

## FEWNOMIALS AND INTERSECTIONS OF LINES WITH REAL ANALYTIC SUBGROUPS IN $\mathbf{G}_m^n$

PAULA B. COHEN AND UMBERTO ZANNIER

### ABSTRACT

In this paper, the authors study intersections of a special class of curves with algebraic subgroups of the multiplicative group of complex dimension at least 2. They show how results of Khovanskii on fewnomials can be used to derive finiteness results and bounds for the degrees of algebraic points for such intersections from more general results on intersections of curves with non-algebraic subgroups. They thereby generalise their earlier results, and recover in some cases, using different methods, more uniform bounds than those given in related work of Bombieri, Masser and Zannier.

### 1. Introduction

This paper is motivated by the problem of intersecting curves with algebraic subgroups of the multiplicative group  $\mathbf{G}_m^n$  of complex dimension  $n \geq 2$ , which has been studied in [2]. A very special case was treated in [4] by completely different techniques which yielded more explicit results, and the present paper represents a natural generalisation of such methods. In particular, a new feature is that we apply results of Khovanskii [6] on fewnomials. This leads us to consider intersections of curves with more general subgroups which are not algebraic. Our results enable us in many cases to recover the finiteness results of [2, Theorem 2], and in these cases we obtain more uniform bounds. The cases where we do not recover the results of [2, Theorem 2] represent a limitation of the present method. For clarity, we study only a special class of curves, which are in fact lines, generalising the one of [4], but the method can be adapted to apply in a more general context. The true restriction of the method does not come from considering just lines, but rather from the appearance of the set  $S$  below.

More precisely, we study the curve  $X$  parametrised by

$$x_s = t + r_s, \quad \text{where } r_s \in \mathbf{Q}, r_s \neq r_{s'}, s \neq s', \quad (1.1)$$

and where the  $x_s$  for  $s = 1, \dots, n$  are coordinates in  $\mathbf{G}_m^n$ . Note that this curve is not contained in a translate of a proper algebraic subgroup of  $\mathbf{G}_m^n$ . This property is relevant for the finiteness statement of Corollary 1 below. We intersect  $X$  with non-algebraic subgroups  $G_V$  of  $\mathbf{G}_m^n$ , where  $V \subset \mathbf{R}^n$  is a real vector space and  $G_V$  is defined by the equations of the form

$$|x_1|^{\alpha_1} |x_2|^{\alpha_2} \cdots |x_n|^{\alpha_n} = 1, \quad (1.2)$$

with the real vectors  $(\alpha_1, \dots, \alpha_n)$  running through  $V$ . The real analytic subgroup  $G_V$  has real codimension twice the dimension of  $V$ . We apply results from real analytic geometry, in particular estimates for the number of solutions of systems of real equations of polynomial-exponential type as in [6]. Note that we expect,

for dimensional reasons, that generically  $X$  will intersect a translate of  $G_V$  only in a finite set when  $V$  has real dimension at least 2. Theorem 1 confirms that this expectation is fulfilled up to few exceptions: we shall see in Section 5 that such exceptions can nonetheless occur.

Our main result is as follows.

**THEOREM 1.** *There is a finite set  $S = S_X$  of vector spaces  $W \subset \mathbb{R}^n$ , defined over  $\mathbb{Q}$ , with the following property. Let  $V$  be a real vector space of dimension at least 2. Then there is a point  $P \in \mathbf{G}_m^n$  such that the set  $(X \cap P \cdot G_V)(\mathbb{C})$  has infinite cardinality if and only if  $V \subset W$  for some  $W \in S$ . If, for  $P \in \mathbf{G}_m^n$ , the cardinality of  $(X \cap P \cdot G_V)(\mathbb{C})$  is finite, then it is bounded above by  $2^{4n^2}$ .*

We have not attempted to obtain an optimal upper bound in Theorem 1. The method in any case gives a bound depending at least quadratically exponentially on  $n$ . We may effectively determine the equations of a suitable set  $S$  such that Theorem 1 holds, and this is useful for applications. Notice that Theorem 1 gives an upper bound for the cardinality of  $(X \cap G_V)(\mathbb{C})$ , when it is finite, which depends only on  $n$  but not on the height of  $X$ , and this is the main point, especially in view of the applications. For more general curves  $X$ , this bound should depend only on  $n$  and the degree of the curve. The set  $S = S_X$  may depend on the curve. However, the proof will show that it is contained in a finite set of subspaces which are independent of  $X$ .

**PROPOSITION 1.** *Given a curve  $X$  parametrised as in equation (1.1), it is possible to effectively determine a suitable set  $S$  as in Theorem 1, such that the following holds. To each  $W \in S$ , we associate the lattice  $L_W = W \cap \mathbb{Z}^n$ . Then  $\text{Vol}(W/L_W) \leq (16n^2)^n$ .*

Here  $\text{Vol}(W/L_W)$  denotes the euclidean volume of a fundamental region for  $L_W$  in  $W$ . The effective procedure will be described in Section 4, in the course of the proof of Proposition 1. It allows us to check whether one can implement the applications described by our Theorem 2 and Proposition 2 below. Any vector space  $W$  defined over  $\mathbb{Q}$  determines a subtorus  $\Gamma_W$ , and conversely, any subtorus  $\Gamma_W$  determines a vector space  $W$  defined over  $\mathbb{Q}$ . This enables us to deduce the following result directly from Theorem 1.

