



**HAL**  
open science

## Bound on the number of maximal torsion cosets

César Martínez

► **To cite this version:**

| César Martínez. Bound on the number of maximal torsion cosets. 2015. hal-01140886v1

**HAL Id: hal-01140886**

**<https://hal.science/hal-01140886v1>**

Preprint submitted on 9 Apr 2015 (v1), last revised 17 Nov 2015 (v3)

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# Bound on the number of maximal torsion cosets

César Martínez \*

April 9, 2015

## Abstract

We obtain a sharp bound on the number of maximal torsion cosets in a subvariety of the complex algebraic torus  $\mathbb{G}_m^n$ .

**Mathematics Subject Classification:** 11G35 (14G25).

## 1 Introduction

Let  $\mathbb{G}_m^n$  be the complex algebraic torus. As an affine variety, we identify  $\mathbb{G}_m^n$  with the Zariski open subset  $x_1 \cdots x_n \neq 0$  of  $\mathbb{A}_{\mathbb{C}}^n$  with the usual multiplication

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

Therefore, a torsion point of  $\mathbb{G}_m^n$  is an  $n$ -tuple of roots of unity. Let  $V$  be a subvariety of  $\mathbb{G}_m^n$ , we denote by  $\overline{V_{\text{tor}}}$  the Zariski closure of the torsion points contained in  $V$ .

Motivated by the conjectures of Mordell and Manin-Mumford, Lang conjectured that  $\overline{V_{\text{tor}}}$  is a finite union of torsion cosets, i.e. translates by torsion points of algebraic subtori of  $\mathbb{G}_m^n$  (see [Lan83, p.220]). This was proved by Ihara, Serre and Tate for  $\dim(V) = 1$  (see [Lan83, Theorem 6.1]) and by Laurent for higher dimensions (see [Lau84, Théorème 2]). This conjecture was originally formulated in a more general setting, which was proved by McQuillan [McQ95]. The following step is, then, to find an upper bound for the number of torsion varieties in  $V$ .

We say that a torsion coset contained in  $V$  is maximal if it is maximal with respect to the inclusion. It was proved by Zhang [Zha95] that, if  $V$  is defined over  $\mathbb{K}$  by a set of polynomials of degree at most  $d$  and height at most  $M$ , the number of maximal torsion cosets in  $V$  and the degree of them is effectively bounded in terms of  $d$ ,  $n$ ,  $M$  and  $[\mathbb{K} : \mathbb{Q}]$ . Later, Bombieri and Zannier [BZ95] showed that both, the number of maximal torsion cosets and the degree of their defining polynomials, can be bounded just in terms of  $n$  and  $d$ .

---

\*Laboratoire de mathématiques Nicolas Oresme, CNRS UMR 6139, Université de Caen. BP 5186, 14032 Caen Cedex, France. This research was partially financed by the CNRS project PICS 6381 "Géométrie diophantienne et calcul formel".

Furthermore, Schmidt [Sch96] obtained an explicit upper bound for the number of maximal torsion cosets in  $V$ , which was then improved with a result of Evertse [Eve99], bounding the number of maximal torsion cosets by

$$(11d)^{n^2} \binom{n+d}{d}^{3\binom{n+d}{d}^2}.$$

Meanwhile, Ruppert [Rup93] and Sarnak and Adams [SA94] presented algorithms to determine the torsion subvariety of some variety  $V \subset \mathbb{G}_m^n$ . In particular, Ruppert's approach treats first the case  $\dim(V) = 1$  where, given  $(d_1, \dots, d_n)$  the multi-degree of  $V \subset (\mathbb{P}^1)^n$ , he is able to bound the number of isolated torsion points in  $V$  by  $22 \max(d_i) \min(d_i)$ . Afterwards, he extends his algorithm to some specific varieties in higher dimension, which leads him to conjecture that, given  $f \in \overline{\mathbb{Q}}[X_1, \dots, X_n]$ , the number of isolated torsion points on  $V(f) \subset \mathbb{G}_m^n$  could be bounded by  $c_n d_1 \cdots d_n$ , where  $c_n$  is some constant depending only on  $n$  and the  $d_i$ 's are the partial degrees of  $f$ . This conjecture followed from trying to generalize some occurrences he observed for the case  $n = 2$  to general dimension.

Beukers and Smyth [BS02] reconsidered the problem for  $n = 2$  from a similar point of view to Ruppert's one, being able to improve the bound in this case. Given  $f \in \overline{\mathbb{Q}}[X, Y]$  a polynomial, they bound the number of torsion points of  $V(f)$  by  $22 \text{vol}_2(f)$ , where  $\text{vol}_2(f)$  denotes the 2-volume of the Newton polytope of  $f$ . This leads Aliev and Smyth to the following reformulation of the original conjecture of Ruppert in [AS12]:

**Conjecture 1.1.** *Let  $f \in \overline{\mathbb{Q}}[X_1, \dots, X_n]$ , the number of isolated torsion points on the hypersurface  $V(f) \subset \mathbb{G}_m^n$  is bounded by  $c_n \text{vol}_n(f)$ , where  $c_n$  is a constant depending only on  $n$  and  $\text{vol}_n(f)$  is the  $n$ -volume of the Newton polytope of  $f$ .*

Aliev and Smyth [AS12] extended Beukers and Smyth's algorithm to higher dimensions and obtained a bound far from the conjecture. For  $f \in \overline{\mathbb{Q}}[X_1, \dots, X_n]$  of degree  $d$ , they bound the number of maximal torsion cosets in  $V$  by

$$c_1(n) d^{c_2(n)},$$

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

For sparse representations of polynomials, Leroux [Ler12] obtained an algorithm to find the maximal torsion cosets in  $V$ . As a consequence, he is able to bound the number of maximal torsion cosets in  $V$  in terms of the number of non-zero coefficients of the defining polynomials of  $V$ . For dense polynomials the bound has similar order to the one of Aliev and Smyth [AS12].

Another approach to this problem has been to conceive it as a particular case of the study of the number of algebraic points of small height. That is because the torsion points on  $V$  can be thought of as the points of height 0 on  $V$ . Thereby, some upper bounds on the number of subvarieties of small height can be translated to our setting. This is how Amoroso and Viada obtained the following bound (see [AV09, Corrolary 5.4]):

**Proposition 1.2.** *Let  $V$  be a subvariety of  $\mathbb{G}_m^n$  of codimension  $k$  and defined by polynomials of degree at most  $\delta$ . Let*

$$\theta = \delta(200n^5 \log(n^2\delta))^{(n-k)n(n-1)}.$$

*Then the number of maximal torsion cosets in  $V$  is bounded by  $\theta^n$ .*

First, note that  $\delta$  can be replaced by the degree of  $V$  in the case that  $V$  is a hypersurface (as in the statement of the conjecture). This way, we can see that this bound is close to the one conjectured by Ruppert, up to a logarithmic factor.

In this article we prove a relaxed conjecture following similar induction processes to the ones introduced in [AV09]. Our main result is:

**Theorem 1.3.** *Let  $V$  be a subvariety of  $\mathbb{G}_m^n$  of codimension  $k$ , defined by polynomials of degree at most  $\delta$ . Let*

$$\theta = ((2n-1)(n-1)(2^{2n} + 2^{n+1} - 2))^{n-k} \delta.$$

*Then the number of maximal torsion cosets in  $V$  is bounded by  $\theta^n$ .*

As before,  $\delta$  can be replaced by the degree of  $V$  in the case that  $V$  is a hypersurface and we obtain the following:

**Corollary 1.4.** *Let  $V \subset \mathbb{G}_m^n$  be a hypersurface of degree  $d$ . Then the number of isolated torsion points in  $V$  is bounded by  $c_n d^n$ , where  $c_n$  is a constant depending only on  $n$ .*

If  $f \in \mathbb{C}[X_1, \dots, X_n]$  is of degree  $d$  and  $V = V(f)$ , we can bound  $\text{vol}_n(f) \leq d^n$ . Hence, we observe that this result is close to proving the conjecture.

To discard the logarithmic error term, we reformulate the main theorems of Amoroso and Viada in [AV09] so that they suit our particular case of torsion subvarieties.

In order to do that, we extend first the argument introduced by Beukers and Smyth in [BS02] to a more algebraic setting. In Proposition 3.2 we get, for any irreducible subvariety  $V$  of  $\mathbb{G}_m^n$ , another variety  $V' \subset \mathbb{G}_m^n$  with the same dimension and similar degree, such that  $\overline{V_{\text{tor}}}$  lies in the intersection  $V \cap V' \subsetneq V$ . Moreover, this  $V'$  can be obtained explicitly from our initial  $V$ .

Next, in Theorem 3.4, we use the Hilbert function to consider, instead of the subvariety  $V'$ , a hypersurface  $Z$  satisfying that  $\overline{V_{\text{tor}}} \subset V \cap Z \subsetneq V$ . To do that, we rely on both, an upper and a lower bound for the Hilbert function; being the upper bound a result of Chardin [Cha89] and the lower bound a result of Chardin and Philippon [CP99]. By using this bounds, we obtain Lemma 2.8, which serves as bridge between  $V'$  and  $Z$  and is, therefore, the key element in our proof of Theorem 3.4.

