FINDING MAXIMAL TORSION COSETS ON VARIETIES

ISKANDER ALIEV AND CHRIS SMYTH

Abstract. We describe a new algorithm for finding all maximal torsion cosets on varieties of $\mathbb{G}_{\mathrm{m}}^n$. We illustrate the algorithm with some examples.

The starting point for this study is the search for points on a given variety whose coordinates are roots of unity. Sometimes these points are isolated, but often they are part of larger families of such points, called torsion cosets. (These are in fact elements of finite order in some quotient group of $\mathbb{G}_{\mathrm{m}}^n$.) Of greatest interest are maximal torsion cosets, not contained in any larger ones. The number of maximal torsion cosets on a variety is known to be finite, and it of interest to find upper bounds for the number of these, in terms of the dimension and the total degree of the variety. We summarise what is known about such bounds.

1. Introduction

Here we are concerned with finding *cyclotomic points* on a given variety, that is, points whose coordinates are roots of unity. One place where finding cyclotomic points on varieties arose was in [18], where the problem was to factorize polynomials

$$R_{d,m}(z) = z^{2d}(z^2 - z - 1) + z^{2(d-m)} + z^{2(m+1)} - z^2 - z + 1.$$

These can readily be shown to have at most one zero in $|z| > 1$, so, for a fixed d, m, all irreducible factors of $R_{d,m}(z)$, except perhaps one, are cyclotomic polynomials. Putting $x = z^{2d}$, $y = z^{2m}$, this leads to the problem of seeking cyclotomic points on the surface

$$x(z^2 - z - 1) + xy^{-1} + yz^2 - z^2 - z + 1 = 0. \qquad (1)$$

For a given variety $\mathcal{V}$, we denote by n its number of variables, by d its total degree, and by h the number of hypersurfaces whose intersection defines $\mathcal{V}$.

A fundamental result needed, as in Beukers and Smyth [2], is the following.

Lemma 1 ([2, Lemma 1])**.** (i) *If $g(x) \in \mathbb{C}[x], g(0) \neq 0$, 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 exactly one of $-\omega, \omega^2$ and $-\omega^2$.*

Conversely, if $\alpha \neq 0$ and either α^2 or $-\alpha^2$ is conjugate to α, then α is a root of unity.

The value of this lemma for our purposes lies in the fact that, for a variety $\mathcal{V}(H)$ defined by a set H of hypersurfaces, the lemma enables us to enlarge H to obtain a collection of (in general smaller) varieties $\mathcal{V}(H')$ with the property that the cyclotomic points on $\cup\mathcal{V}(H')$ are the same as those on $\mathcal{V}(H)$. In particular, for hypersurfaces we have the following.

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

(i) $\deg(f_i) \le 2\deg(f)$ *for* $i = 1, \dots, m$*;*
(ii) *For* $1 \le i \le m$ *the polynomials* f *and* f_i *have no common factor;*
(iii) *For any torsion coset* C *lying on the hypersurface* $f = 0$ *there exists some* $1 \le i \le m$ *such that the coset* C *also lies on the hypersurface* $f_i = 0$*.*

When f is in fact defined over $\mathbb{Q}$, the polynomials f_i are a subset of $f(\pm x_1, \dots, \pm x_n)$ (not all + signs) and $f(\pm x_1^2, \dots, \pm x_n^2)$. We also need the following simple lemma.

Lemma 3. *Suppose that L is a full (i.e. n-dimensional) sublattice of $\mathbb{Z}^n$, with determinant $D > 1$. Then there is a basis of L, and a factor $m > 1$ of D with the property that one of the basis vectors has all its components divisible by m.*

Proof. Consider an $n \times n$ matrix whose rows are a basis of L. Now put this matrix in Hermite Normal Form ([4, Section 2.4.2]), so that the rows of this new matrix are again a basis for L. Then it is upper triangular with diagonal elements $d_1, \dots, d_n$ say, with all elements in a column being nonnegative and strictly less than the diagonal element in that column. Since $\prod_i d_i = D$, not all the d_i are 1. Let i' be the largest index i such that $d_i > 1$. Then $d_{i'} > 1$ is the only nonzero entry in row i' of the matrix. □

