamma$ are defined over a cyclotomic extension of degree $O(1)$, have degree bounded by $d^{O(1)}$, and height and number of nonzero coefficients bounded by $O(1)$. The complexity of the algorithm is bounded by $O(\mathrm{M}(\log(d)) \log(\log(d))) = \widetilde{O}(\log(d))$ ops.

Proof. Let $0 \le k \le N$ and $(\boldsymbol{\eta}, W, \delta) \in \Lambda_k$ be as in line 7 of the algorithm. In case $\varphi^{-1}(\boldsymbol{\eta}) \neq \emptyset$, we denote by Y the locally closed subset associated to this triple. By construction,

$$(\delta\circ\varphi)^{-1}(W\times\{\boldsymbol{\eta}\}) = \begin{cases}\emptyset & \text{if } \varphi^{-1}(\boldsymbol{\eta})=\emptyset,\\ Y & \text{if } \varphi^{-1}(\boldsymbol{\eta})\neq\emptyset.\end{cases} \tag{5.5}$$

The decomposition in (1) then follows from the one in Lemma 5.8(1) and the fact that $\varphi^{-1}(W)=V$.

To prove (2), suppose that Y is nonempty and let C be one of its irreducible components. By (5.5), there is an irreducible component Z of $(W\times\{\boldsymbol{\eta}\})\cap\operatorname{im}(\delta\circ\varphi)$ such that $C=(\delta\circ\varphi)^{-1}(Z)$. Applying Lemmas 2.2 and 5.8(3), we deduce that

$$\operatorname{rank}(C)-\dim(C)=\operatorname{rank}(Z)-\dim(Z)\geq\operatorname{codim}(W)=l. \tag{5.6}$$

On the other hand, we have that $C\subset(\delta\circ\varphi)^{-1}(\boldsymbol{\eta})$ and so $\operatorname{rank}(C)\leq n-t$, thanks to Lemma 2.3. Together with (5.6), this implies that

$$\operatorname{codim}(C)=n-\dim(C)\geq t+l.$$

Since Y is defined by the $t+l$ Laurent polynomials $p_1,\dots,p_{t+l}$ outside the hypersurface $V(q)$, it follows that $\operatorname{codim}(C)=t+l$. Hence, Y is a complete intersection outside $V(q)$, as stated.

Now assume that both n and s are bounded and that each f_i is of degree $\leq d$, of bounded height and number of nonzero coefficients. The variety $W\subset\mathbb{G}_{\mathrm{m}}^N$ in line 2 does not depend on d. Hence, the application of Algorithm 5.4 in line 3 produces a output of size $O(1)$ using $O(1)$ ops. In particular, the collection Γ has cardinality bounded by $O(1)$. Lemma 2.3 shows that the binomials in the collection $\boldsymbol{E}$ in line 10 have coefficients in μ_l for $l\leq O(1)$, that the Laurent polynomials defining Y have degree, height and number of nonzero coefficients as predicted by Theorem 5.10, and that the complexity of this step is bounded by $O(\mathrm{M}(\log(d))\log(\log(d)))$ ops. From this, we deduce that the overall complexity is bounded by $O(\mathrm{M}(\log(d))\log(\log(d)))=\widetilde{O}(\log(d))$ ops. □

Remark 5.11. For $Y\in\Gamma$, the defining equations and inequations come from different sources. In the notation of Algorithm 5.5, the Laurent polynomials p_i, $i=1,\dots,t$, are binomials with coefficients in μ_∞, whereas p_i, $i=t+1,\dots,t+l$ come from the equations defining W. If $Y\neq\emptyset$ and C is an irreducible component of Y, we have that

$$t=n-\operatorname{rank}(C),\quad l=\operatorname{rank}(C)-\dim(C).$$

Theorem 1.3 in the introduction follows by decomposing the affine space $\mathbb{A}^n$ as a disjoint union of tori and applying Theorem 5.10 to each of them.