Finally, we present two induction theorems, Theorem 4.1 and Theorem 4.2, which are the equivalent of [AV09, Theorems 2.2 and 1.2] in our case. As a consequence of Theorem 4.2, we deduce Theorem 1.3 and prove the conjecture.

## Acknowledgments

The autor would like to thank F. Amoroso and M. Sombra for their insight, precious advice and patience.

## 2 Basic results

### 2.1 Notation

We denote  $\mathbf{x} \in \mathbb{G}_m^n$  as  $\mathbf{x} = (x_1, \dots, x_n)$  and, in particular,  $\mathbf{1} = (1, \dots, 1)$  represents the identity element. Given  $\mathbf{x} \in \mathbb{G}_m^n$  and  $\boldsymbol{\lambda} = (\lambda_1, \dots, \lambda_n) \in \mathbb{Z}^n$  we denote

$$\mathbf{x}^\lambda = (x_1^{\lambda_1}, \dots, x_n^{\lambda_n})$$

and, by abuse of notation, given  $\lambda \in \mathbb{Z}$  we understand  $\mathbf{x}^\lambda$  as  $\mathbf{x}^{(\lambda, \dots, \lambda)}$ . Moreover, given  $S \subset \mathbb{G}_m^n$  any subset we denote

$$\mathbf{x} \cdot S = \{\mathbf{x} \cdot \mathbf{y} \mid \mathbf{y} \in S\}.$$

If the context is clear, we might write simply  $\mathbf{x}S$ .

We call homomorphism an algebraic group homomorphism  $\varphi : \mathbb{G}_m^{n_1} \rightarrow \mathbb{G}_m^{n_2}$ . For any  $l \in \mathbb{Z}$ , we define the multiplication by  $[l]$  as the following endomorphism:

$$[l] : \mathbb{G}_m^n \rightarrow \mathbb{G}_m^n \\ \mathbf{x} \mapsto \mathbf{x}^l.$$

We denote  $\zeta_k$  as a primitive  $k$ -th root of unity, for any  $k \in \mathbb{N}_{>0}$ , and  $\mu_k = \{\zeta \in \mathbb{G}_m \mid \zeta^k = 1\}$  as the subgroup of  $k$ -th roots of unity. In particular, we denote  $\mu_\infty = \{\zeta \in \mathbb{G}_m \mid \zeta^k = 1 \text{ for some } k \in \mathbb{N}\}$  as the subgroup of roots of unity in  $\mathbb{G}_m$ . Therefore, we understand  $\mu_\infty^n \subset \mathbb{G}_m^n$  as the subgroup of the torsion points of  $\mathbb{G}_m^n$ , that is

$$\mu_\infty^n = \{\boldsymbol{\xi} \in \mathbb{G}_m^n \mid \boldsymbol{\xi}^k = \mathbf{1} \text{ for some } k \in \mathbb{N}_{>0}\}$$

and  $\mu_k^n = \{\boldsymbol{\xi} \in \mathbb{G}_m^n \mid \boldsymbol{\xi}^k = \mathbf{1}\}$  as the  $k$ -torsion points of  $\mathbb{G}_m^n$ .

By torsion coset we understand a subvariety  $\boldsymbol{\omega}H \subset \mathbb{G}_m^n$ , where  $H$  is an irreducible algebraic subgroup of  $\mathbb{G}_m^n$  and  $\boldsymbol{\omega}$  a torsion point. Let  $V$  be a subvariety of  $\mathbb{G}_m^n$ , then we say that a torsion coset  $\boldsymbol{\omega}H$  is maximal in  $V$  if  $\boldsymbol{\omega}H \subset V$  and it is not contained in any other torsion coset in  $V$ . Observe that  $\overline{V_{\text{tor}}}$  corresponds to the ensemble of torsion cosets in  $V$ , hence we can write it

$$\overline{V_{\text{tor}}} = \bigcup_{\substack{\boldsymbol{\omega}H \subset V \\ \text{torsion coset}}} \boldsymbol{\omega}H.$$

In fact, it is enough to take the maximal torsion cosets in  $V$  in the index of the union.

Let  $V \subset \mathbb{G}_m^n$ . We say that  $V$  is minimally defined over  $\mathbb{K}$ , if  $\mathbb{K}$  is the minimal Galois extension of  $\mathbb{Q}$  such that  $V$  is defined over  $\mathbb{K}$ ; that is

$$\bigcap_{\substack{\mathbb{L} \mid \mathbb{Q} \text{ Galois} \\ V \text{ defined over } \mathbb{L}}} \mathbb{L}.$$

We recall that if  $\mathbb{K}$  is an abelian extension, by the Kronecker-Weber theorem we have that  $\mathbb{K}$  is contained in a cyclotomic extension of  $\mathbb{Q}$ . In fact, there is a unique minimal cyclotomic extension  $\mathbb{Q}(\zeta_N)$  containing  $\mathbb{K}$  (see [Nar04, Theorem 4.27(v)]). If  $N \equiv 2 \pmod{4}$ , then  $\mathbb{Q}(\zeta_N) = \mathbb{Q}(\zeta_{N/2})$ . Therefore, we always choose  $N \not\equiv 2 \pmod{4}$ .

## 2.2 Algebraic subgroups

We understand by lattice a subgroup  $\Lambda$  of  $\mathbb{Z}^n$ . We denote  $\tilde{\Lambda} = (\Lambda \otimes_{\mathbb{Z}} \mathbb{R}) \cap \mathbb{Z}^n$  and call  $[\tilde{\Lambda} : \Lambda]$  the index of  $\Lambda$ . We say that  $\Lambda$  is primitive if  $[\tilde{\Lambda} : \Lambda] = 1$ . We define the algebraic subgroup of  $\mathbb{G}_m^n$  associated to  $\Lambda$  as follows

$$H_\Lambda = \{\mathbf{x} \in \mathbb{G}_m^n \mid \mathbf{x}^\lambda = \mathbf{1}, \lambda \in \Lambda\}.$$

The following result allows us to understand the relation between lattices in  $\mathbb{Z}^n$  and algebraic subgroups of  $\mathbb{G}_m^n$ .

**Theorem 2.1.** *The map  $\Lambda \mapsto H_\Lambda$  is a bijection between subgroups of  $\mathbb{Z}^n$  and algebraic subgroups of  $\mathbb{G}_m^n$ . A subgroup  $H_\Lambda$  is irreducible if and only if  $\Lambda$  is primitive. Moreover, for any two subgroups  $\Lambda$  and  $\Lambda'$  of  $\mathbb{Z}^n$  we have that  $H_\Lambda H_{\Lambda'} = H_{\Lambda \cap \Lambda'}$ .*

*Proof.* See [BG06, Proposition 3.2.7 and Theorem 3.2.19].  $\square$

**Corollary 2.2.** *Let  $H$  be a subgroup of  $\mathbb{G}_m^n$  of dimension  $n - r$ , then there exists a surjective homomorphism*

$$\varphi : \mathbb{G}_m^n \twoheadrightarrow \mathbb{G}_m^r$$

*such that  $\text{Ker}(\varphi) = H$ .*

*Proof.* By Theorem 2.1, there exists a unique lattice  $\Lambda \subset \mathbb{Z}^n$  such that

$$H = H_\Lambda = \{\mathbf{x} \in \mathbb{G}_m^n \mid \mathbf{x}^\lambda = \mathbf{1}, \lambda \in \Lambda\}.$$

Take the primitive subgroup  $\Lambda^\perp = \{\mathbf{x} \in \mathbb{Z}^n \mid \mathbf{x} \cdot \mathbf{y} = 0 \text{ for all } \mathbf{y} \in \Lambda\}$ , so  $H_{\Lambda^\perp}$  is irreducible, that is  $H_{\Lambda^\perp} \simeq \mathbb{G}_m^r$ . By Theorem 2.1 we have that  $\mathbb{G}_m^n = H_{\{0\}} = H \cdot H_{\Lambda^\perp}$  and  $\varphi$  can be obtained as the following composition of homomorphisms:

$$\varphi : \mathbb{G}_m^n = H \cdot H_{\Lambda^\perp} \twoheadrightarrow H_{\Lambda^\perp} \xrightarrow{\simeq} \mathbb{G}_m^r.$$

$\square$

Let  $V$  be a variety in  $\mathbb{G}_m^n$ , we define the stabilizer of  $V$  as

$$\text{Stab}(V) = \{\xi \in \mathbb{G}_m^n \mid \xi V = V\}.$$

In particular,  $\text{Stab}(V)$  is an algebraic subgroup of  $\mathbb{G}_m^n$ . By means of Corollary 2.2 we are able to identify, via a homomorphism,  $V$  and a variety with trivial stabilizer.

**Corollary 2.3.** *Let  $V \subset \mathbb{G}_m^n$  be a variety. Then there exists a homomorphism  $\varphi : \mathbb{G}_m^n \rightarrow \mathbb{G}_m^r$  such that  $r = \text{codim}(\text{Stab}(V))$  and  $\text{Ker}(\varphi) = \text{Stab}(V)$ . Moreover,  $\varphi$  satisfies*

- (i)  $\text{Stab}(\varphi(V)) = \{\mathbf{1}\}$ ;
- (ii)  $\varphi^{-1}(\varphi(V)) = V$ ;
- (iii)  $\varphi^{-1}(\boldsymbol{\eta})V = \boldsymbol{\eta}_0 V$ , for every  $\boldsymbol{\eta} \in \mathbb{G}_m^r$  and for any  $\boldsymbol{\eta}_0 \in \varphi^{-1}(\boldsymbol{\eta})$ .