1.1. **Definitions and earlier results.** Let $\mathbb{G}_{\mathrm{m}}$ denote the multiplicative group of $\mathbb{C}$, as a variety, and let $\mathbb{G}_{\mathrm{m}}^n = (\mathbb{G}_{\mathrm{m}})^n$ be the direct product consisting of n-tuples $\boldsymbol{x} = (x_1, \dots, x_n)$ with $x_i \in \mathbb{G}_{\mathrm{m}}$. By a *subtorus* H of $\mathbb{G}_{\mathrm{m}}^n$ we mean an irreducible algebraic subgroup. By *torsion coset* we will understand a coset $\boldsymbol{u}H$, where H is a subtorus of $\mathbb{G}_{\mathrm{m}}^n$ and $\boldsymbol{u} = (u_1, \dots, u_n)$ is a *torsion point*, that is all u_i are roots of unity. Let V be an algebraic subvariety of $\mathbb{G}_{\mathrm{m}}^n$. A torsion coset $\boldsymbol{u}H \subset V$ will be called *maximal* in V if there is no torsion coset $\boldsymbol{u}H'$ with $\boldsymbol{u}H \subsetneqq \boldsymbol{u}H' \subset V$. By the *dimension* of a torsion coset $\boldsymbol{u}H$ we understand the dimension of the torus H. A maximal 0–dimensional torsion coset will be also called *isolated* torsion point. Let $V^{\cup}(H)$ be the union of all maximal cosets $\boldsymbol{u}H$ contained in V and let

$$V^{\cup} = \bigcup_H V^{\cup}(H)\,,$$

where the union being over all subtori H of $\mathbb{G}_{\mathrm{m}}^n$.

Lang [9] conjectured that if V is a subvariety of $\mathbb{G}_{\mathrm{m}}^n$ defined over $\overline{\mathbb{Q}}$ then $V^{\cup}$ is the union of a finite number of torsion cosets. This conjecture was proved by Ihara, Serre and Tate (see §8.6 of Lang [9]) when $\dim V = 1$, and by Laurent [11] if $\dim V > 1$. Different proofs of this result were also given by Sarnak and Adams [15]. In Zhang [19] and in Bombieri and Zannier [3] it has been shown that $V^{\cup}$ is the union of at most $c(d, n, [K : \mathbb{Q}], M)$ torsion cosets when the defining polynomials of V had coefficients in a number field K and had degrees $\leq d$ and heights $\leq M$. Furthermore, in [17] Schmidt has given a bound of this kind.

Let $\mathcal{T}(V)$ denote the number of maximal torsion cosets lying on the subvariety V and let

$$\mathcal{T}(n,d) = \max_V \ \mathcal{T}(V)\,,$$

where the maximum is being over all subvarieties $V \subset \mathbb{G}_{\mathrm{m}}^n$ defined by the polynomial equations of degree at most d. Schmidt [17] has shown that

$$\mathcal{T}(n,d) \leq (11d)^{n^2} \exp\left(4\binom{n+d}{d}!\right)\,. \tag{2}$$

The proof of this bound is based on a result of Schlickewei [16] about the number of nondegenerate solutions of a linear equation in roots of unity. The latter result was significantly improved by Evertse [7]. Because of his result, the bound (2) can be replaced then by

$$\mathcal{T}(n,d) \leq (11d)^{n^2} \binom{n+d}{d}^{3\binom{n+d}{d}^2}\,. \tag{3}$$

Although the estimate (3) is much better than (2), it is still of exponential growth in d. Recently, such bounds that are polynomial in d have been obtained for varieties defined over $\mathbb{Q}$ by de Piro [6], using methods and results from model theory. Earlier, David and Philippon proved a result [5, Proposition 5.6] from which such a bound can follows, for varieties defined over $\overline{\mathbb{Q}}$. We have also obtained such a bound in [1], improving on these bounds. The main result of [1] asserts that, for any fixed dimension n, the number of maximal torsion cosets on subvarieties of $\mathbb{G}_{\mathrm{m}}^n$ is polynomially bounded in d. First, our bound for maximal torsion cosets on hypersurfaces.

