Canad. Math. Bull Vol. 62 (1), 2019 pp. 169–177
http://dx.doi.org/10.4153/CMB-2018-004-0

The Hermite–Joubert Problem and a Conjecture of Brassil and Reichstein

Khoa Dang Nguyen

Abstract. We show that Hermite's theorem fails for every integer n of the form $3^{k_1} + 3^{k_2} + 3^{k_3}$ with integers $k_1 > k_2 > k_3 \geq 0$. This confirms a conjecture of Brassil and Reichstein. We also obtain new results for the relative Hermite–Joubert problem over a finitely generated field of characteristic 0.

1 Introduction

The Hermite–Joubert problem in characteristic 0 is as follows:

Question 1.1 Let $n \geq 5$ be an integer. Let E/F be a field extension with $\operatorname{char}(F) = 0$ and $[E:F] = n$. Can one always find an element $0 \neq \delta \in E$ such that $\operatorname{Tr}_{E/F}(\delta) = \operatorname{Tr}_{E/F}(\delta^3) = 0$?

The answer is "yes" when $n = 5$ and $n = 6$ thanks to results by Hermite [Her61] and Joubert [Jou67] in the 1860s. Modern proofs of these results can be found in [Cor87, Kra06]. When n has the form 3^k for an integer $k \geq 0$ or the form $3^{k_1} + 3^{k_2}$ for integers $k_1 > k_2 \geq 0$, Reichstein [Rei99] shows that Question 1.1 has a negative answer. The reader is referred to [BR97, Rei99, RY02] for further developments and open questions inspired by the Hermite–Joubert problem. This paper is motivated by results and questions in a recent paper by Brassil and Reichstein [BR] in which the case $n = 3^{k_1} + 3^{k_2} + 3^{k_3}$ for integers $k_1 > k_2 > k_3 \geq 0$ is studied. Our first main result is the following theorem.

Theorem 1.2 *When $n = 3^{k_1} + 3^{k_2} + 3^{k_3}$ for integers $k_1 > k_2 > k_3 \geq 0$, Question 1.1 has a negative answer.*

In fact, we will prove a more precise result (see Theorem 3.1) answering a conjecture of Brassil and Reichstein [BR, Conjecture 14.1]. As in [BR], we can also consider the relative version of Question 1.1 in which F contains a given base field F_0; in particular, Question 1.1 corresponds to the case $F_0 = \mathbb{Q}$. Our second result is the following (see Theorem 2.3 for a more precise result):

Theorem 1.3 *Let F_0 be a finitely generated field of characteristic 0. There is a finite subset $\mathcal{S}$ of $\mathbb{N} \times \mathbb{N}$ depending on F_0 such that the following holds. For every integer n*

Received by the editors September 19, 2017.
Published electronically March 20, 2018.
AMS subject classification: **11D72**, 11G05.
Keywords: Hermite–Joubert problem, Brassil–Reichstein conjecture, diophantine equation.

of the form $3^{k_1} + 3^{k_2} + 3^{k_3}$ *for integers* $k_1 > k_2 > k_3 \ge 0$ *with* $(k_1 - k_3, k_2 - k_3) \notin \mathcal{S}$, *Question 1.1 relative to the base field* F_0 *has a negative answer.*

2 Proof of Theorem 1.3

Throughout this section, F_0 is a finitely generated field of characteristic 0. An abelian group G is said to be of finite rank if $\mathbb{Q} \otimes_{\mathbb{Z}} G$ is a finite dimensional vector space over $\mathbb{Q}$. We start with the following result, which might be of independent interest.

Proposition 2.1 *Let* $P(Z_1, Z_2, Z_3) \in F_0[Z_1, Z_2, Z_3]$ *be a homogeneous polynomial defining a geometrically irreducible plane curve with geometric genus* $g \ge 1$. *Let G be a finite rank subgroup of* $\overline{F_0}^*$. *Then the system of equations:*

$$P(Z_1, Z_2, Z_3) = 0,$$
$$xZ_1 + yZ_2 + Z_3 = 0$$

has only finitely many solutions $(x, y, [Z_1 : Z_2 : Z_3])$ *with* $x, y \in G$, $[Z_1 : Z_2 : Z_3] \in \mathbb{P}^2(F_0)$, *and* $Z_1Z_2Z_3 \ne 0$.