An extra remark should be made regarding the relation between the torsion cosets and the stabilizer of  $V$ . For any torsion coset  $\boldsymbol{\omega}H$  in  $V$ , we have that  $\text{Stab}(V) \cdot \boldsymbol{\omega}H$  is a union torsion cosets in  $V$ . In particular, every maximal torsion coset in  $V$  has dimension at least  $\dim(\text{Stab}(V))$ .

### 2.3 Essential degree and Hilbert function

Let  $V$  be a variety in  $\mathbb{G}_m^n$ . We define  $\delta(V)$  as the minimal degree  $\delta$  such that  $V$  is the intersection of hypersurfaces of degree at most  $\delta$ . We also define  $\delta_0(V)$  as the minimal degree  $\delta_0$  such that there exists an intersection  $X$  of hypersurfaces of degree at most  $\delta_0$  such that any irreducible component of  $V$  is a component of  $X$ . As a direct consequence of the definition, if  $V$  is equidimensional, we have the following inequalities

$$\delta_0(V) \leq \delta(V) \leq \deg(V).$$

Let  $V$  be a subvariety of  $\mathbb{G}_m^n$  and let the closure of  $V$  in  $\mathbb{P}^n$  be defined by the homogeneous radical ideal  $I$  in  $\mathbb{Q}[\mathbf{x}]$ . For  $\nu \in \mathbb{N}$ , we denote by  $H(V; \nu)$  the Hilbert function  $\dim(\overline{\mathbb{Q}[\mathbf{x}]/I})_\nu$ .

The following upper bound for the Hilbert function, is a theorem of Chardin [Cha89].

**Theorem 2.4.** *Let  $V \subseteq \mathbb{G}_m^n$  be an equidimensional variety of dimension  $d = n - k$  and let  $\nu \in \mathbb{N}$ . Then*

$$H(V; \nu) \leq \binom{\nu + d}{d} \deg(V).$$

On the other hand, as a consequence of a result of Chardin and Phillipon [CP99, Corollaire 3] on Castelnuovo's regularity, we have the following lower bound for the Hilbert function:

**Theorem 2.5.** *Let  $V \subseteq \mathbb{G}_m^n$  be an equidimensional variety of dimension  $d = n - k$  and  $m = k(\delta_0(V) - 1)$ . Then, for any integer  $\nu > m$ , we have*

$$H(V; \nu) \geq \binom{\nu + d - m}{d} \deg(V).$$

In order to use these results later, we need effective upper bounds for  $\delta_0(V')$  when  $V'$  is a specific type of equidimensional variety. Let us recall first an easy lemma for  $\delta$ .

**Lemma 2.6.** *Let  $X_1, \dots, X_t$  be subvarieties of  $\mathbb{G}_m^n$ . Then*

$$\delta\left(\bigcup_{i=1}^t X_i\right) \leq \sum_{i=1}^t \delta(X_i).$$

*Proof.* It is enough to prove it for  $t = 2$ . Let  $X_1$  be defined by the equations  $f_1, \dots, f_r$  with  $\deg(f_i) \leq \delta(X_1)$  and equivalently let  $X_2$  be defined  $g_1, \dots, g_s$  with  $\deg(g_i) \leq \delta(X_2)$ . Then  $X_1 \cup X_2$  is defined by the equations  $f_i g_j$  for  $1 \leq i \leq r$  and  $1 \leq j \leq s$ .  $\square$

To state a similar lemma for  $\delta_0$ , we must consider more specific varieties. The following is a variation of [AV12, Lemma 2.5.].

**Lemma 2.7.** *Let  $V$  be an irreducible subvariety of  $\mathbb{G}_m^n$  defined over  $\mathbb{K}$ . Let  $T \subset \mu_\infty^n \times \text{Gal}(\mathbb{K}/\mathbb{Q})$  be a finite family with  $t$  elements. Then*

$$\delta_0\left(\bigcup_{(\mathbf{g}, \phi) \in T} \mathbf{g}V^\phi\right) \leq t\delta_0(V).$$

*Proof.* We say that an irreducible variety  $W \subset \mathbb{G}_m^n$  is imbedded in a variety  $X \subset \mathbb{G}_m^n$  if  $W \subset X$  but  $W$  is not an irreducible component of  $X$ .

By definition of  $\delta_0(V)$ , there exists a variety  $X$  such that  $V$  is an irreducible component of  $X$  and  $\delta_0(V) = \delta(X)$ .

Let  $G \subset \mu_\infty^n \times \text{Gal}(\mathbb{K}/\mathbb{Q})$  be the group generated by  $T$  and let  $S = \{(\mathbf{g}, \phi) \in G \mid \mathbf{g}V^\phi \text{ is imbedded in } X\}$ . Consider

$$\tilde{X} = X \cap \left( \bigcap_{(\mathbf{g}, \phi) \in S} \mathbf{g}^{-1}X^{\phi^{-1}} \right).$$

We have that  $V$  is an irreducible component of  $\tilde{X}$  and  $\delta(\tilde{X}) = \delta(X) = \delta_0(V)$ . Moreover, no  $\mathbf{g}V^\phi$  is imbedded in  $\tilde{X}$ , for  $(\mathbf{g}, \phi) \in G$ . Assume by contradiction that there is a  $\mathbf{g}V^\phi$  imbedded in  $\tilde{X}$ . We are going to show that then  $(\mathbf{g}^n, \phi^n) \in S$  for every  $n \in \mathbb{N}_{>0}$ ; in particular, taking  $n = \text{lcm}(\text{ord}(\mathbf{g}), \text{ord}(\phi))$  we will have  $(\mathbf{1}, \text{Id}) \in S$  which is a contradiction. Since  $\tilde{X} \subset X$ ,  $\mathbf{g}V^\phi$  is imbedded in  $X$  and so  $(\mathbf{g}, \phi) \in S$ . By induction, we suppose  $(\mathbf{g}^n, \phi^n) \in S$  for some  $n \geq 1$ . Then  $\tilde{X} \subset \mathbf{g}^{-n}X^{\phi^{-n}}$  and so  $\mathbf{g}V^\phi$  is imbedded in  $\mathbf{g}^{-n}V^{\phi^{-n}}$  which implies  $(\mathbf{g}^{n+1}, \phi^{n+1}) \in S$ .

Next we define

$$Y = \bigcup_{(\mathbf{g}, \phi) \in T} \mathbf{g}\tilde{X}^\phi.$$

Then  $\bigcup_{(\mathbf{g}, \phi) \in T} \mathbf{g}V^\phi \subset Y$  and, by lemma 2.6,  $\delta(Y) \leq t\delta(\tilde{X}) = t\delta_0(V)$ . Moreover, no  $\mathbf{g}V^\phi$  is imbedded in  $Y$ , for  $(\mathbf{g}, \phi) \in T$ . Assume by contradiction that there is a  $(\mathbf{g}, \phi) \in T$  such that  $\mathbf{g}V^\phi$  is imbedded in  $Y$ . Then, there exists some  $(\mathbf{g}_0, \phi_0) \in T$  such that  $\mathbf{g}V^\phi$  is imbedded in  $\mathbf{g}_0\tilde{X}^{\phi_0}$ . Thus  $\mathbf{g}_0^{-1}\mathbf{g}V^{\phi_0^{-1}\phi}$  is imbedded in  $\tilde{X}$  which contradicts the definition of  $\tilde{X}$  since  $(\mathbf{g}_0^{-1}\mathbf{g}, \phi_0^{-1}\phi) \in G$ . □

The following lemma is a key ingredient in the proof of Theorem 3.4.

**Lemma 2.8.** *Let  $V \subseteq \mathbb{G}_m^n$  be an irreducible variety of dimension  $d = n - k$ , minimally defined over  $\mathbb{K}$ . Let  $\phi \in \text{Gal}(\mathbb{K}/\mathbb{Q})$  and let  $\mathbf{e} \in \mu_\infty^n$ .*

- (a) *If  $\mathbf{e}V^\phi \neq V$ , then there exists a homogeneous polynomial  $F$  of degree at most  $2k(2d + 1)\delta_0(V)$  such that  $F \equiv 0$  in  $\mathbf{e}V^\phi$  and  $F \not\equiv 0$  in  $V$ .*
- (b) *If  $[2]^{-1}(\mathbf{e}V^\phi) \neq V$ , then there exists a homogeneous polynomial  $G$  of degree at most  $2^nk(2d + 1)\delta_0(V)$  such that  $G \equiv 0$  in  $[2]^{-1}(\mathbf{e}V^\phi)$  and  $G \not\equiv 0$  in  $V$ .*

*Proof.*

- (a) Since  $V$  is an irreducible variety,  $\mathbf{e}V^\phi$  is also irreducible and of the same degree. Then, using Theorem 2.4 we get, for any  $\nu \in \mathbb{N}$ ,

$$H(\mathbf{e}V^\phi; \nu) \leq \binom{\nu + d}{d} \deg(V).$$



On the other hand, let  $V' = V \cup eV^\phi$ . This is  $d$ -equidimensional of degree  $2 \deg(V)$ . Thereby using Theorem 2.5 we have, for any  $\nu > m$ ,

$$H(V'; \nu) \geq \binom{\nu + d - m}{d} 2 \deg(V),$$

where  $m = k(\delta_0(V') - 1)$ . By Lemma 2.7,  $m \leq 2k\delta_0(V)$ .