Proof of Theorem 1.3. Given a subset $I\subset\{1,\dots,n\}$, we consider the locally closed subset $G_I=\{\boldsymbol{x}\in\mathbb{A}^n\mid x_i\neq0 \text{ if and only if } i\in I\}$. The affine space then decomposes as a disjoint union

$$\mathbb{A}^n=\bigsqcup_I G_I,$$

and each G_I is an algebraic torus $\mathbb{G}_{\mathrm{m}}^{\#I}$ embedded into the standard linear subspace $V(\{x_i\mid i\notin I\})$ of $\mathbb{A}^n$.

Given a system of equations over $\mathbb{A}^n$, we can split it into 2^n systems of equations over these algebraic tori. For each I, we solve the corresponding system of equations by applying Algorithm 5.5 and we multiply the obtained Laurent polynomials by suitable monomials in order to clear all possible denominators. Finally, we add the set of variables x_i, $i\notin I$, to the obtained equations, and we multiply the polynomial defining the open subset by the monomial $\prod_{i\in I}x_i$.

By Theorem 5.10(1), the resulting polynomials form a collection of systems of equations which define either a complete intersection in the complement of a hypersurface, or the empty set. By Theorem 5.10(2), this collection gives a decomposition of $V(f_1,\dots,f_s)$ as in (1.3). The rest of the statement follows also from Theorem 5.10. □

Remark 5.12. In practice, there are a number of modifications that can be applied to our general procedure. They do not affect the theoretical complexity of the algorithms, but can significantly simplify the computations in concrete examples.

(1) For a given system of equations, it is better to apply Algorithm 5.1 several times, starting with a subtorus $T \subset \mathbb{G}_{\mathrm{m}}^N$ of codimension 1 of small degree and the linear subvariety $W \subset \mathbb{G}_{\mathrm{m}}^N$. If it turns that $\mathrm{im}(\varphi) \subset T$, then this procedure reduces the dimension of the ambient space without breaking W into several pieces, as might happen when applying the descent in Algorithm 5.5.

(2) Both in Algorithms 5.2 and 5.5, one can replace the linear subvariety $W \subset \mathbb{G}_{\mathrm{m}}^N$ by the subvariety of $\mathbb{G}_{\mathrm{m}}^{N-1}$ given by

$$V\Big(\alpha_{1,1}+\sum_{j=2}^{N}\alpha_{1,j}y_j,\dots,\alpha_{s,1}+\sum_{j=2}^{N}\alpha_{s,j}y_j\Big)$$

and φ by the homomorphism associated to the vectors $\boldsymbol{a}_j-\boldsymbol{a}_1$, $j=2,\dots,N$. In this way, computations start in a space of dimension $N-1$ instead of one of dimension N.

(3) The locally closed subsets Y of $\mathbb{G}_{\mathrm{m}}^n$ produced by Algorithm 5.5 have codimension bounded by n. Hence, in line 7 of this algorithm, it suffices to consider only the triples $(\boldsymbol{\eta},W,\delta)$ such that $\mathrm{codim}(W)\le n$. Consequently, in line 5 of Algorithm 5.4, it suffices to compute only the components W_j in the complete intersection stratification of W of codimension bounded by n. A similar remark applies to Algorithm 5.2 for the weakly transverse case.

6. Examples

We illustrate with two examples how our algorithms work. We will systematically use the modifications in Remark 5.12. To shorten the presentation, we will only compute the zeros of these systems in the algebraic torus.

Example 6.1. Let $d\ge 1$ and consider the system of polynomials

$$f_1 = x_1^dx_2^2-5x_1^dx_2-2x_2+10,\quad f_2=x_1^{d+1}x_2-2x_1^dx_2-2x_1+4\in\mathbb{Q}[x_1,x_2]. \tag{6.1}$$

Its zero set in $\mathbb{G}_{\mathrm{m}}^2$ consists of the curve defined by the polynomial $x_1^dx_2-2$ (which is a common factor of f_1 and f_2) and the isolated point $(2,5)$. In the sequel, we describe how our algorithms give this result.

