Forum Math. **24** (2012), 641–665
DOI 10.1515/FORM.2011.087

Forum Mathematicum

Solving algebraic equations in roots of unity

Iskander Aliev and Chris Smyth

Communicated by Peter Sarnak

Abstract. This paper is devoted to finding solutions of polynomial equations in roots of unity. It was conjectured by S. Lang and proved by M. Laurent that all such solutions can be described in terms of a finite number of parametric families called maximal torsion cosets. We obtain new explicit upper bounds for the number of maximal torsion cosets on an algebraic subvariety of the complex algebraic n-torus $\mathbb{G}_{\mathrm{m}}^n$. In contrast to earlier work that gives the bounds of polynomial growth in the maximum total degree of defining polynomials, the proofs of our results are constructive. This allows us to obtain a new algorithm for determining maximal torsion cosets on an algebraic subvariety of $\mathbb{G}_{\mathrm{m}}^n$.

Keywords. Torsion cosets, roots of unity.

2010 Mathematics Subject Classification. Primary 11G35; secondary 11R18.

1 Introduction

Let $f_1, \dots, f_t$ be polynomials in n variables defined over $\mathbb{C}$. In this paper we deal with solutions of the system

$$\begin{cases} f_1(X_1, \dots, X_n) = 0 \\ \qquad\qquad\vdots \\ f_t(X_1, \dots, X_n) = 0 \end{cases} \tag{1.1}$$

in roots of unity. It will be convenient to think of such solutions as *torsion points* on the subvariety $\mathcal{V}(f_1, \dots, f_t)$ of the complex algebraic torus $\mathbb{G}_{\mathrm{m}}^n$ defined by the system (1.1). As an affine variety, we identify $\mathbb{G}_{\mathrm{m}}^n$ with the Zariski open subset $x_1 x_2 \cdots x_n \neq 0$ of affine space $\mathbb{A}^n$, with the usual multiplication

$$(x_1, x_2, \dots, x_n) \cdot (y_1, y_2, \dots, y_n) = (x_1 y_1, x_2 y_2, \dots, x_n y_n).$$

By an *algebraic subvariety* of $\mathbb{G}_{\mathrm{m}}^n$ we understand a Zariski closed subset. An *algebraic subgroup* of $\mathbb{G}_{\mathrm{m}}^n$ is a Zariski closed subgroup. A *subtorus* of $\mathbb{G}_{\mathrm{m}}^n$ is a geometrically irreducible algebraic subgroup. A *torsion coset* is a coset $\boldsymbol{\omega} H$, where H

The authors thank the UK Engineering and Physical Sciences Research Council for financial support under grant GR/T04458/01.

is a subtorus of $\mathbb{G}_\mathrm{m}^n$ and $\boldsymbol{\omega} = (\omega_1, \dots, \omega_n)$ is a torsion point. Given an algebraic subvariety $\mathcal{V}$ of $\mathbb{G}_\mathrm{m}^n$, a torsion coset C is called *maximal* in $\mathcal{V}$ if $C \subset \mathcal{V}$ and it is not properly contained in any other torsion coset in $\mathcal{V}$. A maximal 0-dimensional torsion coset will be also called an *isolated* torsion point.

Let $N_{\mathrm{tor}}(\mathcal{V})$ denote the number of maximal torsion cosets contained in $\mathcal{V}$. A famous conjecture by Lang ([17, p. 221]) proved by McQuillan [22] implies as a special case that $N_{\mathrm{tor}}(\mathcal{V})$ is finite. This special case had been settled by Ihara, Serre and Tate (see Lang [17, p. 201]) when $\dim(\mathcal{V}) = 1$, and by Laurent [18] if $\dim(\mathcal{V}) > 1$. A different proof of this result was also given by Sarnak and Adams [26]. It follows that all solutions of the system (1.1) in roots of unity can be described in terms of a finite number of maximal torsion cosets on the subvariety $\mathcal{V}(f_1, \dots, f_t)$. It is then of interest to obtain an upper bound for this number. Zhang [29] and Bombieri and Zannier [6] showed that if $\mathcal{V}$ is defined over a number field K, then $N_{\mathrm{tor}}(\mathcal{V})$ is effectively bounded in terms of $d, n, [K : \mathbb{Q}]$ and M, when the defining polynomials were of total degrees at most d and heights at most M. Schmidt [28] found an explicit upper bound for the number of maximal torsion cosets on an algebraic subvariety of $\mathbb{G}_\mathrm{m}^n$ that depends only on the dimension n and the maximum total degree d of the defining polynomials. Indeed, let

$$N_{\mathrm{tor}}(n, d) = \max_{\mathcal{V}} N_{\mathrm{tor}}(\mathcal{V}),$$

where the maximum is taken over all subvarieties $\mathcal{V} \subset \mathbb{G}_\mathrm{m}^n$ defined by polynomial equations of total degree at most d. The proof of Schmidt's bound is based on a result of Schlickewei [27] about the number of nondegenerate solutions of a linear equation in roots of unity. This latter result was significantly improved by Evertse [13], and the resulting Evertse–Schmidt bound can then be stated as

$$N_{\mathrm{tor}}(n, d) \le (11d)^{n^2} \binom{n+d}{d}^{3\binom{n+d}{d}^2}. \tag{1.2}$$

Applying techniques from arithmetic algebraic geometry, David and Philippon [10] went even further and obtained a polynomial-in-d upper bound for the number of isolated torsion points, with the exponent being essentially 7^k, where k is the dimension of the subvariety. This result has been since slightly improved by Amoroso and David [2]. A polynomial bound for the number of all maximal torsion cosets also appears in the main result of Rémond [24], with the exponent $(k+1)^{3(k+1)^2}$.

It should be mentioned here that the last two bounds are special cases of more general results. David and Philippon [10] in fact study the number of algebraic points with small height and Rémond [24] deals with subgroups of finite rank and even with the thickness of such subgroups in the sense of the height. The high generality of the results requires applying sophisticated tools from arithmetic algebraic geometry. This approach involves working with heights in the fields of algebraic numbers and a delicate specialization argument (see, e.g., Proposition 6.9 in David and Philippon [11]) that allows one to transfer the results to algebraically closed fields of characteristics 0.

In this paper we present a constructive and more elementary approach to this problem which is based on well-known arithmetic properties of the roots of unity. Roughly speaking, we use the Minkowski geometry of numbers to reduce the problem to a very special case and then apply an intersection/elimination argument. This allows us to obtain a polynomial bound with the exponent 5^n for the number of maximal torsion cosets lying on a subvariety of $\mathbb{G}_\mathrm{m}^n$ defined over $\mathbb{C}$, and implies an algorithm for finding all such cosets. The algorithm is presented in Section 6.

One should point out here that other algorithms for finding all the maximal torsion cosets on a subvariety of $\mathbb{G}_\mathrm{m}^n$ were proposed by Sarnak and Adams in [26] and by Ruppert [25]. In view of its high complexity, the algorithm of Ruppert is described in [25] only for a special choice of defining polynomials. Note also that different algorithms implicitly follow from the papers by Mann [20], Conway and Jones [9] and Dvornicich and Zannier [12].

1.1 The main results

We shall start with the case of hypersurfaces.

Theorem 1.1. *Let $f \in \mathbb{C}[X_1, \dots, X_n]$, $n \geq 2$, be a polynomial of total degree d and let $\mathcal{H} = \mathcal{H}(f)$ be the hypersurface in $\mathbb{G}_\mathrm{m}^n$ defined by f. Then*

$$N_{\mathrm{tor}}(\mathcal{H}) \leq c_1(n) d^{c_2(n)}, \tag{1.3}$$

with

$$c_1(n) = n^{\frac{3}{2}(2+n)5^n} \quad \textit{and} \quad c_2(n) = \frac{1}{16}(49 \cdot 5^{n-2} - 4n - 9).$$

Let $f \in \mathbb{C}[X_1, \dots, X_n]$ be a polynomial of degree d_i in X_i. Ruppert [25] conjectured that the number of isolated torsion points on $\mathcal{H}(f)$ is bounded by $c(n) d_1 \cdots d_n$. Theorem 1.1 is a step towards proving this conjecture. Furthermore, the results of Beukers and Smyth [3] for plane curves (see Lemma 2.2 below) indicate that the following stronger conjecture might be true.

Conjecture. *The number of isolated torsion points on the hypersurface $\mathcal{H}(f)$ is bounded by $c(n)\mathrm{vol}_n(f)$, where $\mathrm{vol}_n(f)$ is the n-volume of the Newton polytope of the polynomial f.*

Concerning general varieties, we obtained the following result.

Theorem 1.2. *For $n \geq 2$, we have*

$$N_{\mathrm{tor}}(n,d) \leq c_3(n) d^{c_4(n)}, \tag{1.4}$$

where

$$c_3(n) = n^{(2+n)2^{n-2}\sum_{i=2}^{n-1} c_2(i)} \prod_{i=2}^{n} c_1(i) \quad \text{and} \quad c_4(n) = \sum_{i=2}^{n} c_2(i) 2^{n-i} + 2^{n-1}.$$

It should be pointed out that the constants $c_i(n)$ in Theorems 1.1 and 1.2 could be certainly improved. To simplify the presentation, we tried to avoid painstaking estimates.

The proof of Theorem 1.1 is based on Theorem 1.3, formulated in the next section. Theorem 1.2, in its turn, is a consequence of Theorem 1.1.

1.2 An intersection argument

For $\boldsymbol{i} = (i_1, \dots, i_n) \in \mathbb{Z}^n$, we abbreviate $\boldsymbol{X}^{\boldsymbol{i}} = X_1^{i_1} \cdots X_n^{i_n}$. Let

$$f(\boldsymbol{X}) = \sum_{\boldsymbol{i} \in \mathbb{Z}^n} a_{\boldsymbol{i}} \boldsymbol{X}^{\boldsymbol{i}}$$

be a Laurent polynomial. By the *support* of f we mean the set

$$S_f = \{\boldsymbol{i} \in \mathbb{Z}^n : a_{\boldsymbol{i}} \neq 0\}$$

and by the *exponent lattice* of f we mean the lattice $L(f)$ generated by the difference set $D(S_f) = S_f - S_f$, so that

$$L(f) = \mathrm{span}_{\mathbb{Z}}\{D(S_f)\}.$$

Our next result and its proof is a generalization of that for $n = 2$ in Beukers and Smyth [3].

Theorem 1.3. *Let $f \in \mathbb{C}[X_1, \dots, X_n]$, $n \geq 2$, be an irreducible polynomial with $L(f) = \mathbb{Z}^n$. Then for some m with $1 \leq m \leq 2^{n+1} - 1$ there exist m polynomials $f_1, f_2, \dots, f_m$ with the following properties:*

(i) $\deg(f_i) \leq 2\deg(f)$ *for* $i = 1, \dots, m$.

