

# DEGREES OF CLOSED POINTS ON DIAGONAL-FULL HYPERSURFACES

F. BALESTRIERI

**ABSTRACT.** Let  $k$  be any field. Let  $X \subset \mathbb{P}_k^N$  be a diagonal-full degree  $d$  hypersurface, where  $d$  is an odd prime. We prove that if  $X(K) \neq \emptyset$  for some extension  $K/k$  with  $n := [K : k]$  prime and  $\gcd(n, d) = 1$ , then  $X(L) \neq \emptyset$  for some extension  $L/k$  with  $\gcd([L : k], nd) = 1$ . Moreover, there exists an explicitly computable positive integer  $B(d, n)$  such that  $[L : k] \mid B(d, n)$ . Finally, if a  $K$ -solution is known explicitly, then we can compute  $L/k$  explicitly as well. When  $n$  or  $d$  is not prime, we can still say something about the possible values of  $[L : k]$ . As an example, we improve upon a theorem by Coray on smooth cubic surfaces  $X \subset \mathbb{P}_k^3$ , in the case when  $X$  is diagonal-full, by showing that if  $X(K) \neq \emptyset$  for some extension  $K/k$  with  $\gcd([K : k], 3) = 1$ , then  $X(L) \neq \emptyset$  for some  $L/k$  with  $[L : k] \in \{1, 10\}$ .

## 1. INTRODUCTION

Springer's theorem for quadratic forms famously states that, if a quadratic form  $\varphi$  on a finite-dimensional vector space over a field  $k$  is isotropic over some extension  $L/k$  of odd degree, then it is already isotropic over  $k$  (see [Spr52] for the case when the characteristic is not 2 and [EKN08, Corollary 18.5] for any characteristic). Equivalently, in more geometric terms, if  $X \subset \mathbb{P}_k^N$  is a degree 2 hypersurface, then  $X(L) \neq \emptyset$  for some extension  $L/k$  of odd degree implies that  $X(k) \neq \emptyset$ . A natural question to ask is whether Springer's theorem generalises to higher degree forms.

**Question 1.1.** Given a degree  $d \geq 3$  hypersurface  $X \subset \mathbb{P}_k^N$  over a field  $k$ , is it true that if  $X(L) \neq \emptyset$  for some extension  $L/k$  with  $\gcd([L : k], d) = 1$ , then  $X(k) \neq \emptyset$ ?

When  $d \geq 4$ , the general answer to Question 1.1 seems to be *no*. When  $d = 3$ , however, Cassels and Swinnerton-Dyer have conjectured that the answer to Question 1.1 should be *yes*. Some progress towards the conjecture by Cassels and Swinnerton-Dyer has been obtained by Coray (see [Cor76]), who proved, for any smooth cubic surface  $X \subset \mathbb{P}_k^3$  over a perfect field  $k$ , that if  $X(K) \neq \emptyset$  for some extension  $K/k$  with  $\gcd([K : k], 3) = 1$ , then  $X(L) \neq \emptyset$  for some extension  $L/k$  with  $[L : k] \in \{1, 4, 10\}$ . In recent work, Ma has been able to remove the condition on the field being perfect, proving Coray's result for any field (see [Ma21]). Moreover, when  $k$  is a global field, Rivera and Viray have shown that, if the Brauer-Manin obstruction is the only one for the Hasse principle for rational points on smooth cubic surfaces in  $\mathbb{P}^3$  over  $k$  (and, by a conjecture by Colliot-Thélène and Sansuc, this should always be the case), then the conjecture by Cassels and Swinnerton-Dyer holds for such surfaces (see [RV21]).

In this paper, we are concerned with the following much weaker version of Question 1.1.

---

*Date:* April 5, 2023.

MSC2020: 11E76, 11D25, 11D41.

**Question 1.2.** Let  $X \subset \mathbb{P}_k^N$  be a degree  $d \geq 3$  hypersurface over a field  $k$ . If  $X(K) \neq \emptyset$  for some finite extension  $K/k$  with  $\gcd([K : k], d) = 1$ , can we find some (somewhat explicit) finite extension  $L/k$  with  $\gcd([L : k], d) = 1$ ,  $[K : k] \nmid [L : k]$ , and  $X(L) \neq \emptyset$ ?

Our main theorem gives a positive answer to Question 1.2 for the class of *diagonal-full* (see Definition 2.3) hypersurfaces of degree  $d$ , under some assumptions on  $d$  and  $[K : k]$ .