**THEOREM 2.** *Let  $S$  be a finite set with the properties of Theorem 1, and consider the corresponding tori  $\Gamma_W$ , where  $W \in S$ . Let  $H$  be an algebraic subgroup of  $\mathbf{G}_m^n$  of codimension at least 2. Then either  $\Gamma_W \subset H$  for some  $W \in S$ , or the points of  $(X \cap H)(\overline{\mathbb{Q}})$  are of degree bounded above by  $2^{4n^2}$ .*

Recall the result of [2, Theorem 1], which states that the absolute height of the points in  $(X \cap H)(\overline{\mathbb{Q}})$  is bounded independently of  $H$ . This, together with Theorem 2, implies the following corollary.

**COROLLARY 1.** *In Theorem 2, if  $\Gamma_W \not\subset H$  for any  $W \in S$ , then the points of  $(X \cap H)(\overline{\mathbb{Q}})$  lie in a finite set which can be chosen independently of  $H$ .*

We compare this to [2, Theorem 2], which implies that for any curve  $X$  not contained in a translate of a proper algebraic subgroup, we may omit in Corollary 1

the condition ‘if  $\Gamma_W \not\subset H$  for any  $W \in S$ ’. On the other hand, the method of proof in that case gives a bound for the degree of the field of rationality of the points in  $(X \cap H)(\overline{\mathbb{Q}})$  which is independent of  $H$  but which depends on the height of the curve  $X$ .

**PROPOSITION 2.** *When  $X$  is such that we may choose the spaces of the set  $S$  of Theorem 1 all to be of dimension 2, then for all subgroups  $H$  of  $\mathbf{G}_m^n$  the points of  $(X \cap H)(\overline{\mathbb{Q}})$  are of degree bounded above by  $2^{4n^2}$  and, moreover, lie in a finite set which can be chosen independently of  $H$ .*

## 2. A result on fewnomials

Let  $P$  be a fixed point of  $\mathbf{G}_m^n$ . We begin by stating a result of [6]. For  $i = 1, \dots, l$ , let  $P_i \in \mathbb{R}[W_1, \dots, W_l, Y_1, \dots, Y_k]$  be polynomials of degree  $m_i$ , and define the functions of real variables

$$S_i(w_1, \dots, w_l) = P_i \left( w_1, \dots, w_l, \exp \left( \sum_{j=1}^l c_{1j} w_j \right), \dots, \exp \left( \sum_{j=1}^l c_{kj} w_j \right) \right), \quad (2.1)$$

with  $c_{nj} \in \mathbb{R}$ ,  $n = 1, \dots, k$  and  $j = 1, \dots, l$ . We consider the system,

$$S_i(w_1, \dots, w_l) = 0, \quad \text{where } i = 1, \dots, l. \quad (2.2)$$

A solution of the system (2.2) is called *degenerate* if it is a zero of the jacobian determinant  $|(\partial S_i)/(\partial w_j)|$ .

**PROPOSITION 3** ([6, p. 12]). *The number of non-degenerate solutions of the system*

$$S_i(w_1, \dots, w_l) = 0, \quad \text{where } i = 1, \dots, l$$

*is finite and of cardinality at most  $m_1 \dots m_l ((\sum_{i=1}^l m_i) + 1)^k 2^{k(k-1)/2}$ .*

We reformulate the problem introduced in Section 1 so as to apply this proposition to prove Theorem 1. As in the statement of that theorem, let  $V$  be a real vector space of dimension at least 2, and choose two linearly independent vectors  $\alpha = (\alpha_1, \dots, \alpha_n)$ ,  $\beta = (\beta_1, \dots, \beta_n) \in \mathbb{R}^n$  in  $V$ . Let  $P \in \mathbf{G}_m^n$ . Points of the intersection  $X \cap P \cdot G_V$  give rise to solutions of simultaneous equations of the form

$$|t + r_1|^{\alpha_1} \cdots |t + r_n|^{\alpha_n} = c_\alpha, \quad |t + r_1|^{\beta_1} \cdots |t + r_n|^{\beta_n} = c_\beta, \quad (2.3)$$

for certain positive real constants  $c_\alpha$  and  $c_\beta$ . We set  $l = n + 2$  and  $k = n$ , and we make the substitutions

$$t = w_{n+1} + \sqrt{-1}w_{n+2} \quad (2.4)$$

and

$$\exp(w_s) = |t + r_s|^2 = (w_{n+1} + r_s)^2 + w_{n+2}^2, \quad \text{where } s = 1, \dots, n. \quad (2.5)$$

If  $t$  satisfies equation (2.3), then using equation (2.5) we see that

$$\exp \left( \sum_{s=1}^n \alpha_s w_s \right) = c_\alpha^2, \quad \exp \left( \sum_{s=1}^n \beta_s w_s \right) = c_\beta^2.$$

To rewrite the system (2.3) in the form of the system  $S_i = 0$  of Proposition 3, we

make the following choice:

$$\begin{aligned}
P_s(W_1, \dots, W_{n+2}, Y_1, \dots, Y_n) &= Y_s - (W_{n+1} + r_s)^2 - W_{n+2}^2, \quad \text{where } s = 1, \dots, n, \\
P_{n+1}(W_1, \dots, W_{n+2}, Y_1, \dots, Y_n) &= \sum_{s=1}^n \alpha_s W_s - 2 \log(c_\alpha), \\
P_{n+2}(W_1, \dots, W_{n+2}, Y_1, \dots, Y_n) &= \sum_{s=1}^n \beta_s W_s - 2 \log(c_\beta). \tag{2.6}
\end{aligned}$$

The  $S_i$ ,  $i = 1, \dots, n+2$  are obtained by substituting  $\exp(w_s)$  for  $Y_s$ ,  $s = 1, \dots, n$  in the above polynomials, and the resulting equations  $S_i = 0$  are equivalent to equations (2.3) and (2.5). Throughout, the variables  $w_s$  run over the reals. We remark that the upper bound for the number of non-degenerate solutions of the system  $S_i = 0$ , where  $i = 1, \dots, n+2$ , is, by Proposition 3, given by  $(2n+3)^n 2^{n(n+1)/2}$ . To prove Theorem 1, we must therefore deal only with the degenerate solutions.