The support of these polynomials consists of the vectors $(d+1,1),(d,2),(d,1),(0,1),(1,0),(0,0)\in\mathbb{Z}^2$. Let $W\subset\mathbb{G}_{\mathrm{m}}^5$ be the subvariety defined by

$$F_1=y_2-5y_3-2y_4+10,\quad F_2=y_1-2y_3-2y_5+4\in\mathbb{Q}[y_1^{\pm1},\dots,y_5^{\pm1}]$$

and $\varphi\colon\mathbb{G}_{\mathrm{m}}^2\to\mathbb{G}_{\mathrm{m}}^5$ the homomorphism given by

$$\varphi(x_1,x_2)=(x_1^{d+1}x_2,x_1^dx_2^2,x_1^dx_2,x_2,x_1),$$

so that $V(f_1,f_2)=\varphi^{-1}(V(F_1,F_2))$.

The subtorus $T = V(y_2y_3^{-1}y_4^{-1} - 1)$ satisfies $\mathrm{im}(\varphi) \subset T$. Following Remark 5.12(1), we apply Algorithm 5.1 at this point, instead of the descent procedure in Algorithm 5.4. We choose the automorphism $\tau \in \mathrm{Aut}(\mathbb{G}_{\mathrm{m}}^5)$ given by

$$\tau(y_1, y_2, y_3, y_4, y_5) = (y_1, y_3, y_4, y_5, y_2y_3^{-1}y_4^{-1}).$$

It satisfies $\tau(T) = V(y_5 - 1)$. The corresponding output of Algorithm 5.1 for the triple (W, T, φ) is the subvariety $\widetilde{W} \subset \mathbb{G}_{\mathrm{m}}^4$ defined by

$$\widetilde{F}_1 = F_1(y_1, y_2y_3, y_2, y_3, y_4) = y_2y_3 - 5y_2 - 2y_3 + 10,$$
$$\widetilde{F}_2 = F_2(y_1, y_2y_3, y_2, y_3, y_4) = y_1 - 2y_2 - 2y_4 + 4,$$

and the homomorphism $\widetilde{\varphi}\colon \mathbb{G}_{\mathrm{m}}^2 \to \mathbb{G}_{\mathrm{m}}^4$ given by $\widetilde{\varphi}(x_1, x_2) = (x_1^{d+1}x_2, x_1^dx_2, x_2, x_1)$.

Set $(W, \varphi) \leftarrow (\widetilde{W}, \widetilde{\varphi})$. We apply again Algorithm 5.1, this time to the triple (W, T, φ) with $T = V(y_1y_2^{-1}y_4^{-1} - 1)$. This subtorus satisfies $\mathrm{im}(\varphi) \subset T$. We choose $\tau \in \mathrm{Aut}(\mathbb{G}_{\mathrm{m}}^4)$ given by $\tau(y_1, y_2, y_3, y_4) = (y_2, y_3, y_4, y_1y_2^{-1}y_4^{-1})$, which satisfies $\tau(T) = V(y_4 - 1)$. The corresponding output of Algorithm 5.1 is the subvariety $\widetilde{W} \subset \mathbb{G}_{\mathrm{m}}^3$ defined by

$$\widetilde{F}_1 = F_1(y_1y_3, y_1, y_2, y_3) = y_1y_2 - 5y_1 - 2y_2 + 10,$$
$$\widetilde{F}_2 = F_2(y_1y_3, y_1, y_2, y_3) = y_1y_3 - 2y_1 - 2y_3 + 4,$$

and the homomorphism $\widetilde{\varphi}\colon \mathbb{G}_{\mathrm{m}}^2 \to \mathbb{G}_{\mathrm{m}}^3$ given by $\widetilde{\varphi}(x_1, x_2) = (x_1^dx_2, x_2, x_1)$.

Set again $(W, \varphi) \leftarrow (\widetilde{W}, \widetilde{\varphi})$. There is no proper subtorus of $\mathbb{G}_{\mathrm{m}}^3$ of degree independent of d and containing the image of φ. Hence, we cannot further apply Remark 5.12(1), at least when $d \gg 0$. Instead, we apply the procedure in Algorithm 5.5.