Proof If $g \ge 2$, then by Faltings' theorem [Fal91, Fal94] (see also [Lan83, Chapter 6]), there are only finitely many $[z_1 : z_2 : z_3] \in \mathbb{P}^2(F_0)$ such that $P(z_1, z_2, z_3) = 0$. For such a $[z_1 : z_2 : z_3]$ with $z_1z_2z_3 \ne 0$, the equation $xz_1 + yz_2 + z_3 = 0$ has only finitely many solutions $(x, y) \in G \times G$ (see, for instance, [BG06, Chapter 5]).

Now assume that $g = 1$. Let $\mathcal{E}$ denote the elliptic curve defined by $P(Z_1, Z_2, Z_3) = 0$ after choosing a point $O_{\mathcal{E}} \in \mathcal{E}(F_0)$ as the identity; we can assume $\mathcal{E}(F_0) \ne \varnothing$, since the proposition is vacuously true otherwise. Let $\Gamma := G \times G \times \mathcal{E}(F_0)$, which is a finite rank subgroup of the semi-abelian variety $S := \mathbb{G}_m \times \mathbb{G}_m \times \mathcal{E}$ [Lan83, Chapter 6]. Let (x, y) denote the coordinates of $\mathbb{G}_m \times \mathbb{G}_m$ and let V be the subvariety of S defined by the equation $xZ_1 + yZ_2 + Z_3 = 0$. We are now studying the set $V \cap \Gamma$. Pick $[z_1 : z_2 : z_3] \in \mathcal{E}$ with $z_1z_2z_3 \ne 0$, since the line $z_1x + z_2y + z_3 = 0$ is not a translate of an algebraic subgroup of $\mathbb{G}_m \times \mathbb{G}_m$, we have that V is not a translate of an algebraic subgroup of $\mathbb{G}_m \times \mathbb{G}_m \times \mathcal{E}$. By the Mordell–Lang conjecture, proved by Faltings [Fal91, Fal94], McQuillan [McQ95], and Vojta [Voj96], we have that $V \cap \Gamma$ is the union of a finite set and finitely many sets of the form $(\gamma + C) \cap \Gamma$ where $\gamma \in \Gamma$, C is an algebraic subgroup of S with $\dim(C) = 1$, and $\gamma + C \subset V$.

Assume that $\gamma + C$ is a translate of an algebraic subgroup satisfying the above properties. If the map $C \to \mathcal{E}$ is nonconstant, then C has genus 1 and, hence the map $C \to \mathbb{G}_m \times \mathbb{G}_m$ is constant, since there cannot be a nontrivial algebraic group homomorphism from C to $\mathbb{G}_m$. Consequently, $\gamma + C$ has the form $\{(\gamma_1, \gamma_2)\} \times \mathcal{E}$, where $(\gamma_1, \gamma_2) \in \mathbb{G}_m \times \mathbb{G}_m$. Since $\gamma + C \subset V$, we have that $\gamma_1 Z_1 + \gamma_2 Z_2 + Z_3 = 0$ for every $[Z_1 : Z_2 : Z_3] \in \mathcal{E}$, a contradiction. Therefore, the map $C \to \mathcal{E}$ must be constant; in other words, C has the form $C_1 \times \{O_{\mathcal{E}}\}$, where C_1 is an algebraic subgroup of $\mathbb{G}_m \times \mathbb{G}_m$ with $\dim(C_1) = 1$. Write $\gamma = (\gamma_x, \gamma_y, \gamma_{\mathcal{E}})$ with $(\gamma_x, \gamma_y) \in G \times G$ and $\gamma_{\mathcal{E}} =: [\widetilde{z}_1 : \widetilde{z}_2 : \widetilde{z}_3] \in \mathcal{E}(F_0)$. Since $\gamma + C \subset V$, the translate of C_1 by (γ_x, γ_y) is given by the equation $\widetilde{z}_1 x + \widetilde{z}_2 y + \widetilde{z}_3 = 0$. Equivalently, the algebraic group C_1 is given by the equation $\gamma_x^{-1}\widetilde{z}_1 x + \gamma_y^{-1}\widetilde{z}_2 y + \widetilde{z}_3 = 0$. This is possible only when $\widetilde{z}_1\widetilde{z}_2\widetilde{z}_3 = 0$, and we complete the proof. ∎

https://doi.org/10.4153/CMB-2018-004-0 Published online by Cambridge University Press