**Theorem** (Theorem 3.1). *Let  $k$  be any field. Let  $X \subset \mathbb{P}_k^N$  be a diagonal-full degree  $d$  hypersurface over  $k$ , where  $d$  is an odd prime. If  $X(K) \neq \emptyset$  for some extension  $K/k$  with  $n := [K : k]$  prime and  $\gcd(n, d) = 1$ , then  $X(L) \neq \emptyset$  for some extension  $L/k$  with  $\gcd([L : k], nd) = 1$ . Moreover, there exists an effectively computable positive integer  $B(d, n)$ , coprime to both  $n$  and  $d$ , such that  $[L : k] \mid B(d, n)$ . Finally, if a  $K$ -solution is known explicitly, then  $L/k$  can be computed explicitly as well.*

When  $n$  or  $d$  is not prime, the proof of Theorem 3.1 can still say something about the possible values of  $[L : k]$ . As an example, we prove the following result, which implies an improvement upon Coray's and Ma's theorems when considering diagonal-full forms.

**Theorem** (Theorem 3.8). *Let  $k$  be a field and let  $X \subset \mathbb{P}_k^N$  be a cubic diagonal-full hypersurface over  $k$ . If  $X(K) \neq \emptyset$  for some simple field extension  $K/k$  with  $[K : k] = 4$ , then  $X(L) \neq \emptyset$  for some extension  $L/k$  with  $[L : k] \in \{1, 5\}$ .*

**Corollary 1.3.** *Let  $k$  be a field and let  $X \subset \mathbb{P}_k^3$  be a smooth diagonal-full cubic surface over  $k$ . If  $X(K) \neq \emptyset$  for some extension  $K/k$  with  $\gcd([K : k], 3) = 1$ , then  $X(L) \neq \emptyset$  for some  $L/k$  with  $[L : k] \in \{1, 10\}$ .*

*Proof.* By Coray's and Ma's results, we know, under the hypothesis of the corollary, that there exists some  $L/k$  with  $[L : k] \in \{1, 4, 10\}$  and  $X(L) \neq \emptyset$ . If  $[L : k] = 4$ , then either  $L/k$  is simple, in which case, by Theorem 3.8, there is some other  $L'/k$  with  $[L' : k] \in \{1, 5\}$  and  $X(L') \neq \emptyset$ , or  $L/k$  is not simple. If  $L/k$  is not simple, then, since it is finite, it must be a tower of simple extensions  $L/k(\alpha)/k$  with  $[L : k(\alpha)] = [k(\alpha) : k] = 2$ . Then  $X_{k(\alpha)}$  is a smooth diagonal-full cubic surface as well, and  $X_{k(\alpha)}(L) \neq \emptyset$ , where  $[L : k(\alpha)] = 2$ ; this implies that  $X(k(\alpha)) \neq \emptyset$ . Repeating the same argument with  $k(\alpha)$  and  $k$ , we get that  $X(k) \neq \emptyset$  and we can let  $L' = k$ . In any case, we have found some  $L'/k$  with  $[L' : k] \in \{1, 5\}$  and  $X(L') \neq \emptyset$ . If  $L' = k$  we are done, and if  $[L' : k] = 5$ , then any quadratic extension  $L''/L'$  (thus with  $[L'' : k] = 10$ ) satisfies  $X(L'') \neq \emptyset$ .  $\square$

## 2. PRELIMINARIES ON DEGREE $d$ FORMS

Hypersurfaces  $X \subset \mathbb{P}_k^N$  of degree  $d$  over a field  $k$  are equivalent to degree  $d$  (homogeneous) forms in  $N + 1$  variables over  $k$ . Since we are going to prove our main theorems in the language of forms, we start by recalling some basic definitions.

**Definition 2.1.** Let  $\varphi$  be a form of degree  $d$  on a finite-dimensional vector space  $V$  over a field  $k$ . We say that  $\varphi$  is **isotropic** if there exists some non-zero  $v \in V$  with  $\varphi(v) = 0$ . Otherwise, we say that  $\varphi$  is **anisotropic**.

**Remark 2.2.** If  $X \subset \mathbb{P}_k^N$  is a degree  $d$  hypersurface over a field  $k$  corresponding to the degree  $d$  form  $\varphi$  on  $k^{N+1}$ , then, for any extension  $L/k$ , we have that  $X(L) \neq \emptyset$  if and only if  $\varphi_L$  is isotropic.

If  $(i_0, \dots, i_N) \in \mathbb{Z}_{\geq 0}^{N+1}$  and  $x := (x_0, \dots, x_N)$ , we denote by  $x^{(i_0, \dots, i_N)}$  the monomial in which  $x_j$  appears with exponent  $i_j$  if  $i_j > 0$  and does not appear at all if  $i_j = 0$ .

**Definition 2.3.** Let  $\varphi$  be a form of degree  $d$  on a finite-dimensional vector space  $V \cong k^{N+1}$  over a field  $k$ , say

$$\varphi(x_0, \dots, x_N) = \sum_{\substack{(i_0, \dots, i_N) \in \mathbb{Z}_{\geq 0}^{N+1}: \\ i_0 + \dots + i_N = d}} a_{(i_0, \dots, i_N)} \underline{x}^{(i_0, \dots, i_N)},$$

with  $a_{(i_0, \dots, i_N)} \in k$ . We say that  $\varphi$  is **diagonal-full** if  $a_{(d, 0, \dots, 0)}, a_{(0, d, 0, \dots, 0)}, \dots, a_{(0, \dots, 0, d)} \neq 0$ .