The subvariety W has two irreducible components, of codimension 1 and 2, respectively. Indeed,

$$W = V(y_1 - 2) \cup V(y_2 - 5, y_3 - 2).$$

Following line 3 of Algorithm 5.5, we apply Algorithm 5.4 to this subvariety in order to construct the collections Λ_k. As in line 1 of this algorithm, we set $\Sigma_0 = \{(1_{\mathbb{G}_{\mathrm{m}}^0}, W, \mathrm{id}_{\mathbb{G}_{\mathrm{m}}^3})\}$, where $1_{\mathbb{G}_{\mathrm{m}}^0}$ denotes the neutral element of the trivial group $\mathbb{G}_{\mathrm{m}}^0$. We now describe what is done in the loop between lines 2 and 12.

Set $k = 0$. There is only one element in Σ_0, namely $(1_{\mathbb{G}_{\mathrm{m}}^0}, W, \mathrm{id}_{\mathbb{G}_{\mathrm{m}}^3})$. A complete intersection stratification of W is given by

$$W_1 = V(y_1 - 2)\backslash V(y_3 - 2), \quad W_2 = V((y_1 - 2)(y_2 - 5), y_3 - 2).$$

It is easy to check that W_1 has empty exceptional subset and that the only maximal atypical subvariety of W_2 is given by $W_2 \cap T = V(y_1 - 2, y_3 - 2)$ for the subtorus $T = V(y_1y_3^{-1} - 1)$. Hence, we may choose $\Omega_{W_1} = \emptyset$ and $\Omega_{W_2} = \{T\}$ in line 6 and we add to Λ_0 the triples $(1_{\mathbb{G}_{\mathrm{m}}^0}, W_1, \mathrm{id}_{\mathbb{G}_{\mathrm{m}}^3})$ and $(1_{\mathbb{G}_{\mathrm{m}}^0}, W_2 \setminus T, 1_{\mathbb{G}_{\mathrm{m}}^3})$ in line 7. Let us consider now the loop between lines 8 and 10. Since Ω_{W_2} consists of the only torsion coset $\{T\}$, we apply Algorithm 5.3 to the quadruple $(1_{\mathbb{G}_{\mathrm{m}}^0}, W_2, T, \mathrm{id}_{\mathbb{G}_{\mathrm{m}}^3})$. We choose $\tau \in \mathrm{Aut}(\mathbb{G}_{\mathrm{m}}^3)$ given by $\tau(y_1, y_2, y_3) = (y_1, y_2, y_1^{-1}y_3)$. Thus $\tau(T) = V(y_3 - 1)$ as required, and

$$\tau(W_2 \cap T) = \widetilde{W} \times \{1\},$$

with $\widetilde{W} = V(y_1 - 2) \subset \mathbb{G}_{\mathrm{m}}^2$. Hence, Algorithm 5.3 gives $(1, \widetilde{W}, \tau)$ as output. We add this element to Σ_1 in line 9.

Set now $k = 1$. The only element of Σ_1 is $(1, \widetilde{W}, \tau)$ and $\widetilde{W} = V(y_1 - 2)$ has no atypical locally closed subset. Thus, we choose $\Omega_{\widetilde{W}} = \emptyset$ and add $(1, \widetilde{W}, \tau)$ to Λ_1 in line 7. The construction of Algorithm 5.4 ends up here.