Theorem 1 ([1]). *Let $f \in \mathbb{C}[X_1,\ldots,X_n]$, $n \geq 2$, 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*

$$N_{tor}(\mathcal{H}) \leq c_1(n)\, d^{\,c_2(n)}\,, \tag{4}$$

where $c_1(n)$ and $c_2(n)$ are effectively computable constants. Indeed we can take

$$c_1(n) = n^{1.5(2+n)5^n} \quad \textit{and} \quad c_2(n) = \frac{1}{16}(49\cdot 5^{n-2} - 4n - 9)..$$

1.2. **Examples.** The following family of examples shows that the upper bound on the number of maximal torsion cosets on a hypersurface cannot be too small. In particular, a general bound must be exponential in the dimension n.

Define the following hypersurfaces $\mathcal{H}_k : f_k(x_1,\ldots,x_n) = 0$ in $\mathbb{G}_{\mathrm{m}}^n$:

- In general for $k = 1,2,\ldots,n$ f_k is the kth elementary symmetric function of the n terms $(x_1^d - 1),\ldots,(x_n^d - 1)$. In general the hypersurface $\mathcal{H}_k$ has degree kd and $\binom{n}{k-1}d^{n-(k-1)}$ $(k-1)$-dimensional maximal torsion cosets obtained by choosing $n-(k-1)$ of $x_1,\ldots,x_n$ to be dth roots of unity.

  In particular

- $f_1(x_1,\ldots,x_n) = (x_1^d - 1) + \cdots + (x_n^d - 1)$.
  The hypersurface $\mathcal{H}_1$ has degree d and d^n isolated torsion points. They are its only torsion cosets.
- $f_2(x_1,\ldots,x_n) = \sum_{i<j}(x_i^d - 1)(x_j^d - 1)$.
  The hypersurface $\mathcal{H}_2$ has degree $2d$ and $\binom{n}{1}d^{n-1}$ 1-dimensional torsion cosets obtained by choosing $n-1$ of $x_1,\ldots,x_n$ to be dth roots of unity. They are its only maximal torsion cosets.
- $f_{n-1}(x_1,\ldots,x_n) = \sum_{i=1}^n \prod_{j\neq i}(x_j^d - 1)$.
  The hypersurface $\mathcal{H}_{n-1}$ has degree $(n-1)d$ and $\binom{n}{n-2}d^2$ $(n-2)$-dimensional maximal torsion cosets obtained by choosing two of $x_1,\ldots,x_n$ to be dth roots of unity.

1.3. **General varieties.** Concerning general varieties, we obtained the following result.

Theorem 2 ([1])**.** *There are effective constants $c_3(n)$ and $c_4(n)$ such that*

$$\mathcal{T}(n,d) \leq c_1(n)\, d^{\,c_2(n)}\,. \tag{5}$$

Indeed we can take

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

2. The algorithm

To motivate our algorithm, we first study a specific example.

2.1. **Example: Maximal torsion cosets on a surface.** Consider the surface $f(x,y,z) = 0$, where

$$f(x,y,z) := (z+1+y)x - z - 1 - zy^{-1}. \tag{6}$$

Let $\alpha := e^{2\pi i/30}$ and $\omega := e^{2\pi i/3}$. Then the maximal torsion cosets on this surface are the 1-dimensional cosets

$$\{(1,t,t^2), (-1/t^2,t,-1), (t,1/t^2,1/t), (t,-1,1/t), (t,-t,t), (t,1/t,t), (t,\omega,\omega^2), (t,\omega^2,\omega),$$
$$(-\omega,\omega,t), (-\omega^2,\omega^2,t), (t,-\omega^2/t,\omega), (t,-\omega/t,\omega^2), (-\omega^2,t,\omega t), (-\omega,t,\omega^2 t)\},$$