(ii) *For $1 \leq i \leq m$, the polynomials f and f_i have no common factor.*

(iii) *For any torsion coset C lying on the hypersurface $\mathcal{H}(f)$ there exists some f_i, $1 \leq i \leq m$, such that the coset C also lies on the hypersurface $\mathcal{H}(f_i)$.*

2 Lemmas required for the proofs

In this section we give the definitions and basic lemmas we need in the rest of paper.

2.1 Finding the cyclotomic part of a polynomial in one variable

Let us consider the following one-variable version of the problem: given a polynomial $f \in \mathbb{C}[X]$, find all roots of unity ω that are zeroes of f. This is equivalent to finding the factor of f consisting of the product of all distinct irreducible cyclotomic polynomial factors of f, which we shall call the *cyclotomic part* of f. Algorithms for finding the cyclotomic part of f follow from several papers, for instance the papers by Mann [20], Conway and Jones [9] and Dvornicich and Zannier [12]. In this paper we use the approach of Bradford and Davenport [7] and Beukers and Smyth [3], who proposed algorithms based on the following properties of roots of unity.

Lemma 2.1 (Beukers and Smyth [3, Lemma 1]). (i) *If $g \in \mathbb{C}[X]$, $g(0) \neq 0$, is a polynomial with the property that for every zero α of g, at least one of $\pm\alpha^2$ is also a zero, then all zeroes of g are roots of unity.*

(ii) *If ω is a root of unity, then it is conjugate to ω^p, where*

$$\begin{cases} p = 2k+1,\ \omega^p = -\omega & \text{for } \omega \text{ a primitive } (4k)\text{th root of unity;} \\ p = k+2,\ \omega^p = -\omega^2 & \text{for } \omega \text{ a primitive } (2k)\text{th root of unity, } k \text{ odd;} \\ p = 2,\ \omega^p = \omega^2 & \text{for } \omega \text{ a } k\text{th root of unity, } k \text{ odd.} \end{cases}$$

In the special case $f \in \mathbb{Z}[X]$, Filaseta and Schinzel [14] constructed a deterministic algorithm for finding the cyclotomic part of f that works especially well when the number of nonzero terms is small compared to the degree of f.

2.2 Torsion points on plane curves

Let $f \in \mathbb{C}[X^{\pm 1}, Y^{\pm 1}]$ be a Laurent polynomial. The problem of finding torsion points on the curve $\mathcal{C}$ defined by the polynomial equation $f(X,Y) = 0$ was implicitly solved already in work of Lang [16] and Liardet [19], as well as in the papers by Mann [20], Conway and Jones [9] and Dvornicich and Zannier [12], already referred to. More recently, it has been also addressed in Beukers and Smyth [3] and Ruppert [25].

The polynomial f can be written in the form

$$f(X,Y) = g(X,Y) \prod_i (X^{a_i} Y^{b_i} - \omega_i),$$

where the ω_j are roots of unity and g is a polynomial (possibly reducible) that has no factor of the form $X^a Y^b - \omega$, for ω a root of unity.

Lemma 2.2 (Beukers and Smyth [3, Main Theorem]). *The curve* $\mathcal{C}$ *has at most* $22\mathrm{vol}_2(g)$ *isolated torsion points.*

Hence, for $f \in \mathbb{C}[X,Y]$, the number of isolated torsion points on the curve $\mathcal{C} = \mathcal{H}(f)$ is at most $11(\deg(f))^2$. Furthermore, by Lemma 2.8 below, each factor $X^{a_i} Y^{b_i} - \omega_i$ of the polynomial f gives precisely one torsion coset. Summarizing the above observations, we get the inequality

$$N_{\mathrm{tor}}(\mathcal{C}) \le 11(\deg(f))^2 + \deg(f). \tag{2.1}$$

2.3 Geometry of numbers

The bijection $\boldsymbol{i} \leftrightarrow \boldsymbol{X}^{\boldsymbol{i}}$ allows us to study polynomials by the use of the geometry of numbers. The following technical tools will be needed.

We first recall some basic definitions. A *lattice* is a discrete subgroup of $\mathbb{R}^n$. Given a lattice L of rank k, any set of vectors $\{\boldsymbol{b}_1, \dots, \boldsymbol{b}_k\}$ that satisfies $L = \mathrm{span}_{\mathbb{Z}}\{\boldsymbol{b}_1, \dots, \boldsymbol{b}_k\}$ or the matrix $\mathbf{B} = (\boldsymbol{b}_1, \dots, \boldsymbol{b}_k)$ with rows $\boldsymbol{b}_i$ will be called a *basis* of L. The *determinant* of a lattice L with a basis $\mathbf{B}$ is defined to be

$$\det(L) = \sqrt{\det(\mathbf{B}\,\mathbf{B}^T)}.$$

Let B_p^n with $p = 1, 2, \infty$ denote the unit n-ball with respect to the l_p-norm, and let γ_n be the Hermite constant for dimension n – see Section 38.1 of Gruber and Lekkerkerker [15]. For a convex body K and a lattice L, we also denote by $\lambda_i(K, L)$ the ith successive minimum of K with respect to L – see Section 9.1 ibid.

Lemma 2.3. *Let* S *be a subspace of* $\mathbb{R}^n$ *with* $\dim(S) = \mathrm{rank}(S \cap \mathbb{Z}^n) = r < n$. *Then there exists a basis* $\{\boldsymbol{b}_1, \boldsymbol{b}_2, \dots, \boldsymbol{b}_n\}$ *of the lattice* $\mathbb{Z}^n$ *such that*

(i) $S \subset \mathrm{span}_{\mathbb{R}}\{\boldsymbol{b}_1, \dots, \boldsymbol{b}_{n-1}\}$;

(ii) $|\boldsymbol{b}_i| < 1 + \frac{1}{2}(n-1)\gamma_{n-1}^{\frac{n-1}{2}} \gamma_{n-r}^{\frac{1}{2}} \det(S \cap \mathbb{Z}^n)^{\frac{1}{n-r}}$, $i = 1, \dots, n$.

Proof. Suppose first that $r < n-1$. By Proposition 1 (ii) of Aliev, Schinzel and Schmidt [1], there exists a subspace $T \subset \mathbb{R}^n$ with $\dim(T) = n-1$ such that $S \subset T$ and

$$\det(T \cap \mathbb{Z}^n) \le \gamma_{n-r}^{\frac{1}{2}} \det(S \cap \mathbb{Z}^n)^{\frac{1}{n-r}}. \tag{2.2}$$

In the case $r = n-1$ we will put $T = S$.

The subspace T can be considered as a standard $(n-1)$-dimensional euclidean space. Then by the Minkowski's second theorem for balls (see Theorem I, Ch. VIII of Cassels [8]) we have

$$\prod_{i=1}^{n-1} \lambda_i(T \cap B_2^n, T \cap \mathbb{Z}^n) \le \gamma_{n-1}^{\frac{n-1}{2}} \det(T \cap \mathbb{Z}^n).$$

Noting that $1 \le \lambda_1(T \cap B_2^n, T \cap \mathbb{Z}^n) \le \cdots \le \lambda_{n-1}(T \cap B_2^n, T \cap \mathbb{Z}^n)$, we get

$$\lambda_{n-1}(T \cap B_2^n, T \cap \mathbb{Z}^n) \le \gamma_{n-1}^{\frac{n-1}{2}} \det(T \cap \mathbb{Z}^n). \tag{2.3}$$

Next, by Corollary of Theorem VII, Ch. VIII of Cassels [8], there exists a basis $\mathbf{B} = (\boldsymbol{b}_1, \dots, \boldsymbol{b}_{n-1})$ of the lattice $T \cap \mathbb{Z}^n$ with $|\boldsymbol{b}_j| \le \max\{1, j/2\}\lambda_j(T \cap B_2^n, T \cap \mathbb{Z}^n)$, $j = 1, \dots, n-1$. Consequently,

$$\begin{aligned} |\boldsymbol{b}_i| &\le \frac{n-1}{2}\lambda_{n-1}(T \cap B_2^n, T \cap \mathbb{Z}^n) \\ &\le \frac{n-1}{2}\gamma_{n-1}^{\frac{n-1}{2}} \det(T \cap \mathbb{Z}^n) \\ &\le \frac{n-1}{2}\gamma_{n-1}^{\frac{n-1}{2}} \gamma_{n-r}^{\frac{1}{2}} \det(S \cap \mathbb{Z}^n)^{\frac{1}{n-r}}, \quad i = 1, \dots, n-1. \end{aligned}$$

Further, we need to extend $\mathbf{B}$ to a basis of the lattice $\mathbb{Z}^n$. Let $\boldsymbol{a}$ be a primitive integer vector from $\operatorname{span}_{\mathbb{R}}^{\perp}(T \cap \mathbb{Z}^n)$. Clearly, all possible vectors $\boldsymbol{b}$ such that $(\boldsymbol{b}_1, \dots, \boldsymbol{b}_{n-1}, \boldsymbol{b})$ is a basis of $\mathbb{Z}^n$ form the set $\{\boldsymbol{x} \in \mathbb{R}^n : \langle \boldsymbol{x}, \boldsymbol{a} \rangle = \pm 1\} \cap \mathbb{Z}^n$, and this set contains a point $\boldsymbol{b}_n$ with

$$|\boldsymbol{b}_n| \le \frac{1}{|\boldsymbol{a}|} + \mu(T \cap B_2^n, T \cap \mathbb{Z}^n), \tag{2.4}$$

where $\mu(\cdot,\cdot)$ is the *inhomogeneous minimum* – see Section 13.1 of Gruber–Lekkerkerker [15]. By Jarnik's inequality (see Theorem 1 on p. 99 ibid.),

$$\begin{aligned} \mu(T \cap B_2^n, T \cap \mathbb{Z}^n) &\le \frac{1}{2}\sum_{i=1}^{n-1} \lambda_i(T \cap B_2^n, T \cap \mathbb{Z}^n) \\ &\le \frac{n-1}{2}\lambda_{n-1}(T \cap B_2^n, T \cap \mathbb{Z}^n). \end{aligned}$$

Consequently, by (2.4), (2.3) and (2.2), we have

$$|\boldsymbol{b}_n| < 1 + \frac{n-1}{2}\gamma_{n-1}^{\frac{n-1}{2}} \gamma_{n-r}^{\frac{1}{2}} \det(S \cap \mathbb{Z}^n)^{\frac{1}{n-r}}. \qquad \square$$

When L is a lattice of rank n, its *polar* lattice L^* is defined as

$$L^* = \{\boldsymbol{x} \in \mathbb{R}^n : \langle \boldsymbol{x}, \boldsymbol{y} \rangle \in \mathbb{Z} \text{ for all } \boldsymbol{y} \in L\}.$$

Given a basis $\mathbf{B} = (\boldsymbol{b}_1, \dots, \boldsymbol{b}_n)$ of L, the basis of L^* *polar* to $\mathbf{B}$ is the basis $\mathbf{B}^* = (\boldsymbol{b}_1^*, \dots, \boldsymbol{b}_n^*)$ with

$$\langle \boldsymbol{b}_i, \boldsymbol{b}_j^* \rangle = \delta_{ij}, \quad i, j = 1, \dots, n,$$

where δ_{ij} is the Kronecker delta.