### 3. The degenerate solutions and a proof of Theorem 1

Recall from Section 2 that the degenerate solutions are given by the zeros of the jacobian of the system  $S_i = 0$ , where  $i = 1, \dots, n+2$ . This jacobian  $J = J(W_1, \dots, W_{n+2})$  is given up to a non-zero constant explicitly by the determinant of the following matrix.

$$\begin{pmatrix}
e^{W_1} & 0 & \dots & 0 & W_{n+1} + r_1 & W_{n+2} \\
0 & e^{W_2} & \dots & 0 & W_{n+1} + r_2 & W_{n+2} \\
\dots & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots \\
0 & 0 & \dots & e^{W_n} & W_{n+1} + r_n & W_{n+2} \\
\alpha_1 & \alpha_2 & \dots & \alpha_n & 0 & 0 \\
\beta_1 & \beta_2 & \dots & \beta_n & 0 & 0
\end{pmatrix} \tag{3.1}$$

Recall from Section 2 that  $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n)$  and  $\beta = (\beta_1, \beta_2, \dots, \beta_n)$  are linearly independent vectors in  $V$ . For  $i, j = 1, \dots, n$ , let  $\Delta_{ij}$  be the determinant of the  $2 \times 2$  matrix

$$\begin{pmatrix}
\alpha_i & \alpha_j \\
\beta_i & \beta_j
\end{pmatrix}.$$

Then we find by the Laplace expansion along the last two rows that

$$J = \sum_{i < j} \pm \Delta_{ij} (r_i - r_j) W_{n+2} \exp \left( \sum_{s \neq i, j} W_s \right).$$

We use equation (2.5) to replace the exponentials by quadratic polynomials in  $w_{n+1}$  and  $w_{n+2}$ . Therefore, the jacobian  $J$  restricted to the corresponding points equals the restriction to  $(w_{n+1}, w_{n+2})$  of a polynomial function  $F = F(W_{n+1}, W_{n+2})$  given by

$$F = \sum_{i < j} \pm \Delta_{ij} (r_i - r_j) W_{n+2} \prod_{s \neq i, j} ((W_{n+1} + r_s)^2 + W_{n+2}^2). \tag{3.2}$$

We now show that the polynomial  $F$  is not identically zero. Assume the contrary. Let  $l \in \{1, \dots, n\}$  and substitute  $W_{n+2} = \sqrt{-1}(W_{n+1} + r_l)$  into  $F$ .

We have the resulting equation:

$$0 = \sum_{j \neq l} \pm \Delta_{lj}(r_l - r_j) \prod_{s \neq \{l, j\}} (r_s - r_l)(2W_{n+1} + r_l + r_s).$$

We then substitute  $W_{n+1} = (-r_l - r_m)/2$  for a given  $m \neq l \in \{1, \dots, n\}$ , and we deduce that we must have  $\Delta_{lm} = 0$ . This works for any  $l, m \in \{1, \dots, n\}$ . Moreover, not all the  $\Delta_{lm}$  can vanish, since  $(\alpha_1, \alpha_2, \dots, \alpha_n)$  and  $(\beta_1, \beta_2, \dots, \beta_n)$  are independent. We therefore deduce a contradiction, so that the polynomial  $F$  cannot be identically zero.

Let  $Q = (w_1, \dots, w_n, w_{n+1}, w_{n+2})$  be a degenerate solution of the system of Section 2, derived from equation (2.6) and equivalent to equations (2.3) and (2.5). For ease of notation, we put  $(U, V) = (W_{n+1}, W_{n+2})$  and  $(u, v) = (w_{n+1}, w_{n+2})$ . Let  $f = f(U, V)$  be an irreducible factor of  $F(U, V)$  over the reals which vanishes at the point  $(u, v)$  corresponding to  $Q$ .

From now on we assume that  $f$  is fixed, and we estimate the corresponding number of possibilities for  $Q$ . We must therefore at the end multiply our estimates by the number of possibilities for  $f$ , which is at most the degree of  $F$ , namely at most  $2n - 3$ . Suppose first that  $f$  is singular at  $(u, v)$ . Then by Bezout's theorem we find that the number of possibilities for  $(u, v)$  is at most  $(2n - 4)(2n - 3)$ . Therefore, we suppose that  $f$  is non-singular at  $(u, v)$ . Our point  $(u, v)$  satisfies  $f(u, v) = 0$  in addition to the equations  $S_i = 0$ , for  $i = 1, \dots, n + 2$ , derived from equation (2.6).

We may consider the system given by any  $n + 2$  of these  $n + 3$  equations, and apply to it Proposition 3 of Section 2. For each of these  $n + 3$  systems, we can thereby bound the number of non-degenerate solutions. Overall, the number of non-degenerate solutions, once we multiply through by the  $(2n - 3)$  to allow for the possibilities for  $f$ , is bounded above by

$$((n + 2)(2n - 3)(4n - 1)^n + (2n + 3)^n)2^{n(n+1)/2}(2n - 3) + (2n - 4)(2n - 3)^2.$$