Example 2.2 Consider the system of equations

$$Z_1^3 + Z_2^3 + 9Z_3^3 = 0,$$
$$3^a Z_1 + 3^b Z_2 + Z_3 = 0$$

with $a, b \in \mathbb{Z}$ and $[Z_1:Z_2:Z_3] \in \mathbb{P}^2(F_0)$. Proposition 2.1 implies that there are only finitely many solutions outside the set $\{(m, m, [1:-1:0]) : m \in \mathbb{Z}\}$. Later on, when $F_0 = \mathbb{Q}$, we will show that there does not exist any solution satisfying $a > b \geq 0$ confirming another conjecture of Brassil–Reichstein [BR, Conjecture 14.3].

Let $n \geq 2$ be an integer. We recall the definition of "the general field extension" E_n/F_n of degree n over the base field F_0 from [BR, p. 2]. Set $L_n := F_0(x_1, \dots, x_n)$, $F_n = L_n^{S_n}$, and $E_n := L_n^{S_{n-1}} = F_n(x_1)$ where $x_1, \dots, x_n$ are independent variables, S_n acts on L_n by permuting $x_1, \dots, x_n$ and S_{n-1} acts on L_n by permuting $x_2, \dots, x_n$. Theorem 1.3 follows from the next theorem.

Theorem 2.3 *There is a finite subset $\mathcal{S}$ of $\mathbb{N} \times \mathbb{N}$ depending only on F_0 such that for every integer n of the form $3^{k_1} + 3^{k_2} + 3^{k_3}$ with integers $k_1 > k_2 > k_3 \geq 0$ and $(k_1 - k_3, k_2 - k_3) \notin \mathcal{S}$, the following holds. For every finite extension F'/F_n of degree prime to 3, there does not exist $0 \neq \delta \in E' := F' \otimes_{F_n} E_n$ such that $\operatorname{Tr}_{E'/F'}(\delta) = \operatorname{Tr}_{E'/F'}(\delta^3) = 0$. In particular, there does not exist $0 \neq \delta \in E_n$ such that $\operatorname{Tr}_{E_n/F_n}(\delta) = \operatorname{Tr}_{E_n/F_n}(\delta^3) = 0$.*

Proof From [BR, Theorem 1.4 and Remark 11.3], and put $a_1 = k_1 - k_3$ and $a_2 = k_2 - k_3$, it suffices to prove that the system of equations

$$3^{a_1} Z_1^3 + 3^{a_2} Z_2^3 + Z_3^3 = 0,$$
$$3^{a_1} Z_1 + 3^{a_2} Z_2 + Z_3 = 0$$

has only finitely many solutions $(a_1, a_2, [Z_1:Z_2:Z_3])$, where $[Z_1:Z_2:Z_3] \in \mathbb{P}^2(F_0)$ and $a_1 > a_2 > 0$ are integers.

Write $a_i = 3q_i + r_i$ with $q_i \in \mathbb{Z}$ and $r_i \in \{0, 1, 2\}$ for $i = 1, 2$. It suffices to show that for every *fixed* pair $(r_1, r_2) \in \{0, 1, 2\}^2$, the system of equations

$$3^{r_1} Z_1^3 + 3^{r_2} Z_2^3 + Z_3^3 = 0,$$
$$9^{q_1} Z_1 + 9^{q_2} Z_2 + Z_3 = 0$$

has only finitely many solutions $(q_1, q_2, [Z_1:Z_2:Z_3])$, where $[Z_1:Z_2:Z_3] \in \mathbb{P}^2(F_0)$, q_1 and q_2 are integers, and $3q_1 + r_1 > 3q_2 + r_2 > 0$. This last condition implies $q_1 > q_2 \geq 0$.