Corollary 2.4. *Let S be a subspace of $\mathbb{R}^n$ with $\dim(S) = \operatorname{rank}(S \cap \mathbb{Z}^n) = r < n$. Then there exists a basis $\mathbf{A} = (\boldsymbol{a}_1, \boldsymbol{a}_2, \dots, \boldsymbol{a}_n)$ of the lattice $\mathbb{Z}^n$ such that $\boldsymbol{a}_1 \in S^\perp$ and the vectors of the polar basis $\mathbf{A}^* = (\boldsymbol{a}_1^*, \boldsymbol{a}_2^*, \dots, \boldsymbol{a}_n^*)$ satisfy the inequalities*

$$|\boldsymbol{a}_i^*| < 1 + \frac{n-1}{2} \gamma_{n-1}^{\frac{n-1}{2}} \gamma_{n-r}^{\frac{1}{2}} \det(S \cap \mathbb{Z}^n)^{\frac{1}{n-r}}, \quad i = 1, \dots, n. \tag{2.5}$$

Proof. Applying Lemma 2.3 to the subspace S we get a basis $\{\boldsymbol{b}_1, \boldsymbol{b}_2, \dots, \boldsymbol{b}_n\}$ of $\mathbb{Z}^n$ satisfying conditions (i)–(ii). Observe that its polar basis $\{\boldsymbol{b}_1^*, \boldsymbol{b}_2^*, \dots, \boldsymbol{b}_n^*\}$ has its last vector $\boldsymbol{b}_n^*$ in $S^\perp$. Therefore, we can put $\boldsymbol{a}_1 = \boldsymbol{b}_n^*, \boldsymbol{a}_2 = \boldsymbol{b}_2^*, \dots, \boldsymbol{a}_{n-1} = \boldsymbol{b}_{n-1}^*, \boldsymbol{a}_n = \boldsymbol{b}_1^*$. □

2.4 Lattices and torsion cosets

In the subsection we describe the standard bijection between lattices and algebraic subgroups of $\mathbb{G}_{\mathrm{m}}^n$. By an *integer* lattice we understand a lattice $A \subset \mathbb{Z}^n$. An integer lattice is called *primitive* if $A = \operatorname{span}_{\mathbb{R}}(A) \cap \mathbb{Z}^n$. For an integer lattice A, we define the subgroup H_A of $\mathbb{G}_{\mathrm{m}}^n$ by

$$H_A = \{\boldsymbol{x} \in \mathbb{G}_{\mathrm{m}}^n : \boldsymbol{x}^{\boldsymbol{a}} = 1 \text{ for all } \boldsymbol{a} \in A\}.$$

Then, for instance, $H_{\mathbb{Z}^n}$ is the trivial subgroup.

Lemma 2.5 (see Schmidt [28, Lemmas 1 and 2]). *The map $A \mapsto H_A$ sets up a bijection between integer lattices and algebraic subgroups of $\mathbb{G}_{\mathrm{m}}^n$. A subgroup $H = H_A$ is irreducible if and only if the lattice A is primitive.*

Let $\boldsymbol{\omega} = (\omega_1, \dots, \omega_n)$ be a torsion point and let $C = \boldsymbol{\omega} H_A$ be an r-dimensional torsion coset with $r \geq 1$. We will need the following parametric representation of C. Let $\operatorname{span}_{\mathbb{R}}^{\perp}(A)$ denote the orthogonal complement of $\operatorname{span}_{\mathbb{R}}(A)$ in $\mathbb{R}^n$ and let $\mathbf{G} = (g_{ij})$ be an $r \times n$ integer matrix of rank r whose rows $\boldsymbol{g}_1, \dots, \boldsymbol{g}_r$ form a basis of the lattice $\mathrm{span}_{\mathbb{R}}^{\perp}(A) \cap \mathbb{Z}^{n}$. Then the coset C can be represented in the form

$$C = \left(\omega_1 \prod_{j=1}^{r} t_j^{g_{j1}}, \ldots, \omega_n \prod_{j=1}^{r} t_j^{g_{jn}}\right)$$

with parameters $t_1, \ldots, t_r \in \mathbb{C}^*$. We will say that $\mathbf{G}$ is an *exponent matrix* for the coset C. If $f \in \mathbb{C}[X_1^{\pm 1}, \ldots, X_n^{\pm 1}]$ is a Laurent polynomial and for $\boldsymbol{j} \in \mathbb{Z}^r$

$$f_{\boldsymbol{j}}(\boldsymbol{X}) = \sum_{\boldsymbol{i} \in S_f:\, \boldsymbol{i}\mathbf{G}^T = \boldsymbol{j}} a_{\boldsymbol{i}} \boldsymbol{X}^{\boldsymbol{i}},$$

then $f(\boldsymbol{X}) = \sum_{\boldsymbol{j} \in \mathbb{Z}^r} f_{\boldsymbol{j}}(\boldsymbol{X})$ and

$$\text{the coset } C \text{ lies on } \mathcal{H}(f) \text{ if and only if } f_{\boldsymbol{j}}(\boldsymbol{\omega}) = 0 \text{ for all } \boldsymbol{j} \in \mathbb{Z}^r. \tag{2.6}$$

Let $\mathbf{U} = (\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n)$ be a basis of the lattice $\mathbb{Z}^{n}$. We will associate with $\mathbf{U}$ the new coordinates $(Y_1, \ldots, Y_n)$ in $\mathbb{G}_{\mathrm{m}}^{n}$ defined by

$$Y_1 = \boldsymbol{X}^{\boldsymbol{u}_1}, \quad Y_2 = \boldsymbol{X}^{\boldsymbol{u}_2}, \quad \ldots, \quad Y_n = \boldsymbol{X}^{\boldsymbol{u}_n}. \tag{2.7}$$

Suppose that the matrix $\mathbf{U}^{-1}$ has rows $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n$. By the *image* of a Laurent polynomial $f \in \mathbb{C}[X_1^{\pm 1}, \ldots, X_n^{\pm 1}]$ in coordinates $(Y_1, \ldots, Y_n)$ we mean the Laurent polynomial

$$f^{\mathbf{U}}(\boldsymbol{Y}) = f(\boldsymbol{Y}^{\boldsymbol{v}_1}, \ldots, \boldsymbol{Y}^{\boldsymbol{v}_n}).$$

By the *image* of a torsion coset $C = \boldsymbol{\omega} H_A$ in coordinates $(Y_1, \ldots, Y_n)$ we mean the torsion coset

$$C^{\mathbf{U}} = (\boldsymbol{\omega}^{\boldsymbol{u}_1}, \ldots, \boldsymbol{\omega}^{\boldsymbol{u}_n}) H_B,$$

where $B = \{\boldsymbol{a}\mathbf{U}^{-1} : \boldsymbol{a} \in A\}$.

Lemma 2.6. *The map $C \mapsto C^{\mathbf{U}}$ sets up a bijection between maximal torsion cosets on the subvarieties $\mathcal{V}(f_1, \ldots, f_t)$ and $\mathcal{V}(f_1^{\mathbf{U}}, \ldots, f_t^{\mathbf{U}})$.*

Proof. It is enough to observe that the map $\phi : \mathbb{G}_{\mathrm{m}}^{n} \to \mathbb{G}_{\mathrm{m}}^{n}$ defined by

$$\phi(\boldsymbol{x}) = (\boldsymbol{x}^{\boldsymbol{u}_1}, \ldots, \boldsymbol{x}^{\boldsymbol{u}_n}) \tag{2.8}$$

is an automorphism of $\mathbb{G}_{\mathrm{m}}^{n}$ (see Ch. 3 in Bombieri and Gubler [4] and Section 2 in Schmidt [28]). □

Remark. The automorphism (2.8) is called a *monoidal transformation*. We introduced the coordinates (2.7) to make the inductive argument used in the proofs of Theorems 1.1–1.2 more transparent.

For $f \in \mathbb{C}[X_1, \ldots, X_n]$ and $k \geq n$, we will denote by $T_i^k(f)$ the number of i-dimensional maximal torsion cosets on $\mathcal{H}(f)$, regarded as a hypersurface in $\mathbb{G}_{\mathrm{m}}^k$. Let $A \subset \mathbb{Z}^n$ be an integer lattice of rank n with $\det(A) > 1$ and let $\mathbf{A} = (\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n)$ be a basis of A.

Lemma 2.7. *Suppose that the Laurent polynomials* $f, f^* \in \mathbb{C}[X_1^{\pm 1}, \ldots, X_n^{\pm 1}]$ *satisfy*

$$f = f^*(\boldsymbol{X}^{\boldsymbol{a}_1}, \ldots, \boldsymbol{X}^{\boldsymbol{a}_n}). \tag{2.9}$$

Then the inequalities

$$T_i^n(f^*) \leq T_i^n(f) \leq \det(A) T_i^n(f^*), \quad i = 0, \ldots, n-1, \tag{2.10}$$

hold.