(In more geometric terms, a degree  $d$  hypersurface  $X \subset \mathbb{P}_k^N$  is **diagonal-full** if  $X$  is given by an equation

$$\sum_{\substack{(i_0, \dots, i_N) \in \mathbb{Z}_{\geq 0}^{N+1}: \\ i_0 + \dots + i_N = d}} \underline{x}^{(i_0, \dots, i_N)} = 0$$

with  $a_{(i_0, \dots, i_N)} \in k$  and  $a_{(d, 0, \dots, 0)}, a_{(0, d, 0, \dots, 0)}, \dots, a_{(0, \dots, 0, d)} \neq 0$ .)

**Example 2.4.** Any non-degenerate diagonal form is diagonal-full.

**Definition 2.5.** We let  $D(\varphi_V) := \{\varphi(v) \neq 0 : v \in V\}$ .

The following is a straightforward modification of [EKN08, Theorem 18.3, proof of (2)  $\Rightarrow$  (3)].

**Lemma 2.6.** *Let  $\varphi$  be a form of degree  $d$  on a finite-dimensional vector space  $V$  over  $k$  and let  $f \in k[t]$  be a non-constant polynomial. If there exists some  $a \in k^\times$  such that  $af \in \langle D(\varphi_{k(t)}) \rangle$ , then  $\varphi_{k(g)}$  is isotropic for each irreducible polynomial  $g$  occurring to a power coprime to  $d$  in the factorisation of  $f$ , where  $k(g) := k[t]/(g(t))$ .*

*Proof.* Since  $af \in \langle D(\varphi_{k(t)}) \rangle$ , there exist some  $0 \neq h \in k[t]$  and  $v_1, \dots, v_m \in V[t]$  such that

$$afh^d = \prod_{i=1}^m \varphi(v_i).$$

If it exists, let  $p \in k[t]$  be a non-constant monic irreducible factor of  $f$  appearing with exponent  $\lambda$  coprime to  $d$  in the factorisation of  $f$  into irreducible polynomials, i.e. say  $f = p^\lambda f'$  with  $p$  monic irreducible,  $\deg(p) \geq 1$ ,  $p \nmid f'$ , and  $\gcd(\lambda, d) = 1$ . Write  $v_i = p^{k_i} v'_i$ , where  $k_i \geq 0$  and  $p \nmid v'_i$ , for each  $i = 1, \dots, m$ . Then

$$ap^\lambda f' h^d = afh^d = \prod_{i=1}^m \varphi(v_i) = \prod_{i=1}^m p^{dk_i} \varphi(v'_i) = p^{d \sum_{i=1}^m k_i} \prod_{i=1}^m \varphi(v'_i).$$

Since

$$\lambda + d\nu_p(h) = \nu_p(ap^\lambda f' h^d) = \nu_p\left(\prod_{i=1}^m p^{dk_i} \varphi(v'_i)\right) = d \sum_{i=1}^m k_i + \sum_{i=1}^m \nu_p(\varphi(v'_i)),$$

where  $\nu_p(-)$  denotes the valuation at  $p$ , and since  $\gcd(\lambda, d) = 1$ , it follows that  $\nu_p(\varphi(v'_j)) \geq 1$  for some  $j \in \{1, \dots, m\}$ . This means that  $\varphi(v'_j) \equiv 0 \pmod{p}$ . Since by construction  $p \nmid v'_j$ , we also have that  $v'_j \not\equiv 0 \pmod{p}$ . Hence,  $\varphi_{k(p)}$  is isotropic, as required.  $\square$

**Lemma 2.7.** *Let  $d$  be a positive integer. Let  $k$  be a field and let  $\varphi$  be a diagonal-full form of degree  $d$  on a finite-dimensional vector space  $V \cong k^{N+1}$  over  $k$ . Suppose that  $\varphi$  is anisotropic. Let  $0 \neq r \in V[t]$ . Then  $\deg(\varphi(r)) = d \deg(r)$ , where  $\deg(r) := \max_{i=0, \dots, N}(\deg(r_i))$ .*

*Proof.* Since  $r \in V[t]$  and since  $V \cong k^{N+1}$ , we can write  $r = (r_0, \dots, r_N)$  with  $r_i \in k[t]$  for each  $i = 0, \dots, N$ . Let  $\deg(r) := \max_{i=0, \dots, N}(\deg(r_i))$ , and let

$$I_{\deg(r)} := \{i \in \{0, \dots, N\} : \deg(r_i) = \deg(r)\}.$$

Since  $\varphi$  is diagonal-full, we can write it as

$$\varphi(x_0, \dots, x_N) = \sum_{\substack{(i_0, \dots, i_N) \in \mathbb{Z}_{\geq 0}^{N+1}: \\ i_0 + \dots + i_N = d}} a_{(i_0, \dots, i_N)} \underline{x}^{(i_0, \dots, i_N)},$$

