Unlikely Intersections and multiple roots of sparse polynomials

Francesco Amoroso, Martin Sombra, Umberto Zannier

UNLIKELY INTERSECTIONS AND MULTIPLE ROOTS OF SPARSE POLYNOMIALS

FRANCESCO AMOROSO, MARTÍN SOMBRA, AND UMBERTO ZANNIER

Abstract. We present a structure theorem for the multiple non-cyclotomic irreducible factors appearing in the family of all univariate polynomials with a given set of coefficients and varying exponents. Roughly speaking, this result shows that the multiple non-cyclotomic irreducible factor of a sparse polynomial, are also sparse.

To obtain this, we give a version of a theorem of Bombieri and Zannier on the intersection of a subvariety of codimension 2 of the multiplicative group with torsion curves, with an explicit dependence on the height of the subvariety. We also apply this to obtain a result in the direction of a conjecture of Bolognesi and Pirola.

1. Introduction

This text is motivated by the following question: let $f \in \overline{\mathbb{Q}}[t^{\pm 1}]$ be a sparse Laurent polynomial, that is, a polynomial of high degree but relatively few nonzero terms. When does f have a multiple root in $\overline{\mathbb{Q}}^\times$?

In precise terms, we consider sparse (univariate) Laurent polynomials given by the restriction of a *fixed* regular functions on $\mathbb{G}_{\mathrm{m}}^N$, namely a multivariate Laurent polynomial, to a *varying* 1-parameter subgroup. Let $N \geq 1$, and fix $\boldsymbol{\gamma} = (\gamma_0, \gamma_1, \ldots, \gamma_N) \in \overline{\mathbb{Q}}^{N+1}$ and, for $\boldsymbol{a} = (a_1, \ldots, a_N) \in \mathbb{Z}^N$, set

$$f_{\boldsymbol{a}} = \gamma_0 + \gamma_1 t^{a_1} + \cdots + \gamma_N t^{a_N} \in \overline{\mathbb{Q}}[t^{\pm 1}].$$

This is the restriction of the affine polynomial

$$L = \gamma_0 + \gamma_1 x_1 + \cdots + \gamma_N x_N \in \overline{\mathbb{Q}}[x_1, \ldots, x_N]$$

to the subgroup of the multiplicative group $\mathbb{G}_{\mathrm{m}}^N = (\overline{\mathbb{Q}}^\times)^N$ parameterized by the monomial map $t \mapsto (t^{a_1}, \ldots, t^{a_N})$.

The occurrence of a multiple root in $f_{\boldsymbol{a}}$ certainly happens in the following situation. Suppose that there is $1 \leq k \leq N-1$ and $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_N, \boldsymbol{\theta} \in \mathbb{Z}^{N-k}$ such that $\langle \boldsymbol{b}_i, \boldsymbol{\theta} \rangle = a_i$, $i = 1, \ldots, N$. Let $\boldsymbol{y} = (y_1, \ldots, y_{N-k})$ be a group of $N-k$ variables and consider the Laurent polynomial

$$F = \gamma_0 + \gamma_1 \boldsymbol{y}^{\boldsymbol{b}_1} + \cdots + \gamma_N \boldsymbol{y}^{\boldsymbol{b}_N} \in \overline{\mathbb{Q}}[y_1^{\pm 1}, \ldots, y_{N-k}^{\pm 1}] \tag{1.1}$$

with $\boldsymbol{y}^{\boldsymbol{b}_i} = y_1^{b_{i,1}} \cdots y_{N-k}^{b_{i,N-k}}$. Suppose also that F has a multiple factor P and that $P(t^{\theta_1}, \ldots, t^{\theta_N})$ is not a monomial. Then

$$f_{\boldsymbol{a}} = F(t^{\theta_1}, \ldots, t^{\theta_N}),$$

Date: December 26, 2014.

2010 *Mathematics Subject Classification.* Primary 11C08; Secondary 11G50.

Key words and phrases. Sparse polynomial, multiple roots, unlikely intersections.

This research was partially financed by the European project ERC Advanced Grant "Diophantine problems" (grant agreement n° 267273), the CNRS project PICS 6381 "Géométrie diophantienne et calcul formel", and the Spanish project MINECO MTM2012-38122-C03-02.

$p = P(t^{\theta_1}, \dots, t^{\theta_N})$ is a multiple nontrivial factor of $f_{\boldsymbol{a}}$, and any root of p is a multiple root of f.

Our main result (Theorem 1.1) shows that there is a *finite* family of multivariate Laurent polynomials as in (1.1) such that the multiple *non-cyclotomic* roots occurring in the family of polynomials $f_{\boldsymbol{a}}$, $\boldsymbol{a} \in \mathbb{Z}^N$, come from restriction of the multiple factors in this finite family, restricted to the subgroup of $\mathbb{G}_{\mathrm{m}}^N$ parameterized by the monomial map $t \mapsto (t^{\theta_1}, \dots, t^{\theta_N})$. In particular, the multiple irreducible and non-cyclotomic factors the $f_{\boldsymbol{a}}$'s are also sparse, in the sense that they are the restriction of a fixed Laurent polynomial as in (1.1) to a varying 1-parameter subgroup of $\mathbb{G}_{\mathrm{m}}^N$.

The following is the precise statement. We denote by μ_∞ the subgroup of $\overline{\mathbb{Q}}^\times$ of roots of unity.

Theorem 1.1. *Let $N \geq 1$ and $\boldsymbol{\gamma} = (\gamma_0, \gamma_1, \dots, \gamma_N) \in \overline{\mathbb{Q}}^{N+1}$. There exists a constant C depending only on N and $\boldsymbol{\gamma}$ such that the following holds.*

Let $\boldsymbol{a} = (a_1, \dots, a_N) \in \mathbb{Z}^N$ such that the Laurent polynomial

$$f_{\boldsymbol{a}} = \gamma_0 + \gamma_1 t^{a_1} + \cdots + \gamma_N t^{a_N} \in \overline{\mathbb{Q}}[t^{\pm 1}]$$

is nonzero and has a multiple root $\xi \in \overline{\mathbb{Q}}^\times \setminus \mu_\infty$. Set $D = max_j |a_j|$.

Then there exist $1 \leq k \leq N-1$ and $\boldsymbol{b}_1, \dots, \boldsymbol{b}_N, \boldsymbol{\theta} \in \mathbb{Z}^{N-k}$ such that

(1) $|\boldsymbol{b}_i| \leq C$, $i = 1, \dots, N$, and $|\boldsymbol{\theta}| \leq CD$;

(2) the matrix $\boldsymbol{B} = (b_{i,j})_{i,j} \in \mathbb{Z}^{N \times (N-k)}$ has rank $N-k$ and $\boldsymbol{a} = \boldsymbol{B} \cdot \boldsymbol{\theta}$;

(3) the Laurent polynomial $F = \gamma_0 + \gamma_1 \boldsymbol{y}^{\boldsymbol{b}_1} + \cdots + \gamma_N \boldsymbol{y}^{\boldsymbol{b}_N} \in \overline{\mathbb{Q}}[y_1^{\pm 1}, \dots, y_{N-k}^{\pm 1}]$ has a multiple factor P such that ξ is a root of $P(t^{\theta_1}, \dots, t^{\theta_N})$.

The situation is different for multiple cyclotomic roots. The following example shows that the hypothesis that the root ξ is not cyclotomic is necessary for the conclusion of this result to hold.

Example 1.2. Let $\boldsymbol{a} = (a_1, a_2, a_3) \in \mathbb{Z}^3$ coprime with $0 < a_1 < a_2$, $a_3 = a_1 + a_2$ and set $D = a_3 \gg 0$. We consider the polynomial

$$f_{\boldsymbol{a}} = 1 - t^{a_1} - t^{a_2} + t^{a_1 + a_2} \in \mathbb{Q}[t^{\pm 1}],$$

which has the point $\xi = 1$ as a double root.

We use the notation in Theorem 1.1. In the present situation, $N = 3$ and $k = 1, 2$. The case $k = 2$ is easily discarded since then, by (2), the polynomial F coincides with f and so its degree cannot be small, as searched.

Hence $k = 1$. Let $\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3, \boldsymbol{\theta} \in \mathbb{Z}^2$ with $\boldsymbol{b}_i$ bounded and such that

$$\langle \boldsymbol{b}_1, \boldsymbol{\theta} \rangle = a_1, \quad \langle \boldsymbol{b}_2, \boldsymbol{\theta} \rangle = a_2, \quad \langle \boldsymbol{b}_3, \boldsymbol{\theta} \rangle = a_1 + a_2. \tag{1.2}$$

Write $F = 1 - \boldsymbol{y}^{\boldsymbol{b}_1} - \boldsymbol{y}^{\boldsymbol{b}_2} + \boldsymbol{y}^{\boldsymbol{b}_3} \in \mathbb{Q}[y_1^{\pm 1}, y_2^{\pm 1}]$ with $\boldsymbol{b}_i$ bounded by a constant independent of D. By (1.2), we have that θ_1 and θ_2 are coprime and $\boldsymbol{b}_3 - \boldsymbol{b}_1 - \boldsymbol{b}_2 \in \mathbb{Z}(\theta_2, -\theta_1)$. Since $\boldsymbol{b}_i$'s are bounded, $\boldsymbol{b}_3 = \boldsymbol{b}_1 + \boldsymbol{b}_2$ and so

$$F = 1 - \boldsymbol{y}^{\boldsymbol{b}_1} - \boldsymbol{y}^{\boldsymbol{b}_2} + \boldsymbol{y}^{\boldsymbol{b}_1 + \boldsymbol{b}_2} = (1 - \boldsymbol{y}^{\boldsymbol{b}_1})(1 - \boldsymbol{y}^{\boldsymbol{b}_2}).$$

By (2), $\boldsymbol{b}_1$ and $\boldsymbol{b}_2$ are linearly independent, and so F has no multiple factor.

Hence, the presence of the double root $\xi = 1$ cannot be explained as coming from a multiple factor of a multivariate Laurent polynomial of low degree restricted to a 1-parameter subgroup.