Taking  $\nu = m(2d + 1)$  we obtain:

$$\binom{\nu + d}{d} \binom{\nu + d - m}{d}^{-1} \leq \left(1 + \frac{m}{\nu - m}\right)^d = \left(1 + \frac{1}{2d}\right)^d \leq e^{1/2} < 2.$$

Hence,  $H(eV^\phi; \nu) < H(V'; \nu)$ .

This means that there exists a homogeneous polynomial  $F$  of degree  $\nu$  such that  $F \equiv 0$  on  $eV^\phi$  and  $F \not\equiv 0$  on  $V' = eV^\phi \cup V$ , in particular  $F \not\equiv 0$  on  $V$ . Moreover,  $\deg(F) = \nu \leq 2k(2d + 1)\delta_0(V)$ , which proves (a).

- (b) Let  $W = [2]^{-1}(eV^\phi)$ . Since  $W$  is  $d$ -equidimensional of degree  $2^k \deg(V)$ , by using Theorem 2.4 we get, for any  $\nu \in \mathbb{N}$ ,

$$H(W; \nu) \leq \binom{\nu + d}{d} 2^k \deg(V).$$

On the other hand, let  $E = \{e_0 \in \mu_\infty^n \mid e_0^2 \in \text{Stab}(V)\}$  and let  $W' = E \cdot V$ . This variety is also  $d$ -equidimensional and of degree  $2^r \deg(V)$ , for some  $k < r \leq n$ , that is because  $E/\text{Stab}(V) \simeq \mu_2^r$  (see Corollary 2.3,  $r = \text{codim}(\text{Stab}(V))$ ) and  $E = \varphi^{-1}(\mu_2^r)$ . Thereby, using Proposition 2.5 we have, for any  $\nu > m$ ,

$$H(W'; \nu) \geq \binom{\nu + d - m}{d} 2^r \deg(V),$$

where  $m = k(\delta_0(W') - 1)$ . By Lemma 2.7,  $m \leq 2^r k \delta_0(V)$ .

Taking  $\nu = m(2d + 1)$ , we obtain:

$$\binom{\nu + d}{d} \binom{\nu + d - m}{d}^{-1} \leq e^{1/2} < 2^{r-k}.$$

Hence,  $H(W; \nu) < H(W', \nu)$ .

This means that there exists a homogeneous polynomial  $\tilde{G}$  of degree  $\nu$  such that  $\tilde{G} \equiv 0$  on  $W = [2]^{-1}(eV^\phi)$  and  $\tilde{G} \not\equiv 0$  on  $W' = E \cdot V$ , in particular there exists  $e_0 \in E$  such that  $\tilde{G} \not\equiv 0$  on  $e_0V$ .

Let  $G(x) = \tilde{G}(e_0^{-1}x)$ . We have that  $G \equiv 0$  on  $e_0[2]^{-1}(eV)$ . By definition of  $E$ ,  $e_0 \in \text{Stab}([2]^{-1}(eV))$ . Hence,  $G \equiv 0$  on  $[2]^{-1}(eV)$ . We also have that  $G \not\equiv 0$  on  $e_0^2V$ . Since  $e_0^2 \in \text{Stab}(V)$ , that is  $G \not\equiv 0$  on  $V$ . Moreover,  $\deg(G) = \nu \leq 2^r k(2d + 1)$ , which proves (b). □

### 3 Algebraic interpolation

We generalize [BS02, Lemma 1] to general dimension  $n$  and to any abelian extension of  $\mathbb{Q}$  with the following result.

**Lemma 3.1.** *Let  $V \subset \mathbb{G}_m^n$  be a variety defined over  $\mathbb{Q}(\zeta_N)$ , with  $N \not\equiv 2 \pmod{4}$ , and let  $\omega \in V$  be a torsion point.*

1. *If  $4 \nmid N$ , then one of the following is true:*

- (a) *there exists  $\eta \in \mu_2^n \setminus \{\mathbf{1}\}$  such that  $\eta \cdot \omega \in V$ ; or*
- (b) *there exists  $\eta \in \mu_2^n$  such that  $\eta \cdot \omega^2 \in V^\sigma$ , where  $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$  maps  $\zeta_N \mapsto \zeta_N^2$ .*

2. *If  $N = 4N'$ , then one of the following is true:*

- (c) *there exists  $\eta \in \mu_2^n \setminus \{\mathbf{1}\}$  such that  $\eta \cdot \omega \in V$ ; or*
- (d) *there exists  $\eta \in \mu_2^n$  such that  $\eta \cdot \omega \in V^\tau$ , where  $\tau \in \text{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$  maps  $\zeta_N \mapsto \zeta_N^{1+2N'}$ .*

Note first that the case  $\mathbb{K} = \mathbb{Q}$  is included in case 1, corresponding to  $N = 1$  (and so  $\sigma$  is the identity).

*Proof.* Let  $l$  be the order of  $\omega$ , in particular  $\omega \in \mathbb{Q}(\zeta_l)$ .

1. Let  $M = \text{lcm}(N, l)$ . We distinguish 3 cases.

- (i) If  $l = 4l'$ , then  $M = 4M'$ . We have  $\gcd(1 + 2M', M) = 1$  and thus we can take  $\tau \in \text{Gal}(\mathbb{Q}(\zeta_M)/\mathbb{Q})$  mapping  $\zeta_M \mapsto \zeta_M^{1+2M'}$ . Since  $2M' \equiv 2l' \pmod{l}$ , we have that  $\tau$  maps  $\zeta_l \mapsto \zeta_l^{1+2l'}$ . On the other hand,  $2M' \equiv 0 \pmod{N}$  because  $N$  is odd (in fact  $N \mid M'$ ), therefore  $\tau$  maps  $\zeta_N \mapsto \zeta_N$ . Hence  $V^\tau = V$  and  $\omega^{1+2l'} \in V$ . Therefore (a) holds choosing  $\eta = \omega^{2l'} \in \mu_2^n \setminus \{\mathbf{1}\}$ .
- (ii) If  $l = 2l'$  with  $2 \nmid l'$ , then  $M = 2M'$  with  $2 \nmid M'$ . We have  $\gcd(2 + M', M) = 1$  and thus we can extend  $\sigma$  to a Galois automorphism in  $\text{Gal}(\mathbb{Q}(\zeta_M)/\mathbb{Q})$ , mapping  $\zeta_M \mapsto \zeta_M^{2+M'}$  (this extends  $\sigma$  because  $N$  is odd and so  $N \mid M'$ ). Since  $M' \equiv l' \pmod{l}$ , we have that  $\sigma$  maps  $\zeta_l \mapsto \zeta_l^{2+l'}$ . Hence  $\omega^{2+l'} \in V^\sigma$ . Therefore (b) holds choosing  $\eta = \omega^{l'} \in \mu_2^n \setminus \{\mathbf{1}\}$ .
- (iii) If  $2 \nmid l$ , then  $2 \nmid M$  and  $\sigma$  can be extended to a Galois automorphism in  $\text{Gal}(\mathbb{Q}(\zeta_M)/\mathbb{Q})$  mapping  $\zeta_M \mapsto \zeta_M^2$ . In particular,  $\sigma$  maps  $\zeta_l \mapsto \zeta_l^2$ , hence  $\omega^2 \in V^\sigma$ . Therefore (b) holds choosing  $\eta = \mathbf{1}$ .

2. Let  $M = 4M' = \text{lcm}(N, l)$  and  $\tilde{\tau}$  be an automorphism in  $\text{Gal}(\mathbb{Q}(\zeta_M)/\mathbb{Q})$  mapping  $\zeta \mapsto \zeta_M^{2M'+1}$ . We distinguish 2 cases.

- (i) If  $N \mid 2M'$ , then  $l \nmid 2M'$  (otherwise, we would have  $\text{lcm}(N, l) = 2M'$ ). Since  $2M' \equiv 2l' \pmod{l}$ , we have that  $\tilde{\tau}$  maps  $\zeta_l \mapsto \zeta_l^{1+2l'}$ . On the other hand,  $2M' \equiv 0 \pmod{N}$ , therefore  $\tilde{\tau}$  maps  $\zeta_N \mapsto \zeta_N$ . Hence  $V^{\tilde{\tau}} = V$  and  $\omega^{1+2M'} \in V$ . Therefore (c) holds choosing  $\eta = \omega^{2l'} \in \mu_2^n \setminus \{\mathbf{1}\}$ .

- (ii) If  $N \nmid 2M'$ , then  $2N' \equiv 2M' \pmod{N}$ . So, we have that  $\tilde{\tau}$  maps  $\zeta_N \mapsto \zeta_N^{1+2N'}$  and thus  $\tilde{\tau}_{\mathbb{Q}(\zeta_N)} = \tau$ . Therefore (d) holds choosing  $\boldsymbol{\eta} = \boldsymbol{\omega}^{2M'} \in \mu_2^n$ .

□

As a consequence of this lemma, for any irreducible variety  $V$  we can find another variety  $V'$  containing the torsion subvariety of  $V$  but not containing  $V$ .