where t is a free parameter, and the isolated points

$$\{(\alpha^8,\alpha^6,\alpha^{17}),(\alpha^{22},\alpha^{24},\alpha^{13}),\ (\alpha^{14},\alpha^{13},\alpha^{19}),(\alpha^{26},\alpha^6,\alpha^{29}),\ (\alpha^3,\alpha^{29},\alpha^6),(\alpha^{28},\alpha^{11},\alpha^{23}),$$
$$(\alpha^{22},\alpha^{29},\alpha^{17}),(\alpha^9,\alpha^{17},\alpha^{18}),\ (\alpha^{22},\alpha^{11},\alpha^{17}),(\alpha^4,\alpha^{24},\alpha^1),\ (\alpha^2,\alpha^{12},\alpha^{23}),(\alpha^9,\alpha^7,\alpha^{18}),$$
$$(\alpha^{16},\alpha^6,\alpha^{19}),(\alpha^{22},\alpha^{12},\alpha^{13}),\ (\alpha^{21},\alpha^{13},\alpha^{12}),(\alpha^{14},\alpha^{18},\alpha^{11}),\ (\alpha^{16},\alpha^{12},\alpha^{19}),(\alpha^2,\alpha^{24},\alpha^{23}),$$
$$(\alpha^{21},\alpha^1,\alpha^{18}),(\alpha^{16},\alpha^{23},\alpha^{11}),\ (\alpha^{27},\alpha^1,\alpha^{24}),(\alpha^{27},\alpha^{11},\alpha^{24}),\ (\alpha^3,\alpha^{19},\alpha^6),(\alpha^{26},\alpha^{12},\alpha^{29}),$$
$$(\alpha^{27},\alpha^7,\alpha^6),(\alpha^2,\alpha^{19},\alpha^7),\ (\alpha^{28},\alpha^{18},\alpha^7),(\alpha^3,\alpha^{13},\alpha^{24}),\ (\alpha^{21},\alpha^{23},\alpha^{12}),(\alpha^8,\alpha^{18},\alpha^{17}),$$
$$(\alpha^4,\alpha^{23},\alpha^{29}),(\alpha^9,\alpha^{29},\alpha^{12}),\ (\alpha^8,\alpha^{19},\alpha^{13}),(\alpha^4,\alpha^{17},\alpha^{29}),\ (\alpha^{21},\alpha^{11},\alpha^{18}),(\alpha^4,\alpha^{18},\alpha^1),$$
$$(\alpha^{26},\alpha^{13},\alpha^1),(\alpha^2,\alpha^1,\alpha^7),\ (\alpha^3,\alpha^{23},\alpha^{24}),(\alpha^8,\alpha^1,\alpha^{13}),\ (\alpha^{28},\alpha^6,\alpha^7),(\alpha^9,\alpha^{19},\alpha^{12}),$$
$$(\alpha^{27},\alpha^{17},\alpha^6),(\alpha^{28},\alpha^{29},\alpha^{23}),\ (\alpha^{14},\alpha^7,\alpha^{19}),(\alpha^{16},\alpha^{17},\alpha^{11}),\ (\alpha^{14},\alpha^{24},\alpha^{11}),(\alpha^{26},\alpha^7,\alpha^1)\}.$$

How are these found? Well, generalising from the case of curves, we compute the resultant of $f(x,y,z)$ with each of the 7 polynomials $f(\pm x,\pm y,\pm z)\neq f(x,y,z)$ and the 8 polynomials $f(\pm x^2,\pm y^2,\pm z^2)$. By Lemma 1, all cyclotomic points of f also lie on at least one of these 15 surfaces. We then take further resultants, on the same principle, as necessary.

Techniques such as this led us to formalise the process for finding all torsion cosets on a subvariety of $\mathbb{G}_{\mathrm{m}}^n$ as an algorithm. We now give this algorithm . A different algorithm for this purpose was given in [1]. We denote by n the number of variables of the polynomials describing our variety. Of course this is an upper bound for its dimension. We also denote by $V_n(f_1,\dots,f_h)$ the union of all maximal torsion cosets on the variety defined by the h polynomials $f_1,\dots,f_h$ in $\mathbb{Z}[x_1,\dots,x_n]$.