Theorem 1.1 restricts the possible exponents $\boldsymbol{a}$ whose associate polynomial has a multiple non-cyclotomic root, to a finite union of proper linear subspaces.

Corollary 1.3. *Let $N \geq 1$ and $\boldsymbol{\gamma} = (\gamma_0, \gamma_1, \dots, \gamma_N) \in \overline{\mathbb{Q}}^{N+1}$ nonzero. Then the set of vectors $\boldsymbol{a} = (a_1, \dots, a_N) \in \mathbb{Z}^N$ such that the Laurent polynomial*

$$\gamma_0 + \gamma_1 t^{a_1} + \cdots + \gamma_N t^{a_N} \in \overline{\mathbb{Q}}[t^{\pm 1}]$$

has a multiple non-cyclotomic root, is contained in a finite union of proper linear subspaces of $\mathbb{Z}^N$.

To prove Theorem 1.1, we give a version of a theorem of Bombieri and Zannier on the intersection of a subvariety of codimension 2 of the multiplicative group with torsion curves, with an explicit dependence on the height of the subvariety (Theorem 2.3). This allows us to prove a general result concerning the greatest common divisor of two sparse polynomials with coefficients of low height (Theorem 2.6). These two theorems are presented in § 2 and proved in § 3 and § 4, respectively. Theorem 1.1 is an easy consequence of the latter result, as shown in § 5.

Theorem 2.6 is also used in § 6 to prove Theorem 6.1, which gives some evidence on a recent conjecture of Bolognesi and Pirola [BP11].

Acknowledgments. Part of this work was done while the authors met at the Scuola Normale Superiore (Pisa), the Universitat de Barcelona, and the Université de Caen. We thank these institutions for their hospitality.

2. Intersections of subvarieties with torsion curves and gcd of sparse polynomials of low height

We first recall some definitions and basic facts. Boldface letters denote finite sets or sequences of objects, whose 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 $\overline{\mathbb{Q}}[\boldsymbol{x}^{\pm 1}]$ denotes the ring of Laurent polynomials $\overline{\mathbb{Q}}[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$. Given a vector $\boldsymbol{a} = (a_1, \dots, a_N) \in \mathbb{Z}^N$ we set

$$|\boldsymbol{a}| = \max_j |a_j|.$$

Let $\varphi\colon \mathbb{G}_{\mathrm{m}}^n \to \mathbb{G}_{\mathrm{m}}^N$ be a group homomorphism. Then there exist unique vectors $\boldsymbol{b}_1, \dots, \boldsymbol{b}_N \in \mathbb{Z}^n$ such that $\varphi(\boldsymbol{x}) = (\boldsymbol{x}^{\boldsymbol{b}_1}, \dots, \boldsymbol{x}^{\boldsymbol{b}_N})$ for $\boldsymbol{x} \in \mathbb{G}_{\mathrm{m}}^n$. We set

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

for the *size* of φ. We also denote by

$$\varphi^{\#}\colon \overline{\mathbb{Q}}[y_1^{\pm 1}, \dots, y_N^{\pm 1}] \longrightarrow \overline{\mathbb{Q}}[x_1^{\pm 1}, \dots, x_n^{\pm 1}], \quad y_i \longmapsto \boldsymbol{x}^{\boldsymbol{b}_i}$$

the associated morphism of algebras. If $\psi\colon \mathbb{G}_{\mathrm{m}}^N \to \mathbb{G}_{\mathrm{m}}^M$ is a further homomorphism, then $(\psi \circ \varphi)^{\#} = \varphi^{\#} \circ \psi^{\#}$.

Let f_1, $f_2 \in \mathbb{Z}[t]$ be polynomials of degree $\leq D$ with fixed coefficients and fixed number of nonzero terms. Filaseta, Granville and Schinzel [FGS08] have shown that, if either f_1 or f_2 do not vanish at any root of unity, then the greatest common divisor $\gcd(f_1, f_2)$ can be computed in time polynomial in $\log(D)$. More recently, Amoroso, Leroux and Sombra gave an improved version of this result. The following is its precise statement.

Theorem 2.1 ([ALS13], Theorem 4.3)**.** *There is an algorithm that, given a number field $\mathbb{K}$ and polynomials f_1, $f_2 \in \mathbb{K}[t]$, computes a polynomial $p \in \mathbb{K}[t]$ dividing $\gcd(f_1, f_2)$ and such that $\gcd(f_1, f_2)/p$ is a product of cyclotomic polynomials.*

If both f_1 and f_2 have degree bounded by D, height bounded by h_0 and number of nonzero coefficients bounded by N, this computation is done with $O_{\mathbb{K},N,h_0}(\log(D))$ bit operations.

In more detail, write

$$f_i = \gamma_{i,0} + \gamma_{i,1}t^{a_1} + \cdots + \gamma_{i,N}t^{a_N} \in \mathbb{K}[t], \quad i = 1, 2,$$

with $a_j \in \mathbb{Z}$ and $\gamma_{i,j} \in \mathbb{K}$. Denote by $\varphi\colon \mathbb{G}_{\mathrm{m}} \to \mathbb{G}_{\mathrm{m}}^N$ the homomorphism defined by $\varphi(t) = (t^{a_1}, \dots, t^{a_N})$ and set

$$L_i = \gamma_{i,0} + \gamma_{i,1}x_1 + \cdots + \gamma_{i,N}x_N, \quad i = 1, 2,$$

so that $f_i = \varphi^{\#}(F_i)$.

Then, the algorithm underlying Theorem 2.1 computes an integer $1 \le k \le N-1$ and two homomorphisms $\psi\colon \mathbb{G}_{\mathrm{m}}^{N-k} \to \mathbb{G}_{\mathrm{m}}^N$ and $\varphi_1\colon \mathbb{G}_{\mathrm{m}} \to \mathbb{G}_{\mathrm{m}}^{N-k}$ with ψ injective, such that $\psi \circ \varphi_1 = \varphi$ and

$$p = \varphi_1^{\#}(\gcd(\psi^{\#}(L_1), \psi^{\#}(L_2))).$$

Moreover, the size of ψ and φ_1 is respectively bounded by B and BD, where B is a constant depending only on $\mathbb{K}$, N and h_0.

This algorithm relies heavily on a former conjecture of Schinzel on the intersection of a subvariety of the multiplicative group with 1-parameter subgroups. This conjecture was proved by Bombieri and Zannier in [Sch00, Appendix]. For the reader convenience, we recall an improved version of this result.

Theorem 2.2 ([BMZ07], Theorem 4.1)**.** *Let $N \ge 1$ and $P, Q \in \overline{\mathbb{Q}}[x_1, \dots, x_N]$ coprime polynomials. Then there exists a constant B depending only on P and Q with the following property.*

Let $\zeta_j \in \mu_\infty$ and $a_j \in \mathbb{Z}$, $j = 1, \dots, N$, and $\xi \in \mathbb{C}^\times$ with

$$P(\zeta_1\xi^{a_1}, ..., \zeta_N\xi^{a_N}) = Q(\zeta_1\xi^{a_1}, ..., \zeta_N\xi^{a_N}) = 0.$$

Then there exist $b_j \in \mathbb{Z}$, $j = 1, \dots, N$, with $0 < \max_j |b_j| \le B$ and

$$\prod_{j=1}^{N} (\zeta_j\xi^{a_j})^{b_j} = 1.$$

In particular, if $\xi \notin \mu_\infty$, then $\sum_{j=1}^N a_j b_j = 0$.

We are interested in extension of Theorem 2.1 to polynomials f_1, f_2 having low, but unbounded, height. To this end, we need first a version of Theorem 2.2 with explicit dependence on the height of the input polynomials P and Q.

As already remarked by Schinzel, the constant B in this theorem cannot depend only on N, on the field of definition and on the degrees of P and Q. For instance, for $N = 2$,

$$P(x, y) = x - 2, \quad Q(x, y) = y - 2^a \quad \text{and} \quad (\zeta_1\xi^{a_1}, \zeta_2\xi^{a_2}) = (2, 2^a)$$

one has $B(P, Q) \ge a$, see [BMZ07, page 7] for the details.

The following result gives, under some restrictive hypothesis, the dependence of the constant B in the height of the input polynomials. Recall that a *coset* of $\mathbb{G}_{\mathrm{m}}^N$ is a translate of a subtorus, and that a *torsion coset* is a translate of a subtorus by a torsion point. A *torsion curve* (respectively, a *torsion hypersurface*) is a torsion coset of dimension 1 (respectively, of codimension 1). Following [BZ95]), given a subvariety $\mathcal{X}$ of $\mathbb{G}_{\mathrm{m}}^N$, we denote by $\mathcal{X}^{\mathrm{o}}$ be the complement in $\mathcal{X}$ of the union of all cosets of positive dimension contained in $\mathcal{X}$.

We consider the standard inclusion

$$\iota\colon \mathbb{G}_{\mathrm{m}}^N \hookrightarrow \mathbb{P}^N \quad , \quad (x_1,\dots,x_N) \longmapsto (1 : x_1 : \cdots : x_N).$$

We define the *degree* of an irreducible subvariety $\mathcal{X} \subset \mathbb{G}_{\mathrm{m}}^N$, denoted by $\deg(\mathcal{X})$, as the degree of the Zariski closure $\iota(\mathcal{X}) \subset \mathbb{P}^N$ and, the *height* of a point $\xi \in \mathbb{G}_{\mathrm{m}}^N$, denoted by $\mathrm{h}(\xi)$, as the Weil height of the projective point $\iota(\xi) \in \mathbb{P}^N$.

Theorem 2.3. *Let $\mathcal{X} \subset \mathbb{G}_{\mathrm{m}}^N$ be a subvariety defined over a number field of degree δ by polynomials of degree bounded by d_0 and height bounded by h_0. Let $0 < \varepsilon < 1$. Then there exists a constant B depending only on N, d_0, δ and ε, with the following property.*

Let $\mathcal{W}$ be an irreducible component of $\mathcal{X}$ of codimension at least 2, T a torsion curve and $\boldsymbol{x} \in \mathcal{W}^{\mathrm{o}} \cap T$ a non-torsion point. Then either

$$\deg(T)^{\frac{1-\varepsilon}{N-1}} \leq B \cdot (1 + h_0)$$

or $\boldsymbol{x}$ is contained in a torsion hypersurface T' of degree bounded by B.