**Proposition 3.2.** *Let  $V \subset \mathbb{G}_m^n$  be an irreducible variety, minimally defined over  $\mathbb{K}$ , of dimension  $d = n - k$ ,  $\overline{V_{\text{tor}}} \neq V$  and let  $\varphi : \mathbb{G}_m^n \rightarrow \mathbb{G}_m^r$  be a homomorphism such that  $\text{Stab}(V) = \text{Ker}(\varphi)$ ,  $k < r \leq n$ , where  $r$  is the codimension of  $\text{Stab}(V)$  (which exists by Corollary 2.2).*

1. *If  $\mathbb{K}$  is abelian and  $\mathbb{Q}(\zeta_N)$  is a cyclotomic extension of  $\mathbb{K}$ , with  $4 \nmid N$ , then*

$$\overline{V_{\text{tor}}} \subset V' = \bigcup_{\boldsymbol{\eta} \in \mu_2^r \setminus \{\mathbf{1}\}} (\varphi^{-1}(\boldsymbol{\eta})V) \cup \bigcup_{\boldsymbol{\eta} \in \mu_2^r} [2]^{-1}(\varphi^{-1}(\boldsymbol{\eta})V^\sigma),$$

where  $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ , mapping  $\zeta_N \mapsto \zeta_N^2$ , and  $V' \cap V \subsetneq V$ .

2. *If  $\mathbb{K}$  is abelian and  $\mathbb{Q}(\zeta_N)$  is its minimal cyclotomic extension, with  $N = 4N'$ , then*

$$\overline{V_{\text{tor}}} \subset V' = \bigcup_{\boldsymbol{\eta} \in \mu_2^r \setminus \{\mathbf{1}\}} (\varphi^{-1}(\boldsymbol{\eta})V) \cup \bigcup_{\boldsymbol{\eta} \in \mu_2^r} (\varphi^{-1}(\boldsymbol{\eta})V^\tau),$$

where  $\tau \in \text{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ , mapping  $\zeta_N \mapsto \zeta_N^{1+2N'}$ , and  $V' \cap V \subsetneq V$ .

3. *If  $\mathbb{K}$  is not abelian, then  $\overline{V_{\text{tor}}} \subset V \cap V^\varsigma \subsetneq V$ , for any  $\varsigma \in \text{Gal}(\mathbb{K}/\mathbb{Q}^{\text{ab}} \cap \mathbb{K})$  such that  $\varsigma \neq \text{Id}$ .*

Note that the  $V'$  in the proposition are finite unions of varieties. That is because, using Corollary 2.3(iii), it suffices to take, for each  $\boldsymbol{\eta} \in \mu_2^r$ , just one preimage  $\boldsymbol{\eta}_0 \in \varphi^{-1}(\boldsymbol{\eta})$  instead of the the whole  $\varphi^{-1}(\boldsymbol{\eta})$  in the definition of  $V'$ .

*Proof.*

1. Let  $V_{\text{tor}} = \{\boldsymbol{\omega}' \in V \mid \boldsymbol{\omega}' \text{ torsion point}\}$ , therefore, it is enough to see that  $V_{\text{tor}} \subset V'$  to prove  $\overline{V_{\text{tor}}} \subset V'$ . To show that, we take  $\boldsymbol{\omega}' \in S$ , then  $\varphi(\boldsymbol{\omega}')$  is a torsion point in  $\varphi(V)$ . Since  $\varphi(V)$  is defined over  $\mathbb{Q}(\zeta_N)$ , with  $N$  odd, we can apply point 1 in Lemma 3.1 to  $\varphi(V)$ , hence one of the following is true:

- (a) There exists  $\boldsymbol{\eta} \in \mu_2^r \setminus \{\mathbf{1}\}$  such that  $\varphi(\boldsymbol{\omega}') \in \boldsymbol{\eta}\varphi(V)$ , hence  $\boldsymbol{\omega}' \in \varphi^{-1}(\boldsymbol{\eta})V$ . Moreover, by definition of  $\varphi$  we have that  $\varphi^{-1}(\boldsymbol{\eta}) \notin \text{Stab}(V)$  and therefore  $(\varphi^{-1}(\boldsymbol{\eta})V) \cap V \subsetneq V$ .

- (b) There exists  $\boldsymbol{\eta} \in \mu_2^r$  such that  $\varphi(\boldsymbol{\omega}')^2 \in \boldsymbol{\eta}\varphi(V)^\sigma$ , then  $\boldsymbol{\omega}' \in [2]^{-1}(\varphi^{-1}(\boldsymbol{\eta})V^\sigma)$ . Moreover, we have that  $[2]^{-1}(\varphi^{-1}(\boldsymbol{\eta})V^\sigma) \cap V \subsetneq V$ . To prove that, assume  $V \subset [2]^{-1}(\varphi^{-1}(\boldsymbol{\eta})V^\sigma)$ , hence, since  $\varphi^{-1}(\boldsymbol{\eta}_0) \in \text{Stab}([2]^{-1}(\varphi^{-1}(\boldsymbol{\eta})V^\sigma))$  for every  $\boldsymbol{\eta}_0 \in \mu_2^r$ , we have

$$\bigcup_{\boldsymbol{\eta}_0 \in \mu_2^r} \varphi^{-1}(\boldsymbol{\eta}_0)V \subset [2]^{-1}(\varphi^{-1}(\boldsymbol{\eta})V^\sigma).$$

Since  $\varphi^{-1}(\mu_2^r) \cap \text{Stab}(V) = \{\mathbf{1}\}$  (see (a) above) and all the translates of  $V$  have the same stabilizer, we have that  $\deg(\bigcup \varphi^{-1}(\boldsymbol{\eta}_0)V) = 2^r \deg(V)$ . On the other hand,  $\deg([2]^{-1}(\varphi^{-1}(\boldsymbol{\eta})V^\sigma)) = 2^k \deg(V)$  (see [Hin88, Lemme 6(i)]) and since  $k < r$ , this leads to a contradiction.

Thereby,  $\boldsymbol{\omega}' \in V'$  for every  $\boldsymbol{\omega}' \in V_{\text{tor}}$  and thus  $\overline{V_{\text{tor}}} \subset V'$ . Moreover,  $V' \cap V \subsetneq V$ .

2. The proof follows similar to the previous one, using point 2 in Lemma 3.1. Note that, in this case, we need the minimality of  $N$  to guarantee that  $V^r \neq V$  and, as a consequence, that  $V \cap V' \neq V$ .
3. Since every torsion coset is defined over  $\mathbb{Q}^{\text{ab}}$ , it is invariant by  $\varsigma$ . Hence, for every torsion coset  $\boldsymbol{\omega}H \subset V$ , we have that  $\boldsymbol{\omega}H \subset V^\varsigma$  and  $V \neq V^\varsigma$ , due to the minimality of  $\mathbb{K}$ .

□

**Remark 3.3.** We can consider  $\mathbb{K} = \mathbb{C}$  as the field of definition of  $V$ . Then it follows equivalently to the case when  $\mathbb{K}$  is not abelian to prove that

$$\overline{V_{\text{tor}}} \subset V \cap V^\varsigma \subsetneq V,$$

for any  $\varsigma \in \text{Gal}(\mathbb{C}/\mathbb{Q}^{\text{ab}})$  such that  $\varsigma \neq \text{Id}$ .

The following theorem is a specialization of [AV09, Theorem 1.2] to torsion subvarieties. Keeping the notation of the proposition above, note that  $\varphi^{-1}(\boldsymbol{\eta})^2$  lies in the stabilizer of  $V$ , for any  $\boldsymbol{\eta} \in \mu_\infty^r$ . This is a fundamental so that we can use Lemma 2.8 in the proof of the following theorem.

**Theorem 3.4.** *Let  $V \subset \mathbb{G}_m^n$  be an irreducible variety of dimension  $d = n - k$  and not a torsion coset. Let*

$$\theta_0 = \theta_0(V) = k(2^{2n} + 2^{n+1} - 2)(2d + 1)\delta_0(V).$$

*Then  $\overline{V_{\text{tor}}}$  is contained in a hypersurface  $Z$  of degree at most  $\theta_0$ , which does not contain  $V$ ; i.e.  $\overline{V_{\text{tor}}} \subset V \cap Z \subsetneq V$ .*

*Proof.* Let  $V$  be minimally defined over  $\mathbb{K}$ . To prove this theorem, we distinguish three cases, according to Proposition 3.2.

1. If  $\mathbb{K}$  is abelian and  $\mathbb{Q}(\zeta_N)$  is a cyclotomic extension of  $\mathbb{K}$ , with  $4 \nmid N$ , then by point 1 in Proposition 3.2 we have that

$$\overline{V_{\text{tor}}} \subset V' = \left( \bigcup_{\boldsymbol{\eta} \in \mu_2^r \setminus \{1\}} (\varphi^{-1}(\boldsymbol{\eta})V) \cup \bigcup_{\boldsymbol{\eta} \in \mu_2^s} [2]^{-1}(\varphi^{-1}(\boldsymbol{\eta})V^\sigma) \right),$$

where  $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ , mapping  $\zeta_N \mapsto \zeta_N^2$  and  $V \cap V' \subsetneq V$ .

To prove the theorem we find, for each component of  $V'$ , a hypersurface containing it, but not containing  $V$ . To conclude, it is enough to take  $Z$  as the union of these hypersurfaces and the only thing left to check is the degree of  $Z$ .