By Proposition 2.1, it remains to consider solutions satisfying $Z_1 Z_2 Z_3 = 0$. If $Z_3 = 0$, we have $-(Z_2/Z_1)^3 = 3^{r_1 - r_2}$, $-Z_2/Z_1 = 9^{q_1 - q_2}$, and hence $6 \leq 6(q_1 - q_2) = r_1 - r_2$, a contradiction. Similarly, if $Z_2 = 0$, we have $6 \leq 6q_1 = r_1$, contradiction. Finally, if $Z_1 = 0$, we have $6q_2 = r_2$, which implies $q_2 = r_2 = 0$ (otherwise, $6 \leq 6q_2 = r_2$), contradicting the condition $3q_2 + r_2 > 0$. This completes the proof. ∎

3 Proof of Theorem 1.2

Throughout this section, let $F_0 = \mathbb{Q}$. Let E_n/F_n be the general field extension of degree n over $F_0 = \mathbb{Q}$ as in the previous section. Theorem 1.2 follows from the next theorem.

https://doi.org/10.4153/CMB-2018-004-0 Published online by Cambridge University Press

Theorem 3.1 *For every n of the form $3^{k_1}+3^{k_2}+3^{k_3}$ with integers $k_1>k_2>k_3\geq 0$ and for every finite extension F'/F_n of degree prime to 3, there does not exist $0\neq\delta\in E':=F'\otimes_{F_n}E_n$ such that $\mathrm{Tr}_{E'/F'}(\delta)=\mathrm{Tr}_{E'/F'}(\delta^3)=0$. In particular, there does not exist $0\neq\delta\in E_n$ such that $\mathrm{Tr}_{E_n/F_n}(\delta)=\mathrm{Tr}_{E_n/F_n}(\delta^3)=0$.*

As explained in [BR, Chapter 14], Theorem 3.1 follows from another conjecture of Brassil and Reichstein [BR, Conjecture 14.3].

Conjecture 3.2 (Brassil, Reichstein) The system of equations

$$Z_1^3+Z_2^3+9Z_3^3=0,$$
$$3^aZ_1+3^bZ_2+Z_3=0$$

has no solution $(a,b,[Z_1:Z_2:Z_3])$, where $a>b\geq 0$ are integers and $[Z_1:Z_2:Z_3]\in\mathbb{P}^2(\mathbb{Q})$.

In Example 2.2, we explained why there are only finitely many solutions $(a,b,[Z_1:Z_2:Z_3])$. This follows from Proposition 2.1, which uses the Mordell–Lang conjecture proved by Faltings, McQuillan, and Vojta. On the other hand, to prove that there is no solution, we need a different method using effective estimates. In fact, we establish a slightly stronger result than the statement of Conjecture 3.2.

Theorem 3.3 *The only solution $(w,b,[Z_1:Z_2:Z_3])$ of the system*

$$Z_1^3+Z_2^3+9Z_3^3=0, \tag{3.1}$$

$$wZ_1+3^bZ_2+Z_3=0 \tag{3.2}$$

with $w,b\in\mathbb{Z}$, $b\geq 0$, $3^{b+1}\mid w$, and $[Z_1:Z_2:Z_3]\in\mathbb{P}^2(\mathbb{Q})$ is $(0,0,[2:1:1])$.

We now spend the rest of this paper proving Theorem 3.3. From (3.1), we cannot have $Z_1Z_2=0$. If $Z_3=0$, then $Z_1/Z_2=-1$ and (3.2) gives $w=3^b$ violating the condition $3^{b+1}\mid w$. Let $(\widetilde{w},\widetilde{b},[\widetilde{z}_1:\widetilde{z}_2:\widetilde{z}_3])$ be a solution, and we can assume that $\widetilde{z}_1,\widetilde{z}_2$, and $\widetilde{z}_3$ are nonzero integers with $\gcd(\widetilde{z}_1,\widetilde{z}_2,\widetilde{z}_3)=1$.

From $\gcd(\widetilde{z}_1,\widetilde{z}_2,\widetilde{z}_3)=1$, we have $3\nmid\widetilde{z}_1\widetilde{z}_2$ and $-\widetilde{z}_3=3^b\widetilde{z}_4$ for some integer $\widetilde{z}_4$ with $3\nmid\widetilde{z}_4$. Hence, we have $\widetilde{z}_1^3\mid 3^{3b+2}\widetilde{z}_4^3-\widetilde{z}_2^3$ and $\widetilde{z}_1\mid\widetilde{z}_4-\widetilde{z}_2$. This implies

$$\widetilde{z}_1\mid 3^{3b+2}-1. \tag{3.3}$$

We now have

$$|\widetilde{z}_2^3+9\widetilde{z}_3^3|=|\widetilde{z}_1^3|<3^{9b+6}. \tag{3.4}$$