Proof. First, for any torsion point $\boldsymbol{\zeta} = (\zeta_1, \ldots, \zeta_n)$ on $\mathcal{H}(f^*)$, we will find all torsion points $\boldsymbol{\omega}$ on $\mathcal{H}(f)$ with $\boldsymbol{\zeta} = (\boldsymbol{\omega}^{\boldsymbol{a}_1}, \ldots, \boldsymbol{\omega}^{\boldsymbol{a}_n})$. Putting the matrix $\mathbf{A}$ into Smith Normal Form (see Newman [23, p. 26]) yields two matrices $\mathbf{V}$ and $\mathbf{W}$ in $\mathrm{GL}_n(\mathbb{Z})$ with $\mathbf{WAV} = \mathbf{D}$, where $\mathbf{D} = \mathrm{diag}(d_1, \ldots, d_n)$. Therefore, by Lemma 2.6, we may assume without loss of generality that $\mathbf{A} = \mathrm{diag}(d_1, \ldots, d_n)$. Let $\vartheta_1, \ldots, \vartheta_n$ be primitive d_1th, d_2th, $\ldots$, d_nth roots of $\zeta_1, \ldots, \zeta_n$, respectively. Then as we let $\vartheta_1, \ldots, \vartheta_n$ vary over all possible such choices of these primitive roots

the torsion point $\boldsymbol{\zeta} \in \mathcal{H}(f^*)$ gives precisely $\det(A)$ torsion points $\boldsymbol{\omega} = (\vartheta_1, \ldots, \vartheta_n)$ on $\mathcal{H}(f)$ with $\boldsymbol{\zeta} = (\boldsymbol{\omega}^{\boldsymbol{a}_1}, \ldots, \boldsymbol{\omega}^{\boldsymbol{a}_n})$. (2.11)

Let now M_f and M_{f^*} denote the sets of all maximal torsion cosets of *positive* dimension on $\mathcal{H}(f)$ and $\mathcal{H}(f^*)$ respectively. We will define a map $\tau : M_f \to M_{f^*}$ as follows. Let $C \in M_f$ be an r-dimensional maximal torsion coset. Given any torsion point $\boldsymbol{\omega} = (\omega_1, \ldots, \omega_n) \in C$, we can write the coset as $C = \boldsymbol{\omega} H_B$ for some primitive integer lattice B. Recall that C can be also represented in the form

$$C = \left(\omega_1 \prod_{j=1}^{r} t_j^{g_{j1}}, \ldots, \omega_n \prod_{j=1}^{r} t_j^{g_{jn}} \right), \tag{2.12}$$

where $t_1, \ldots, t_r \in \mathbb{C}^*$ are parameters and the vectors $\boldsymbol{g}_j = (g_{j1}, \ldots, g_{jn})$, $j = 1, \ldots, r$, form a basis of the integer lattice $\mathrm{span}_{\mathbb{R}}^{\perp}(B) \cap \mathbb{Z}^n$. We consider $M = \mathrm{span}_{\mathbb{Z}}\{\boldsymbol{g}_1 \mathbf{A}^T, \ldots, \boldsymbol{g}_r \mathbf{A}^T\}$ and $L = \mathrm{span}_{\mathbb{R}}(M) \cap \mathbb{Z}^n$. Then we define

$$\tau(C) = \left(\boldsymbol{\omega}^{\boldsymbol{a}_1} \prod_{k=1}^{r} t_k^{s_{k1}}, \ldots, \boldsymbol{\omega}^{\boldsymbol{a}_n} \prod_{k=1}^{r} t_k^{s_{kn}} \right),$$

where $t_1, \ldots, t_r \in \mathbb{C}^*$ are parameters and the vectors $\boldsymbol{s}_k = (s_{k1}, \ldots, s_{kn})$, $k = 1, \ldots, r$, form a basis of the lattice L. Let us show that τ is well-defined. First, the observation (2.6) implies that $\tau(C)$ is a maximal r-dimensional torsion coset on $\mathcal{H}(f^*)$. Now we have to show that $\tau(C)$ does not depend on the choice of $\boldsymbol{\omega} \in C$. Observe that any torsion point $\boldsymbol{\eta} \in C$ has the form

$$\boldsymbol{\eta} = \left(\omega_1 \prod_{j=1}^{r} \nu_j^{g_{j1}}, \ldots, \omega_n \prod_{j=1}^{r} \nu_j^{g_{jn}} \right),$$

where $\nu_1, \ldots, \nu_r$ are some roots of unity. Put $\boldsymbol{h}_j = \boldsymbol{g}_j \mathbf{A}^T$, $j = 1, \ldots, r$. It is enough to show that for any roots of unity $\nu_1, \ldots, \nu_r$ there exist roots of unity $\mu_1, \ldots, \mu_r$ such that

$$\prod_{j=1}^{r} \nu_j^{h_{ji}} = \prod_{k=1}^{r} \mu_k^{s_{ki}}, \quad i = 1, \ldots, n.$$

Since $M \subset L$, we have $\boldsymbol{h}_j \in L$, so that

$$\boldsymbol{h}_j = l_{j1} \boldsymbol{s}_1 + \cdots + l_{jr} \boldsymbol{s}_r, \quad l_{j1}, \ldots, l_{jr} \in \mathbb{Z}.$$

Now we can put

$$\mu_k = \nu_1^{l_{1k}} \nu_2^{l_{2k}} \cdots \nu_r^{l_{rk}}, \quad k = 1, \ldots, r.$$

Thus, the map τ is well-defined. It can be also easily shown that the map τ is surjective. This observation immediately implies the left hand side inequality in (2.10) for positive i. Moreover, by (2.11), we clearly have

$$T_0^n(f) = \det(A) T_0^n(f^*), \tag{2.13}$$

so that the lemma is proved for the isolated torsion points.

Let now $D = \boldsymbol{\zeta} H' \in M^*$ be an r-dimensional maximal torsion coset, where $r \geq 1$. Suppose that $D = \tau(C)$ for some $C \in M_f$. We will show that $C = \boldsymbol{\omega} H$, where $\boldsymbol{\omega}$ can be chosen among the $\det(A)$ torsion points listed in (2.11). This will immediately imply the right hand side inequality in (2.10) for positive i. We may assume without loss of generality that $H = H_B$ and $H' = H_{\mathrm{span}_{\mathbb{R}}^{\perp}(L) \cap \mathbb{Z}^n}$, with the lattices B and L defined as above. Let $\mu_1, \ldots, \mu_r$ be any roots of unity. Then the coset D can be represented as

$$D = \left(\zeta_1 \prod_{k=1}^{r} \mu_k^{s_{k1}} \prod_{k=1}^{r} t_k^{s_{k1}}, \ldots, \zeta_n \prod_{k=1}^{r} \mu_k^{s_{kn}} \prod_{k=1}^{r} t_k^{s_{kn}} \right)$$

for $\boldsymbol{\zeta} = (\zeta_1, \dots, \zeta_n)$. Thus, it is enough to prove the existence of roots of unity $\nu_1, \dots, \nu_r$ with

$$\prod_{k=1}^{r} \mu_k^{s_{ki}} = \prod_{j=1}^{r} \nu_j^{h_{ji}}, \quad i = 1, \dots, n.$$

The lattice M is a sublattice of L and rank $(M) =$ rank (L). Therefore, there exist positive integers $n_1, \dots, n_r$ such that $n_i \boldsymbol{s}_i \in M$, $i = 1, \dots, r$, and, consequently, we have

$$n_i \boldsymbol{s}_i = m_{i1} \boldsymbol{h}_1 + \cdots + m_{ir} \boldsymbol{h}_r, \quad m_{i1}, \dots, m_{ir} \in \mathbb{Z}.$$

Now, if the roots of unity $\rho_1, \dots, \rho_r$ satisfy $\rho_i^{n_i} = \mu_i$, $i = 1, \dots, r$, we can put

$$\nu_j = \rho_1^{m_{1j}} \rho_2^{m_{2j}} \cdots \rho_r^{m_{rj}}, \quad j = 1, \dots, r. \qquad \square$$

2.5 Torsion cosets of codimension 1 in $\mathbb{G}_{\mathrm{m}}^{n}$

The next lemma is an immediate consequence of the structure of torsion cosets, explained for example in Bombieri and Gubler [4]. We give a proof here for the sake of completeness.

Lemma 2.8. *Suppose that the hypersurface $\mathcal{H}$ is defined by $f \in \mathbb{C}[X_1, \dots, X_n]$ with $f = \prod_i h_i$, where h_i are irreducible polynomials. Then the $(n-1)$-dimensional torsion cosets on $\mathcal{H}$ are precisely the hypersurfaces $\mathcal{H}(h_j)$ defined by the factors h_j of the form $\boldsymbol{X}^{\boldsymbol{m}_j} - \omega_j \boldsymbol{X}^{\boldsymbol{n}_j}$, where ω_j are roots of unity.*

Proof. Let ω be a root of unity and let $h = \boldsymbol{X}^{\boldsymbol{m}} - \omega \boldsymbol{X}^{\boldsymbol{n}}$ be a factor of f. Multiplying h by a monomial we may assume that h is a Laurent polynomial of the form $\boldsymbol{X}^{\boldsymbol{a}} - \omega$, where $\boldsymbol{a} = (a_1, \dots, a_n)$ is a *primitive* integer vector, so that $\gcd(a_1, \dots, a_n) = 1$. Let A be the integer lattice generated by the vector $\boldsymbol{a}$, $\boldsymbol{b} = (b_1, \dots, b_n)$ be an integer vector with $\langle \boldsymbol{b}, \boldsymbol{a} \rangle = 1$, where $\langle \cdot, \cdot \rangle$ is the usual inner product, and put

$$\boldsymbol{\omega} = (\omega^{b_1}, \dots, \omega^{b_n}).$$

Now, all points of the torsion coset $C = \boldsymbol{\omega} H_A$ clearly satisfy the equation $\boldsymbol{X}^{\boldsymbol{a}} = \omega$. To show that any solution $\boldsymbol{x} = (x_1, \dots, x_n)$ of this equation belongs to C we observe that the point $(x_1 \omega^{-b_1}, \dots, x_n \omega^{-b_n})$ belongs to the subtorus H_A.

Conversely, let $C = \boldsymbol{\omega} H$ be an $(n-1)$-dimensional coset on $\mathcal{H}$. Since the exponent matrix of the coset C has rank $n-1$, there exists a primitive integer vector $\boldsymbol{a}$ such that and for all $\boldsymbol{j} \in \mathbb{Z}^{n-1}$ we have $\mathrm{span}_{\mathbb{R}}(L(f_{\boldsymbol{j}})) \cap \mathbb{Z}^n = \mathrm{span}_{\mathbb{Z}}\{\boldsymbol{a}\}$. Since $f_{\boldsymbol{j}}(\boldsymbol{\omega}) = 0$, the Laurent polynomial $h_C = \boldsymbol{X}^{\boldsymbol{a}} - \boldsymbol{\omega}^{\boldsymbol{a}}$ will divide all $f_{\boldsymbol{j}}$ and, consequently, f. Multiplying by a monomial, we may assume that h_C is a factor of the desired form. Finally, noting that $H = H_{\mathrm{span}_{\mathbb{Z}}\{\boldsymbol{a}\}}$ and applying the result of the previous paragraph, we see that $C = \mathcal{H}(h_C)$. $\square$

3 Proof of Theorem 1.3

The proof of Theorem 1.3 is divided into several cases, in the similar way to Section 3 of Beukers and Smyth [3].