We now construct the collection Γ in Algorithm 5.5. Recall that $\varphi\colon \mathbb{G}_{\mathrm{m}}^2 \to \mathbb{G}_{\mathrm{m}}^3$ is the homomorphism given by

$$\varphi(x_1, x_2) = (x_1^d x_2, x_2, x_1).$$

The elements of Λ_0 are $(1_{\mathbb{G}_{\mathrm{m}}^0}, W_1, \mathrm{id}_{\mathbb{G}_{\mathrm{m}}^3})$ and $(1_{\mathbb{G}_{\mathrm{m}}^0}, W_2 \setminus T, \mathrm{id}_{\mathbb{G}_{\mathrm{m}}^3})$. These triples contribute to Γ with the locally closed subsets

$$\begin{aligned} Y_1 &= V(x_1^d x_2 - 2) \backslash V(x_1 - 2), \\ Y_2 &= V((x_1^d x_2 - 2)(x_2 - 5), x_1 - 2) \backslash V(x_1^{d-1} x_2 - 1) = \{(2,5)\}. \end{aligned}$$

The only triple in Λ_1 is $(1, \widetilde{W}, \tau)$, and it contributes to Γ with the locally closed subset

$$Y_3 = V(x_1^d x_2 - 2, x_1^{d-1} x_2 - 1) = \{(2, 2^{1-d})\}.$$

By Theorem 5.10, the zero set of the system (6.1) decomposes as $Y_1 \cup Y_2 \cup Y_3$.

Example 6.2. Let $d \geq 1$ and consider the system of polynomials

$$f_1 = x_1^{3d+1} x_2^{3d} + x_1^2 x_2 + 5, f_2 = x_1^{3d+2} x_2^{3d} + 5x_1 + 25,$$
$$f_3 = x_1 + x_1^2 x_2 + 25 x_2 \in \mathbb{Q}[x_1, x_2]. \tag{6.2}$$

Its zero set in $\mathbb{G}_{\mathrm{m}}^2$ consists of two points $(5\zeta, \zeta/5)$ of rank 1, with ζ a primitive third root of unity. As in the previous example, we will describe how our algorithms give this result.

The support of f_1 and f_2 consists of the vectors $(0,0), (3d+1, 3d), (3d+2, 3d), (2,1), (1,0), (0,1) \in \mathbb{Z}^2$. Let $W \subset \mathbb{G}_{\mathrm{m}}^5$ be the subvariety defined by

$$F_1 = y_1 + y_3 + 5, \quad F_2 = y_2 + 5y_4 + 25, \quad F_3 = y_4 + y_3 + 25 y_5$$

and $\varphi\colon \mathbb{G}_{\mathrm{m}}^2 \to \mathbb{G}_{\mathrm{m}}^5$ the homomorphism given by

$$\varphi(x_1, x_2) = (x_1^{3d+1} x_2^{3d}, x_1^{3d+2} x_2^{3d}, x_1^2 x_2, x_1, x_2).$$

The subtorus $T = V(y_1 y_2^{-1} y_4 - 1)$ satisfies $\mathrm{im}(\varphi) \subset T$. Following Remark 5.12(1), we apply Algorithm 5.1 to the triple (W, T, φ). We choose $\tau \in \mathrm{Aut}(\mathbb{G}_{\mathrm{m}}^5)$ given by $\tau(y_1, y_2, y_3, y_4, y_5) = (y_2, y_1 y_2^{-1}, y_3, y_5, y_1 y_2^{-1} y_4)$ as one of the automorphisms that satisfies $\tau(T) = V(y_5 - 1)$. The corresponding output of this algorithm is the subvariety $\widetilde{W} \subset \mathbb{G}_{\mathrm{m}}^4$ defined by $\widetilde{F}_i = F_i(y_1 y_2, y_1, y_3, y_2^{-1}, y_4)$, $i = 1, 2, 3$, that is

$$\widetilde{F}_1 = y_1 y_2 + y_3 + 5, \quad \widetilde{F}_2 = y_1 + 5 y_2^{-1} + 25, \quad \widetilde{F}_3 = y_2^{-1} + y_3 + 25 y_4,$$

and the homomorphism $\widetilde{\varphi}\colon \mathbb{G}_{\mathrm{m}}^2 \to \mathbb{G}_{\mathrm{m}}^4$ given by $\widetilde{\varphi}(x_1, x_2) = (x_1^{3d+2} x_2^{3d}, x_1^{-1}, x_1^2 x_2, x_2)$.