For any  $\boldsymbol{\eta} \in \mu_2^r \setminus \{1\}$ , by setting  $\mathbf{e} = \varphi^{-1}(\boldsymbol{\eta})$  and  $\phi = \text{Id}$ , we can use (a) of Lemma 2.8 and we obtain a homogeneous polynomial  $F_\boldsymbol{\eta}$  of degree at most  $2k(2d+1)\delta_0(V)$  such that  $F_\boldsymbol{\eta} \equiv 0$  on  $\varphi^{-1}(\boldsymbol{\eta})V$  and  $F_\boldsymbol{\eta} \not\equiv 0$  on  $V$ .

On the other hand, for any  $\boldsymbol{\eta} \in \mu_2^s$ , by setting  $\mathbf{e} = \varphi^{-1}(\boldsymbol{\eta})$  and  $\phi = \sigma$ , we can use (b) of Lemma 2.8 and we obtain a homogeneous polynomial  $G_\boldsymbol{\eta}$  of degree at most  $2^nk(d+1)\delta_0(V)$  such that  $G_\boldsymbol{\eta} \equiv 0$  on  $[2]^{-1}(\varphi^{-1}(\boldsymbol{\eta})V)$  and  $G_\boldsymbol{\eta} \not\equiv 0$  on  $V$ .

Therefore, if we take

$$Z = V \left( \prod_{\boldsymbol{\eta} \in \mu_2^r \setminus \{1\}} F_\boldsymbol{\eta} \cdot \prod_{\boldsymbol{\eta} \in \mu_2^s} G_\boldsymbol{\eta} \right),$$

we have

$$\deg(Z) \leq \left( \sum_{\boldsymbol{\eta} \in \mu_2^r \setminus \{1\}} 2k(2d+1)\delta_0(V) \right) + \left( \sum_{\boldsymbol{\eta} \in \mu_2^s} 2^nk(2d+1)\delta_0(V) \right) \leq \theta_0$$

and  $\overline{V_{\text{tor}}} \subset V \cap V' \subset V \cap Z \subsetneq V$ .

2. If  $\mathbb{K}$  is abelian and  $\mathbb{Q}(\zeta_N)$  is its minimal cyclotomic extension, with  $N = 4N'$ , then by point 2 in Proposition 3.2 we have

$$\overline{V_{\text{tor}}} \subset V' = \left( \bigcup_{\boldsymbol{\eta} \in \mu_2^r \setminus \{1\}} (\varphi^{-1}(\boldsymbol{\eta})V) \cup \bigcup_{\boldsymbol{\eta} \in \mu_2^s} (\varphi^{-1}(\boldsymbol{\eta})V^\tau) \right),$$

where  $\tau \in \text{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ , mapping  $\zeta_N \mapsto \zeta_N^{1+2N'}$  and  $V \cap V' \subsetneq V$ . We proceed as before.

For any  $\boldsymbol{\eta} \in \mu_2^r \setminus \{1\}$ , by setting  $\mathbf{e} = \varphi^{-1}(\boldsymbol{\eta})$  and  $\phi = \text{Id}$ , we can use (a) of Lemma 2.8 and we obtain a homogeneous polynomial  $F_\boldsymbol{\eta}$  of degree at most  $2k(2d+1)\delta_0(V)$  such that  $F_\boldsymbol{\eta} \equiv 0$  on  $\varphi^{-1}(\boldsymbol{\eta})V$  and  $F_\boldsymbol{\eta} \not\equiv 0$  on  $V$ .

On the other hand, for any  $\boldsymbol{\eta} \in \mu_2^s$ , by setting  $\mathbf{e} = \varphi^{-1}(\boldsymbol{\eta})$  and  $\phi = \tau$ , we can use again (a) of Lemma 2.8 and we obtain a homogeneous polynomial  $F'_\boldsymbol{\eta}$  of degree at most  $2k(2d+1)\delta_0(V)$  such that  $F'_\boldsymbol{\eta} \equiv 0$  on  $\varphi^{-1}(\boldsymbol{\eta})V^\tau$  and  $F'_\boldsymbol{\eta} \not\equiv 0$  on  $V$ .

Therefore, if we take

$$Z = V \left( \prod_{\eta \in \mu_2^r \setminus \{1\}} F_\eta \cdot \prod_{\eta \in \mu_2^r} F'_\eta \right),$$

we have

$$\deg(Z) \leq \left( \sum_{\eta \in \mu_2^r \setminus \{1\}} 2k(2d+1)\delta_0(V) \right) + \left( \sum_{\eta \in \mu_2^r} 2k(2d+1)\delta_0(V) \right) \leq \theta_0$$

and  $\overline{V_{\text{tor}}} \subset V \cap V' \subset V \cap Z \subsetneq V$ .

3. If  $\mathbb{K}$  is not abelian, by point 3 in Proposition 3.2, we have that  $\overline{V_{\text{tor}}} \subset V \cap V^\varsigma$  for any  $\varsigma \in \text{Gal}(\mathbb{K}/\mathbb{Q}^{\text{ab}} \cap \mathbb{K})$  such that  $\varsigma \neq \text{Id}$ .

By setting  $e = 1$  and  $\phi = \varsigma$  we can use (a) in Lemma 2.8 and we obtain a homogeneous polynomial  $F$  of degree at most  $2k(2d+1)\delta_0(V)$  such that  $F \equiv 0$  on  $V^\varsigma$  and  $F \not\equiv 0$  on  $V$ . Therefore, if we take  $Z = V(F)$ , then we have that  $\deg(Z) \leq \theta_0$  and  $\overline{V_{\text{tor}}} \subset V \cap V^\varsigma \subset V \cap Z \subsetneq V$ .

If  $V$  is not defined over an extension of  $\mathbb{Q}$ , using Remark 3.3 it follows analogous to point 3 that the theorem also holds in this case.  $\square$

## 4 Induction theorems

The following theorems correspond to Theorem 2.2 and Theorem 1.2 in [AV09]. The steps followed in both proofs are analogous to the ones in the proofs of Amoroso and Viada. For the convenience of the reader, we reproduce the proofs.

**Theorem 4.1.** *Let  $V_0 \subset V_1$  subvarieties of  $\mathbb{G}_m^n$  of codimension  $k_0$  and  $k_1$  respectively and  $V_0$  irreducible. Let*

$$\theta = \theta(V_1) = ((2n-1)k_0(2^{2n} + 2^{n+1} - 2))^{k_0 - k_1 + 1} \delta(V_1).$$

*Then either*

- (a) *there exists a torsion coset  $B$  such that  $V_0 \subseteq B \subseteq V_1$ ; or*
- (b) *there exists a hypersurface  $Z$  of degree at most  $\theta$  such that  $V_0 \not\subseteq Z$  and  $\overline{V_{0,\text{tor}}} \subseteq Z$ .*

*Proof.* We assume the statement is false, that is

- (a')  $V_0$  is not contained in any torsion coset  $B \subset V_1$ ; and
- (b') for every hypersurface  $Z$  satisfying  $\overline{V_{0,\text{tor}}} \subset Z$ , we also have that  $V_0 \subset Z$ .

We define, for  $r = 0, \dots, k_0 - k_1 + 1$ ,

$$D_r = ((2n - 1)k_0(2^{2n} + 2^{n+1} - 2))^r \delta(V_1),$$

and we build a chain of varieties

$$X_0 = V_1 \supseteq \dots \supseteq X_{k_0 - k_1 + 1}$$

such that, for every  $r = 0, \dots, k_0 - k_1 + 1$ , the following holds:

- (i)  $V_0 \subseteq X_r$ ,
- (ii) each irreducible component of  $X_r$  containing  $V_0$  has codimension at least  $r + k_1$ , and
- (iii)  $\delta(X_r) \leq D_r$ .

If this holds for  $r = k_0 - k_1 + 1$ , we arrive to a contradiction (because we would have a component of  $X_r$  of codimension at least  $k_0 + 1$  containing  $V_0$ ).

We build the chain by recursion:

- For  $r = 0$ ,  $X_0 = V_1$  satisfies the properties.
- For  $r + 1 > 1$ , we assume we have already constructed  $X_r$ . Let  $W_1, \dots, W_t$  be the irreducible components of  $X_r$  such that

$$V_0 \subset W_j \Leftrightarrow 1 \leq j \leq s.$$

The property (i) guaranties  $s > 0$  and, together with property (ii), says  $r + k_1 \leq \text{codim}(W_j) \leq k_0$  for  $1 \leq j \leq s$ .

For every  $j = 1, \dots, s$  we have  $\delta_0(W_j) \leq \delta(X_r) \leq D_r \leq \theta$  and  $V_0 \subseteq W_j \subset V_1$ , with  $\text{codim}(W_j) = k$ . Hence, by hypothesis (a'),  $W_j$  is not a torsion coset and we can apply Theorem 4.1 to  $W_j$ . Let  $Z_j$  be the hypersurface of degree at most  $(2d + 1)k(2^{2k} + 2^{k+1} - 2)\delta_0(W_j) \leq (2n - 1)k_0(2^{2k_0} + 2^{k_0+1} - 2)D_r = D_{r+1}$  such that  $\overline{W_{j,\text{tor}}} \subseteq W_j \cap Z_j \subsetneq W_j$ . Since  $V_0 \subseteq W_j$ ,  $\overline{V_{0,\text{tor}}} \subseteq \overline{W_{j,\text{tor}}} \subset Z_j$  and, together with the fact that  $\deg(Z_j) \leq D_{r+1} \leq \theta$ , hypothesis (b') guaranties  $V_0 \subset Z_j$ .