3.1 f with rational coefficients

Suppose that $f \in \mathbb{Q}[X_1, \dots, X_n]$, $n \geq 2$, is irreducible and has $L(f) = \mathbb{Z}^n$. We will show that the $m = 2^{n+1} - 1$ polynomials

$$f(\epsilon_1 X_1, \dots, \epsilon_n X_n), \quad \epsilon_i = \pm 1, \text{ not all } \epsilon_i = 1, \tag{3.1}$$

$$f(\epsilon_1 X_1^2, \dots, \epsilon_n X_n^2), \quad \epsilon_i = \pm 1, \tag{3.2}$$

satisfy all the conditions of the theorem.

Condition (i) clearly holds for all polynomials (3.1)–(3.2). Suppose now that f divides one of the polynomials (3.1). Let us consider the lattice

$$L_2 = \left\{ (x_1, \dots, x_n) \in \mathbb{Z}^n : \frac{1-\epsilon_1}{2} x_1 + \dots + \frac{1-\epsilon_n}{2} x_n \equiv 0 \mod 2 \right\},$$

with the same choice of ϵ_i. Note that $\det(L_2) = 2$ and thus $L_2 \subsetneq \mathbb{Z}^n$. Then, for some $z \in \mathbb{Z}^n$, we have $z + S_f \subset L_2$. Therefore, the lattice $L(f)$ cannot coincide with $\mathbb{Z}^n$, a contradiction. This argument also implies that the polynomials (3.1) are pairwise coprime. Next, if f divides a polynomial f' from (3.2) then, since $f' \in \mathbb{Q}[X_1^2, \dots, X_n^2]$, we have that each of the polynomials (3.1) also divides f'. Hence, $2^n \deg f \leq \deg f' = 2 \deg f$, so that $n = 1$, a contradiction. Consequently, the set of polynomials $f_1, \dots, f_m$ consists of all the polynomials (3.1)–(3.2). Then condition (ii) is satisfied.

It remains only to check that condition (iii) holds. Let $C = \boldsymbol{\omega} H$ be a torsion r-dimensional coset on the hypersurface $\mathcal{H} = \mathcal{H}(f)$. There is a root of unity ω such that $\boldsymbol{\omega} = (\omega^{i_1}, \dots, \omega^{i_n})$, where we may assume that $\gcd(i_1, \dots, i_n) = 1$, so that, in particular, not all of the $i_1, \dots, i_n$ are even. Next, we have

$$f(\omega^{i_1}, \dots, \omega^{i_n}) = 0$$

and, by part (ii) of Lemma 2.1, also at least one of the $2^{n+1} - 1$ equalities

$$f(\epsilon_1 \omega^{i_1}, \dots, \epsilon_n \omega^{i_n}) = 0, \quad \epsilon_i = \pm 1, \text{ not all } \epsilon_i = 1,$$

$$f(\epsilon_1 \omega^{2i_1}, \dots, \epsilon_n \omega^{2i_n}) = 0, \quad \epsilon_i = \pm 1,$$

holds. Therefore, the torsion point $\boldsymbol{\omega}$ lies on a hypersurface $\mathcal{H}' = \mathcal{H}(f')$, where f' is one of the polynomials $f_1, \dots, f_m$. This settles the case $r = 0$.

Suppose now that $r \geq 1$. We claim that the torsion coset C lies on $\mathcal{H}'$. To see this we observe that for all $\boldsymbol{j} \in \mathbb{Z}^r$ we have

$$f'_{\boldsymbol{j}}(\boldsymbol{\omega}) = f_{\boldsymbol{j}}(\omega^{p\,i_1}, \ldots, \omega^{p\,i_n}) = 0,$$

where p is the exponent from part (ii) of Lemma 2.1. Hence, by (2.6), C lies on $\mathcal{H}'$.

3.2 f with coefficients in $\mathbb{Q}^{\mathrm{ab}}$

We now define the polynomials $f_1, \ldots, f_m$ in the case of f having coefficients lying in a cyclotomic field. Let us choose N to be the smallest integer such that, for some roots of unity $\zeta_1, \ldots, \zeta_n$, the polynomial $f(\zeta_1 x_1, \ldots, \zeta_n x_n)$ has all its coefficients in $K = \mathbb{Q}(\omega_N)$, for ω_N a primitive Nth root of unity. Since for N odd $-\omega_N$ is a primitive $(2N)$th root of unity, we may assume either that N is odd or a multiple of 4.

We then replace f by this polynomial. When we have found the polynomials $f_1, \ldots, f_m$ for this new f, it is easy to go back and find those for the original f.

***N* odd.** Take σ to be an automorphism of K taking ω_N to ω_N^2. We keep the polynomials f_i that come from (3.1) and replace the polynomials that come from (3.2) by

$$f^{\sigma}(\epsilon_1 X_1^2, \ldots, \epsilon_n X_n^2), \quad \epsilon_i = \pm 1, \quad \text{not divisible by } f. \tag{3.3}$$

We then claim that any torsion coset of $\mathcal{H}(f)$ either lies on one of the $2^n - 1$ hypersurfaces defined by (3.1) or on one of the 2^n hypersurfaces defined by one of the polynomials (3.3). Take a torsion coset $C = (\omega_l^{i_1}, \ldots, \omega_l^{i_n})H$ of $\mathcal{H}(f)$, with $\gcd(i_1, \ldots, i_n) = 1$. If $4 \nmid l$, then we can extend σ to an automorphism of $K(\omega_l)$ which takes ω_l to one of $\pm\omega_l^2$. Therefore, the coset C also lies on a hypersurface defined by one of the polynomials (3.3). On the other hand, if $4 \mid l$, we put $4k = \operatorname{lcm}(l, N)$. Then the automorphism, τ say, of $K(\omega_l) = \mathbb{Q}(\omega_{4k})$ mapping $\omega_{4k} \mapsto \omega_{4k}^{2k+1}$ takes $\omega_l \mapsto \omega_l^{2k+1} = -\omega_l$ and $\omega_N \mapsto \omega_N^{2k+1} = \omega_N$. Thus, C lies on a hypersurface defined by one of the polynomials (3.1).

$4 \mid N$. We take the same coset C as in the previous case, again put $4k = \operatorname{lcm}(l, N)$, and use the same automorphism τ. Then τ takes $\omega_l \mapsto \omega_l^{2k}\omega_l = \pm\omega_l$ and $\omega_N \mapsto \omega_N^{2k}\omega_N = \pm\omega_N$. We now consider separately the four possibilities for these signs. Firstly, from the definition of k they cannot both be $+$ signs.

If

$$\tau(\omega_l) = \omega_l, \quad \tau(\omega_N) = -\omega_N,$$

then C also lies on $\mathcal{H}(f^{\tau})$. Note that $f^{\tau} \neq f$, by the minimality of N, so that they have a proper intersection.

If

$$\tau(\omega_l) = -\omega_l, \quad \tau(\omega_N) = \omega_N,$$

then C also lies on a hypersurface defined by one of the polynomials (3.1). As $L(f) = \mathbb{Z}^n$, each has proper intersection with f, as we saw in Section 3.1.

Finally, if

$$\tau(\omega_l) = -\omega_l, \quad \tau(\omega_N) = -\omega_N,$$

then C also lies on one of the hypersurfaces $\mathcal{H}(f_i^\tau)$, for f_i in (3.1). Suppose that for instance f and $f^\tau(-X_1, X_2, \ldots, X_n)$ have a common component, so that $f^\tau(-X_1, X_2, \ldots, X_n) = f(X_1, X_2, \ldots, X_n)$. Then we have

$$f(\omega_N X_1, X_2, \ldots, X_n)^\tau = f^\tau(-\omega_N X_1, X_2, \ldots, X_n) = f(\omega_N X_1, X_2, \ldots, X_n).$$

For any coefficient c of $f(\omega_N X_1, X_2, \ldots, X_n)$, write $c = a + \omega_N \mathrm{b}$, where $a, b \in \mathbb{Q}(\omega_N^2)$. Then $c^\tau = a - \omega_N b = c$, so that $b = 0$, $c \in \mathbb{Q}(\omega_N^2)$. Consequently, $f(\omega_N X_1, X_2, \ldots, X_n) \in \mathbb{Q}(\omega_N^2)[X_1, \ldots, X_n]$, contradicting the minimality of N. The same argument applies for other polynomials (3.1). Thus, C lies on one of $2^{n+1} - 1$ subvarieties defined by the polynomials (3.1) and the polynomials

$$f^\tau(\epsilon_1 X_1, \ldots, \epsilon_n X_n), \quad \epsilon_i = \pm 1.$$

3.3 f with coefficients in $\mathbb{C}$

Let K be the coefficient field of f. Suppose that K is not a subfield of $\mathbb{Q}^{\mathrm{ab}}$. Without loss of generality, assume that at least one coefficient of f is equal to 1 and choose an automorphism $\sigma \in \mathrm{Gal}(K/\mathbb{Q}^{\mathrm{ab}})$ which does not fix f. Then since all roots of unity belong to $\mathbb{Q}^{\mathrm{ab}}$, f and f^σ have the same torsion cosets. Further, f and f^σ have no common component. Thus, in this case we can take the set of f_i to be the single polynomial f^σ.

4 Proof of Theorem 1.1

The lemmas of the next two subsections will allow us to assume that $L(f) = \mathbb{Z}^n$.

4.1 $L(f)$ of rank less than n

Lemma 4.1. *Let $f \in \mathbb{C}[X_1, \ldots, X_n]$, $n \geq 2$, be a polynomial of (total) degree d. Suppose that $L(f)$ has rank r less than n. Then there exists $f^* \in \mathbb{C}[X_1, \ldots, X_r]$ of degree at most d such that $L(f^*)$ also has rank r and*

$$T_i^n(f) \leq T_{i-n+r}^r(f^*), \quad i = n-r, \ldots, n-1. \tag{4.1}$$

Proof. Multiplying f by a monomial, we will assume without loss of generality that $S_f \subset L(f)$. Then there exists an integer vector $\boldsymbol{s} = (s_1, \ldots, s_n) \in \mathrm{span}_{\mathbb{R}}^{\perp}(S_f)$ and we may assume that $s_n \neq 0$. Consider the integer lattice $A \subset \mathbb{Z}^n$ with the basis

$$\mathbf{A} = \begin{pmatrix} 1 & 0 & \ldots & 0 & s_1 \\ 0 & 1 & \ldots & 0 & s_2 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & s_{n-1} \\ 0 & 0 & \ldots & 0 & s_n \end{pmatrix}.$$

Observe that

$$f(X_1, \ldots, X_{n-1}, 1) = f(\boldsymbol{X}^{\boldsymbol{a}_1}, \ldots, \boldsymbol{X}^{\boldsymbol{a}_n}),$$

and, by Lemma 2.7, we have

$$T_i^n(f) \leq T_{i-1}^{n-1}(f(X_1, \ldots, X_{n-1}, 1)), \quad i = 1, \ldots, n-1.$$