A result of Bennett [Ben97, Theorem 6.1] gives

$$|\widetilde{z}_2^3+9\widetilde{z}_3^3|\geq\frac{1}{3}\max\left\{|\widetilde{z}_2|,|3\widetilde{z}_3|\right\}^{0.24}. \tag{3.5}$$

Combining (3.4) and (3.5), we have

$$\max\left\{|\widetilde{z}_2|,|3\widetilde{z}_3|\right\}<3^{37.5b+30}. \tag{3.6}$$

https://doi.org/10.4153/CMB-2018-004-0 Published online by Cambridge University Press

This is our first step. Our next step is to give a lower bound for a quantity that is closely related to $\max\{|\widetilde{z}_2|, |3\widetilde{z}_3|\}$, and such a lower bound is much larger than $3^{37.5b+30}$ when b is large. This will yield a strong upper bound on b.

Since $\widetilde{z}_1^2 - \widetilde{z}_1\widetilde{z}_2 + \widetilde{z}_2^2 = (\widetilde{z}_1 + \widetilde{z}_2)^2 - 3\widetilde{z}_1\widetilde{z}_2$ we have that $\gcd(\widetilde{z}_1 + \widetilde{z}_2, \widetilde{z}_1^2 - \widetilde{z}_1\widetilde{z}_2 + \widetilde{z}_2^2) \in \{1, 3\}$ depending on whether 3 divides $\widetilde{z}_1 + \widetilde{z}_2$. Moreover, if $3 \mid \widetilde{z}_1 + \widetilde{z}_2$, then $9 \nmid \widetilde{z}_1^2 - \widetilde{z}_1\widetilde{z}_2 + \widetilde{z}_2^2$. Therefore, (3.1) gives

(3.7) $\widetilde{z}_1 + \widetilde{z}_2 = 3^{3b+1}\alpha^3, \quad \widetilde{z}_1^2 - \widetilde{z}_1\widetilde{z}_2 + \widetilde{z}_2^2 = 3\beta^3, \quad \alpha\beta = \widetilde{z}_4, \quad 3 \nmid \alpha\beta, \quad \gcd(\alpha, \beta) = 1.$

We wish to write the cubic curve given by equation (3.1) into the standard Weierstrass form $y^2 = x^3 + Ax + B$. We have:

$$\frac{1}{4}(Z_1 + Z_2)^3 + \frac{3}{4}(Z_1 + Z_2)(Z_1 - Z_2)^2 = -9Z_3^3, \tag{3.8}$$
$$\frac{1}{4} + \frac{3}{4}V^2 = 9U^3, \quad V^2 = 12U^3 - \frac{1}{3}$$

with $U = \frac{-Z_3}{Z_1+Z_2}$ and $V = \frac{Z_1 - Z_2}{Z_1+Z_2}$. Overall, we have

$$y^2 = x^3 - 48, \quad x = 12U = \frac{-12Z_3}{Z_1 + Z_2}, \quad y = 12V = \frac{12(Z_1 - Z_2)}{Z_1 + Z_2}. \tag{3.9}$$

Let $\mathcal{E}$ be the elliptic curve given by the equation $y^2 = x^3 - 48$. By a result of Selmer [Sel51, p. 357] as noted in [BR, Section 14], we have that $\mathcal{E}(\mathbb{Q})$ is cyclic and generated by the point $G = (4, 4)$. For every $P \in \mathcal{E}(\overline{\mathbb{Q}})$, let $x(P)$ denote its x-coordinate.

By (3.8) and (3.9), the solution $(\widetilde{w}, \widetilde{b}, [\widetilde{z}_1 : \widetilde{z}_2 : \widetilde{z}_3])$ gives the point $(\widetilde{x}, \widetilde{y}) \in \mathcal{E}(\mathbb{Q})$ with

$$\widetilde{x} = \frac{-12\widetilde{z}_3}{\widetilde{z}_1 + \widetilde{z}_2} = \frac{12 \cdot 3^b \alpha\beta}{3^{3b+1}\alpha^3} = \frac{4\beta}{3^{2b}\alpha^2}. \tag{3.10}$$

Let $N \geq 1$ such that $\widetilde{x} = x([N]G)$. Let $|\cdot|_3$ denote the 3-adic absolute value on $\mathbb{Q}$. By inspecting the powers of 3 that appear in the denominator of $x(G), x([2]G), \ldots$ we observe that N can be bounded below due to $|\widetilde{x}|_3 = 3^{2b}$. Indeed, we have the following proposition.