The algorithm is recursive. We can clearly assume that all hypersurfaces considered are irreducible. For instance, if $f=\prod_\ell g_\ell^{k_\ell}$, then $V_n(f)=\cup_\ell V_n(g_\ell)$. Further, where more than one hypersurface is considered, we can assume that they are distinct, that is, their defining polynomials are not simply rational multiples of one another. In the algorithm, the notation x^A for $x=(x_i)\in\mathbb{G}_m^n$ and $A=(a_{ij})\in Z^{n\times r}$ denotes $(\prod_i {x_i}^{a_{i1}},\dots,\prod_i {x_i}^{a_{ir}})\in\mathbb{G}_{\mathrm{m}}^r$.

We start with hypersurfaces, computing $V_n(g)$. We then proceed to the 2-hypersurface case, followed by the general case.

(1) **One hypersurface.**
  - (a) $n=1$. Use the 1-variable algorithm in [2]. Alternatively, write $g(x)=g_1(x^r)$ with r maximal, and put $g_2(x)=\gcd(g_1(y),g_1(y^2),g_1(-y^2))$. Then $V_1(g_1)$ is the set of roots of g_2 and so $V_1(g)$ is the set of k-th roots of these roots.
  - (b) $n\geq 2$.
    - (b1) If g r-dimensional with $r<n$, say $x^A=t$, where A is $n\times r$ and, for some c, $x^c g(x)=g_1(t)$, where $t=(t_1,\dots,t_r)$ and g_1 is again irreducible. Then maximal torsion cosets of g_1 readily give maximal torsion cosets of g.
    - (b2) If g is n-dimensional and $D>1$ is the determinant of its lattice, then for some factor $m>1$ of D we can, by Lemma 3, find $B\in\mathbb{Z}^{n\times n}$ of determinant D/m such that if $y=x^B$ then and $c\in\mathbb{Z}^n$ we have

$x^c g(x) = g_2(y_1^m, y_2, \ldots, y_n)$. Then maximal torsion cosets of g_2 readily give maximal torsion cosets of g.

(b3) If g is n-dimensional and $D = 1$ is the determinant of its lattice (so its lattice is $\mathbb{Z}^n$), then from Lemma 2 there are polynomials f_i with $\gcd(g, f_i) = 1$ such that $V_n(g) = \cup_i V_n(g, f_i)$.

(2) **Two hypersurfaces.** $V_n(g, f)$, where $g(x_1, \ldots, x_n)$ is irreducible and n-dimensional, and $f(x_1, \ldots, x_n)$ is at most n-dimensional.
   (a) If f is r-dimensional, where $r < n$, find $V_n(f)$ and then, for each maximal torsion coset in $V_n(f)$, write each variable x_i as a monomial in $t_1, \ldots, t_s$, where $s \leq r - 1 \leq n - 2$. Thus the dimension of the problem is reduced.
   (b) If f is n-dimensional, then $V_n(g, f) = V_n(g, f, s)$, where $s = \mathrm{Res}_{x_1}(g, f)$. We then proceed as in (a) to reduce the number of variables.

(3) **General case.** To compute $V_n(f_1, \ldots, f_h)$, find $V_n(f_1)$ (say). Then proceed as in part 2(a).

It is not difficult to prove that this algorithm is recursive. Indeed, consider the ordered pair (r, D), where r is the smallest dimension of any hypersurface defining the variety, and D is the determinant of its lattice. Ordering such pairs lexicographically, we see that, essentially, each step of the algorithm produces only smaller (in this ordering) such associated pairs. Here, we say 'essentially' because in step 1(b3) it is necessary to merge this step with 2(b) (i.e. replace $V_n(g, f_i)$ with $V_n(g, f_i, r)$) so that the dimension is reduced.