So

$$V_0 \subset \bigcap_{j=1}^s Z_j,$$

and we define

$$X_{r+1} = X \cap \bigcap_{j=1}^s Z_j.$$

In particular,  $V_0 \subseteq X_{r+1}$  and property (i) is satisfied. Moreover, property (iii) is also satisfied, because

$$\delta(X_{r+1}) = \max\{\delta(X_r), \deg Z_1, \dots, \deg Z_s\} \leq \max\{D_r, D_{r+1}\} = D_{r+1}.$$

By taking  $W'_j = W_j \cap Z_1 \cap \cdots \cap Z_s$  for every  $j = 1, \dots, t$  we have

$$X_{r+1} = W'_1 \cup \cdots \cup W'_s \cup W'_{s+1} \cup W'_t.$$

For  $j = 1, \dots, s$ , we have that every irreducible component of  $W'_j$  has codimension at least  $\text{codim}(W_j) + 1 \geq r + k_1 + 1$ ; and for  $j = s + 1, \dots, t$   $V_0 \not\subset W_j$  and thus  $V_0$  is not contained in any irreducible component of  $W'_j$ . This shows that property (ii) is satisfied. □

**Theorem 4.2.** *Let  $V \subset \mathbb{G}_m^n$  be a variety of dimension  $d = n - k > 0$ , and let*

$$\theta = \theta(V) = ((2n - 1)(n - 1)(2^{2n} + 2^{n+1} - 2))^{n-k} \delta(V).$$

Let

$$\overline{V}_{\text{tor}} = G_k \cup \cdots \cup G_n,$$

where  $G_j$  is the reunion of the maximal torsion cosets in  $V$  of codimension  $j$  (possibly empty). Then, for  $r = k, \dots, n$ ,

$$\sum_{i=k}^r \theta^{r-i} \deg(G_i) \leq \theta^r.$$

*Proof.* Let  $V = X_k \cup \cdots \cup X_n$ , where  $X_j$  is the  $(n - j)$ -equidimensional part of  $V$  for every  $j$ . We build the family  $G_k, \dots, G_n$  of the statement recursively.

CLAIM. For every  $r = k, \dots, n$  there exist equidimensional varieties  $G_k, \dots, G_{r-1}$  and  $X'_r$  of codimension  $k, \dots, r$  respectively, such that

- (i) for  $j = k, \dots, r - 1$ , the variety  $G_j$  is a finite union of torsion cosets;
- (ii)  $\overline{V}_{\text{tor}} \subseteq G_k \cup \cdots \cup G_{r-1} \cup X'_r \cup X_{r+1} \cup \cdots \cup X_n$ ; and
- (iii)  $\sum_{i=k}^{r-1} \theta^{r-i} \deg(G_i) + \deg(X'_r) \leq \sum_{i=k}^r \theta^{r-i} \deg(X_i)$ .

If the claim holds for  $r = n$ , we take  $G_n = X'_n$ . By assertion (ii) of our claim,  $\overline{V}_{\text{tor}} \subset G_k \cup \cdots \cup G_n$ . Moreover, assertion (ii) also guaranties that  $G_r \subset X'_r$  which, using assertion (iii), implies that

$$\sum_{i=k}^r \theta^{r-i} \deg(G_i) \leq \sum_{i=k}^r \theta^{r-i} \deg(X_i)$$

A result of Philippon [Phi95, Corollaire 5] (with  $m = n$  and  $S = \mathbb{P}^n$ ) shows that, for  $\theta \geq \delta(V)$ , we have

$$\sum_{i=k}^r \theta^{r-i} \deg(X_i) \leq \theta^r,$$

which gives the inequality of the statement.

It remains to proof the claim. We build the family as follows.



- For  $r = k$ , we take  $X'_k = X_k$  and the claim holds.
- For  $k < r + 1 \leq n$ , we assume we have already a family  $G_k, \dots, G_{r-1}, X'_r$  which satisfies the claim. If  $X'_r$  has a component which is imbedded in  $G_k, \dots, G_{r-1}$  or a component such that does not intersect  $\overline{V_{\text{tor}}}$ , we discard it (this won't have any effect on the veracity of our claim). Next, let

$$X'_r = G_r \cup W_1 \cup \dots \cup W_s$$

be the decomposition of  $X'_r$  such that  $G_r$  is the union of all torsion cosets  $B$  which are components of  $X'_r$ , and  $W_1, \dots, W_s$  are the rest of irreducible components of  $X'_r$ .

For every  $j = 1, \dots, s$ ,  $W_j$  satisfies the following.

**Remark.** There does not exist any torsion coset  $B$  such that  $W_j \subseteq B \subseteq V$ .

*Proof.* If a torsion coset  $B$  as such exists,  $B \subset \overline{V_{\text{tor}}}$  and  $\text{codim}(B) \leq r$ . Therefore

$$W_j \subseteq B \subseteq G_k \cup \dots \cup G_r,$$

which contradicts the definition of  $G_r$  or the fact that no component of  $X'_r$  is imbedded in  $G_k \cup \dots \cup G_{r-1}$ .  $\square$

We apply Theorem 4.1 to  $V_0 = W_j$  and  $V_1 = V$ , where  $k_0 = r \leq n - 1$  and  $k_1 = k$ . Conclusion (a) of the theorem cannot be true, due to the previous remark; hence there exists a hypersurface  $Z_j$  of degree at most  $\theta$  such that  $\overline{W_{j,\text{tor}}} \subset W_j \cap Z_j \subsetneq W_j$ . Krull's Hauptsatz implies that  $W_j \cap Z_j$  is either empty or a equidimensional variety of codimension  $r + 1$ . That allows us to define

$$X'_{r+1} = X_{r+1} \cup \bigcup_{j=1}^s (W_j \cap Z_j).$$

By construction, properties (i) and (ii) of our claim are satisfied for  $r+1$ . Moreover, by Bézout's theorem, the following inequality holds

$$\deg(X'_{r+1}) \leq \theta \left( \sum_{j=1}^s \deg(W_j) \right) + \deg(X_{r+1}).$$

Since  $X'_r = G_r \cup W_1 \cup \dots \cup W_s$ , we obtain

$$\deg(X'_{r+1}) \leq \theta (\deg(X'_r) - \deg(G_r)) + \deg(X_{r+1})$$

and then, adding  $\sum_{i=k}^r \theta^{r+1-i} \deg(G_i)$  to both sides of the inequality,

$$\begin{aligned} \sum_{i=k}^r \theta^{r+1-i} \deg(G_i) + \deg(X'_{r+1}) &\leq \sum_{i=k}^r \theta^{r+1-i} \deg(G_i) \\ &\quad + \theta(\deg(X'_r) - \deg(G_r)) + \deg(X_{r+1}) \\ &= \theta \left( \sum_{i=k}^{r-1} \theta^{r-i} \deg(G_i) + \deg(X'_r) \right) \\ &\quad + \deg(X_{r+1}). \end{aligned}$$

By the induction, we have  $\sum_{i=k}^{r-1} \theta^{r-i} \deg(G_i) + \deg(X'_r) \leq \sum_{i=k}^r \theta^{r-i} \deg(X_i)$ , therefore

$$\theta \left( \sum_{i=k}^r \theta^{r-i} \deg(G_i) + \deg(X'_r) \right) + \deg(X_{r+1}) \leq \sum_{i=k}^{r+1} \theta^{r+1-i} \deg(X_i),$$

proving that (iii) of our claim is satisfied for  $r + 1$ .

□

## 5 Conclusion

Theorem 1.3 follows naturally from Theorem 4.2. Observe that the number of maximal torsion cosets in  $V$  is bounded by the degree of  $\overline{V_{\text{tor}}}$  and  $\deg(\overline{V_{\text{tor}}}) = \sum_{i=k}^n \deg(G_i)$ . Moreover, we have that

$$\sum_{i=k}^n \deg(G_i) \leq \sum_{i=k}^n \theta^{n-1} \deg(G_i) \leq \theta^n$$

and we can bound the number of torsion cosets in  $V$  by  $\theta^n$ , proving Theorem 1.3. We obtain Corollary 1.4 as a particular case of this result.

**Corollary 1.4.** *Let  $V$  be a hypersurface in  $\mathbb{G}_m^n$ , then the number of maximal torsion cosets in  $V$  is bounded by*

$$c_n \deg(V)^n,$$

where  $c_n = ((2n-1)(n-1)(2^n + 2^{n+1} - 2))^{n(n-1)}$ .