Proposition 3.4 *For $n \in \mathbb{N}$, write $n = 3^m \ell$ with $\gcd(n, \ell) = 1$. Then we have*

$$|x([n]G)|_3 = 3^{2m}.$$

Proof We have $G = (4, 4)$, $[2]G = (28, -148)$, and $[3]G = (73/9, 595/27)$.

Claim 1 Assume that $P = [k]G$ for some $k \geq 1$ and $k \neq 3$. If $|x(P)|_3 = 1$, then $|x(P + [3]G)|_3 = 1$.

Proof of Claim 1 Write $P = (x_P, y_P)$. Since $|x_P|_3 = 1$ and $y_P^2 = x_P^3 - 48$, we have $|y_P|_3 = 1$. Let

$$\lambda = \frac{y_P - \frac{595}{27}}{x_P - \frac{73}{9}}, \quad \nu = \frac{\frac{595}{27}x_P - \frac{73}{9}y_P}{x_P - \frac{73}{9}}.$$

https://doi.org/10.4153/CMB-2018-004-0 Published online by Cambridge University Press

From [Sil09, p. 54], the x-coordinate of $P+[3]G$ is

$$\lambda^2-\frac{73}{9}-x_P=\frac{-x_P^3+\frac{73}{9}x_P^2+\frac{5329}{81}x_P+y_P^2-\frac{1190}{27}y_P-48}{(x_P-\frac{73}{9})^2}.$$

This proves Claim 1, since

$$\Big|-x_P^3+\frac{73}{9}x_P^2+\frac{5329}{81}x_P+y_P^2-\frac{1190}{27}y_P-48\Big|_3=\Big|\Big(x_P-\frac{73}{9}\Big)^2\Big|_3=81. \qquad \blacksquare$$

By induction, Claim 1 shows that $|x([n]G)|_3=1$ if $3\nmid n$. By induction again, it remains to prove the following claim.

Claim 2 Assume that $P=[k]G$ with $k\geq 1$. If $|x(P)|_3\geq 1$, then $|x([3]P)|_3=9|x(P)|_3$.

Proof of Claim 2 Write $P=(x_P,y_P)$. From [Sil09, pp. 105–106], consider

$$\begin{aligned}
\psi_3&=3x^4-576x=3x(x^3-192)\\
\psi_2&=2y,\\
\psi_4&=2y(2x^6-1920x^3-192^2),\\
\psi_2\psi_4&=4y^2(2x^6-1920x^3-192^2)=4(x^3-48)(2x^6-1920x^3-192^2),\\
\phi_3&=x\psi_3^2-\psi_2\psi_4=x^9+4608x^6+110592x^3-7077888,\\
f(x)&=\frac{\phi_3}{\psi_3^2}=\frac{x^9+4608x^6+110592x^3-7077888}{9x^2(x^3-192)^2},
\end{aligned}$$

so that $x([3]P)=f(x_P)$. This proves Claim 2, since

$$|x_P^9+4608x_P^6+110592x_P^3-7077888|_3=|x_P^9|_3,$$
$$|9x_P^2(x_P^3-192)^2|_3=\frac{1}{9}|x_P^8|_3. \qquad \blacksquare$$

Let h denote the absolute logarithmic Weil height on $\mathbb{P}^1(\overline{\mathbb{Q}})$ and let $\widehat{h}$ denote the Néron–Tate canonical height on $\mathcal{E}(\overline{\mathbb{Q}})$; see [Sil09, Chapter 8]. We have $\Delta=-3^5\times 2^{12}$ and $j=0$. Then a result of Silverman [Sil90, p. 726] gives

$$-2.13<\widehat{h}(P)-\frac{1}{2}h(x(P))<2.222. \tag{3.11}$$

We calculate the point $[25]G$ explicitly; then apply (3.11) for this point and use $\widehat{h}([25]G)=625\widehat{h}(G)$ to obtain

$$0.25<\widehat{h}(G). \tag{3.12}$$

From (3.11) and (3.12), we have

$$h(\widetilde{x})>2\widehat{h}([N]G)-4.444>0.5N^2-4.444. \tag{3.13}$$

From (3.10) and (3.13), we have

$$\frac{1}{3^{b+1}\alpha}\max\big\{|12z_3|,|z_1+z_2|\big\}=\max\big\{|4\beta|,|3^{2b}\alpha^2|\big\}\geq e^{h(\widetilde{x})}>e^{0.5N^2-4.444}. \tag{3.14}$$

https://doi.org/10.4153/CMB-2018-004-0 Published online by Cambridge University Press