We next assume that the solution is degenerate for all the  $n + 3$  systems derived from a given  $f$ . This means that the matrix

$$\begin{pmatrix} e^{W_1} & 0 & \dots & 0 & U + r_1 & V \\ 0 & e^{W_2} & \dots & 0 & U + r_2 & V \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & e^{W_n} & U + r_n & V \\ \alpha_1 & \alpha_2 & \dots & \alpha_n & 0 & 0 \\ \beta_1 & \beta_2 & \dots & \beta_n & 0 & 0 \\ 0 & 0 & \dots & 0 & \partial f / \partial U & \partial f / \partial V \end{pmatrix} \quad (3.3)$$

has less than maximal rank at the point  $Q = (w_1, \dots, w_n, u, v)$ . As before, we may express each of the subdeterminants of order  $n + 2$  evaluated at the point  $Q$  as the value of a polynomial function in  $U$  and  $V$  which depends only on  $f$ . The degree of this polynomial function is at most  $4n - 7$  (in fact, it may even vanish). Suppose first that not all of these polynomials are divisible by  $f$ . Then since  $Q$  is a zero both of  $f$  and of all the polynomials, by an application of Bezout's theorem, we deduce that our point has at most  $(2n - 3)(4n - 7)^2$  possibilities. Therefore, combining this with our previous estimate for the non-degenerate solutions, we so far have an upper

bound for the number of solutions given by

$$\begin{aligned} & ((n+2)(2n-3)(4n-1)^n + (2n+3)^n)2^{n(n+1)/2}(2n-3) \\ & \quad + (2n-4)(2n-3)^2 + (4n-7)^2(2n-3)^2. \end{aligned}$$

This is clearly bounded above by  $2^{4n^2}$  (which is far from optimal), which corresponds to the bound in the statement of Theorem 1. In fact, we shall show that the remaining solutions, if any, are not isolated. We therefore in this case have infinitely many of them, which we now analyse in more detail.

We may therefore assume that  $f$  divides all the polynomials coming from the subdeterminants of the matrix (3.3), and this for all pairs of linearly independent vectors  $\alpha$  and  $\beta$  in  $V$ , one of which we fix. We shall show that we are then in the situation described in the first part of Theorem 1.

In a neighbourhood of the point  $(u, v)$ , we parametrise the curve  $f(U, V) = 0$  by  $U = \mu(T)$ ,  $V = v(T)$  where  $\mu$  and  $v$  are smooth functions in a neighbourhood of  $T = 0$ . We have  $\mu(0) = u$  and  $v(0) = v$ . We may choose  $\mu$  and  $v$  such that, in a neighbourhood of  $T = 0$ , not both  $\mu'(T)$  and  $v'(T)$  vanish, by appealing to the implicit function theorem. We have

$$\mu'(T)\frac{\partial f}{\partial U}(\mu(T), v(T)) + v'(T)\frac{\partial f}{\partial V}(\mu(T), v(T)) = 0. \quad (3.4)$$

For every point in a small neighbourhood of  $T = 0$ , define the  $(n+3)$  by  $(n+2)$  matrix  $M(T)$  as the matrix obtained from that of (3.3) by substituting

$$U = \mu(T), \quad V = v(T) \quad (3.5)$$

and

$$\exp(W_s(T)) = (\mu(T) + r_s)^2 + v^2(T), \quad \text{where } s = 1, \dots, n. \quad (3.6)$$

We remark that the entries of our matrix are smooth functions of  $T$  near  $T = 0$ . For all such  $T$ , the rank is less than  $(n+2)$ , so that there is a non-zero vector orthogonal to all the rows, which we denote by  $\lambda(T) = (\lambda_1(T), \dots, \lambda_{n+2}(T))$ . Since it is in particular orthogonal to the last row, and since the last row is non-zero for  $T$  near to zero, we see from equation (3.4) that  $(\lambda_{n+1}(T), \lambda_{n+2}(T))$  is proportional to  $(\mu'(T), v'(T))$ , and in fact we may assume that they are equal after multiplying  $\lambda(T)$  by a non-zero constant. From the orthogonality of  $\lambda(T)$  to the first  $n$  rows, we obtain that

$$\lambda_s(T)e^{W_s(T)} + \mu'(T)(\mu'(T) + r_s) + v'(T)v(T) = 0, \quad \text{where } s = 1, \dots, n.$$

Differentiating equation (3.6), we find that in fact

$$\lambda_s(T) = -\frac{1}{2}W'_s(T), \quad \text{where } s = 1, \dots, n.$$

Finally, since  $\lambda(T)$  is orthogonal to the  $(n+1)$ st and  $(n+2)$ nd rows, we have

$$\sum_{s=1}^n \alpha_s W'_s(T) = \sum_{s=1}^n \beta_s W'_s(T) = 0, \quad (3.7)$$

so that there are constants  $C_\alpha, C_\beta \neq 0$  such that

$$\prod_{s=1}^n \exp(W_s(T))^{z_s} = C_\alpha$$

and

$$\prod_{s=1}^n \exp(W_s(T))^{\beta_s} = C_\beta.$$

Putting  $T = 0$ , we find that  $C_\alpha = c_\alpha$  and  $C_\beta = c_\beta$ . By using equation (3.6), we write the last two equations as

$$\prod_{s=1}^n ((\mu(T) + r_s)^2 + v^2(T))^{\alpha_s} = c_\alpha, \quad \text{and} \quad \prod_{s=1}^n ((\mu(T) + r_s)^2 + v^2(T))^{\beta_s} = c_\beta. \quad (3.8)$$

Let  $g = g(U, V)$  be an irreducible factor over  $\mathbf{C}$  of  $f(U, V)$ , vanishing at the points  $(\mu(T), v(T))$  in a neighbourhood of  $T = 0$ . (Note that  $f(U, V)$  may not be absolutely irreducible). Let  $\mathcal{C}$  be a non-singular model of the curve corresponding to  $g$ . The total degree of  $g$  is at most  $2n - 3$ . Consider the rational functions on the curve  $\mathcal{C}$  given for  $s = 1, \dots, n$  by

$$\varphi_s(U, V) = (U + r_s)^2 + V^2.$$

By equations (3.6) and (3.7), and as  $\alpha$  and  $\beta$  can be any two linearly independent vectors in  $V$ , we have

$$\sum_{s=1}^n \gamma_s \frac{(d/dT)\varphi_s}{\varphi_s}(\mu(T), v(T)) = 0,$$

for all vectors  $\gamma = (\gamma_s)_{s=1}^n$  in  $V$  and for all  $T$  in a neighbourhood of  $T = 0$ . This implies the global relation among differentials on  $\mathcal{C}$  given by

$$\sum_{s=1}^n \gamma_s \frac{d\varphi_s}{\varphi_s} = 0 \quad (3.9)$$

for all  $\gamma \in V$ . For convenience, we give the following standard lemma.