Remark 2.4. We can restate Theorem 2.3 in a slightly different way for the case when the torsion curve T is a subtorus. Let $\varphi\colon \mathbb{G}_{\mathrm{m}} \to \mathbb{G}_{\mathrm{m}}^N$ be a homomorphism and keep $\mathcal{X}$, $\mathcal{W}$ and ε as in the statement of the theorem. Let $\xi \in \overline{\mathbb{Q}}^\times \setminus \mu_\infty$ such that $\varphi(\xi) \in \mathcal{W}^{\mathrm{o}}$. Taking $T = \mathrm{im}(\varphi)$, Theorem 2.3 asserts that, if

$$\mathrm{size}(\varphi)^{\frac{1-\varepsilon}{N-1}} > B \cdot (1 + h_0),$$

then $\boldsymbol{x}$ is contained in a subtorus T' of codimension 1 and degree bounded by B.

Indeed, by Theorem 2.3, $\varphi(\xi) \in T'$ for a torsion hypersurface T' of degree bounded by B. This torsion hypersurface is defined by the single equation $\boldsymbol{x}^{\boldsymbol{b}} = \omega$ for some $\boldsymbol{b} \in \mathbb{Z}^N$ with $|\boldsymbol{b}| \leq B$ and $\omega \in \mu_\infty$. Write also $\varphi(t) = (t^{a_1},\dots,t^{a_N})$ with $a_i \in \mathbb{Z}$. Then

$$\xi^{a_1 b_1 + \cdots + a_N b_N} = \omega.$$

Since ξ is not torsion, $\sum_j a_j b_j = 0$ and $\omega = 1$. Equivalently, T' is a subtorus and $\mathrm{im}(\varphi) \subseteq T'$.

The following variant of Schinzel's example shows that the hypothesis that $\boldsymbol{x} \in \mathcal{X}^{\mathrm{o}}$ is necessary for the conclusion of Theorem 2.3 to hold.

Example 2.5. Let $1 < a < b$ and consider the irreducible subvariety given by

$$\mathcal{X} = \{(2, 2^a)\} \times \mathbb{G}_{\mathrm{m}} \subset \mathbb{G}_{\mathrm{m}}^3.$$

With notation as in the theorem, $N = 3$, $h_0 \approx a$ and $d_0 = 1$. Since $\mathcal{X}$ is a coset of positive dimension, $\mathcal{X}^{\mathrm{o}} = \emptyset$. Let $T \subset \mathbb{G}_{\mathrm{m}}^3$ be the subtorus parameterized by $t \mapsto (t, t^a, t^b)$ and pick the point $\boldsymbol{x} = (2, 2^a, 2^b) \in \mathcal{X} \cap T$. It is easy to verify that, for any fixed $0 < \varepsilon < 1$ and $B > 0$, if a and b/a are sufficiently large, neither $\deg(T)^{\frac{1-\varepsilon}{2}} \leq B \cdot (1 + h_0)$ nor $\boldsymbol{x} \in T'$ for any torsion hypersurface of degree bounded by B.

Theorem 2.3 allows us to prove the desired extension of Theorem 2.1 to polynomials of low height. The following statement gives the quantitative aspects of this result.

Theorem 2.6. *Let $\mathbb{K}$ be a number field of degree δ. For a family of elements $\gamma_{i,j} \in \mathbb{K}$, $i = 1,\dots,s$, $j = 1,\dots,N$, and a sequence of N coprime integers $a_1,\dots,a_N$, we consider the system of Laurent polynomials*

$$f_i = \gamma_{i,0} + \gamma_{i,1} t^{a_1} + \cdots + \gamma_{i,N} t^{a_N}, \qquad i = 1,\dots,s.$$

We assume $f_1, \dots, f_s$ not all zeros. Set

$$L_i = \gamma_{i,0} + \gamma_{i,1}x_1 + \cdots + \gamma_{i,N}x_N, \qquad i = 1, \dots, s,$$

and let $\varphi\colon \mathbb{G}_{\mathrm{m}} \to \mathbb{G}_{\mathrm{m}}^N$ be the homomorphism given by $\varphi(t) = (t^{a_1}, \dots, t^{a_N})$. Put $D = |\boldsymbol{a}|$ and $h_0 = \max_{i,j} h(\gamma_{i,j})$.

Then there exists a constant B' depending only on N and δ, with the following property. If

$$D^{\frac{1}{2(N-1)}} > B' \cdot (1 + h_0), \tag{2.1}$$

there exists $1 \le k \le N-1$ and homomorphisms $\psi\colon \mathbb{G}_{\mathrm{m}}^{N-k} \to \mathbb{G}_{\mathrm{m}}^N$ and $\varphi_1\colon \mathbb{G}_{\mathrm{m}} \to \mathbb{G}_{\mathrm{m}}^{N-k}$ such that

(1) ψ is injective and $\psi \circ \varphi_1 = \varphi$;

(2) $\operatorname{size}(\psi) \le B'$ and $\operatorname{size}(\varphi_1) \le B'D$;

(3) Set

$$G = \gcd(\psi^{\#}(L_1), \dots \psi^{\#}(L_s)) \quad \text{and} \quad g = \varphi_1^{\#}(G).$$

Then $g \mid \gcd(f_1, \dots, f_s)$. Moreover, if ξ is a root of $\gcd(f_1, \dots, f_s)/g$, then either $\xi \in \mu_\infty$ or there exists a nonempty proper subset $\Lambda \subset \{1, \dots, N\}$ such that $\gamma_{i,0} + \sum_{j\in\Lambda} \gamma_{i,j}\xi^{a_j} = 0$, $i = 1, \dots, s$.

Similarly as for Theorem 2.1, the datum k, ψ and φ_1 can be effectively computed. In the present situation, this is done by the procedure described in § 4, and this computation costs $O_{\delta,N,s}(\log(D))$ bit operations.

A first application of this result concerns the computation of multiple roots of sparse Laurent polynomials and, indeed, Theorem 1.1 will follow from it. As a second application, we will deduce a result in the direction of a conjecture of Bolognesi and Pirola.

3. Proof of Theorem 2.3

All irreducible components of $\mathcal{X}$ are defined over a number field of degree bounded by C by polynomials of degree bounded by C and height bounded by Ch_0, for a constant C depending only on N, d_0 and δ. Using this, we reduce without loss of generality to the case when $\mathcal{X}$ is an irreducible subvariety of codimension at least 2.

We follow closely the proof of [BMZ07, Theorem 4.1]. Since we assume that $\boldsymbol{x} \in \mathcal{X}^{\mathrm{o}} \cap T$, the first reduction of the proof in *loc. cit.* is unnecessary in our present situation. Write

$$T = \{(\zeta_1 t^{a_1}, \dots, \zeta_N t^{a_N}) \mid t \in \mathbb{G}_{\mathrm{m}}\} \subseteq \mathbb{G}_{\mathrm{m}}^N$$

with $a_1, \dots, a_N \in \mathbb{Z}$ coprime and $\zeta_1, \dots, \zeta_N \in \mu_\infty$. Thus $\deg(T) = |\boldsymbol{a}|$. As in *loc. cit.* we construct, using geometry of numbers, a 2-dimensional torsion coset T_2 containing T and such that

$$\deg(T_2) \le B_1 |\boldsymbol{a}|^{\frac{N-2}{N-1}} \tag{3.1}$$

for a constant B_1 depending only on N. The proof goes on by distinguishing two cases.

Suppose first that the point $\boldsymbol{x}$ is an isolated component of $\mathcal{X} \cap T_2$. Since $\boldsymbol{x} \in \mathcal{X} \cap T$, we can write $\boldsymbol{x} = (\zeta_1 \xi^{a_1}, \dots, \zeta_N \xi^{a_N})$ with $\overline{\mathbb{Q}}^\times \setminus \mu_\infty$. Let $\mathbb{K}$ be a field of definition of $\mathcal{X}$ and set $\mathbb{E} = \mathbb{K}(\zeta_1, \dots, \zeta_N)$, which is a field of definition for both $\mathcal{X}$ and T. Put $\mathcal{D} = [\mathbb{E}(\boldsymbol{x}) : \mathbb{E}]$. Using Bézout theorem and (3.1), we deduce that this degree satisfies the bound

$$\mathcal{D} \le \deg(\mathcal{X} \cap T_2) \le B_1 |\boldsymbol{a}|^{\frac{N-2}{N-1}} \deg(\mathcal{X}). \tag{3.2}$$

Moreover, since $a_1, \dots, a_N$ are coprime, $[\mathbb{E}(\xi) : \mathbb{E}] = \mathcal{D}$.

Let $0 < \varepsilon < 1$. We have that $\mathbb{E}(\xi)$ is an extension of degree $\leq [\mathbb{K} : \mathbb{Q}]\mathcal{D}$ of the cyclotomic extension $\mathbb{Q}(\zeta_1, \dots, \zeta_N)$. By the relative Dobrowolski lower bound of [AZ00], the height of ξ is bounded from below by

$$\mathrm{h}(\xi) \geq B_2 \mathcal{D}^{-1-\varepsilon}, \tag{3.3}$$

where B_2 is a constant that depends only on ε and $[\mathbb{K} : \mathbb{Q}]$.