Set $(W, \varphi) \leftarrow (\widetilde{W}, \widetilde{\varphi})$. We apply again Algorithm 5.1, this time to the triple (W, T, φ) with $T = V(y_2^2 y_3 y_4^{-1} - 1)$. This subtorus satisfies $\mathrm{im}(\varphi) \subset T$. We choose $\tau \in \mathrm{Aut}(\mathbb{G}_{\mathrm{m}}^4)$ given by $\tau(y_1, y_2, y_3, y_4) = (y_1, y_2^{-2} y_4, y_2, y_2^2 y_3 y_4^{-1})$, which satisfies $\tau(T) = V(y_4 - 1)$. The corresponding output of Algorithm 5.1 is subvariety $\widetilde{W} \subset \mathbb{G}_{\mathrm{m}}^3$ defined by $\widetilde{F}_i = F_i(y_1, y_3, y_2, y_2 y_3^2)$, $i = 1, 2, 3$, that is

$$\widetilde{F}_1 = y_1 y_3 + y_2 + 5, \quad \widetilde{F}_2 = y_1 + 5 y_3^{-1} + 25, \quad \widetilde{F}_3 = y_3^{-1} + y_2 + 25 y_2 y_3^2,$$

and the homomorphism $\widetilde{\varphi}\colon \mathbb{G}_{\mathrm{m}}^2 \to \mathbb{G}_{\mathrm{m}}^3$ given by $\widetilde{\varphi}(x_1, x_2) = (x_1^{3d+2} x_2^{3d}, x_1^2 x_2, x_1^{-1})$.

Set again $(W, \varphi) \leftarrow (\widetilde{W}, \widetilde{\varphi})$. We apply for a third time Algorithm 5.1, this time to the triple (W, T, φ) with $T = V(y_1 y_3^2 - 1)$. This subtorus satisfies $\mathrm{im}(\varphi) \subset T$. We choose $\tau \in \mathrm{Aut}(\mathbb{G}_{\mathrm{m}}^3)$ given by $\tau(y_1, y_2, y_3) = (y_1, y_3, y_1 y_3^2)$, which satisfies $\tau(T) = V(y_3 - 1)$. The subvariety $\widetilde{W} \subset \mathbb{G}_{\mathrm{m}}^2$ in the output of Algorithm 5.1 is defined by

$$\widetilde{F}_1 = F_1(y_2^{-2}, y_1, y_2) = y_2^{-1} + y_1 + 5, \quad \widetilde{F}_2 = F_2(y_2^{-2}, y_1, y_2) = y_2^{-2} + 5 y_2^{-1} + 25,$$

because the Laurent polynomial $\widetilde{F}_3 = F_3(y_2^{-2}, y_1, y_2) = y_2^{-1} + y_1 + 25y_1y_2^2$ lies in the ideal $(\widetilde{F}_1, \widetilde{F}_2)$. The corresponding homomorphism $\widetilde{\varphi}\colon \mathbb{G}_{\mathrm{m}}^2 \to \mathbb{G}_{\mathrm{m}}^2$ is given by $\widetilde{\varphi}(x_1, x_2) = (x_1^2x_2, x_1^{-1}, x_1^{3d}x_2^{3d})$.

Again set $(W, \varphi) \leftarrow (\widetilde{W}, \widetilde{\varphi})$. There exists no proper subtorus of $\mathbb{G}_{\mathrm{m}}^2$ of degree independent of d such that $\mathrm{im}(\varphi) \subset T$. Thus we cannot further apply the Algorithm 5.1 when $d \gg 0$. Instead, we apply the general procedure in Algorithm 5.5. As indicated in Algorithm 5.5, line 3, we apply Algorithm 5.4 to the subvariety $W \subset \mathbb{G}_{\mathrm{m}}^2$ to construct the sets Λ_k. We describe what is done in the loop in lines 2 to 12 of this algorithm.