LEMMA 1. *Consider the real vector space*

$$\tilde{V} = \left\{ (\delta_1, \dots, \delta_n) \in \mathbb{R}^n : \sum_{s=1}^n \delta_s \frac{d\varphi_s}{\varphi_s} = 0 \right\}.$$

Then  $\tilde{V}$  is defined by linear equations over  $\mathbf{Q}$ .

*Proof.* For  $R \in \mathcal{C}(\mathbf{C})$  and  $s = 1, \dots, n$ , we denote by  $m_R(\varphi_s)$  the multiplicity of  $\varphi_s$  at  $R$ . Consider the vector space

$$Z = \left\{ (\delta_1, \dots, \delta_n) \in \mathbb{R}^n : \sum_{s=1}^n \delta_s m_R(\varphi_s) = 0, R \in \mathcal{C}(\mathbf{C}) \right\}.$$

We observe that  $Z$  is defined over  $\mathbf{Q}$ . Looking locally at its defining equations, we see that  $\tilde{V} \subset Z$ . Moreover, the converse inclusion is also true. To see this, let  $(\delta_1^*, \dots, \delta_n^*) \in \mathbb{Z}^n \cap Z$ . Then the rational function on  $\mathcal{C}$  defined by  $\varphi = \prod_{s=1}^n \varphi_s^{\delta_s^*}$  has no zeros or poles. Indeed, by the definition of  $Z$ , we see that  $\varphi$  has vanishing multiplicity at every point of  $\mathcal{C}$ . Therefore  $\varphi$  is constant, and so  $d\varphi/\varphi = 0$ . This is equivalent to

$$\sum_{s=1}^n \delta_s^* \frac{d\varphi_s}{\varphi_s} = 0;$$

that is,  $(\delta_1^*, \dots, \delta_n^*) \in \tilde{V}$ . As  $Z$  has a basis made up of vectors in  $\mathbb{Z}^n$ , we see that  $Z \subset \tilde{V}$  as required. Hence  $\tilde{V} = Z$ , and so  $\tilde{V}$  is defined over  $\mathbb{Q}$ .  $\square$

We define the set  $S$  of vector spaces of the statement of Theorem 1 as the set of these  $\tilde{V}$  arising in this way. Observe that  $V \subset \tilde{V}$  for all  $\tilde{V} \in S$  by equation (3.9) and the definition of  $\tilde{V}$ . We now show that this set is finite. Continuing with the notations of the proof of Lemma 1, the polynomial  $g$  to which the curve  $\mathcal{C}$  corresponds has degree bounded above by  $2n - 3$ . Recall that  $\varphi_s = (U + r_s)^2 + V^2$ . The lattice  $\tilde{L} = \tilde{V} \cap \mathbb{Z}^n$  is given by

$$\tilde{L} = \{m_R = (m_R(\varphi_1), \dots, m_R(\varphi_n)) : R \in \mathcal{C}(\mathbb{C})\}^{\text{orth}}.$$

We recall that the degree  $\deg(\psi)$  of a rational function  $\psi$  on  $\mathcal{C}$  is the sum of the orders of its poles. We have

$$\sum_{R \in \mathcal{C}(\mathbb{C})} |m_R(\varphi_s)| = 2 \deg(\varphi_s) \leq 8 \deg(g) \leq 8(2n - 3). \quad (3.10)$$

We have used here the fact that  $\deg(\varphi_s) \leq 2(\deg(U) + \deg(V))$  and  $\deg(U), \deg(V) \leq \deg(g)$ . On summing inequality (3.10) over all  $s = 1, \dots, n$ , we deduce that

$$\sum_{R \in \mathcal{C}(\mathbb{C})} \|m_R\| \leq 8n(2n - 3), \quad (3.11)$$

where  $\|\cdot\|$  is the supremum norm. We remark that inequality (3.11) shows that the number of lattices  $\tilde{L}$  obtained in this way, and hence the cardinality of  $S$ , is finite and is bounded above by a function of  $n$  only. This completes the proof of the ‘only if’ part of Theorem 1.

To prove the ‘if’ part, we start by observing that for  $l = (l_1, \dots, l_n) \in \tilde{L}$ , the function  $\varphi_1^{l_1} \dots \varphi_n^{l_n}$  is a constant  $c_l$  on  $\mathcal{C}$ . Recall that  $\mathcal{C}$  contains the infinitely many real points given by equation (3.5), and hence  $c_l$  is real and positive. In fact, we claim that there exist real positive constants  $c_1, \dots, c_n$  such that

$$c_l = c_1^{l_1} \dots c_n^{l_n}, \quad \text{for all } l = (l_1, \dots, l_n) \in \tilde{L}. \quad (3.12)$$

To see this, it suffices to show that it holds for a basis of  $\tilde{L}$ . This reduces to solving a linear system of the form

$$\log c_l = l_1 x_1 + \dots + l_n x_n,$$

where  $l$  runs over the elements of a basis of  $\tilde{L}$  and the  $x_i$  are the unknowns. We then set, for a given solution,  $c_i = \exp(x_i)$ , where  $i = 1, \dots, n$ . This gives a solution of equation (3.12).