By [Sch00, Appendix, Theorem 1], since the point $\boldsymbol{x}$ lies in $\mathcal{X}^{\mathrm{o}} \cap T$, its height is bounded above by a constant depending only on $\mathcal{X}$. Indeed, a close inspection of the proof of this result shows that

$$\mathrm{h}(\boldsymbol{x}) \leq B_3 \cdot (1 + h_0). \tag{3.4}$$

for a constant B that depends only on δ and N. Alternatively, this can be obtained by applying Habegger's effective version of the bounded height theorem [Hab12, Theorem 11] with the choice of parameters $r = 2$ and $s = n - 1$ with respect to the notation therein, together with the arithmetic Bézout theorem in [KPS01, Corollary 2.11]. Thus

$$|\boldsymbol{a}| \, \mathrm{h}(\xi) \leq \sum_{i=1}^{N} \mathrm{h}(\zeta_i \xi^{a_i}) \leq N \mathrm{h}(\boldsymbol{x}). \tag{3.5}$$

Combining (3.2), (3.3), (3.4) and (3.5), we get

$$\deg(T) = |\boldsymbol{a}| \leq B_2^{-1} \Big(B_1 |\boldsymbol{a}|^{\frac{N-2}{N-1}} \deg(\mathcal{X}) \Big)^{1+\varepsilon} N B_3 \cdot (1 + h_0).$$

From here, we deduce that

$$\deg(T)^{\frac{1-\varepsilon'}{N-1}} \leq B \cdot (1 + h_0).$$

with $\varepsilon' = (N-2)\varepsilon$ and where B is any constant $\geq B_4 = B_2^{-1}(B_1 \deg(\mathcal{X}))^{1+\varepsilon} N B_3$, which shows the result in this case.

Now suppose that $\boldsymbol{x}$ lies in an irreducible component of positive dimension of $\mathcal{X} \cap T_2$. Denote by $\mathcal{Y}$ this irreducible component, which is thus a $\mathcal{X}$-anomalous subvariety. Let $\mathcal{Y}_{\max}$ be a a maximal $\mathcal{X}$-anomalous subvariety containing $\mathcal{Y}$. From the Bombieri-Masser-Zannier uniform structure theorem [BMZ07, Theorem 1.4], this subvariety $\mathcal{Y}_{\max}$ is contained in a coset $\boldsymbol{g}H$ whose degree is bounded in terms of $\mathcal{X}$. Indeed, by [BMZ07, (3.4)], this degree is bounded by a constant B_5 depending only on δ and $\deg(\mathcal{X})$.

The intersection $T_2 \cap \boldsymbol{g}H$ is a union of cosets associated to the same subtorus. Denote by K the unique coset in this intersection that contains $\mathcal{Y}$. Its dimension is either 1 or 2. The case $\dim(K) = 1$ is not possible since, otherwise, $\mathcal{Y} = K$ is a coset, which is forbidden by the hypothesis that $\boldsymbol{x} \in \mathcal{X}^{\mathrm{o}}$. Hence $\dim(K) = 2$, which means that some irreducible component of T_2 lies in $\boldsymbol{g}H$. Take a torsion point $\boldsymbol{g}_0$ lying in this irreducible component. Then $\boldsymbol{g}_0 \in \boldsymbol{g}H$ and $\boldsymbol{g}H = \boldsymbol{g}_0 H$ is a torsion coset of degree bounded by B_5. We can find a further constant B_6 depending only on δ and $\deg(\mathcal{X})$ such that there exists a torsion hypersurface T' with $\boldsymbol{g}_0 H \subseteq T'$ and $\deg(T') \leq B_6$. We then choose $B = \max(B_4, B_6)$, concluding the proof.

4. Proof of Theorem 2.6

We follow the proof of [ALS13, Theorem 4.3], replacing the use of Theorem 2.2 by Theorem 2.3. We first need to prove some auxiliary lemmas.

Lemma 4.1. *Let $\varphi\colon \mathbb{G}_{\mathrm{m}} \to \mathbb{G}_{\mathrm{m}}^N$ be a homomorphism of size D and $T \subseteq \mathbb{G}_{\mathrm{m}}^N$ a subtorus of codimension 1. We can test if $\mathrm{im}(\varphi) \subseteq T$ and, if this is the case, we can compute two homomorphisms $\widetilde{\psi}\colon \mathbb{G}_{\mathrm{m}}^{N-1} \to \mathbb{G}_{\mathrm{m}}^N$ and $\widetilde{\varphi}\colon \mathbb{G}_{\mathrm{m}} \to \mathbb{G}_{\mathrm{m}}^{N-1}$ such that*

(1) $\widetilde{\psi}$ is injective and $\widetilde{\psi} \circ \widetilde{\varphi} = \varphi$;

(2) $\mathrm{size}(\widetilde{\psi}) = O(1)$ and $\mathrm{size}(\widetilde{\varphi}) = O(D)$.

This computation can be done with $O(\log(D))$ bit operations. All the implicit constants depend only on N and $\deg(T)$.

Proof. Let $\boldsymbol{x}^{\boldsymbol{b}} = 1$ be an equation for T and write $\varphi(\boldsymbol{x}) = (\boldsymbol{x}^{a_1}, \dots, \boldsymbol{x}^{a_N})$ with $a_1, \dots, a_N \in \mathbb{Z}$ coprime. Then $\mathrm{im}(\varphi) \subseteq T$ if and only if $\sum_j a_j b_j = 0$. Let us assume that this is the case. We choose an automorphism τ of $\mathbb{G}_{\mathrm{m}}^N$ such that $\tau(T)$ is defined by the equation $x_N = 1$. 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 of equation $x_N = 1$, and consider the projection onto the first $N-1$ coordinates

$$\pi\colon \mathbb{G}_{\mathrm{m}}^N \to \mathbb{G}_{\mathrm{m}}^{N-1} \quad , \quad \pi(x_1, \dots, x_N) = (x_1, \dots, x_{N-1}, 1).$$

We then set $\widetilde{\psi} = \tau^{-1} \circ \iota$ and $\widetilde{\varphi} = \pi \circ \tau \circ \varphi$.

We leave to the reader the verification on the correctness and the complexity of this algorithm, see [ALS13, Lemma 4.1] for further details. □

We now describe the algorithm underlying Theorem 2.6.

Algorithm 4.1

Input: a subvariety $\mathcal{X} \subset \mathbb{G}_{\mathrm{m}}^N$ defined over a number field $\mathbb{K}$ and a homomorphism $\varphi\colon \mathbb{G}_{\mathrm{m}} \to \mathbb{G}_{\mathrm{m}}^N$.

Output: an integer k with $0 \le k \le N-1$ and two homomorphisms $\psi\colon \mathbb{G}_{\mathrm{m}}^{N-k} \to \mathbb{G}_{\mathrm{m}}^N$ and $\varphi_1\colon \mathbb{G}_{\mathrm{m}} \to \mathbb{G}_{\mathrm{m}}^{N-k}$.

```
Set k ← 0, ψ ← Id_{G_m^N} and φ_1 ← φ;
while k < N do
    let B the constant in Theorem 2.3 for the subvariety ψ^{-1}(X) ⊂ G_m^{N-k}
    and the choice ε = 1/2;
    set Φ ← {{x^b = 1} | b ∈ Z^N primitive such that |b| ≤ B};
    while Φ ≠ ∅ do
        choose T' ∈ Φ;
        if im(φ_1) ⊆ T' then
            compute as in Lemma 4.1 homomorphisms ψ̃: G_m^{N-k-1} → G_m^{N-k}
            and φ̃: G_m → G_m^{N-k-1} such that φ_1 = ψ̃ ∘ φ̃;
            set ψ ← ψ ∘ ψ̃, φ_1 ← φ̃, k ← k + 1, Φ ← ∅;
        else
            set Φ ← Φ \ {T'};
        end if
    end while
end while
```

Lemma 4.2. *Let $\mathcal{X} \subset \mathbb{G}_{\mathrm{m}}^N$ be a subvariety defined over a number field of degree δ by polynomials of degree bounded by d_0. Let also $\varphi\colon \mathbb{G}_{\mathrm{m}} \to \mathbb{G}_{\mathrm{m}}^N$ be a homomorphism of size D. Algorithm 4.1 computes an integer k with $0 \le k < N-1$ and two homomorphisms $\psi\colon \mathbb{G}_{\mathrm{m}}^{N-k} \to \mathbb{G}_{\mathrm{m}}^N$ and $\varphi_1\colon \mathbb{G}_{\mathrm{m}} \to \mathbb{G}_{\mathrm{m}}^{N-k}$ such that*

(1) ψ *is injective and* $\psi \circ \varphi_1 = \varphi$*;*

(2) $\operatorname{size}(\psi) = O(1)$ *and* $\operatorname{size}(\varphi_1) = O(D)$*.*

This computation is done with $O(\log D)$ *bit operations. All the implicit constants in the* O*-notation depend only on* N*,* d_0 *and* δ*.*

Proof. We show by induction on k that the homomorphisms ψ and φ_1 constructed by the algorithm at the level k satisfy both (1) and (2).

This is certainly true at the level $k = 0$. Indeed at this level $\psi = \mathrm{Id}_{\mathbb{G}_{\mathrm{m}}^N}$ and $\varphi_1 = \varphi$.

Let k be an integer with $1 \le k < N$ and assume that at the level $k-1$ the homomorphisms ψ and φ_1 satisfy (1) and (2). By Lemma 4.1, the homomorphisms $\widetilde{\psi}$ and $\widetilde{\varphi}$ at line 8 satisfy $\widetilde{\psi} \circ \widetilde{\varphi} = \varphi_1$. Hence the updated values of ψ and φ_1, that is $\psi \circ \widetilde{\psi}$ and $\widetilde{\varphi}$, satisfy

$$(\psi \circ \widetilde{\psi}) \circ \widetilde{\varphi} = \psi \circ \varphi_1 = \varphi.$$

Moreover, since ψ and $\widetilde{\psi}$ are injective, by induction and by Lemma 4.1(1), $\psi \circ \widetilde{\psi}$ is also injective.