Set $k = 0$ and choose at line 1 the only element of Σ_0, namely $(1_{\mathbb{G}_{\mathrm{m}}^0}, W, \mathrm{id}_{\mathbb{G}_{\mathrm{m}}^2})$. The subvariety W consists of the two points $(5\zeta, \zeta/5)$ with ζ a primitive third root of unity. In particular, it is 0-dimensional and is already given as a complete intersection. Moreover, these two points are atypical since

$$W \cap T_\zeta = \{(5\zeta, \zeta/5)\}$$

where T_ζ is the torsion coset $V(y_1y_2 - \zeta^2)$ for $\zeta \in \mu_3 \setminus \{1\}$. Hence we may choose $\Omega_W = \{T_\zeta\}_{\zeta\in\mu_3\setminus\{1\}}$ in line 6. We have that $W \subset \bigcup \Omega_W$ and so $\Lambda_0 = \emptyset$.

Now fix $\zeta \in \mu_3 \setminus \{1\}$ and apply Algorithm 5.3 to the quadruple $(1_{\mathbb{G}_{\mathrm{m}}^0}, W, T_\zeta, \mathrm{id}_{\mathbb{G}_{\mathrm{m}}^2})$. We choose $\tau \in \mathrm{Aut}(\mathbb{G}_{\mathrm{m}}^2)$ given by $\tau(y_1, y_2) = (y_1, y_1y_2)$. This automorphism satisfies $\tau(T_\zeta) = V(y_2 - \zeta^2)$ as required, and

$$\tau(W \cap T_\zeta) = \widetilde{W}_\zeta \times \{\zeta^2\}$$

with $\widetilde{W}_\zeta = V(y_1 - 5\zeta) = \{5\zeta\} \subset \mathbb{G}_{\mathrm{m}}$. The output of Algorithm 5.3 is the triple $(\zeta^2, \widetilde{W}_\zeta, \tau)$, which we add to Σ_1. Hence, at the end of the loop between lines 8 and 10,

$$\Sigma_1 = \{(\zeta^2, \widetilde{W}_\zeta, \tau)\}_{\zeta\in\mu_3\setminus\{1\}}.$$

Set now $k = 1$ in the loop between lines 2 and 12. The subvariety $\widetilde{W}_\zeta$ has no atypical component because it is 0-dimensional and contains no torsion point. Thus we choose $\Omega_{W_\zeta} = \emptyset$ and add to Λ_1 the two elements $(\zeta^2, \widetilde{W}_\zeta, \tau)$ for $\zeta \in \mu_3 \setminus \{1\}$. The construction of Algorithm 5.4 finishes here.

We now construct the collection Γ in Algorithm 5.5. Recall that $\varphi\colon \mathbb{G}_{\mathrm{m}}^2 \to \mathbb{G}_{\mathrm{m}}^2$ is given by

$$\varphi(x_1, x_2) = (x_1^2x_2, x_1^{-1}, x_1^{3d}x_2^{3d}).$$

The collection Λ_1 contributes to Γ with the locally closed subsets

$$Y_\zeta = V(x_1^2x_2 - 5\zeta, x_1x_2 - \zeta^2) \setminus V(1) = \left\{\left(5\zeta, \frac{\zeta}{5}\right)\right\} \quad \text{for } \zeta \in \mu_3 \setminus \{1\}.$$

By Theorem 5.10, the zero set of the system (6.2) decomposes as the union of these two points.

References

[BG06] E. Bombieri and W. Gubler, *Heights in Diophantine geometry*, New Math. Monogr., vol. 4, Cambridge Univ. Press, 2006.

[BMZ99] E. Bombieri, D. Masser, and U. Zannier, *Intersecting a curve with algebraic subgroups of multiplicative groups*, Internat. Math. Res. Notices **1999** (1999), 1119–1140.

[BMZ07] ______, *Anomalous subvarieties — structure theorems and applications*, Int. Math. Res. Notices **2007** (2007), Art. ID rnm057, 33 pp..

[Cha12] A. Chambert-Loir, *Relations de dépendance et intersections exceptionnelles*, Séminaire Bourbaki 2010/11, Astérisque, vol. 348, Soc. Math. France, 2012, pp. 149–188.