Applying the same procedure to the polynomial $f(X_1, \ldots, X_{n-1}, 1)$ and so on, we will remove $n - r$ variables and get the desired polynomial f^*. □

4.2 $L(f)$ of rank n, $L(f) \subsetneq \mathbb{Z}^n$

Lemma 4.2. *Let $f \in \mathbb{C}[X_1, \ldots, X_n]$, $n \geq 2$, be an irreducible polynomial of degree d. Suppose that $L(f)$ has rank n and $L(f) \subsetneq \mathbb{Z}^n$. Then there exists an irreducible polynomial $f^* \in \mathbb{C}[X_1, \ldots, X_n]$ of degree at most $c_1(n, d) = n^2(n+1)!d$ such that $L(f^*) = \mathbb{Z}^n$ and*

$$T_0^n(f) = \det(L(f)) T_0^n(f^*), \tag{4.2}$$

$$T_i^n(f) \leq \det(L(f)) T_i^n(f^*), \quad i = 1, \ldots, n-1. \tag{4.3}$$

Proof. Since $S_f \subset dB_1^n$, we have $D(S_f) \subset dD(B_1^n) = 2dB_1^n$. Thus, multiplying f by a monomial, we may assume that f is a Laurent polynomial with $S_f \subset L(f) \cap 2dB_1^n$. Let $L^*(f)$ be the polar lattice for the lattice $L(f)$ and let $\mathbf{A}^* = (\boldsymbol{a}_1^*, \ldots, \boldsymbol{a}_n^*)$ be a basis of $L^*(f)$. Consider the map $\psi : L(f) \to \mathbb{Z}^n$ defined by

$$\psi(\boldsymbol{u}) = (\langle \boldsymbol{u}, \boldsymbol{a}_1^* \rangle, \ldots, \langle \boldsymbol{u}, \boldsymbol{a}_n^* \rangle).$$

The Laurent polynomial

$$f^*(\boldsymbol{X}) = \sum_{\boldsymbol{u} \in S_f} a_{\boldsymbol{u}} \boldsymbol{X}^{\psi(\boldsymbol{u})}$$

has $L(f^*) = \mathbb{Z}^n$. Observe that we have

$$f = f^*(\boldsymbol{X}^{\boldsymbol{a}_1}, \ldots, \boldsymbol{X}^{\boldsymbol{a}_n}). \tag{4.4}$$

Therefore, the polynomial f^* is irreducible and, by Lemma 2.7, the inequalities (4.3) hold. Note also that the equality (4.2) follows from (2.13).

Let us estimate the size of S_{f^*}. Recall that B_∞^n is the *polar reciprocal body* of B_1^n – see Theorem III of Ch. IV in Cassels [8]. Thus, by Theorem VI of Ch. VIII ibid., we have

$$\lambda_i(B_1^n, L(f))\lambda_{n+1-i}(B_\infty^n, L^*(f)) \le n!.$$

Noting that $\lambda_i(B_1^n, L(f)) \ge 1$, we get the inequality

$$\lambda_n(B_\infty^n, L^*(f)) \le n!. \tag{4.5}$$

Next, by Corollary of Theorem VII, Ch. VIII of Cassels [8], there exists a basis $\mathbf{A}^* = (\boldsymbol{a}_1^*, \ldots, \boldsymbol{a}_n^*)$ of the lattice $L^*(f)$ such that

$$\boldsymbol{a}_j^* \in \max\{1, j/2\}\lambda_j(B_\infty^n, L^*(f))B_\infty^n. \tag{4.6}$$

Combining the inequalities (4.5) and (4.6) we get the bound

$$\|\boldsymbol{a}_j^*\|_\infty \le \frac{n \cdot n!}{2}.$$

Then, by the definition of the Laurent polynomial f^*, we have

$$S_{f^*} \subset (\max_{1\le j\le n} \|\boldsymbol{a}_j^*\|_\infty) 2ndB_1^n \subset n^2 n! dB_1^n.$$

Thus, multiplying f^* by a monomial, we may assume that $f^* \in \mathbb{C}[X_1, \ldots, X_n]$ and

$$\deg(f^*) \le n^2(n+1)!d = c_1(n,d). \qquad \square$$

4.3 The case $L(f) = \mathbb{Z}^n$

Let

$$T(i,n,d) = \max_{\substack{f\in\mathbb{C}[X_1,\ldots,X_n] \\ \deg f\le d}} T_i^n(f), \quad i = 0, \ldots, n-1,$$

be the maximum number of maximal torsion i-dimensional cosets lying on a subvariety of $\mathbb{G}_{\mathrm{m}}^n$ defined by a polynomial of degree at most d.

Lemma 4.3. *Let $f \in \mathbb{C}[X_1, \dots, X_n]$, $n \geq 2$, be an irreducible polynomial of degree at most d with $L(f) = \mathbb{Z}^n$. Then*

$$T_0^n(f) \leq (2^{n+1} - 1)\Big(T(0, n-1, c_2(n,d)) \sum_{s=1}^{n-2} T(s, n-1, 2d^2) + d\,T(0, n-1, 2d^2)\Big), \tag{4.7}$$

$$T_1^n(f) \leq (2^{n+1} - 1)\Big(T(1, n-1, c_2(n,d)) \sum_{s=1}^{n-2} T(s, n-1, 2d^2) + T(0, n-1, 2d^2)\Big), \tag{4.8}$$

$$T_i^n(f) \leq (2^{n+1} - 1)T(i, n-1, c_2(n,d)) \sum_{s=i-1}^{n-2} T(s, n-1, 2d^2), \quad i = 2, \dots, n-2, \tag{4.9}$$

$$T_{n-1}^n(f) \leq 1, \tag{4.10}$$

where $c_2(n,d) = n(n+1)d + 2(n-1)(n^2-1)n!d^3$.

Proof. By Lemma 2.8, we immediately get the inequality (4.10). Assume now that $\mathcal{H}(f)$ contains no $(n-1)$-dimensional cosets. Applying Theorem 1.3 to the polynomial f, we obtain $m \leq 2^{n+1} - 1$ polynomials $f_1, f_2, \dots, f_m$ satisfying conditions (i)–(iii) of this theorem. For $1 \leq k \leq m$, put $g_k = \mathrm{Res}(f, f_k, X_n)$. By Theorem 1.3 (ii), the polynomials f and f_k have no common factor and thus $g_k \neq 0$. Recall also that g_k lies in the elimination ideal $\langle f, f_k\rangle \cap \mathbb{C}[X_1, \dots, X_{n-1}]$ and $\deg(g_k) \leq \deg(f)\deg(f_k) \leq 2d^2$.

Given a maximal i-dimensional torsion coset C on $\mathcal{H}(f)$, $i \leq n-2$, its orthogonal projection $\pi(C)$ into the coordinate subspace corresponding to the indeterminates $X_1, \dots, X_{n-1}$ is a torsion coset in $\mathbb{G}_{\mathrm{m}}^{n-1}$. Note that the coset $\pi(C)$ is either i- or $(i-1)$-dimensional. The proof of inequalities (4.7)–(4.9) is based on the following observation.

Lemma 4.4. *Suppose that $1 \leq k \leq m$, $1 \leq s \leq n-2$ and $0 \leq i \leq s+1$. Then for any maximal torsion s-dimensional coset D on the hypersurface $\mathcal{H}(g_k)$ of $\mathbb{G}_{\mathrm{m}}^{n-1}$, the number of maximal torsion i-dimensional cosets C on $\mathcal{H}(f)$ with $\pi(C) \subset D$ is at most $T(i, n-1, c_2(n,d))$.*

Proof. Let $D = \boldsymbol{\omega} H_B$, where B is a primitive sublattice of $\mathbb{Z}^{n-1}$ with rank $(B) = n-1-s$. By Corollary 2.4, applied to the subspace $\mathrm{span}_{\mathbb{R}}^{\perp}(B)$, there exists a basis

$\mathbf{A} = (\boldsymbol{a}_1, \dots, \boldsymbol{a}_{n-1})$ of the lattice $\mathbb{Z}^{n-1}$ such that $\boldsymbol{a}_1 \in B$ and its polar basis $\mathbf{A}^* = (\boldsymbol{a}_1^*, \dots, \boldsymbol{a}_{n-1}^*)$ satisfies the inequality (2.5). Let C be a maximal torsion i-dimensional coset on $\mathcal{H}(f)$ with $\pi(C) \subset D$. Observe that the coset D and, consequently, the coset C satisfy the equation

$$(X_1, \dots, X_{n-1})^{\boldsymbol{a}_1} = \omega, \tag{4.11}$$

with the root of unity $\omega = \boldsymbol{\omega}^{\boldsymbol{a}_1}$. The basis $\mathbf{A}$ of $\mathbb{Z}^{n-1}$ can be extended to the basis $\mathbf{B} = ((\boldsymbol{a}_1, 0), \dots, (\boldsymbol{a}_{n-1}, 0), \boldsymbol{e}_n)$ of $\mathbb{Z}^n$, where $(\boldsymbol{a}_i, 0)$ denotes the vector $(a_{i1}, \dots, a_{in-1}, 0)$ and $\boldsymbol{e}_n = (0, \dots, 0, 1)$. Let $(Y_1, \dots, Y_n)$ be the coordinates associated with $\mathbf{B}$. By Lemma 2.6, the coset $C^{\mathbf{B}}$ is a maximal i-dimensional torsion coset on $\mathcal{H}(f^{\mathbf{B}})$ and, by (4.11), it lies on the subvariety of $\mathcal{H}(f^{\mathbf{B}})$ defined by the equation $Y_1 = \omega$. Therefore, the orthogonal projection of the coset $C^{\mathbf{B}}$ into the coordinate subspace corresponding to the indeterminates $Y_2, \dots, Y_n$ is a maximal i-dimensional torsion coset on the hypersurface $\mathcal{H}(f^{\mathbf{B}}(\omega, Y_2 \dots, Y_n))$ of $\mathbb{G}_{\mathrm{m}}^{n-1}$. Here the polynomial $f^{\mathbf{B}}(\omega, Y_2, \dots, Y_n)$ is not identically zero. Otherwise the $(n-1)$-dimensional coset defined by (4.11) would lie on the hypersurface $\mathcal{H}(f)$.