Let B be as in line 3 of the algorithm 4.1, that is, the constant in Theorem 2.3 for the subvariety $\psi^{-1}(\mathcal{X})$ and the choice $\varepsilon = \frac{1}{2}$. Since $\operatorname{size}(\psi) = O(1)$ and $\mathcal{X}$ is linear, $\psi^{-1}(\mathcal{X})$ is defined over a number field of degree $O(1)$ by polynomials of degree $O(1)$ and height $O(h_0)$, with implicit constants depending only on N and δ. In particular, $B = O(1)$. The same is therefore true for the degree of the subtorus T' at line 6. By Lemma 4.1(2), the homomorphisms $\widetilde{\psi}$ and $\widetilde{\varphi}$ at line 8 have size $O(1)$ and $O(D)$ respectively. Thus $\psi \circ \widetilde{\psi}$ and $\widetilde{\varphi}$ have also size $O(1)$ and $O(D)$, respectively.

We left to the reader the verification on the complexity of the algorithm. □

We are now able to conclude the proof of Theorem 2.6. Let $\mathbb{K}$ and $f_1, \dots, f_s$ be as in that theorem. Thus $\mathbb{K}$ is a number field of degree δ and

$$f_i = \gamma_{i,0} + \gamma_{i,1} t^{a_1} + \cdots + \gamma_{i,N} t^{a_N}, \qquad i = 1, \dots, s,$$

are Laurent polynomials, not all zeros, with $a_1, \dots, a_N$ coprime. Set $D = |\boldsymbol{a}|$ and assume $\max_{i,j} h(\gamma_{i,j}) \le h_0$. We consider the homomorphism $\varphi\colon \mathbb{G}_{\mathrm{m}} \to \mathbb{G}_{\mathrm{m}}^N$ given by $\varphi(t) = (t^{a_1}, \dots, t^{a_N})$. Since $a_1, \dots, a_N$ are coprime, $\deg(\mathrm{im}(\varphi)) = D$. We let

$$L_i = \gamma_{i,0} + \gamma_{i,1} x_1 + \cdots + \gamma_{i,N} x_n, \qquad i = 1, \dots, s.$$

Thus $f_i = \varphi^{\#}(L_i)$. We apply Algorithm 4.1 to the linear subvariety $\mathcal{X}$ defined in $\mathbb{G}_{\mathrm{m}}^N$ by the system of equations $L_1 = \ldots = L_s = 0$.

From now on, we denote by $k \in \{0, \dots, N-1\}$, $\psi\colon \mathbb{G}_{\mathrm{m}}^{N-k} \to \mathbb{G}_{\mathrm{m}}^N$ and $\varphi_1\colon \mathbb{G}_{\mathrm{m}} \to \mathbb{G}_{\mathrm{m}}^{N-k}$ the output of Algorithm 4.1 applied to this subvariety. Put for short $F_i = \psi^{\#}(L_i)$. By Lemma 4.2, $\varphi_1^{\#}(F_i) = f_i$. Since $f_1, \dots, f_s$ are not all zeros, the same holds for $F_1, \dots, F_s$. Now set

$$G = \gcd(F_1, \dots, F_s) \quad \text{ and } \quad g = \varphi_1^{\#}(G).$$

Then $g | \gcd(f_1, \dots, f_s)$, as in Theorem 2.6(3).

Let B' be a constant depending only on N and δ such that

$$D^{\frac{1}{2(N-1)}} > B' \cdot (1 + h_0), \tag{4.1}$$

as in the statement of Theorem 2.6, to be fixed later on.

Let Ω be the set of points $\xi \in \mathbb{C}^\times$ which are either a root of unity or a common root of the system of polynomials $\gamma_{i,0} + \sum_{j \in \Lambda} \gamma_{i,j} t^{a_j}$, $i = 1, \dots, s$, for a nonempty proper subset $\Lambda \subset \{1, \dots, N\}$.

Let $\xi \notin \Omega$ be a common zero of $f_1, \dots, f_s$ and $\mathcal{W}$ a component of $\psi^{-1}(\mathcal{X})$ such that $\varphi_1(\xi) \in \mathcal{W}$.

We first remark that $\varphi_1(\xi) \in \mathcal{W}^{\mathrm{o}}$. If it is not, the point $\boldsymbol{y} = \varphi_1(\xi)$ is in a coset $gH \subseteq \mathcal{W} \subseteq \psi^{-1}(\mathcal{X})$ of positive dimension. By Lemma 4.2(2), the point $\boldsymbol{x} = \varphi(\xi) = \psi(\boldsymbol{y})$ is contained in the coset $\psi(gH) \subseteq \mathcal{X}$, which is also of positive dimension since ψ is injective.

The cosets included in a linear variety $\mathcal{X}$ have been explicitly classified in [Sch96, page 161]. By this result, there exists a nonempty proper subset $\Lambda \subset \{1, \dots, N\}$ such that $\gamma_{i,0} + \sum_{j\in\Lambda} \gamma_{i,j} x_j = 0$, $i = 1, \dots, s$. Hence ξ is a common root of $\gamma_{i,0} + \sum_{j\in\Lambda} \gamma_{i,j} t^{a_j}$, $i = 1, \dots, s$, but this is not possible because $\xi \notin \Omega$.

Thus ξ is not a root of unity and $\varphi_1(\xi) \in \mathcal{W}^{\mathrm{o}}$. We apply Theorem 2.3 in the simplified form of Remark 2.4, choosing $N \leftarrow N - k$, $\mathcal{X} \leftarrow \psi^{-1}(\mathcal{X})$, $\varepsilon \leftarrow 1/2$ and $\varphi \leftarrow \varphi_1$. Let B be as in line 3 of the algorithm 4.1. As already remarked in the proof of Lemma 4.2, $\psi^{-1}(\mathcal{X})$ is defined over a number field of degree $O(1)$ by polynomials of degree $O(1)$ and height $O(h_0)$, with implicit constants depending only on N and δ. In particular, $B = O(1)$. By the quoted Remark 2.4, one of the following assertions holds:

(1) there exists a subtorus T' of codimension 1 and degree bounded by B such that $\mathrm{im}(\varphi_1) \subseteq T'$;

(2) $\deg(\mathrm{im}(\varphi_1))^{\frac{1}{2(N-k-1)}} = O(1 + h_0)$;

(3) $\mathcal{W}$ has codimension 1.

By construction, (1) is not possible because $T' \in \Phi$. Let us assume that (2) holds. By Lemma 4.2, $D = \deg(\mathrm{im}(\varphi)) = \deg(\mathrm{im}(\psi \circ \varphi_1)) = O(\deg(\mathrm{im}(\varphi_1)))$. Thus

$$D^{\frac{1}{2(N-1)}} \leq D^{\frac{1}{2(N-k-1)}} = O(\deg(\mathrm{im}(\varphi_1))^{\frac{1}{2(N-k-1)}}) = O(1 + h_0).$$

Choosing the constant B' sufficiently large, this contradicts the inequality (4.1). Thus (3) must hold and $\mathcal{W}$ has codimension 1.

This discussion implies that the ideal $(F_1, \dots, F_s) \subset \mathbb{K}[y_1^{\pm 1}, \dots, y_{N-k}^{\pm 1}]$ becomes principal when restricted to a suitable neighborhood $U \subset \mathbb{G}_{\mathrm{m}}^{N-k}$ of $\psi^{-1}(\mathcal{X}) \setminus \varphi_1(\Omega)$. Hence, $(F_1, \dots, F_s) = (G)$ for some Laurent polynomial G on that neighborhood. We deduce that $\varphi_1^{-1}(U)$ is a neighborhood of the set of common zeros $\xi \notin \Omega$ of $f_1, \dots, f_s$ and $(f_1, \dots, f_s) = (g)$ on $\varphi_1^{-1}(U)$. This completes the proof of the theorem.

Remark 4.3. For the study of multiple roots of sparse polynomials and, in particular, to prove Theorem 2.6, it is not enough to dispose of a version of Theorem 2.2 with an explicit dependence of its constant B on the height of the input polynomials. We really need the dichotomy that appears in Theorem 2.3, with a bound for the degree of T' independent of the height of the equations defining $\mathcal{X}$, whenever the degree of the torsion curve T is large enough.

In any case, it is possible to adapt the proof of [BMZ07, Theorem 4.1] to prove such effective version of Theorem 2.2.

5. Proof of Theorem 1.1

Let $N \geq 1$ and $\boldsymbol{\gamma} = (\gamma_0, \gamma_1, \dots, \gamma_N) \in \overline{\mathbb{Q}}^{N+1}$. Consider the number field $\mathbb{K} = \mathbb{Q}(\boldsymbol{\gamma})$ and the affine polynomial

$$L = \gamma_0 + \gamma_1 x_1 + \cdots + \gamma_N x_N \in \mathbb{K}[x_1, \dots, x_N].$$

Set $\delta = [\mathbb{K} : \mathbb{Q}]$ and $h_0 = \max_j \mathrm{h}(\gamma_j)$.

Let $\boldsymbol{a} = (a_1, \dots, a_N) \in \mathbb{Z}^N$ such that the univariate Laurent polynomial

$$f = L(t^{a_1}, \dots, t^{a_N}) = \gamma_0 + \gamma_1 t^{a_1} + \cdots + \gamma_N t^{a_N}$$

is nonzero and has a multiple root at a point $\xi \in \overline{\mathbb{Q}} \setminus \mu_\infty$. Set $a_0 = 0$ and assume for the moment that

$$\text{(5.1)} \qquad \xi \text{ is } \textit{not} \text{ a multiple root of } \sum_{j\in\Lambda} \gamma_j t^{a_j} \text{ for every nonempty } \Lambda \subsetneq \{0, \dots, N\}.$$

We remark that $(a_1, \dots, a_N) \neq (0, \dots, 0)$, since otherwise f is a nonzero constant and cannot vanish at ξ. Set $d = \gcd(a_1, \dots, a_N)$ and put $a'_j = a_j/d$, $j = 1, \dots, N$. We apply Theorem 2.6 to the polynomials

$$f_1 = \gamma_0 + \gamma_1 t^{a'_1} + \cdots + \gamma_N t^{a'_N} \quad \text{and} \quad f_2 = t f'_1 = \gamma_1 a'_1 t^{a'_1} + \cdots + \gamma_N a'_N t^{a'_N},$$

and the homomorphism $\varphi\colon \mathbb{G}_{\mathrm{m}} \to \mathbb{G}_{\mathrm{m}}^N$ defined by $\varphi(t) = (t^{a'_1}, \dots, t^{a'_N})$.