2.2. **Example: Maximal torsion cosets on the surface (1).** Consider the surface $p(x, y, z) = 0$, where

$$p(x, y, z) := x(z^2 - z - 1) + x/y + yz^2 - z^2 - z + 1. \tag{7}$$

is the polynomial defining the surface (1). Let $\alpha := e^{2\pi i/30}$ as before, and put $\beta := e^{2\pi i/24}$, $\gamma := e^{2\pi i/18}$, $\delta := e^{2\pi i/12}$. Then the 1-torsion cosets on this surface are

$$\{(t, 1, 1), (t, -1, -1), (t, -t, -t), (t, t^3, t^{-1}), (t, t, 1), (t, -t, -1), (t, -t^{-2}, -t), (t, 1, t^{-1}), (1, t, t^{-1})\},$$

where t is a free parameter. This time, the 68 isolated points are given by the representatives of their Galois orbits:

$$\{(\alpha^2, \alpha, \alpha^{26}), (\alpha^2, \alpha^9, \alpha^{26}), (\alpha^8, \alpha^2, \alpha), (\alpha^8, \alpha^4, \alpha), (\beta^{18}, \beta, \beta^2), (\gamma, \gamma^2, \gamma^{14}),$$
$$(\gamma, \gamma^3, \gamma^{13}), (\gamma, \gamma^7, \gamma^{14}), (\gamma, \gamma^8, \gamma^{13}), (-1, \delta^2, \delta)\},$$

the orbits being of sizes $8, 8, 8, 8, 8, 6, 6, 6, 6, 4$, respectively. The determination of these maximal torsion cosets enables a complete factorization of the polynomials $R_{d,m}(z)$ to be made. The details are given in [18], albeit by a somewhat more *ad hoc* version of this method.

References

[1] Aliev I., Smyth C.J., Torsion points on subvarieties of $\mathbb{G}_{\mathrm{m}}^n$, submitted.

[2] Beukers F., Smyth C.J., Cyclotomic points on curves. Number theory for the millennium, I (Urbana, IL, 2000), 67–85, A.K. Peters, Natick, MA, 2002.

[3] Bombieri E., Zannier U., Algebraic points on subvarieties of $\mathbf{G}_m^n$. Internat. Math. Res. Notices 1995, 333–347.
[4] Cohen, H., A course in computational algebraic number theory. Graduate Texts in Mathematics, 138. Springer-Verlag, Berlin, 1993.
[5] David, S., Philippon, P., Minorations des hauteurs normalises des sous-varits des tores. Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **28** (1999), 489–543.
[6] de Piro, T. Bounding the number of maximal torsion cosets on algebraic varieties. Preprint.
[7] J-H. Evertse, The number of solutions of linear equations in roots of unity, Acta Arith. **89** (1999), no. 1, 45–51.
[8] Hindry M., Silverman J.H., Diophantine geometry: an Introduction, Springer-Verlag, New York 2000.
[9] Lang S., Fundamentals of diophantine geometry, Springer-Verlag, New York, 1983.
[10] ———, Division points on curves, Ann. Mat. Pura Appl. (4) **70** (1965), 229–234.
[11] Laurent M., Équations diophantiennes exponentielles. Invent. Math. **78** (1984), 299–327.
[12] Liardet P., Sur une conjecture de Serge Lang, Astérisque **24**–**25** (1975), 187–209.
[13] McKee J., Smyth C.J., There are Salem numbers of every trace, Bull. London Math. Soc. **37** (2005),
[14] McQuillan M., Division points on semi-abelian varieties, Inv. Math. **120** (1995), 143–159.
[15] Sarnak P., Adams S., Betti numbers of congruence groups, with an appendix by Ze'ev Rudnick, Israel J. Math. **88** (1994), no. 1-3, 31–72.
[16] Schlickewei H.P., Equations in roots of unity, Acta Arith. **76** (1996), no. 2, 99–108.
[17] Schmidt W.M., Heights of points on subvarieties of $\mathbb{G}_{\mathrm{m}}^n$. Number theory (Paris, 1993–1994), 157–187, London Math. Soc. Lecture Note Ser., 235, Cambridge Univ. Press, Cambridge, 1996.
[18] Smyth C.J., Salem numbers of negative trace. Math. Comp. **69** (2000), 827–838.
[19] Zhang S., Positive line bundles on arithmetic varieties, J. Amer. Math. Soc. **8** (1995), 187–221.

School of Mathematics and Maxwell Institute for Mathematical Sciences, University of Edinburgh, James Clerk Maxwell Building, King's Buildings, Mayfield Road, Edinburgh EH9 3JZ, UK