with  $a_{(i_0, \dots, i_N)} \in k$  and  $a_{(d, 0, \dots, 0)}, a_{(0, d, 0, \dots, 0)}, \dots, a_{(0, \dots, 0, d)} \neq 0$ . If  $\deg(\varphi(r)) \neq d \deg(r)$ , then some cancellation must have occurred among the leading coefficients (not all 0, since  $\varphi$  is diagonal-full) of those polynomials  $a_{(i_0, \dots, i_N)} \underline{r}(t)^{(i_0, \dots, i_N)}$  of degree  $d \deg(r)$ . (We note that, since  $d \deg(r)$  is the maximal degree that can possibly be attained, the polynomial  $\underline{r}(t)^{(i_0, \dots, i_N)}$  has degree  $d \deg(r)$  if and only if  $i_j = 0$  for all  $j \notin I_{\deg(r)}$ .) In particular, if we let  $0 \neq \tilde{r} \in k^{N+1} \cong V$  be defined by

$$\tilde{r}_i = \begin{cases} r_i^* & \text{if } i \in I_{\deg(r)}, \\ 0 & \text{if } i \notin I_{\deg(r)}, \end{cases}$$

where  $r_i^* \in k$  denotes the leading coefficient of  $r_i(t)$ , then  $\tilde{r}$  must satisfy

$$\varphi(\tilde{r}) = \sum_{\substack{(i_0, \dots, i_N) \in \mathbb{Z}_{\geq 0}^{N+1}: \\ i_0 + \dots + i_N = d}} a_{(i_0, \dots, i_N)} \tilde{r}^{(i_0, \dots, i_N)} = 0,$$

which would imply that  $\varphi$  is isotropic, a contradiction. Hence,  $\deg(\varphi(r)) = d \deg(r)$ , as required.  $\square$

### 3. PROOF OF THE MAIN THEOREMS

In this section, using fairly simple arguments, we prove (in the language of forms) the two main theorems of the paper.

**Theorem 3.1.** *Let  $k$  be a field and let  $\varphi$  be a diagonal-full form of degree  $d$  on a finite-dimensional vector space  $V$  over  $k$ , where  $d$  is an odd prime. If there exists an extension  $K/k$  with  $n := [K : k]$  prime and  $\gcd(n, d) = 1$  such that  $\varphi_K$  is isotropic, then there exists a finite extension  $L/k$  with  $\gcd([L : k], nd) = 1$  and  $\varphi_L$  isotropic. Moreover, there exists an effectively computable positive integer  $B(d, n)$ , coprime to both  $n$  and  $d$ , such that  $[L : k] \mid B(d, n)$ . Finally, if an explicit non-trivial solution over  $K$  is known, then we can compute  $L/k$  explicitly.*

*Proof.* If  $\varphi$  is isotropic over  $k$ , we can take  $L = k$  and  $[L : k] = 1$  is coprime to  $nd$  and it divides any positive integer  $B(d, n)$ . So, from now on, we assume that  $\varphi$  is anisotropic over  $k$ .

Since  $[K : k]$  is prime,  $K/k$  is a simple extension. Let  $K = k(\alpha)$  and let  $f \in k[t]$  be the minimal (irreducible) polynomial of  $\alpha$  over  $k$ . Since, by assumption,  $\varphi_{k(f)}$  is isotropic, it follows that there exists some  $v \in V[t]$  such that  $\varphi(v) \equiv 0 \pmod{f}$  but  $v \not\equiv 0 \pmod{f}$ . By the division algorithm, there exist some  $0 \neq h \in k[t]$  and  $w, r \in V[t]$  such that

$$hv = fw + r$$

and with  $\deg(h) < \deg(f) = n$  and  $\deg(r) < \deg(f) = n$ . Since

$$h^d \varphi(v) = \varphi(hv) = \varphi(fw + r) = f^d \varphi(w) + f(\text{other stuff}) + \varphi(r)$$

and since  $f \mid \varphi(v)$ , it follows that  $f \mid \varphi(r)$ .

If  $r = 0$ , then  $f \mid hv$ . But since  $f$  is irreducible and  $f \nmid v$ , it follows that  $f \mid h$ , which is a contradiction since  $\deg(h) < \deg(f)$ . Hence,  $r \neq 0$ . Let  $\varphi(r) = fg$  for some  $g \in k[t]$ . Since  $r \neq 0$  and since, by assumption,  $\varphi$  is anisotropic, it follows that  $\varphi(r) \neq 0$ : indeed, since

$r(t) \neq 0$ , there is some  $\tilde{t} \in k$  such that the specialisation  $r(\tilde{t}) \in V$  is also not 0; if, however,  $\varphi(r) = 0$ , then we would have in particular that  $\varphi(r(\tilde{t})) = 0$ , which would imply that  $\varphi$  is isotropic over  $k$ , a contradiction. Since  $\varphi(r) \neq 0$ , it follows that  $g \neq 0$ . Hence, we have that  $fg \in \langle D(\varphi_{k(t)}) \rangle$ . Since  $\varphi(r) = fg$  and  $\deg(r) < \deg(f)$ , it follows that

$$\deg(g) + \deg(f) = \deg(\varphi(r)) < d \deg(f) = dn,$$

that is,  $\deg(g) < n(d-1)$ . Notice also that  $\deg(g) \geq 1$ , since otherwise we would get, by Lemma 2.7, that  $d \deg(r) = \deg(\varphi(r)) = \deg(f) = n$ , which is a contradiction to the fact that  $\gcd(d, n) = 1$ .