We now select any complex numbers  $q_1, \dots, q_n$  such that  $|q_i| = c_i$ , where  $i = 1, \dots, n$ . Observe that the set  $X \cap Q \cdot G_{\tilde{V}}$  has infinite cardinality. Indeed, it contains the points of  $X$  parametrised by  $t = \mu(T) + \sqrt{-1}v(T)$  introduced above. We conclude that for all  $W \in S$ , there exists a  $Q \in \mathbf{G}_m^n$  such that

$$|X \cap Q \cdot G_W| = \infty. \quad (3.13)$$

Now, if a vector space  $V$  is contained in  $W \in S$ , then  $G_W \subset G_V$ , so that by equation (3.13) the set  $X \cap Q \cdot G_V$  has infinite cardinality. This is precisely the ‘if’ part of the statement of Theorem 1.

This completes the proof of Theorem 1.

We end this section with the following remark. The proof of Theorem 1 shows in fact that the number of isolated points in  $(X \cap P \cdot G_V)(\mathbb{C})$  is bounded above by  $2^{4n^2}$ .

#### 4. Proofs of the remaining results

*Proof of Proposition 1.* We begin by bounding the volume of a lattice  $L_W = W \cap \mathbb{Z}^n$  for  $W \in S$ . By the arguments of Section 3, there exists a basis  $w_1, \dots, w_r$  for  $L_W^{\text{orth}}$  such that

$$\sum_{i=1}^r \|w_i\| \leq 8n(2n-3). \quad (4.1)$$

From this we deduce the rather crude bound (see also [1]),

$$\text{vol}(W/L_W) = \text{vol}(W/L_W^{\text{orth}}) \leq \prod_{i=1}^r \|w_i\| \leq (16n^2)^n. \quad (4.2)$$

As stated in Proposition 1, the set  $S$  may be effectively determined. Recall that we have  $W \in S$  if and only if there exists a  $Q \in \mathbf{G}_m^n$  such that  $X \cap Q \cdot G_W$  is infinite. The proof of Theorem 1 given in Section 3 shows that we have a corresponding lattice  $L_W$  with volume bounded as in inequality (4.2). For each of the finitely many lattices  $L$  satisfying this bound, we check whether the corresponding vector space is in  $S$  as follows. Let  $r$  be the rank of  $L$ , and pick a basis of  $L$ . For a vector  $l \in L$ , where  $l = (l_1, \dots, l_n)$ , we consider the function

$$\psi = \psi(U, V) = \phi_1^{l_1} \dots \phi_n^{l_n}$$

for  $\phi_s = (U + r_s)^2 + V^2 \in \mathbb{Q}(U, V)$ . Denote  $\psi_1, \dots, \psi_r$  the functions obtained in this way from the chosen basis of  $L$ . From the proof of Theorem 1 given in Section 3, it is clear that the vector space generated by  $L$  will belong to  $S$  if and only if there are real positive constants  $c_1, \dots, c_r$  such that the zero locus of the rational functions  $\psi_j - c_j$ , for  $j = 1, \dots, r$  in  $U, V$ , share a common component. By elimination theory, it follows that the set of non-zero complex constants  $c_1, \dots, c_r$  such that this holds form an effectively determined algebraic set of dimension at most 1. By using, for example, [3], we may effectively find whether this algebraic set contains real positive points.  $\square$

*Proof of Theorem 2 and Corollary 1.* Let  $H$  be an algebraic subgroup of  $\mathbf{G}_m^n$  of codimension at least 2. Then  $H$  corresponds to a lattice  $L$  and to a vector space  $V$  defined over  $\mathbb{Q}$ . Clearly,  $H \subset G_V$ . If  $V \notin S$ , then  $X \cap H$  is finite and bounded above by  $2^{4n^2}$ . But if  $P \in (X \cap H)(\overline{\mathbb{Q}})$ , then so are its conjugates over  $\mathbb{Q}$ , since both  $X$  and  $H$  are defined over  $\mathbb{Q}$ . Therefore the degree of  $P$  is also bounded above by  $2^{4n^2}$ . This proves Theorem 2. Combining this with [2, Theorem 1], we deduce that the absolute height of the points in  $(X \cap H)(\overline{\mathbb{Q}})$  is bounded independently of  $H$ , and the result of Corollary 1 follows from Northcott's theorem.  $\square$

*Proof of Proposition 2.* By assumption, for all  $W \in S$  the corresponding torus  $\Gamma_W$  has codimension 2 in  $\mathbf{G}_m^n$ . Therefore, if  $H$  is an algebraic subgroup of  $\mathbf{G}_m^n$  of codimension at least 2, and  $\Gamma_W \subset H$ , then  $\Gamma_W$  is of finite index in  $H$ . Therefore, we may write  $H = \cup_{\zeta \in F} \zeta \Gamma_W$ , where  $F$  is a finite set of roots of unity  $\zeta$ . We may suppose that the torus  $\Gamma_W$  is defined by the equations  $\prod_i x_i^{a_i} = \prod_i x_i^{b_i} = 1$ , where the vectors

$a$  and  $b$  span a lattice of volume bounded by  $(16n^2)^n$ , by Proposition 1 of Section 1. We consider the map  $f : X \rightarrow \mathbf{G}_m^2$  given by  $(x_1, \dots, x_n) \mapsto (\prod_i x_i^{a_i}, \prod_i x_i^{b_i})$ . The image  $Y$  will in turn be a curve of degree bounded above by  $2(16n^2)^n$ . We remark that  $Y$  is not contained in a torsion coset.