[Coh93] H. Cohen, *A course in computational algebraic number theory*, Grad. Texts in Math., vol. 138, Springer-Verlag, 1993.

[FGS08] M. Filaseta, A. Granville, and A. Schinzel, *Irreducibility and greatest common divisor algorithms for sparse polynomials*, Number theory and polynomials, London Math. Soc. Lecture Notes Ser., vol. 352, Cambridge Univ. Press, 2008, pp. 155–176.

[GG03] J. von zur Gathen and J. Gerhard, *Modern computer algebra. 2nd ed.*, Cambridge Univ. Press, 2003.

[Hab09] P. Habegger, *On the bounded height conjecture*, Int. Math. Res. Notices **2009** (2009), 860–886.

[Lau84] M. Laurent, *Équations diophantiennes exponentielles*, Invent. Math. **78** (1984), 299–327.

[Ler11] L. Leroux, *Algorithmes pour les polynômes lacunaires*, Ph.D. thesis, Université de Caen, 2011, downloadable from `http://tel.archives-ouvertes.fr/tel-00580656`.

[Ler12] ______, *Computing the torsion points of a variety defined by lacunary polynomials*, Math. Comp. **81** (2012), 1587–1607.

[Mau08] G. Maurin, *Courbes algébriques et équations multiplicatives*, Math. Ann. **341** (2008), 789–824.

[Pla77] D. A. Plaisted, *Sparse complex polynomials and polynomial reducibility*, J. Comput. System Sci. **14** (1977), 210–221.

[Schi65] A. Schinzel, *On the reducibility of polynomials and in particular of trinomials*, Acta Arith. **11** (1965), 1–34.

[Schi00] ______, *Polynomials with special regard to reducibility. With an appendix by Umberto Zannier*, Encyclopedia Math. Appl., vol. 77, Cambridge Univ. Press, 2000.

[Schi02] ______, *On the greatest common divisor of two univariate polynomials. I*, A panorama of number theory or the view from Baker's garden (Zürich, 1999), Cambridge Univ. Press, 2002, pp. 337–352.

[Schm96] W. M. Schmidt, *Heights of points on subvarieties of* $\mathbb{G}_m^n$, Number theory (Paris, 1993–1994), London Math. Soc. Lecture Notes Ser., vol. 235, Cambridge Univ. Press, 1996, pp. 157–187.

[Via08] E. Viada, *The intersection of a curve with a union of translated codimension-two subgroups in a power of an elliptic curve*, Algebra Number Theory **2** (2008), 249–298.

[Zan09] U. Zannier, *Lecture notes on Diophantine analysis. With an appendix by Francesco Amoroso*, Appunti. Sc. Norm. Super. Pisa (N. S.), vol. 8, Edizioni della Normale, 2009.

[Zan12] ______, *Some problems of unlikely intersections in arithmetic and geometry. With appendixes by David Masser*, Ann. of Math. Stud., vol. 181, Princeton Univ. Press, 2012.

[Zil02] B. Zilber, *Exponential sums equations and the Schanuel conjecture*, J. London Math. Soc. (2) **65** (2002), 27–44.

Laboratoire de mathématiques Nicolas Oresme, CNRS UMR 6139, Université de Caen, BP 5186, 14032 Caen Cedex, France
Email address: `francesco.amoroso@unicaen.fr`
URL: `http://www.math.unicaen.fr/~amoroso/`

Laboratoire de mathématiques Nicolas Oresme, CNRS UMR 6139, Université de Caen, BP 5186, 14032 Caen Cedex, France
Email address: `louis.leroux@ac-caen.fr`
URL: `http://www.math.unicaen.fr/~lleroux/`

ICREA & Departament d'Àlgebra i Geometria, Universitat de Barcelona. Gran Via 585, 08007 Barcelona, Spain
Email address: `sombra@ub.edu`
URL: `http://atlas.mat.ub.es/personals/sombra/`