In the remainder of the proof, we aim to show that there exists an irreducible factor  $p$  of  $fg$  of exponent  $\lambda$  coprime to  $d$  and with  $\gcd(\deg(p), dn) = 1$  and  $\deg(p) > 1$  (with the goal of then applying Lemma 2.6 to it). Let the factorisation of  $g$  into irreducible factors be

$$g = g^* \prod_{i=1}^r p_i^{\lambda_i}$$

where  $g^* \in k^\times$  and, for each  $i = 1, \dots, r$ , the distinct polynomials  $p_i \in k[t]$  are monic and irreducible, with  $\deg(p_i) =: u_i$  and  $\lambda_i \geq 1$ . Then

$$\deg(g) = \sum_{i=1}^r u_i \lambda_i < n(d-1).$$

We now introduce some terminology and notation.

**Definition 3.2.** Let  $n^* \in \{1, \dots, d-1\}$  be the unique integer such that  $n^* \equiv -n \pmod{d}$ . We define the set

$$S_{d,n} := \{n^* + jd : j \in \mathbb{Z}_{\geq 0} \text{ and } n^* + jd < n(d-1)\}.$$

**Definition 3.3.** Let  $u \in S_{d,n}$ . We call any partition  $u = \lambda_1 u_1 + \dots + \lambda_r u_r$  in which there exists some  $i$  with  $u_i = 1$  and  $\gcd(\lambda_i, d) = 1$  an **inadmissible partition**. We call all the other partitions of  $u$  **admissible**.

**Claim 3.4.** Let  $\lambda_1 u_1 + \dots + \lambda_r u_r$  be an admissible partition of  $u \in S_{d,n}$ . Then there exists at least one  $i \in \{1, \dots, r\}$  with  $\lambda_i$  coprime to  $d$  and  $u_i > 1$  coprime to both  $n$  and  $d$ .

*Proof.* Indeed, suppose, for a contradiction, that this is not the case. Then, for any  $i \in \{1, \dots, r\}$ , either  $\lambda_i$  is not coprime to  $d$  or  $u_i$  is not coprime to both  $n$  and  $d$ . (We note that if  $\gcd(\lambda_i, d) = 1$ , then  $u_i > 1$  since the partition is admissible.) Since  $u \in S_{d,n}$  and since  $d$  is prime and  $\gcd(d, n) = 1$ , it follows that  $u$  is coprime to  $d$ . Hence, since  $u = \sum_{i=1}^r u_i \lambda_i$ , there exists at least one  $i$  with  $\lambda_i$  coprime to  $d$ . Let

$$I_d := \{i \in \{1, \dots, r\} : \lambda_i \text{ is coprime to } d\},$$

which is non-empty, as noted above. Since the partition is admissible, we must have that  $u_i > 1$  for all  $i \in I_d$ . Moreover, by assumption, we must have that  $u_i$  is not coprime to both  $n$  and  $d$  for all  $i \in I_d$ . Consider the subset of  $I_d$  defined by

$$J_d := \{j \in I_d : u_j \text{ is coprime to } d\}.$$

Since we are assuming that, for any  $i$ , either  $\lambda_i$  is not coprime to  $d$  or  $u_i$  is not coprime to both  $n$  and  $d$ , using the fact that  $n$  is prime we must have that  $u_j$  is divisible by  $n$  for all

$j \in J_d$ , and thus that  $\sum_{j \in J_d} \lambda_j u_j \in n\mathbb{Z}$ . Moreover, again using our assumptions, it follows by definition that if  $i \in \{1, \dots, r\} - J_d$ , then  $\lambda_i u_i \in d\mathbb{Z}$ . Hence, we can write  $u$  as

$$u = \underbrace{\sum_{i \notin J_d} \lambda_i u_i}_{\in d\mathbb{Z}} + \underbrace{\sum_{j \in (I_d - J_d)} \lambda_j u_j}_{\in d\mathbb{Z}} + \underbrace{\sum_{j \in J_d} \lambda_j u_j}_{\in n\mathbb{Z}}. \quad (3.1)$$

Using the fact that  $\gcd(u, d) = 1$ , it follows that  $J_d \neq \emptyset$ . Moreover, we must also have that  $\sum_{j \in J_d \neq \emptyset} \lambda_j u_j \notin d\mathbb{Z}$ .