From (3.3) and (3.6), we have

(3.15) $$\max\left\{|z_1+z_2|, |12z_3|\right\} < 3^{37.5b+31.5}.$$

Equations (3.14) and (3.15) give

$$0.5N^2 - 4.444 < (36.5b + 30.5)\ln(3).$$

Proposition 3.4 together with $|\widetilde{x}|_3 = 3^{2b}$ imply $3^b \mid N$. Together with (3.6), we have

$$3^{2b} \le N^2 < 81b + 76.$$

Hence, $b < 3$. We check the following cases:

(i) $b = 0$. So $z_1 \mid 8$ and $N^2 < 76$, which gives $N \in \{1, \ldots, 8\}$.
(ii) $b = 1$. So $z_1 \mid 242$, $3 \mid N$ and $N^2 < 157$, which give $N \in \{3, 6, 9, 12\}$.
(iii) $b = 2$. So $z_1 \mid 6560$, $9 \mid N$ and $N^2 < 238$, which give $N = 9$.

(N,b)	$x([N]G)$	α	β
$(2,0)$	28	1	7
$(3,0)$	$\frac{73}{9}$	6	73
$(3,1)$	$\frac{73}{9}$	2	73
$(4,0)$	$\frac{9772}{1369}$	37	2443
$(5,0)$	$\frac{1184884}{32041}$	179	296221
$(6,0)$	$\frac{48833569}{12744900}$	7140	48833569
$(6,1)$	$\frac{48833569}{12744900}$	2380	48833569
$(7,0)$	$\frac{238335887764}{143736121}$	11989	59583971941
$(8,0)$	$\frac{292913655316492}{69305008951369}$	8324963	73228413829123
$(9,1)$	$\frac{587359987541570953}{26773203784287249}$	109083462	587359...
$(9,2)$	$\frac{587359987541570953}{26773203784287249}$	36361154	587359...
$(12,1)$	$\frac{4450718627559402206478189717312 1}{8710044537858069957030952164 00}$	622184...	445071...

Table 1

https://doi.org/10.4153/CMB-2018-004-0 Published online by Cambridge University Press

Since we can replace (z_1, z_2, z_3) by $(-z_1, -z_2, -z_3)$, we always choose $\alpha > 0$. The pair (α, β) is determined using $x([N]G) = \frac{4\beta}{3^{2b}\alpha^2}$, $3 \nmid \alpha\beta$, and $\gcd(\alpha, \beta) = 1$.

The case $N = 1$ and $b = 0$ gives $x(G) = 4 = \frac{4\beta}{\alpha^2}$, hence $\alpha = \beta = 1$, $\widetilde{z}_1 + \widetilde{z}_2 = 3$, $\widetilde{z}_1^2 - \widetilde{z}_1\widetilde{z}_2 + \widetilde{z}_2^2 = 3$, $\widetilde{z}_1 \mid 8$. Overall, we have the solution $(0, 0, [2{:}1{:}1])$.

For other values of (N, b), from (3.3) and (3.7), we have:

$$|\widetilde{z}_1| < 3^{2b+2} \quad \text{and} \quad |\widetilde{z}_2| < 3^{3b+1}|\alpha^3| + 3^{2b+2}.$$

Then using

$$\widetilde{z}_1\widetilde{z}_2 = \frac{1}{3}\Big((\widetilde{z}_1 + \widetilde{z}_2)^2 - (\widetilde{z}_1 - \widetilde{z}_1\widetilde{z}_2 + \widetilde{z}_2^2) \Big) = 3^{6b+1}\alpha^6 - \beta^3,$$

we have

$$3^{2b+2}\Big(3^{3b+1}|\alpha^3| + 3^{2b+2} \Big) > |3^{6b+1}\alpha^6 - \beta^3|. \tag{3.16}$$

We can readily check that (3.16) fails for the data in table 1, and this finishes the proof.