The $(n-1-s)$-dimensional subspace $\mathrm{span}_{\mathbb{R}}(B)$ is generated by $n-1-s$ vectors of the difference set $D(S_{g_k})$ (see for instance the proof of Theorem 8 in [21] for details). Therefore,

$$\det(B) \le (\mathrm{diam}(S_{g_k}))^{n-1-s} < (4d^2)^{n-1-s},$$

where $\mathrm{diam}(\cdot)$ denotes the diameter of the set. It is well known (see, e.g., Bombieri and Vaaler [5, pp. 27–28]) that $\det(B) = \det(\mathrm{span}_{\mathbb{R}}^{\perp}(B) \cap \mathbb{Z}^{n-1})$. Hence, by (2.5), we have

$$S_{f^{\mathbf{B}}} \subset \Big(n \max_{1 \le j \le n-1} \|\boldsymbol{a}_j^*\|_\infty\Big) d B_1^n \subsetneq \Big(nd + 2n(n-1)\gamma_{n-1}^{\frac{n-1}{2}} \gamma_{n-1-s}^{\frac{1}{2}} d^3\Big) B_1^n.$$

Multiplying $f^{\mathbf{B}}$ by a monomial, we may assume that $f^{\mathbf{B}} \in \mathbb{C}[Y_1, \dots, Y_n]$. Now, observing that $\gamma_k^{k/2} \le k!$, we get

$$\deg(f^{\mathbf{B}}) < c_2(n, d).$$

Therefore, we have shown that the maximal torsion coset D can contain projections of at most $T_i^{n-1}(f^{\mathbf{B}}(\omega, Y_2 \dots, Y_n)) \le T(i, n-1, c_2(n, d))$ maximal torsion i-dimensional cosets of $\mathcal{H}(f)$. □

By part (iii) of Theorem 1.3, given a maximal torsion i-dimensional coset C on $\mathcal{H}(f)$, its projection $\pi(C)$ lies on $\mathcal{H}(g_k)$ for some $1 \le k \le m$. If $i \ge 2$, then the coset $\pi(C)$ has positive dimension, and Lemma 4.4 implies inequality (4.9). Suppose now that $i \le 1$. Let C be a maximal i-dimensional coset on $\mathcal{H}(f)$. The case when $\pi(C)$ lies in a torsion coset of positive dimension of one of the hypersurfaces $\mathcal{H}(g_k)$ is settled by Lemma 4.4. It remains only to consider the case when $\pi(C)$ is an isolated torsion point. The number of isolated torsion points $\boldsymbol{u}$ on $\mathcal{H}(f)$ whose projection $\pi(\boldsymbol{u})$ is an isolated torsion point on $\mathcal{H}(g_k)$ is at most $dT_0^{n-1}(g_k) \le dT(0, n-1, 2d^2)$. Now, each isolated torsion point on $\mathcal{H}(g_k)$ is the π-projection of at most one torsion 1-dimensional coset on $\mathcal{H}(f)$. These observations together with Lemma 4.4 imply the inequalities (4.7)–(4.8). □

4.4 Completion of the proof

Put $T(n,d) = \sum_{i=0}^{n-1} T(i,n,d)$. We will show that for $n \ge 2$

$$T(n,d) \le (2nd)^{n+1} T(n-1, n^{8+4n} d^2) T(n-1, n^{8+4n} d^3). \tag{4.12}$$

This inequality implies Theorem 1.1. Indeed, noting that, by (2.1), we have $T(2,d) \le 11d^2 + d$ and $N_{\mathrm{tor}}(\mathcal{H}(f)) \le T(n,d)$, we get from (4.12) the inequality (1.3).

Suppose that $f \in \mathbb{C}[X_1, \dots, X_n]$ is a polynomial of degree d. The lattice $L(f)$ clearly has n linearly independent points in the difference set $D(S_f)$ and $D(S_f) \subset dD(B_1^n) = 2dB_1^n$. Therefore, by Lemma 8 in Cassels [8, Ch. V], the lattice $L(f)$ has a basis lying in ndB_1^n. Since $B_1^n \subset B_2^n$, for each irreducible factor f' of f the inequality

$$\det(L(f')) \le (nd)^n$$

holds. Then, by Lemmas 4.1–4.3 applied to all irreducible factors of f, we have for all $0 \le i \le n-1$

$$\begin{aligned} T_i^n(f) \le\ & d(2^{n+1}-1)(nd)^n \\ & \times T(i, n-1, c_2(n, c_1(n,d))) T(n-1, 2(c_1(n,d))^2). \end{aligned} \tag{4.13}$$

To avoid painstaking estimates we simply observe that for $n \ge 3$ and for all d we have $n^{8+4n} d^2 > 2(c_1(n,d))^2$ and $n^{8+4n} d^3 > c_2(n, c_1(n,d))$. Then the inequality (4.13) implies (4.12).

5 Proof of Theorem 1.2

Lemma 5.1. *For $n \ge 2$, the inequality*

$$N_{\mathrm{tor}}(n,d) \le T(n,d) N_{\mathrm{tor}}(n-1, n^{2+n} d^2) \tag{5.1}$$

holds.

Proof. Let the variety $\mathcal{V}$ be defined by the polynomials $f = f_1, f_2, \dots, f_t$. Then any maximal torsion coset $\boldsymbol{\omega} H$ on $\mathcal{V}$ is contained in a maximal torsion coset $\boldsymbol{\omega} H'$ on the hypersurface $\mathcal{H}(f)$. Now, let $C = \boldsymbol{\omega} H_A$ with $\boldsymbol{\omega} = (\omega_1, \dots, \omega_n)$ be a maximal i-dimensional torsion coset on $\mathcal{H}(f)$ and suppose C does not lie on $\mathcal{V}$. By Corollary 2.4, applied to the subspace $\mathrm{span}_{\mathbb{R}}^{\perp}(A)$, there exists a basis $\mathbf{A} = (\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n)$ of the lattice $\mathbb{Z}^n$ such that $\boldsymbol{a}_1 \in A$ and its polar basis $\mathbf{A}^* = (\boldsymbol{a}_1^*, \boldsymbol{a}_2^*, \ldots, \boldsymbol{a}_n^*)$ satisfies the inequality (2.5). Let $(Y_1, \ldots, Y_n)$ be the coordinates associated with the basis $\mathbf{A}$. By (2.7), the coset $C^{\mathbf{A}}$ lies on the hypersurface of $\mathbb{G}_{\mathrm{m}}^n$ defined by the equation

$$Y_1 = \omega, \tag{5.2}$$

with $\omega = \boldsymbol{\omega}^{\boldsymbol{a}_1}$. Observe that for any torsion coset $\boldsymbol{\zeta} H_B \subset \boldsymbol{\omega} H_A$, the lattice A is a sublattice of the lattice B and $\boldsymbol{\zeta} = (\omega_1 x_1, \ldots, \omega_n x_n)$ for some $(x_1, \ldots, x_n) \in H_A$. Consequently, $\boldsymbol{\zeta} H_B$ also satisfies (5.2). Then the number of maximal torsion cosets on $\mathcal{V}$ that are subcosets of C is at most the number of maximal torsion cosets on the subvariety of $\mathbb{G}_{\mathrm{m}}^{n-1}$ defined by the equations

$$\begin{aligned} f_2^{\mathbf{A}}(\omega, Y_2, \ldots, Y_n) &= 0, \\ &\vdots \\ f_t^{\mathbf{A}}(\omega, Y_2, \ldots, Y_n) &= 0. \end{aligned}$$

Note that since $C \not\subseteq \mathcal{V}$, not all Laurent polynomials $f_i^{\mathbf{A}}(\omega, Y_2, \ldots, Y_n)$ are identically zero. The $(n-i)$-dimensional subspace $\mathrm{span}_{\mathbb{R}}(A)$ is spanned by $n-i$ vectors of the difference set $D(S_f)$. Therefore,

$$\det(A) \leq (\mathrm{diam}(S_f))^{n-i} < (2d)^{n-i}.$$

Note that $\det(A) = \det(\mathrm{span}_{\mathbb{R}}^{\perp}(A) \cap \mathbb{Z}^n)$. Hence, by (2.5), we have

$$S_{f_j^{\mathbf{A}}} \subset d\Big(n \max_{1 \leq j \leq n} \|\boldsymbol{a}_j^*\|_\infty\Big) B_1^n \subsetneq \Big(nd + n(n-1)\gamma_{n-1}^{\frac{n-1}{2}} \gamma_{n-i}^{\frac{1}{2}} d^2\Big) B_1^n$$

for $j = 2, \ldots, t$. Multiplying the Laurent polynomials $f_j^{\mathbf{A}}$ by a monomial, we may assume that $f_j^{\mathbf{A}} \in \mathbb{C}[Y_2, \ldots, Y_n]$. Noting that $\gamma_k^{k/2} \leq k!$, we get the inequalities

$$\deg(f_j^{\mathbf{A}}) < n(n+1)d + (n-1)(n^2-1)n!d^2, \quad j = 2, \ldots, t.$$

Finally, observe that for $n \geq 2$, $1 \leq i \leq n-1$ and for all d, we have

$$n^{2+n} d^2 > n(n+1)d + (n-1)(n^2-1)n!d^2. \qquad \square$$

By Theorem 1.1, $T(n,d) \leq c_1(n) d^{c_2(n)}$ and, consequently,

$$N_{\mathrm{tor}}(n,d) \leq c_1(n) d^{c_2(n)} N_{\mathrm{tor}}(n-1, n^{2+n} d^2).$$

Noting that $N_{\mathrm{tor}}(1,d) = T(1,d) = d$ we obtain the inequality (1.4).

6 The algorithm

Let $\mathcal{V}$ be an algebraic subvariety of $\mathbb{G}_{\mathrm{m}}^{n}$. In this section we will describe a new recursive algorithm that finds all maximal torsion cosets on $\mathcal{V}$. The algorithm consists of several steps that reduce the problem to finding maximal torsion cosets of a finite number of subvarieties of $\mathbb{G}_{\mathrm{m}}^{n-1}$. When $n = 2$, we can apply the algorithm of Beukers and Smyth [3].

6.1 Hypersurfaces

We first consider a hypersurface $\mathcal{H}$ defined by a polynomial $f \in \mathbb{C}[X_1, \dots, X_n]$ with $f = \prod h_i$, where h_i are irreducible polynomials. By Lemma 2.8, the $(n-1)$-dimensional torsion cosets on $\mathcal{H}$ will precisely correspond to the factors h_j of the form $\boldsymbol{X}^{\boldsymbol{u}_j} - \omega_j \boldsymbol{X}^{\boldsymbol{v}_j}$, where ω is a root of unity. Now we will assume without loss of generality that f is irreducible and $\mathcal{H}$ contains no torsion cosets of dimension $n-1$. Then we proceed as follows.

H1. The proofs of Lemmas 4.1, 4.2 and Theorem 1.3 are effective. Consequently, applying Lemmas 4.1 and 4.2, we may assume without loss of generality that $L(f) = \mathbb{Z}^n$. Next, applying Theorem 1.3, we get $m < 2^{n+1}$ polynomials $f_1, \dots, f_m$ satisfying conditions (i)–(iii) of this theorem.