Write  $\sum_{j \in J_d} \lambda_j u_j = nc$ , for some  $c \in \mathbb{Z}_{>0}$ . Recall that  $u = n^* + md$ , for some  $m \in \mathbb{Z}_{\geq 0}$  such that  $u < (d-1)n$ . It follows that  $c < d-1$  (note that  $d \geq 3$ ). Moreover, reducing (3.1) modulo  $d$ , we get

$$\begin{aligned} n^* &\equiv nc \pmod{d} \\ \therefore -n &\equiv nc \pmod{d} \\ \therefore n(c+1) &\equiv 0 \pmod{d}. \end{aligned}$$

Since  $n$  is coprime to  $d$ , it follows that  $c+1 \equiv 0 \pmod{d}$ . But  $c \in \{1, \dots, d-2\}$ , meaning that  $c+1 \in \{2, \dots, d-1\}$  is coprime to  $d$ , a contradiction. Hence, for each admissible partition  $u = \lambda_1 u_1 + \dots + \lambda_r u_r$ , there exists at least one  $i \in \{1, \dots, r\}$  with  $\lambda_i$  coprime to  $d$  and  $u_i \neq 1$  coprime to both  $n$  and  $d$ .  $\square$

We now resume the proof of the main theorem. We make two claims.

**Claim 3.5.** *In the notation and assumptions as above,*

- (1)  $\deg(g) \in S_{d,n}$ ;
- (2)  $\deg(g) = \sum_{i=1}^r \lambda_i u_i$  is an admissible partition.

*Proof.* (1) By Lemma 2.7, we have that  $\deg(\varphi(r)) = d \deg(r)$ . Since  $\varphi(r) = fg$ , it follows that  $\deg(g) = -n + d \deg(r)$ . Since, moreover,  $1 \leq \deg(g) < n(d-1)$ , it follows that  $\deg(g) \in S_{d,n}$ , as claimed.

- (2) Suppose, for a contradiction, that

$$\deg(g) = \sum_{i=1}^r \lambda_i u_i$$

is an inadmissible partition. This means that there exists some  $i$  with  $u_i = 1$  and  $\gcd(\lambda_i, d) = 1$ . Since  $u_i = \deg(p_i)$ , this means that  $g$  has a monic linear factor  $p_i \in k[t]$  with exponent coprime to  $d$ . We note that  $p_i \nmid f$ , since  $f$  is irreducible and  $\deg(p_i) = 1 < \deg(f) = n$ . Hence,  $p_i$  is a monic linear factor of  $fg$  appearing with exponent coprime to  $d$  in the factorisation of  $fg$ . By Lemma 2.6, this means that  $\varphi_{k(p_i)}$  is isotropic. But  $k(p_i) \cong k$ , which implies that  $\varphi$  is isotropic, a contradiction to the assumption that  $\varphi$  is anisotropic. Hence,  $\deg(g) = \sum_{i=1}^r \lambda_i u_i$  is an admissible partition, as claimed.  $\square$

By Claims 3.5 and 3.4, there exists some  $i \in \{1, \dots, r\}$  with  $\gcd(\lambda_i, d) = 1$  and  $u_i > 1$  with  $\gcd(u_i, nd) = 1$ . This corresponds to an irreducible factor  $p_i$  of degree  $u_i$  of  $g$  with exponent  $\lambda_i$  coprime to  $d$ . We notice that  $p_i \nmid f$ , since if  $p_i \mid f$ , then  $p_i = af$  for some  $a \in k^\times$ , since  $f$  is irreducible. But this would mean that  $u_i = \deg(p_i) = \deg(f) = n$ , which contradicts  $\gcd(u_i, nd) = 1$ . Hence,  $p_i$  is a monic irreducible factor of  $fg$  of exponent  $\lambda_i$  coprime to  $d$ . By Lemma 2.6, this implies that  $\varphi_{k(p_i)}$  is isotropic. By letting  $L := k(p_i) = k[t]/(p_i(t))$ , we see that  $[L : k] = u_i$  satisfies  $\gcd([L : k], nd) = 1$ , as required.

For the an explicit and effective algorithm computing an integer  $B(d, n) \in \mathbb{N}$  with  $\gcd(B(d, n), nd) = 1$  and  $[L : k] \mid B(d, n)$ , we refer to Section 4 below. We note that the above proof gives possible degrees  $[L : k]$  explicitly, for each partition of  $\deg(g)$ ; we then take  $B(d, n)$  to be the least common multiple of these possible degrees.