From the inequality in Theorem 4.2, we obtain also the following result:

**Corollary 5.1.** *Let  $V$  be a subvariety of  $\mathbb{G}_m^n$  of codimension  $k$  and let*

$$\theta = ((2n-1)(n-1)(2^{2n} + 2^{n+1} - 2))^{n-k} \delta(V).$$

*The number of maximal torsion cosets in  $V$  of codimension  $r$  is bounded by  $\theta^r$ .*

*Proof.* First observe that  $G_r$  in Theorem 4.2 is the union of the maximal torsion cosets in  $V$  of codimension  $r$ . Hence, it is enough to show that  $\deg(G_r) \leq \theta^r$  to prove the statement. By Theorem 4.2 we have that  $\sum_{i=k}^r \theta^{r-k} \deg(G_i) \leq \theta^r$  and, in particular,  $\deg(G_r) \leq \theta^r$ .  $\square$

**Remark.** Following the theorems presented by Amoroso and Viada [AV09], we could obtain, for each maximal torsion coset  $\omega H$  in  $V$ ,  $\delta_0(H) \leq \theta$ . However, we have the following sharper bound:

$$\delta(H) \leq n\delta(V),$$

which is a result of Bombieri and Gubler [BG06, Theorem 3.3.8].

**Remark.** In Theorem 1.3 we could give a more precise bound, depending on the field of definition of our variety  $V$ . To understand this, first observe that the varieties  $V'$  we obtain in Proposition 3.2 are defined over the same field as  $V$ . Hence, in Theorem 3.4 we could consider changing the definition of  $\theta_0$ , depending on the field of definition of  $V$ .

In the case that  $V$  is not defined over  $\mathbb{Q}^{\text{ab}}$ , Theorem 3.4 remains true for

$$\theta_0 = 2k(2d + 1)\delta_0(V).$$

Using this definition of  $\theta_0$  in the induction theorems, we can improve the bound in Theorem 1.3 for this case. Hence, if  $V$  is not defined over  $\mathbb{Q}^{\text{ab}}$ , the number of maximal torsion cosets in  $V$  is bounded by  $\theta^n$ , where

$$\theta = (2(2n - 1)(n - 1))^{n-k} \delta(V).$$

In the case that  $V$  is defined over  $\mathbb{Q}^{\text{ab}}$ , this does not change significantly our bound since the order of  $n$  in the constant would remain essentially the same.

## 5.1 Example

We present a final example to show that, in Corollary 1.4, the exponent of  $d$  is optimal and the constant  $c_n$  must depend on  $n$ . To do this, we need first a result of Conway and Jones on vanishing sums of roots of unity. Let us define for  $m \in \mathbb{N}_{>0}$ :

$$\Psi(m) := 2 + \sum_{\substack{p|m \\ p \text{ prime}}} (p - 2).$$

Then we have:

**Theorem 5.2** ([CJ76]). *Let  $\xi_1, \dots, \xi_N$  be  $N$  roots of unity. Let  $a_1, \dots, a_N \in \mathbb{Z}$  such that  $S = a_1\xi_1 + \dots + a_N\xi_N = 0$  and minimal (i.e. there are no non-trivial vanishing subsums of  $S$ ). Let*

$$m = \text{lcm}(\text{ord}(\xi_2/\xi_1), \dots, \text{ord}(\xi_N/\xi_1)).$$

*Then  $m$  is squarefree and  $\Psi(m) \leq N$ .*

**Example.** First of all, let  $p_1, \dots, p_n$  be  $n$  different primes such that  $p_i > 2n$  for all  $i = 1, \dots, n$ . In particular, we will have that  $\Psi(p_j p_k) > 2n$  for every different  $j, k = 1, \dots, n$ . Let  $W$  be the variety defined by

$$g(X_1, \dots, X_n) = \zeta_{p_1} + \dots + \zeta_{p_n} + X_1 + \dots + X_n.$$

We claim that, if  $\omega \in W_{\text{tor}}$ , then

$$\{\omega_1, \dots, \omega_n\} = \{-\zeta_{p_1}, \dots, -\zeta_{p_n}\}.$$

*Proof.* Take  $\omega \in \mu_\infty^n$  such that  $g(\omega) = 0$  and consider

$$S = g(\omega) = \zeta_{p_1} + \dots + \zeta_{p_n} + \omega_1 + \dots + \omega_n.$$

Let  $S = S_1 + \dots + S_t$  be a decomposition of  $S$  in minimal subsums, such that  $S_i = 0$  for every  $i = 1, \dots, r$ . If, up to reordering,  $t = n$  and  $S_i = \zeta_{p_i} + \omega_i$ , we are done.

Suppose that this is not the case. Hence, there exists a minimal vanishing non-trivial subsum  $S'$  with at least three elements. Without loss of generality, we can assume that  $S'$  has  $\zeta_{p_j}$  and  $\zeta_{p_k}$  as summands, for some different  $j, k = 1, \dots, n$ . Taking  $m'$  as in Theorem 5.2, we have that  $p_j p_k \mid m'$  and so  $\Psi(m') \geq \Psi(p_j p_k) > 2n$ . On the other hand, since  $S'$  is a minimal sum with at most  $2n$  summands and Theorem 5.2 affirms  $\Psi(m') \leq 2n$  which contradicts the fact that  $\Psi(m') > 2n$ . Therefore, a vanishing subsum as  $S'$  does not exist and our claim is proved.  $\square$

Since our claim holds, we have

$$W_{\text{tor}} = \{\omega \in \mu_\infty^n \mid \{\omega_1, \dots, \omega_n\} = \{-\zeta_{p_1}, \dots, -\zeta_{p_n}\}\}.$$

So  $\overline{W_{\text{tor}}} = W_{\text{tor}}$  is a discrete ensemble with  $n!$  elements.

It is enough to take  $V = [d]^{-1}(W)$ , which is the hypersurface in  $\mathbb{G}_m^n$  defined by

$$f(X_1, \dots, X_n) = \zeta_{p_1} + \dots + \zeta_{p_n} + X_1^d + \dots + X_n^d.$$

Then, we have that  $\overline{V_{\text{tor}}} = [d]^{-1}(\overline{W_{\text{tor}}})$  which is the following discrete ensemble:

$$\overline{V_{\text{tor}}} = \left\{ \omega \in \mathbb{G}_m^n \mid \{\omega_1^d, \dots, \omega_n^d\} = \{-\zeta_{p_1}, \dots, -\zeta_{p_n}\} \right\}.$$

Hence, the number of isolated torsion points in  $V$  is  $n!d^n$ . In this case this is, in fact, the number of maximal torsion cosets in  $V$ .

## References

- [AS12] I. Aliev and C. Smyth, *Solving algebraic equations in roots of unity*, Forum Math. **24** (2012), 641–665.
- [AV09] F. Amoroso and E. Viada, *Small points on subvarieties of a torus*, Duke Math. J. **150** (2009), 407–442.

- [AV12] ———, *Small points on rational subvarieties of tori*, Comment. Math. Helv. **87** (2012), 355–383.
- [BG06] E. Bombieri and W. Gubler, *Heights in Diophantine geometry*, New Mathematical Monographs, Cambridge University Press, Cambridge, 2006.
- [BS02] F. Beukers and C. J. Smyth, *Cyclotomic points on curves*, Number theory for the millennium, I (Urbana, IL, 2000), A K Peters, Natick, MA, 2002, pp. 67–85.
- [BZ95] E. Bombieri and U. Zannier, *Algebraic points on subvarieties of  $\mathbf{G}_m^n$* , Internat. Math. Res. Notices (1995), 333–347.
- [Cha89] M. Chardin, *Une majoration de la fonction de Hilbert et ses conséquences pour l'interpolation algébrique*, Bull. Soc. Math. France **117** (1989), 305–318.
- [CJ76] J. H. Conway and A. J. Jones, *Trigonometric Diophantine equations (On vanishing sums of roots of unity)*, Acta Arith. **30** (1976), 229–240.
- [CP99] M. Chardin and P. Philippon, *Régularité et interpolation*, J. Algebraic Geom. **8** (1999), 471–481.
- [Eve99] J-H. Evertse, *The number of solutions of linear equations in roots of unity*, Acta Arith. **89** (1999), 45–51.
- [Hin88] M. Hindry, *Autour d'une conjecture de Serge Lang*, Invent. Math. **94** (1988), 575–603.
- [Lan83] S. Lang, *Fundamentals of Diophantine geometry*, Springer-Verlag, New York, 1983.
- [Lau84] M. Laurent, *Équations diophantiennes exponentielles*, Invent. Math. **78** (1984), 299–327.
- [Ler12] L. Leroux, *Computing the torsion points of a variety defined by lacunary polynomials*, Math. Comp. **81** (2012), 1587–1607.
- [McQ95] M. McQuillan, *Division points on semi-abelian varieties*, Invent. Math. **120** (1995), 143–159.
- [Nar04] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, third ed., Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2004.
- [Phi95] P. Philippon, *Sur des hauteurs alternatives. III*, J. Math. Pures Appl. (9) **74** (1995), 345–365.
- [Rup93] W. M. Ruppert, *Solving algebraic equations in roots of unity*, J. Reine Angew. Math. **435** (1993), 119–156.
- [SA94] P. Sarnak and S. Adams, *Betti numbers of congruence groups*, Israel J. Math. **88** (1994), 31–72, With an appendix by Ze'ev Rudnick.

- [Sch96] W. M. Schmidt, *Heights of points on subvarieties of  $\mathbf{G}_m^n$* , Number theory (Paris, 1993–1994), London Math. Soc. Lecture Note Ser., vol. 235, Cambridge Univ. Press, Cambridge, 1996, pp. 157–187.
- [Zha95] S. Zhang, *Positive line bundles on arithmetic varieties*, J. Amer. Math. Soc. **8** (1995), 187–221.