H2. For $1 \le k \le m$, calculate $g_k = \mathrm{Res}(f, f_k, X_n)$. Find all isolated torsion points $\boldsymbol{\zeta}_1, \boldsymbol{\zeta}_2, \dots$ and all maximal torsion cosets $D_1, D_2, \dots$ of positive dimension on the hypersurfaces $\mathcal{H}(g_k)$ of $\mathbb{G}_{\mathrm{m}}^{n-1}$. For each coset $D_i = \boldsymbol{\eta}_i H_{B_i}$, take a primitive vector $\boldsymbol{a}_i \in B_i$ and put $\omega_i = \boldsymbol{\eta}_i^{\boldsymbol{a}_i}$.

H3. For each torsion point $\boldsymbol{\zeta}_i = (\zeta_{i1}, \dots, \zeta_{i\,n-1})$, if $f(\zeta_{i1}, \dots, \zeta_{i\,n-1}, X_n)$ is identically zero, then the coset

$$(\zeta_{i\,1}, \dots, \zeta_{i\,n-1}, t)$$

lies on $\mathcal{H}$. Otherwise, solving the polynomial equation $f(\zeta_{i1}, \dots, \zeta_{i\,n-1}, X_n)$ in X_n, we will find all torsion points $\boldsymbol{\zeta}$ on $\mathcal{H}$ with $\pi(\boldsymbol{\zeta}) = \boldsymbol{\zeta}_i$. When all torsion cosets of positive dimension on $\mathcal{H}$ are found, we can easily determine which of the torsion points $\boldsymbol{\zeta}$ are isolated.

H4. For each D_i, extend the vector $\boldsymbol{a}_i$ to a basis $\mathbf{B}_i = ((\boldsymbol{a}_i, 0), \boldsymbol{z}_2, \dots, \boldsymbol{z}_n)$ of $\mathbb{Z}^n$. Find all maximal torsion cosets $E_1, E_2, \dots$ on the hypersurface in $\mathbb{G}_{\mathrm{m}}^{n-1}$ defined by the polynomial $f^{\mathbf{B}_i}(\omega_i, Y_2, \dots, Y_n)$. For each $E_j = \boldsymbol{\rho}_j H_{P_j}$ say with $\boldsymbol{\rho}_j = (\rho_{j2}, \dots, \rho_{jn})$, put $\boldsymbol{\omega}_j = (\omega_i, \rho_{j2}, \dots, \rho_{jn})$ and consider the set $A_j = \{(z, p_2, \dots, p_n) : z \in \mathbb{Z},\ (p_2, \dots, p_n) \in P_j\}$. Now the cosets $(\boldsymbol{\omega}_j H_{A_j})^{\mathbf{B}_i^{-1}}$ are the maximal torsion cosets on $\mathcal{H}$.

6.2 General subvarieties

Suppose now that $\mathcal{V}$ is defined by the polynomials $f_1, \ldots, f_t \in \mathbb{C}[X_1, \ldots, X_n]$ when $t \geq 2$.

V1. Find all isolated torsion points $\boldsymbol{\zeta}_1, \boldsymbol{\zeta}_2, \ldots$ and all maximal torsion cosets $D_1, D_2, \ldots$ of positive dimension on the hypersurface $\mathcal{H}(f_1)$. Then the points $\boldsymbol{\zeta}_1, \boldsymbol{\zeta}_2, \ldots$, if on $\mathcal{V}$, are isolated torsion points on $\mathcal{V}$ as well.

V2. For each coset $D_i = \boldsymbol{\eta}_i H_{B_i}$, take a primitive vector $\boldsymbol{a}_i \in B_i$, put $\omega_i = \boldsymbol{\eta}_i^{\boldsymbol{a}_i}$ and extend the vector $\boldsymbol{a}_i$ to a basis $\mathbf{B}_i = (\boldsymbol{a}_i, \boldsymbol{z}_2, \ldots, \boldsymbol{z}_n)$ of $\mathbb{Z}^n$. Find all maximal torsion cosets $E_1, E_2, \ldots$ on the subvariety of $\mathbb{G}_{\mathrm{m}}^{n-1}$ defined by the polynomials $f_k^{\mathbf{B}_i}(\omega_i, Y_2, \ldots, Y_n)$, $k = 2, \ldots, t$. For each $E_j = \boldsymbol{\rho}_j H_{P_j}$ with $\boldsymbol{\rho}_j = (\rho_{j2}, \ldots, \rho_{jn})$, put $\boldsymbol{\omega}_j = (\omega_i, \rho_{j2}, \ldots, \rho_{jn})$ and

$$A_j = \{(z, p_2, \ldots, p_n) : z \in \mathbb{Z},\ (p_2, \ldots, p_n) \in P_j\}.$$

Now the cosets $(\boldsymbol{\omega}_j H_{A_j})^{\mathbf{B}_i^{-1}}$, along with the isolated torsion points found in step V1, are the maximal torsion cosets on $\mathcal{V}$.

The algorithm described clearly stops after a finite number of steps and the proofs of Theorems 1.1 and 1.2 show that the algorithm finds all maximal torsion cosets on $\mathcal{V}$. Furthermore, the constants $c_i(n, d)$ give explicit bounds for the degrees of the polynomials generated at each step.

Acknowledgments. The authors are very grateful to Professor Patrice Philippon and Professor Andrzej Schinzel for important comments and to Dr. Tristram De Piro for helpful discussions.

Bibliography

[1] I. Aliev, A. Schinzel and W. M. Schmidt, On vectors whose span contains a given linear subspace, *Monatsh. Math.* **144** (2005), no. 3, 177–191.

[2] F. Amoroso and S. David, Points de petite hauteur sur une sous-variété d'un tore, *Compositio Math.* **142** (2006), no. 3, 551–562.

[3] F. Beukers and C. J. Smyth, Cyclotomic points on curves, in: *Number Theory for the Millennium I (Urbana, IL, 2000)*, pp. 67–85, A. K. Peters, Natick, MA, 2002.

[4] E. Bombieri and W. Gubler, *Heights in Diophantine Geometry*, New Mathematical Monographs 4, Cambridge University Press, Cambridge, 2006.

[5] E. Bombieri and J. Vaaler, On Siegel's lemma, *Invent. Math.* **73** (1983), 11–32; Addendum, *ibid.* **75** (1984), 377.

[6] E. Bombieri and U. Zannier, Algebraic points on subvarieties of $\mathbb{G}_{\mathrm{m}}^{n}$, *Internat. Math. Res. Notices* 1995, no. 7, 333–347.

[7] R. J. Bradford and J. H. Davenport, Effective tests for cyclotomic polynomials, in: *Symbolic and Algebraic Computation (Rome, 1988)*, pp. 244–251, Lecture Notes in Computer Science 358, Springer-Verlag, Berlin, 1989.

[8] J. W. S. Cassels, *An Introduction to the Geometry of Numbers*, Grundlehren der mathematischen Wissenschaften 99, Springer-Verlag, Berlin, 1959.

[9] J. H. Conway and A. J. Jones, Trigonometric Diophantine equations (On vanishing sums of roots of unity), *Acta Arith.* **30** (1976), no. 3, 229–240.

[10] S. David and P. Philippon, Minorations des hauteurs normalisées des sous-variétés des tores, *Ann. Scuola Norm. Sup. Pisa IV* **28** (1999), 489–543; Erratum, *ibid.* **29** (2000), 729–731.

[11] S. David and P. Philippon, Minorations des hauteurs normalisées des sous-variétés des puissances des courbes elliptiques, *Intern. Math. Res. Papers* 2007, article ID rpm006, 113 pages.

[12] R. Dvornicich and U. Zannier, On sums of roots of unity, *Monatsh. Math.* **129** (2000), no. 2, 97–108.

[13] J-H. Evertse, The number of solutions of linear equations in roots of unity, *Acta Arith.* **89** (1999), no. 1, 45–51.

[14] M. Filaseta and A. Schinzel, On testing the divisibility of lacunary polynomials by cyclotomic polynomials, *Math. Comp.* **73** (2004), no. 246, 957–965.

[15] P. M. Gruber and C. G. Lekkerkerker, *Geometry of Numbers*, North-Holland, Amsterdam 1987.

[16] S. Lang, *Diophantine Geometry*, Interscience Tracts in Pure and Applied Mathematics 11, Interscience Publishers, New York, London, 1962.

[17] S. Lang, *Fundamentals of Diophantine Geometry*, Springer-Verlag, New York, 1983.

[18] M. Laurent, Equations diophantiennes exponentielles, *Invent. Math.* **78** (1984), no. 2, 299–327.

[19] P. Liardet, Sur une conjecture de Serge Lang, *C. R. Acad. Sci. Paris Sér. A* **279** (1974), 435–437.

[20] H. B. Mann, On linear relations between roots of unity, *Mathematika* **12** (1965), 107–117.

[21] J. McKee and C. J. Smyth, There are Salem numbers of every trace, *Bull. London Math. Soc.* **37** (2005), no. 1, 25–36.

[22] M. McQuillan, Division points on semi-abelian varieties, *Invent. Math.* **120** (1995), no. 1, 143–159.

[23] M. Newman, *Integral Matrices*, Academic Press, New York, London, 1972.

[24] G. Rémond, Sur les sous-variétés des tores, *Compositio Math.* **134** (2002), 337–366.

[25] W. M. Ruppert, Solving algebraic equations in roots of unity, *J. Reine Angew. Math.* **435** (1993), 119–156.

[26] P. Sarnak and S. Adams, Betti numbers of congruence groups, with an appendix by Ze'ev Rudnick, *Israel J. Math.* **88** (1994), no. 1–3, 31–72.

[27] H. P. Schlickewei, Equations in roots of unity, *Acta Arith.* **76** (1996), no. 2, 99–108.

[28] W. M. Schmidt, Heights of points on subvarieties of $\mathbb{G}_{\mathrm{m}}^n$, in: *Number Theory (Paris, 1993–1994)*, pp. 157–187, London Mathematical Society Lecture Note 235, Cambridge University Press, Cambridge, 1996.

[29] S. Zhang, Positive line bundles on arithmetic varieties, *J. Amer. Math. Soc.* **8** (1995), no. 1, 187–221.

Received February 1, 2008; revised May 12, 2010.

Author information

Iskander Aliev, School of Mathematics and Wales Institute of Mathematical and Computational Sciences, Cardiff University, Senghennydd Road, Cardiff CF24 4AG, UK.
E-mail: `alievi@cf.ac.uk`

Chris Smyth, School of Mathematics and Maxwell Institute for Mathematical Sciences, University of Edinburgh, Kings Buildings, Edinburgh EH9 3JZ, UK.
E-mail: `C.Smyth@ed.ac.uk`