Finally, if we have an explicit non-trivial solution over  $K$ , then, in the above proof, we also have an explicit  $v \in V[t]$ , which implies that  $h, w, r$  are also explicit, and thus that  $g$  is explicit as well. Then the factorisation  $g = g^* \prod_{i=1}^r p_i^{\lambda_i}$  into its irreducible factors is also explicit, and we get all its irreducible factors  $p_i$  with  $\gcd(\deg(p_i), nd) = 1$  and  $\gcd(\lambda_i, d) = 1$ ; for each such factor,  $L = k[t]/(p_i(t))$  is explicitly computed.  $\square$

**Example 3.6.** Let  $\varphi$  be a diagonal-full cubic form on a finite-dimensional vector space  $V$  over a field  $k$  with  $\varphi_K$  isotropic for some simple extension  $K/k$  of degree  $n := [K : k] = 2$ . Since  $(d, n) = (3, 2)$ , we have  $S_{d,n} = \{1\}$ . By following the proof of Theorem 3.1, this implies that  $\varphi$  is already isotropic over  $k$ .

**Example 3.7.** Let  $\varphi$  be a diagonal-full cubic form on a finite-dimensional vector space  $V$  over a field  $k$  with  $\varphi_K$  isotropic for some simple extension  $K/k$  of degree  $n := [K : k] = 5$ . Since  $(d, n) = (3, 5)$ , we have  $S_{d,n} = \{1, 4, 7\}$ . By considering the partitions into positive integers of each  $u \in S_{d,n}$ , we can find possible values for  $[L : k]$ . We note that all the partitions into positive integers of  $u \in \{1, 4\}$  appear as subpartitions of  $u = 7$ , so we just need to consider  $u = 7$ .

- $u = 7$ . If a partition of 7 into positive integers involves 1 or 2, then, following the notation in the proof of Theorem 3.1, we know that there exists some  $i \in \{1, \dots, r\}$  with  $u_i \in \{1, 2\}$  and  $\gcd(\lambda_i, 3) = 1$ , which implies that there exists some  $L/k$  with  $[L : k] \in \{1, 2\}$  and  $\varphi_L$  isotropic; if  $[L : k] = 2$ , then we can use Example 3.6 to conclude that  $\varphi$  is isotropic over  $k$ . Hence, it suffices to consider those partitions of 7 not involving 1 or 2. The only partitions of 7 into positive integers not involving 1 or 2 are (7) and (4, 3). Hence, in this case, there always exists some  $i \in \{1, \dots, r\}$  with  $\gcd(\lambda_i, 3) = 1$  and  $u_i \in \{1, 2(\leftrightarrow 1), 4, 7\}$ .

Hence, we conclude that there is always an extension  $L/k$  with  $[L : k] \in \{1, 4, 7\}$  and  $\varphi_L$  isotropic.

**3.1. The case when  $n$  or  $d$  is not prime.** When  $n := [K : k]$  or  $d$  is not prime, the proof of Claim 3.4 might fail. However, even in this case, we can use the proof of Theorem 3.1, with some care, to determine the possible degrees of  $L/k$  with  $\varphi_L$  isotropic. We illustrate this procedure by specialising to the case when  $d = 3$  and  $n = 4$ .

**Theorem 3.8.** *Let  $k$  be a field and let  $\varphi$  be a cubic diagonal-full form on a finite-dimensional vector space  $V$  over  $k$ . If there exists a simple extension  $K/k$  with  $[K : k] = 4$  such that  $\varphi_K$  is isotropic, then there exists a finite extension  $L/k$  with  $[L : k] \in \{1, 5\}$  such that  $\varphi_L$  is isotropic.*

*Proof.* The first part of the proof of Theorem 3.8 is identical to that of Theorem 3.1, so we just sketch it. Let  $K = k(\alpha)$  and let  $f \in k[t]$  be the minimal (irreducible) polynomial of  $\alpha$  over  $k$ . Since, by assumption,  $\varphi_{k(f)}$  is isotropic, it follows that there exists some  $v \in V[t]$  such that  $\varphi(v) \equiv 0 \pmod{f}$  but  $v \not\equiv 0 \pmod{f}$ . By the division algorithm, there exist some  $0 \neq h \in k[t]$  and  $w, r \in V[t]$  such that

$$hv = fw + r,$$

with  $\deg(r) < \deg(f) = 4$ , with  $f \mid \varphi(r)$ , and with  $\varphi(r) \neq 0$ . We write  $\varphi(r) = fg$  for some  $g \in k[t]$ , which we can show satisfies  $0 < \deg(g) < n(d-1) = 8$ .

Let the factorisation of  $g$  into irreducible factors be

$$g = g^* \prod_{i=1}^r p_i^{\lambda_i}$$

where  $g^* \in k^\times$  and, for each  $i = 1, \dots, r$ , the distinct polynomials  $p_i \in k[t]$  are monic and irreducible, with  $\deg(p_i) =: u_i$  and  $\lambda_i \geq 1$ . Then

$$\deg(g) = \sum_{i=1}^r u_i \lambda_i < 8.$$

Let us compute  $S_{d,n}$  for  $(d, n) = (3, 4)$ . We have  $n^* = 2$ . Hence,

$$S_{3,4} = \{2 + 3j : j \in \mathbb{Z}_{\geq 0} \text{ and } 2 + 3j < 8\} = \{2, 5\}.$$

We notice that  $\deg(g) \in S_{3,4} = \{2, 5\}$ , since, by Lemma 2.7, we have that  $\deg(\varphi(r)) = 3 \deg(r)$  and since  $\varphi(r) = fg$ , implying that  $0 < \deg(g) = -4 + 3 \deg(r) < 8$ .