Thus $f = f_1(t^d)$ and, in the notation of Theorem 2.6, $D = |\boldsymbol{a}'|$,

$$L_1 = \gamma_0 + \gamma_1 x_1 + \cdots + \gamma_N x_N \quad \text{and} \quad L_2 = \gamma_1 a'_1 x_1 + \cdots + \gamma_N a'_N x_N.$$

We have

$$\mathrm{h}(f_i) \leq h_0 + \log(D).$$

Let $B' = B'(N, \delta)$ be the constant which appears in Theorem 2.6. If the inequality (2.1) is not satisfied, we have

$$D^{\frac{1}{2(N-1)}} \leq B' \cdot (1 + h_0 + \log(D)),$$

which shows that $D \leq C_1$ for some positive constant $C_1 = C_1(N, \delta, h_0)$. In this case, we choose $k = N - 1$, $\boldsymbol{b}_j = a'_j$, $j = 1, \dots, N$, $\theta_1 = d$ and $C \geq C_1$. Assertions (1), (2) and (3) of Theorem 1.1 are then clearly verified.

We now assume that the inequality (2.1) is satisfied. Theorem 2.6 then gives a positive integer $1 \leq k \leq N$ and two morphisms $\psi\colon \mathbb{G}_{\mathrm{m}}^{N-k} \to \mathbb{G}_{\mathrm{m}}^N$ and $\varphi_1\colon \mathbb{G}_{\mathrm{m}} \to \mathbb{G}_{\mathrm{m}}^{N-k}$ satisfying the conditions (1), (2) and (3) of that theorem. Write $\psi(\boldsymbol{y}) = (\boldsymbol{y}^{\boldsymbol{b}_1}, \dots, \boldsymbol{y}^{\boldsymbol{b}_N})$ and $\varphi_1(t) = (t^{\theta'_1}, \dots, t^{\theta'_{N-k}})$ with $\boldsymbol{b}_1, \dots, \boldsymbol{b}_N \in \mathbb{Z}^{N-k}$ of size $\leq B'$ and $\theta'_1, \dots, \theta'_{N-k} \in \mathbb{Z}$ of size $\leq B'D$. By (1), the $N \times (N-k)$ matrix $\boldsymbol{B} = (b_{j,i})$ has maximal rank $N - k$ and $\boldsymbol{a}' = \boldsymbol{B} \cdot \boldsymbol{\theta}'$. We set

$$F_1 = \psi^{\#}(L_1) = \gamma_0 + \gamma_1 \boldsymbol{y}^{\boldsymbol{b}_1} + \cdots + \gamma_N \boldsymbol{y}^{\boldsymbol{b}_N}, \quad F_2 = \psi^{\#}(L_2) = \gamma_1 a'_1 \boldsymbol{y}^{\boldsymbol{b}_1} + \cdots + \gamma_N a'_N \boldsymbol{y}^{\boldsymbol{b}_N},$$

and we consider the differential operator

$$\Delta = \theta'_1 y_1 \frac{\partial}{\partial y_1} + \cdots + \theta'_{N-k} y_{N-k} \frac{\partial}{\partial y_{N-k}}.$$

Let $\boldsymbol{b} \in \mathbb{Z}^{N-k}$. The monomial $\boldsymbol{y}^{\boldsymbol{b}}$ is an eigenvector of Δ with eigenvalue the scalar product $\langle \boldsymbol{b}, \boldsymbol{\theta}' \rangle$. Hence

$$\Delta F_1 = \sum_{i=1}^{N} \gamma_i \langle \boldsymbol{b}_i, \boldsymbol{\theta}' \rangle \boldsymbol{y}^{\boldsymbol{b}_i} = F_2.$$

Set $G = \gcd(F_1, F_2)$. By hypothesis, ξ^d is a common non-cyclotomic root of f_1 and f_2 and, by the additional assumption (5.1), ξ^d is not a multiple root of $\sum_{j\in\Lambda} \gamma_j t^{a'_j}$ for any nonempty proper subset Λ of $\{0, \dots, N\}$. By Theorem 2.6(3), there exists an irreducible factor P of G such that $\pi = \varphi_1^{\#}(P) \in \mathbb{K}[t]$ vanishes at ξ^d.

We want to show that P is a multiple factor of G. Since $P \mid F_1$ and $P \mid F_2 \Delta F_1$, by standard arguments either $P^2 \mid F_1$ as we want, or $\Delta P = \lambda P$ for a constant λ. Let us assume that this last assertion holds. Write

$$P = \sum_{\boldsymbol{b} \in \mathbb{Z}^{N-k}} c_{\boldsymbol{b}} \boldsymbol{y}^{\boldsymbol{b}}$$

and set $\operatorname{supp}(P) = \{\boldsymbol{b} \in \mathbb{Z}^{N-k} \mid c_{\boldsymbol{b}} \neq 0\}$ for the support of P. The differential equation $\Delta P = \lambda P$ then says that the scalar product $\langle \boldsymbol{b}, \boldsymbol{\theta}' \rangle$ is constant over $\operatorname{supp}(P)$, which in turns implies that π is a monomial. But then π cannot vanish at ξ^d because the latter is nonzero, which is a contradiction.

Thus P is a multiple factor of F_1. Set $\theta_i = d\theta_i'$, so that $P(t^{\theta_1}, \dots, t^{\theta_N})$ is a multiple factor of f which vanishes at the point ξ, as required. Theorem 1.1 thus follows, under the additional hypothesis (5.1), by choosing $C = \max\{C_1, B'\}$.

We now explain how to remove the extra assumption (5.1). Let as assume that (5.1) does not hold. We decompose $\{0, \dots, N\}$ as a maximal union of $u \geq 2$ nonempty disjoint subsets $\Lambda_1, \dots, \Lambda_u$ in such a way that ξ is a multiple root of $\sum_{j \in \Lambda_i} \gamma_j t^{a_j}$ for $i = 1, \dots, u$. To simplify the notation, we assume $u = 2$ and $\Lambda_1 = \{0, \dots, M\}$ with $0 \leq M \leq N - 1$. Thus ξ is a multiple root of both

$$\gamma_0 + \sum_{j=1}^{M} \gamma_j t^{a_j} \quad \text{and} \quad \sum_{j=M+1}^{N} \gamma_j t^{a_j}. \tag{5.2}$$

Moreover, ξ is *not* a multiple root of $\sum_{j \in \Delta} \gamma_j t^{a_j}$ for any nonempty Δ which is a proper subset of $\{0, \dots, M\}$ or of $\{M+1, \dots, N\}$.

We write

$$\begin{aligned} \gamma_0 + \gamma_1 t^{a_1} + \cdots + \gamma_N t^{a_N} = {} & (\gamma_0 + \gamma_1 t^{a_1} + \cdots + \gamma_M t^{a_M}) \\ & + t^{a_{M+1}} (\gamma_{M+1} + \gamma_{M+2} t^{a_{M+2} - a_{M+1}} + \cdots + \gamma_N t^{a_N - a_{M+1}}). \end{aligned}$$

We remark that $a_1, \dots, a_M$, $a_{M+2} - a_{M+1}, \dots, a_N - a_{M+1}$ are not all zeros, since otherwise the polynomials (5.2) are monomials vanishing at ξ, and hence they are both zero, which in turns implies that f is also zero, contrary to the assumption of Theorem 1.1.

Set $d = \gcd(a_1, \dots, a_M, a_{M+2} - a_{M+1}, \dots, a_N - a_{M+1})$ and put

$$a_j' = \begin{cases} a_j/d, & \text{for } j = 1, \dots, M, \\ (a_j - a_{M+1})/d, & \text{for } j = M+3, \dots, N. \end{cases}$$

Thus $a_1', \dots, a_M', a_{M+2}', \dots, a_N'$ are coprime, pairwise distinct, nonzero integers. We apply Theorem 2.6 to the homomorphism $\varphi \colon \mathbb{G}_{\mathrm{m}} \to \mathbb{G}_{\mathrm{m}}^{N-1}$ defined by

$$\varphi(t) = (t^{a_1'}, \dots, t^{a_M'}, t^{a_{M+2}'}, \dots, t^{a_N'}) \,,$$

and for the four polynomials

$$f_1 = \gamma_0 + \sum_{j=1}^{M} \gamma_j t^{a_j'}, \quad f_2 = \gamma_{M+1} + \sum_{j=M+2}^{N} \gamma_j t^{a_j'}, \quad f_3 = t f_1', \quad f_4 = t f_2'.$$

Thus $f = f_1(t^d) + t^{a_{M+1}} f_2(t^d)$ and $D = |\boldsymbol{a}'|$.

We argue as in the first part of the proof. We remark that $\mathrm{h}(f_i) \leq h_0 + \log(2D)$. Let $B' = B'(N, \delta)$ be the constant that appears in Theorem 2.6.

If the inequality (2.1) is not satisfied, then $D \le C_1 = C_1(N, \delta, h_0)$. In this case, we choose $k = N-2$, $\theta_1 = d$, $\theta_2 = a_{M+1}$ and

$$\boldsymbol{b}_j = \begin{cases} (a'_j, 0) & \text{for } j = 1, \dots, M, \\ (0, 1) & \text{for } j = M+1, \\ (a'_j, 1) & \text{for } j = M+2, \dots, N. \end{cases}$$

Thus, in the notation of Theorem 1.1(3),

$$F = f_1(y_1) + y_2^{a_{M+1}} f_2(y_1) \in \overline{\mathbb{Q}}[y_1^{\pm 1}, y_2^{\pm 1}].$$

Since ξ is a multiple root of both $f_1(t^d)$ and $f_2(t^d)$, the polynomials $f_1(y_1)$ and $f_2(y_1)$ have a common multiple factor, say $P(y_1)$, which vanishes at ξ^d. Thus $P(y_1)$ is a multiple factor of F and $P(t^d)$ vanishes at ξ, as required.