We then apply an explicit bound for the number of torsion points on  $Y$ . We may use [5, Theorem 1.3], for example, with the  $V$  of that paper replaced by our  $Y$ . In our situation, the parameters  $g$ ,  $d(V)$  and  $d$  of [5] satisfy  $g = 2$ ,  $d(V) \leq 2(16n^2)^n$  and  $d = 1$ . We obtain finally an upper bound for the number of torsion points  $q$  on  $Y$  of the form  $q \leq 2^{97}((16n^2)^n)^5$ . This is also an upper bound for the number of cosets  $\zeta\Gamma_W$  for which the intersection  $X \cap \zeta\Gamma_W$  is not empty. For a given coset  $\zeta\Gamma_W$ , the cardinality of  $X \cap \zeta\Gamma_W$  is bounded above by  $\deg(\Gamma_W)$ . This last quantity is in turn bounded above by  $\text{vol}(L_W) \leq (16n^2)^n$ . In total, we obtain at most  $2^{97}((16n^2)^n)^6$  points.

### 5. Some remarks on the structure of $S_X$

**PROPOSITION 4.** *There exists a proper algebraic subset  $E$  of  $\mathbf{C}^n$  such that, if  $(r_1, \dots, r_n) \notin E$ , then the set  $S_X$  of Theorem 1 may be chosen to consist of spaces of dimension 2.*

**REMARK.** The proof will effectively (and easily) construct a suitable  $E$ , for any given integer  $n$ . Inspection will also show that for  $n \leq 4$  we can take  $E = \emptyset$ .

*Proof.* Let the notation be as in the proof of Proposition 1. We change variables by putting

$$X = U + \sqrt{-1}V, \quad Y = U - \sqrt{-1}V.$$

Let  $W \in S$  be of dimension  $\geq 3$ , and let  $L = L_W$  be the corresponding lattice. Recall that, for given  $n$ ,  $L$  has finitely many possibilities, which may be (easily) computed in terms of  $n$ .

In Proposition 1 we have seen that, if  $\mathbf{l} = (l_1, \dots, l_n) \in L$  and

$$R(X) = R_{\mathbf{l}}(X) = \prod_i (X + r_i)^{l_i}, \quad (5.1)$$

then there exist nonzero constants  $c_{\mathbf{l}}$  such that the curves defined by

$$R_{\mathbf{l}}(X)R_{\mathbf{l}}(Y) = c_{\mathbf{l}} \quad (5.2)$$

share a common (irreducible) component. We now view  $X$  and  $Y$  as rational functions on such a component.

By Lüroth's theorem, the field generated over  $\mathbf{C}$  by the  $R_{\mathbf{l}}(X)$ , where  $\mathbf{l} \in L$ , is of the form  $\mathbf{C}(G(X))$  for some rational function  $G$ . We first show that, provided that  $(r_1, \dots, r_n)$  lies outside a certain proper algebraic set  $E_1$ , we may take  $G(X) = X$ .

We may certainly write

$$R_{\mathbf{l}}(X) = F_{\mathbf{l}}(G(X)), \quad (5.3)$$

for suitable rational functions  $F_{\mathbf{l}}$ . It follows that if  $\alpha \in \mathbf{C}$  is a zero or pole of some  $F_{\mathbf{l}}$ , then  $G(X) - \alpha$  has zeros in the set  $A := \{-r_1, \dots, -r_n, \infty\}$ . As  $L$  has rank at least 2, there is a  $\beta \neq \alpha$  with the same property, and  $G_1(X) := (G(X) - \alpha)/(G(X) - \beta)$  has zeros and poles in  $A$ . On the other hand,  $\mathbf{C}(G(X)) = \mathbf{C}(G_1(X))$ , so by replacing  $G$  with  $G_1$  if necessary, we may assume that  $G$  has all zeros and poles in  $A$ . Note that

by equation (5.3) the degree of  $G$  is bounded in terms of  $n$  only. We may therefore write

$$G(X) = \prod (X + r_s)^{g_s}, \quad (5.4)$$

for certain integers  $g_s$  bounded in terms of  $n$ . (The *abc* theorem for rational functions leads to a good bound. In fact, if  $\alpha \in \mathbb{C}^*$  is a zero or pole of some  $F_I$ , we see that both  $G$  and  $G - \alpha$  have zeros and poles in  $A$ . Therefore  $\deg G \leq \#A - 1 = n$ .)  $\square$

Let  $\alpha \in \mathbb{C}^*$  such that  $F_I(\alpha) = 0$ , so  $G(X) - \alpha$  has all zeros in  $A$ . Suppose that  $G$  has degree at least 2; then there are two zeros, say  $-r_i$  and  $-r_j$  (the argument is similar if  $\infty$  is a zero). If  $r_i \neq r_j$ , we have a nontrivial relation  $G(-r_i) = G(-r_j) \neq 0$ . If there is a single zero  $-r_s$ , we get similar relations by substituting  $-r_s$  for  $X$ , where  $r_s$  is any zero of  $G(X)$ .

In this way we deduce that at least one out of finitely many relations among  $r_1, \dots, r_n$  is valid, the relations depending only on  $n$ . The union of the sets defined by each single relation constitutes a certain proper algebraic set  $E_1 \subset \mathbb{C}^n$ .

We have shown that if  $(r_1, \dots, r_n) \notin E_1$ , then  $G(X)$  has degree 1, so that we may take  $G(X) = X$ . From now on, we assume that this is the case.

REMARK. Observe that the relations that we have obtained so far for  $E_1$  imply that, if  $(r_1, \dots, r_n) \in E_1$ , then the  $r_i - r_j$  are multiplicatively dependent. Therefore, if we impose a priori that the  $r_i - r_j$  are multiplicatively independent, we may forget about the special form of the relations.