Acknowledgments We wish to thank Professor Zinovy Reichstein for communicating to us his conjecture with Brassil and for many useful discussions. We are grateful to Professor Dragos Ghioca and the anonymous referee for helpful comments.

References

[Ben97] M. A. Bennett, *Effective measures of irrationality for certain algebraic numbers*. J. Austral. Math. Soc. Ser. A **62**(1997), no. 3, 329–344. http://dx.doi.org/10.1017/S144678870000104X

[BG06] E. Bombieri and W. Gubler, *Heights in Diophantine geometry*. New Mathematical Monographs, 4, Cambridge University Press, Cambridge, 2006. http://dx.doi.org/10.1017/CBO9780511542879

[BR] M. Brassil and Z. Reichstein, *The Hilbert-Joubert problem over p-closed fields*. In: Algebraic groups, structure and actions, Proc. Sympos. Pure Math., 94, American Mathematical Society, RI, 2017.

[BR97] J. Buhler and Z. Reichstein, *On the essential dimension of a finite group*. Compositio. Math. **106**(1997), 159–179. http://dx.doi.org/10.1023/A:1000144403695

[Cor87] D. F. Coray, *Cubic hypersurfaces and a result of Hermite*. Duke Math. J. **54**(1987), 657–670. http://dx.doi.org/10.1215/S0012-7094-87-05428-7

[Fal91] G. Faltings, *Diophantine approximation on abelian varieties*. Ann. of Math. (2) **133**(1991), no. 3, 549–576. http://dx.doi.org/10.2307/2944319

[Fal94] ———, *The general case of S. Lang's conjecture*. In: Barsotti Symposium in Algebraic Geometry (Abano Terme, 1991), Perspect. Math., 15, Academic Press, San Diego, CA, 1994, pp. 175–182.

[Her61] C. Hermite, *Sur l'invariant du* 18^e *ordre des formes du cinquième degré et sur le rôle qu'il joue dans la résolution de l'équation du cinquième degré, extrait de deux lettres de M. Hermite á l'éditeur.*. J. Reine Angew. Math. **59**(1861), 304–305. http://dx.doi.org/10.1515/crll.1861.59.304

[Jou67] P. Joubert, *Sur l'equation du sixième degré*. C. R. Acad. Sci. Paris **64**(1867), 1025–1029.

[Kra06] H. Kraft, *A result of Hermite and equations of degree* 5 *and* 6. J. Algebra **297**(2006), 234–253. http://dx.doi.org/10.1016/j.jalgebra.2005.04.015

[Lan83] S. Lang, *Fundamentals of diophantine geometry*. Springer-Verlag, New York, 1983. http://dx.doi.org/10.1007/978-1-4757-1810-2

[McQ95] M. McQuillan, *Division points on semi-abelian varieties*. Invent. Math. **120**(1995), 143–159. http://dx.doi.org/10.1007/BF01241125

[Rei99] Z. Reichstein, *On a theorem of Hermite and Joubert*. Canad. J. Math. **51**(1999), 69–95. http://dx.doi.org/10.4153/CJM-1999-005-x

[RY02] Z. Reichstein and B. Youssin, *Conditions satisfied by characteristic polynomials in fields and division algebras*. J. Pure Appl. Algebra **166**(2002), 165–189. http://dx.doi.org/10.1016/S0022-4049(01)00009-3

[Sel51] E. S. Selmer, *The diophantine equation* $ax^3 + by^3 + cz^3 = 0$. Acta Math. **85**(1951), 203–362. http://dx.doi.org/10.1007/BF02395746

[Sil90] J. H. Silverman, *The difference between the Weil height and the canonical height on elliptic curves*. Math. Comp. **55**(1990), 723–743. http://dx.doi.org/10.2307/2008444

[Sil09] ———, *The Arithmetic of elliptic curves.* Second ed., Graduate Texts in Mathematics, 106, Springer, Dordrecht, 2009.

[Voj96] P. Vojta, *Integral points on subvarieties of semiabelian varieties. I*. Invent. Math. **126**(1996), no. 1, 133–181. http://dx.doi.org/10.1007/s002220050092

Department of Mathematics and Statistics, University of Calgary, 2500 University Drive NW, Calgary, Alberta T2N 1N4
e-mail: dangkhoa.nguyen@ucalgary.ca