It remains to consider the case when the inequality (2.1) is satisfied. Theorem 2.6 then gives a positive integer $1 \le k \le N-1$, vectors $\boldsymbol{b}'_1, \dots, \boldsymbol{b}'_M, \boldsymbol{b}'_{M+2}, \dots, \boldsymbol{b}'_N \in \mathbb{Z}^{N-1-k}$ of size $\le B'$ and $\theta'_1, \dots, \theta'_{N-1-k} \in \mathbb{Z}$ of size $\le B'D$ such that the $(N-1) \times (N-1-k)$ matrix $(b'_{j,i})_{j,i}$ has maximal rank $N-1-k$ and $a'_j = \sum_{i=1}^{N-1-k} b'_{j,i}\theta'_i$ for $j = 1, \dots, M$ and $j = M+2, \dots, N$. We set $\boldsymbol{y} = (y_1, \dots, y_{N-1})$ and

$$F_1 = \gamma_0 + \sum_{j=1}^{M} \gamma_j \boldsymbol{y}^{\boldsymbol{b}_j}, \qquad F_2 = \gamma_{M+1} + \sum_{j=M+2}^{N} \gamma_j \boldsymbol{y}^{\boldsymbol{b}_j},$$

$$F_3 = \sum_{j=1}^{M} \gamma_j a'_j \boldsymbol{y}^{\boldsymbol{b}_j}, \qquad F_4 = \sum_{j=M+2}^{N} \gamma_j a'_j \boldsymbol{y}^{\boldsymbol{b}_j},$$

and consider the differential operator

$$\Delta = \theta'_1 y_1 \frac{\partial}{\partial y_1} + \cdots + \theta'_{N-1k} y_{N-1-k} \frac{\partial}{\partial y_{N-1-k}}.$$

As in the first part of the proof, we have that $\Delta F_1 = F_3$ and $\Delta F_2 = F_4$.

Set $G = \gcd(F_1, F_2, F_3, F_4)$ and write $f_i = \sum_{\alpha \in S} f_{i,\alpha} t^\alpha$, $i = 1, \dots, 4$, with

$$S = \bigcup_{i=1}^{4} \operatorname{supp}(f_i) = \{0, a'_1, \dots, a'_M, a'_{M+2}, \dots, a'_N\}.$$

By hypothesis, ξ^d is a common non-cyclotomic root of f_1, f_2, f_3 and f_4. We want to deduce from Theorem 2.6(3) that $\varphi_1^{\#}(G)$ vanishes at ξ^d. This certainly happens unless there exists a nonempty proper subset Γ of S such that ξ^d is a common root of $\sum_{\alpha \in \Gamma} f_{i,\alpha} t^\alpha$, $i = 1, \dots, 4$.

Assume by contradiction that this is the case. Then ξ^d is a multiple root of $\sum_{\alpha \in \Gamma} f_{i,\alpha} t^\alpha$, $i = 1, 2$. We recall that

$$\operatorname{supp}(f_1) = \{0, a'_1, \dots, a'_M\}, \qquad \operatorname{supp}(f_2) = \{0, a'_{M+2}, \dots, a'_N\}.$$

Since ξ is not a multiple root of $\sum_{j \in \Delta} \gamma_j t^{a_j}$ for any nonempty Δ which is a proper subset of $\{0, \dots, M\}$ or of $\{M+1, \dots, N\}$, we have

$$\Gamma \cap \operatorname{supp}(f_1) = \emptyset \qquad \text{or} \qquad \Gamma \cap \operatorname{supp}(f_1) = \operatorname{supp}(f_1)$$

and

$$\Gamma \cap \operatorname{supp}(f_2) = \emptyset \qquad \text{or} \qquad \Gamma \cap \operatorname{supp}(f_2) = \operatorname{supp}(f_2).$$

Since $\operatorname{supp}(f_1) \cap \operatorname{supp}(f_2) \neq \emptyset$, we deduce that $\Gamma = \operatorname{supp}(f_1) \cup \operatorname{supp}(f_2)$, which contradict the previous assumption. Thus, by Theorem 2.6(3), $\varphi_1^{\#}(G)$ vanishes at ξ^d.

Let P be an irreducible factor of G such that $\pi = \varphi_1^{\#}(P) \in \mathbb{K}[t]$ vanishes at ξ^d. As in the first part of the proof, P is a multiple factor of both F_1 and F_2 and thus of the polynomial

$$F = \gamma_0 + \gamma_1 \widetilde{\boldsymbol{y}}^{\boldsymbol{b}_1} + \cdots + \gamma_N \widetilde{\boldsymbol{y}}^{\boldsymbol{b}_N} = F_1(y_1, \ldots, y_{N-1}) + y_N^{a_{M+1}} F_2(y_1, \ldots, y_{N-1})$$

with $\widetilde{\boldsymbol{y}} = (y_1, \ldots, y_N)$. Set $\theta_i = d\theta_i'$ for $i = 1, \ldots, N-1-k$, $\theta_{N-k} = a_{M+1}$ and

$$\boldsymbol{b}_j = \begin{cases} (b'_{j,1}, \ldots, b'_{j,N-1-k}, 0) & \text{for } j = 1, \ldots, M, \\ (0, \ldots, 0, 1) & \text{for } j = M+1, \\ (b'_{j,1}, \ldots, b'_{j,N-1-k}, 1) & \text{for } j = M+2, \ldots, N. \end{cases}$$

Then the $N \times (N-k)$ matrix $\boldsymbol{B} = (b_{j,i})_{j,i}$ has maximal rank and $\boldsymbol{a} = \boldsymbol{B} \cdot \boldsymbol{\theta}$, so that $P(t^{\theta_1}, \ldots, t^{\theta_{N-1}})$ is a multiple factor of f which vanishes at the point ξ. Theorem 1.1 then follows by choosing $C = \max\{C_1, B'\}$.

6. On a conjecture of Bolognesi and Pirola

Let $\varphi\colon \mathbb{G}_{\mathrm{m}} \to \mathbb{G}_{\mathrm{m}}^N$ be a homomorphism given by $\varphi(t) = (t^{a_1}, \ldots, t^{a_N})$ for a sequence of integers $a_1, \ldots, a_N$ such that $0 < a_1 < \cdots < a_N$, and consider the curve $\mathcal{U} = \mathrm{im}(\varphi)$. It is easy to verify that the linear subspace $X \subset \mathbb{C}^{N-1}$ defined by the condition

$$\operatorname{rank} \begin{pmatrix} a_1 & a_1^2 & \cdots & a_1^{N-2} & x_1 - 1 \\ a_2 & a_2^2 & \cdots & a_2^{N-2} & x_2 - 1 \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ a_N & a_N^2 & \cdots & a_N^{N-2} & x_N - 1 \end{pmatrix} < N - 1$$

has codimension 2, and that the restriction of its defining equations to $(t^{a_1}, \ldots, t^{a_N})$ vanish to order $N-1$ at $t = 1$. Thus, X is the osculating $(N-2)$-linear dimensional space of $\mathcal{U}$ at the point $(1, \ldots, 1) \in \mathbb{G}_{\mathrm{m}}^N$.

It is convenient to homogenize by letting $a_0 = 0$ and considering the $(N+1) \times N$ matrix given by

$$A(\boldsymbol{a}, (x_0 : \ldots : x_N)) = \begin{pmatrix} 1 & a_0 & a_0^2 & \cdots & a_0^{N-2} & x_0 \\ 1 & a_1 & a_1^2 & \cdots & a_1^{N-2} & x_1 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 1 & a_N & a_N^2 & \cdots & a_N^{N-2} & x_N \end{pmatrix}.$$

Then we identify X with the linear subspace of $\mathbb{P}^N$ defined by condition

$$\operatorname{rank}(A(\boldsymbol{a}, (x_0 : \ldots : x_N))) < N.$$

For simplicity, we assume that $a_1, \ldots, a_N$ are coprime. Then L intersects $\mathcal{U}$ in a second point different from the osculating one if and only if there exists $\xi \neq 1$ such that $\operatorname{rank}(A(\boldsymbol{a}, (1 : \xi^{a_1} : \ldots : \xi^{a_N}))) < N$. In [BP11], Bolognesi and Pirola conjecture that this can never happen. It easily seen that, to prove their conjecture, we may assume that ξ is not torsion.

In the case $N = 2$ the conjecture is trivial. Bolognesi and Pirola proved the conjecture for $N = 3$. In [CZ11], Corvaja and Zannier proved a weak form of the conjecture for $N = 4$, namely that the set of exceptional pairs $(\boldsymbol{a}, \xi)$ such that the matrix $A(\boldsymbol{a}, (1 : \xi^{a_1} : \ldots : \xi^{a_N}))$ has rank $< N$ is finite.

As a second application of Theorem 2.6, we prove the following result.

Theorem 6.1. *There is a constant C depending only on N such that the following holds.*

Let $a_1, \dots, a_N$ be integers such that $0 = a_0 < a_1 < a_2 < \cdots < a_N =: D$ and $\xi \in \overline{\mathbb{Q}}^\times \setminus \mu_\infty$. If the matrix $A(\boldsymbol{a}, (1 : \xi^{a_1} : \ldots : \xi^{a_N}))$ has rank $< N$, then there exist $1 \le k \le N-1$ and vectors $\boldsymbol{b}_1, \dots, \boldsymbol{b}_N, \boldsymbol{\theta} \in \mathbb{Z}^{N-k}$ such that

(1) $|\boldsymbol{b}_i| \le C$, $i = 1, \dots, N$, and $|\boldsymbol{\theta}| \le CD$;

(2) the matrix $\boldsymbol{B} = (b_{i,j})_{i,j} \in \mathbb{Z}^{N \times (N-k)}$ has maximal rank $N-k$ and $\boldsymbol{a} = \boldsymbol{B} \cdot \boldsymbol{\theta}$;

(3) the subvariety of $\mathbb{G}_{\mathrm{m}}^{N-k}$ defined by

$$V = \{\boldsymbol{y} \in \mathbb{G}_{\mathrm{m}}^{N-k} \mid \operatorname{rank}(A(\boldsymbol{a}, (1 : \boldsymbol{y}^{\boldsymbol{b}_1} : \ldots : \boldsymbol{y}^{\boldsymbol{b}_N}))) < N\}$$

has a component of codimension 1 containing the point $(\xi^{\theta_1}, \dots, \xi^{\theta_{N-k}})$.