The relations  $R_I(X) = c_I/R_I(Y)$  now show that  $\mathbb{C}(X) \subset \mathbb{C}(Y)$ , and by symmetry we actually get  $\mathbb{C}(X) = \mathbb{C}(Y)$ . Therefore  $Y = \sigma(X)$ , where  $\sigma \in PGL_2(\mathbb{C})$  is some linear fractional transformation satisfying identically

$$R_I(X)R_I(\sigma(X)) = c_I, \quad \text{where } I \in L. \quad (5.5)$$

Putting  $\sigma(X)$  in place of  $X$  in these identical equations, we find that all the  $R_I$  are invariant by  $\sigma^2$ . Since the  $R_I(X)$  generate  $\mathbb{C}(X)$  over  $\mathbb{C}$ , we get

$$\sigma^2 = 1, \quad \text{where } \sigma \neq 1.$$

Observe that equation (5.5) shows that the set  $A'$  of zeros and poles of all the  $R_I$  is preserved by  $\sigma$ , and we have  $A' \subset A$ . From equation (5.5) we also deduce that  $A'$  does not contain any fixed point of  $\sigma$ .

Moreover (using, for example, Hilbert Theorem 90), the multiplicative group of rational functions  $R$  satisfying  $R(X)R(\sigma(X)) \in \mathbb{C}^*$  is generated by  $\mathbb{C}^*$  and by the functions  $(X - \alpha)/(X - \sigma(\alpha))$ , for  $\alpha \in \mathbb{P}^1(\mathbb{C})$  (where a term  $X - \infty$  is to be interpreted as 1). Therefore, since  $L$  has rank  $\geq 3$ , we have  $A' \geq 6$  (and, in particular,  $n \geq 5$ ).

Since  $\sigma$  has order 2, we may write

$$\sigma(X) = \frac{aX + b}{cX - a}.$$

Suppose, for example, that  $A'$  contains the set  $A'' = \{\mu_1, \nu_1, \mu_2, \nu_2, \mu_3, \nu_3\}$  of six complex numbers, where

$$\sigma(\mu_i) = \nu_i, \quad \text{for } i = 1, 2, 3.$$

We get

$$c\mu_i\nu_i - a(\mu_i + \nu_i) - b = 0, \quad \text{where } i = 1, 2, 3.$$

This gives a linear system of three equations in the unknowns  $c$ ,  $-a$  and  $-b$ . If the determinant is nonzero, we get  $a = b = c = 0$ , which is excluded. If, on the other hand, the determinant is zero, we obtain a nontrivial equation among the  $\mu_i, v_i$ . Recall now that  $A''$  is a subset of  $A$ , and it may be chosen and ordered in at most  $6! \binom{n}{6}$  ways. We therefore obtain a corresponding set of equations in the  $r_i$ , one of which is satisfied. The argument is similar if  $A''$  contains  $\infty$ . We have thus constructed an algebraic set dependent only on  $n$  and containing  $(r_1, \dots, r_n)$ , and this concludes the proof.  $\square$

REMARK. We conclude by observing that the above construction, in particular equation (5.5), allows us to show that the set  $S_X$  may be non-empty. For example, for  $n = 3$ , let  $L$  be generated by  $(1, 0, 0), (0, 1, -1)$ , and let  $W = L \otimes \mathbb{R}$ . We may take  $R_1(x) = x$  and  $R_2(x) = (x - \alpha)/(1 - \alpha x)$  for  $\alpha \in \mathbb{Q}^*$  and  $\sigma(x) = 1/x$ . This corresponds to the line  $X$  defined by

$$x_1 = t, \quad x_2 = t - \alpha, \quad x_3 = t - 1/\alpha.$$

Let  $P = (1, 1, -\alpha)$ . Then it is immediate that  $X \cap P \cdot G_W$  contains the unit circle.

*Acknowledgements.* The authors thank the Ellentuck Fund, the James D. Wolfensohn Foundation and the School of Mathematics of the Institute for Advanced Study, Princeton, for their support during the preparation of this paper.

### References

1. D. BERTRAND, 'Duality on tori and multiplicative dependence relations', *J. Austral. Math. Soc. Ser. A* 62 (1997) 198–216.
2. E. BOMBIERI, D. MASSER and U. ZANNIER, 'Intersecting a curve with algebraic subgroups of multiplicative groups', *Internat. Math. Res. Notices* 20 (1999) 1119–1140.
3. P. COHEN, 'Decision procedures for real and  $p$ -adic fields', *Comm. Pure Appl. Math.* 22 (1969) 131–151.
4. P. B. COHEN and U. ZANNIER, 'Multiplicative dependence and bounded height, an example', *Proceedings of the Algebraic Number Theory and Diophantine Approximation Conference, Graz, 1998* (Walter de Gruyter, 2000) 93–101.
5. S. DAVID and P. PHILIPPON, 'Minors des hauteurs normalisées des sous-variétés des tores', *Ann. Scuola Norm. Sup. Pisa Cl. Sci.* 28 (1999) 489–544.
6. E. G. KHOVANSKII, *Fewnomials*, Transl. Math. Monogr. 88 (Amer. Math. Soc., Providence, RI, 1991).

School of Mathematics  
Institute for Advanced Study  
Einstein Drive  
Princeton, 08540 NJ  
USA

and

UMR AGAT au CNRS  
Mathématiques  
Bât M2  
UFR de Mathématiques  
Villeneuve d'Ascq, 59655  
France

Paula.Cohen@univ-lille1.fr

School of Mathematics  
Institute for Advanced Study  
Einstein Drive  
Princeton, 08540 NJ  
USA

and

Istituto Universitario di Architettura  
Dipartimento di Costruzione  
dell'Architettura  
Santa Croce 191  
30135 Venezia  
Italy

zannier@dimi.uniud.it