Proof. The proof is very similar to that of Theorem 1.1.

Let $0 = a_0 < a_1 < a_2 < \cdots < a_N =: D$ and $\xi \in \overline{\mathbb{Q}}^\times \setminus \mu_\infty$ such that the matrix $A(\boldsymbol{a}, (1 : \xi^{a_1} : \ldots : \xi^{a_N}))$ has rank $< N$. For each subset $\Lambda \subset \{0, \dots, N\}$, we put $v_{\Lambda,j} = \xi^{a_j}$ if $j \in \Lambda$ and $v_{\Lambda,j} = 0$ otherwise. Then we assume that

$$\text{for all nonempty } \Lambda \subsetneq \{0, \dots, N\}, \operatorname{rank}(A(\boldsymbol{a}, (v_{\Lambda,0} : v_{\Lambda,1} : \ldots : v_{\Lambda,N}))) = N. \tag{6.1}$$

This extra assumption may be removed, proceeding as in the last part of the proof of Theorem 1.1.

Let $d = \gcd(a_1, \dots, a_N)$ and put $a_i' = a_i/d$, $i = 1, \dots, N$. As in the proof of Theorem 1.1, we may assume, by replacing $\boldsymbol{a}$ by $\boldsymbol{a}'$, that $d = 1$.

As already remarked, the linear space X defined by

$$\operatorname{rank}(A(\boldsymbol{a}, (x_0 : x_1 : \ldots : x_N))) < N$$

is defined by two linear equations, say

$$L_i = \gamma_{i,0} x_0 + \gamma_{i,1} x_1 + \cdots + \gamma_{i,N} x_n, \qquad i = 1, 2,$$

with coefficients $\gamma_{i,j}$ bounded by $N! D^{N^2}$. We apply Theorem 2.6, choosing $K_0 = \mathbb{Q}$, $s = 2$ and $\varphi(t) = (t^{a_1}, \dots, t^{a_N})$. Thus

$$f_i = \gamma_{i,0} + \gamma_{i,1} t^{a_1} + \cdots + \gamma_{i,N} t^{a_N}, \qquad i = 1, 2.$$

These two polynomials are not both zeros, since otherwise

$$\operatorname{rank}(A(\boldsymbol{a}, (1 : t^{a_1} : \ldots : t^{a_N}))) < N$$

identically, which is not possible by the assumption $0 < a_1 < a_2 < \cdots < a_N$.

Let $B' = B'(N, 1)$ be the constant which appears in Theorem 2.6. If the inequality (2.1) of that theorem is not satisfied, we have that

$$D^{\frac{1}{2(N-1)}} \le B' \cdot (1 + N^2 \log D + N \log N),$$

which shows that $D \le C_1'$ for some positive constant $C_1' = C_1'(N)$. In this case we simply choose $k = N-1$, $\boldsymbol{b}_i = a_i$ for $i = 1, \dots, N$ and $\theta_1 = 1$. Assertions (1), (2) and (3) of Theorem 6.1 are clearly verified for $C' \ge C_1'$.

Thus we may assume that the inequality (2.1) is satisfied. Theorem 2.6 then gives a positive integer $k < N$ and two homomorphisms $\psi\colon \mathbb{G}_{\mathrm{m}}^{N-k} \to \mathbb{G}_{\mathrm{m}}^{N}$ and $\varphi_1\colon \mathbb{G}_{\mathrm{m}} \to \mathbb{G}_{\mathrm{m}}^{N-k}$ satisfying (1), (2) and (3) of that theorem. Let $\psi(\boldsymbol{y}) = (\boldsymbol{y}^{\boldsymbol{b}_1}, \dots, \boldsymbol{y}^{\boldsymbol{b}_N})$ and $\varphi_1(t) = (t^{\theta_1}, \dots, t^{\theta_{N-k}})$ with $\boldsymbol{b}_1, \dots, \boldsymbol{b}_N \in \mathbb{Z}^{N-k}$ of size $\le B'$ and $\theta_1, \dots, \theta_{N-k} \in \mathbb{Z}$ of size $\le B'D$. By Theorem 2.6(1), the matrix $\boldsymbol{B} = (b_{i,j})_{i,j}$ has maximal rank $N-k$ and $\boldsymbol{a} = \boldsymbol{B} \cdot \boldsymbol{\theta}$.

By the assumption (6.1), ξ is not a common root of $\sum_{j\in\Lambda}\gamma_{i,j}t^{a_j}$, $i=1,2$, for any nonempty $\Lambda\subsetneq\{0,\dots,N\}$. Thus, by Theorem 2.6(3), the greatest common divisor of $F_1(\boldsymbol{y}^{\boldsymbol{b}_1},\dots,\boldsymbol{y}^{\boldsymbol{b}_N})$ and $F_2(\boldsymbol{y}^{\boldsymbol{b}_1},\dots,\boldsymbol{y}^{\boldsymbol{b}_N})$ must vanish at $(\xi^{\theta_1},\dots,\xi^{\theta_{N-k}})$. This means that V has a component of codimension 1 through the point $(\xi^{\theta_1},\dots,\xi^{\theta_{N-k}})$, as required. Theorem 6.1 follows by choosing $C'=\max\{C'_1,B'\}$. □

Remark 6.2. An immediate consequence of Theorem 6.1(1,2) is that the vectors $\boldsymbol{a}$ such that the matrix $A(\boldsymbol{a},(1:\xi^{a_1}:\ldots:\xi^{a_N}))$ has rank $<N$ for some $\xi\in\overline{\mathbb{Q}}^\times\setminus\mu_\infty$, lie on a finite union of proper vector subspaces of $\mathbb{Q}^N$, which is effectively computable for every given N.

Moreover, the condition (3) can be translated in terms of resultants, and can be checked by the search of integral points $\boldsymbol{\theta}=(\theta_1,\dots,\theta_{N-k})\in\mathbb{Z}^{N-k}$ on a finite family of varieties, depending only on N. More precisely, fix $k\in\{1,\dots,N-1\}$ and fix one of the finitely many $N\times(N-k)$ matrix $\boldsymbol{B}=(b_{i,j})_{i,j}$ of maximal rank and with entries of size bounded by $C(N)$. Let $F_i(\theta_1,\dots,\theta_{N-k};y_1,\dots,y_{N-k})$, $i=1,2$, be any two distinct $(N-1)\times(N-1)$ determinants of the matrix

$$\begin{pmatrix} (\sum b_{1j}\theta_j) & (\sum b_{1j}\theta_j)^2 & \cdots & (\sum b_{1j}\theta_j)^{N-2} & \boldsymbol{y}^{b_1}-1\\ (\sum b_{2j}\theta_j) & (\sum b_{2j}\theta_j)^2 & \cdots & (\sum b_{2j}\theta_j)^{N-2} & \boldsymbol{y}^{b_2}-1\\ \vdots & \vdots & \cdots & \vdots & \vdots\\ (\sum b_{Nj}\theta_j) & (\sum b_{Nj}\theta_j)^2 & \cdots & (\sum b_{Nj}\theta_j)^{N-2} & \boldsymbol{y}^{b_N}-1 \end{pmatrix}.$$

Compute the resultant $R\in\mathbb{Z}[\boldsymbol{\theta}][y_1,\dots,y_{N-k-1}]$ of F_1 and F_2 with respect to, say, y_{N-k} and let W be the variety defined by the vanishing of the coefficients of R, viewed as a polynomial in the variables $y_1,\dots,y_{N-k-1}$. Then V has a component of codimension 1 if and only if $\boldsymbol{\theta}\in W$ and $\boldsymbol{a}=\boldsymbol{B}\cdot\boldsymbol{\theta}$.

References

[ALS13] F. Amoroso, L. Leroux, and M. Sombra, *Overdetermined systems of sparse polynomial equations*, to appear in Found. Comput. Math., e-print arXiv:1307.5788v2, 2013.

[AZ00] F. Amoroso and U. Zannier, *A relative Dobrowolski lower bound over abelian extensions*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **29** (2000), 711–727.

[BMZ07] E. Bombieri, D. Masser, and U. Zannier, *Anomalous subvarieties — structure theorems and applications*, Int. Math. Res. Notices **2007** (2007), Art. ID rnm057, 33 pp..

[BP11] M. Bolognesi and G. Pirola, *Osculating spaces and Diophantine equations (with an appendix by Pietro Corvaja and Umberto Zannier)*, Math. Nachr. **284** (2011), 960–972.

[BZ95] E. Bombieri and U. Zannier, *Algebraic points on subvarieties of* $\mathbf{G}_m^n$, Internat. Math. Res. Notices (1995), 333–347.

[CZ11] P. Corvaja and U. Zannier, *On the rank of certain matrices*, Math. Nachr. **284** (2011), 1652–1657.

[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.

[Hab12] P. Habegger, *Effective height upper bounds on algebraic tori*, e-print arXiv:1201.3255v1, 2012.

[KPS01] T. Krick, L. M. Pardo, and M. Sombra, *Sharp estimates for the arithmetic Nullstellensatz*, Duke Math. J. **109** (2001), 521–598.

[Sch96] 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.

[Sch00] A. Schinzel, *Polynomials with special regard to reducibility. With an appendix by Umberto Zannier*, Encyclopedia Math. Appl., vol. 77, Cambridge Univ. Press, 2000.

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

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

Scuola Normale Superiore, Classe di Scienze. Piazza dei Cavalieri 7, 56126 Pisa, Italy
E-mail address: u.zannier@sns.it
URL: http://www.sns.it/didattica/scienze/menunews/personale/docenti/zannierumberto/