We remark that if  $\deg(g) = \sum_{j=1}^r u_j \lambda_j$  is such that  $u_i \in \{1, 2\}$  and  $\gcd(\lambda_i, 3) = 1$  for some  $i \in \{1, \dots, r\}$ , then we know that  $g$  has an irreducible factor  $p_i$  of degree either 1 or 2 appearing in the factorisation of  $g$  with exponent  $\lambda_i$ . Moreover, such a factor  $p_i$  cannot divide  $f$ , since  $f$  is irreducible and  $\deg(f) = 4$ , while  $\deg(p_i) < \deg(f) = 4$ . Hence,  $p_i$  is an irreducible factor of  $fg$  appearing with exponent  $\lambda_i$ , and thus Lemma 2.6 yields that  $L := k[t]/(p_i(t))$  is a field of degree 1 or 2 with  $\varphi_L$  isotropic. But if  $[L : k] = 2$ , it is easy to check that  $S_{3,2} = \{1\}$  and thus  $\varphi$  is already isotropic over  $k$ . Hence, since if  $\deg(g) = \sum_{j=1}^r u_j \lambda_j$  satisfies  $u_i \in \{1, 2\}$  and  $\gcd(\lambda_i, 3) = 1$  for some  $i \in \{1, \dots, r\}$  then  $\varphi$  is already isotropic over  $k$ , in the considerations below we will omit considering any partitions of 2 or 5 into positive integers having a 1 or a 2 in them, since any such partition would imply that  $u_i \lambda_i \in \{1, 2\}$  for some  $i$ , meaning that  $u_i \in \{1, 2\}$ .

We distinguish two cases, depending on whether  $\deg(g)$  is 2 or 5.

- **Case  $\deg(g) = 2$ .** Since any partition of 2 into positive integers involves a 1 or a 2, this implies that, in  $2 = \sum_{j=1}^r u_j \lambda_j$ , there is always some  $u_i \in \{1, 2\}$  with  $\gcd(\lambda_i, 3) = 1$ . Hence, by the discussion above,  $\varphi$  is already isotropic over  $k$ .
- **Case  $\deg(g) = 5$ .** Since the only partition of 5 into positive integers that does not involve a 1 or a 2 is (5), we have, for this partition, that  $r = 1$  and  $u_1 \lambda_1 = 5$ , implying that  $u_1 \in \{1, 5\}$  and  $\gcd(\lambda_1, 3) = 1$ . Notice that  $p_1 \nmid f$  since  $f$  is irreducible of degree 4 and  $\deg(p_1) = u_1 \in \{1, 5\}$ ; hence,  $p_1$  is an irreducible factor in  $fg$  of exponent  $\lambda_i$  coprime to 3 and by Lemma 2.6, there is some  $L/k$  with  $[L : k] \in \{1, 5\}$  and  $\varphi_L$  isotropic. It follows that, by considering all the partitions of 5 into positive integers, if  $\deg(g) = 5 = \sum_{j=1}^r u_j \lambda_j$ , then we can always find some  $L/k$  with  $[L : k] \in \{1, 5\}$  and  $\varphi_L$  isotropic.

Hence, putting together all the possibilities from the two cases above, we conclude that there is always an extension  $L/k$  with  $[L : k] \in \{1, 5\}$  and  $\varphi_L$  isotropic, as required.  $\square$

A similar proof as the one of Theorem 3.8 yields a procedure that can also give information about the possible degrees  $[L : k]$  for other values of  $n$  (and  $d$ ).

**Example 3.9.** Let  $\varphi$  be a diagonal-full cubic form on a finite-dimensional vector space  $V$  over a field  $k$  with  $\varphi_K$  isotropic for some simple extension  $K/k$  of degree  $n := [K : k] = 10$ . Since  $(d, n) = (3, 10)$ , we have  $S_{d,n} = \{2, 5, 8, 11, 14, 17\}$ . By considering the partitions into



positive integers of each  $u \in S_{d,n}$ , and by using the knowledge that we have about the cases  $(d, n) \in \{(3, 2), (3, 4)\}$ , we can find possible values for  $[L : k]$ . We note that all the partitions into positive integers of  $u \in \{2, 5, 8, 11, 14\}$  appear as subpartitions of  $u = 17$ , so we just need to consider  $u = 17$ .

- $u = 17$ . If a partition of 17 into positive integers involves 1, 2, or 4, then we know that there exists some  $L/k$  with  $[L : k] \in \{1, 5\}$  and  $\varphi_L$  isotropic. The only partitions of 17 into positive integers not involving 1, 2, or 4 are (17), (14, 3), (12, 5), (11, 6), (11, 3, 3), (10, 7), (9, 8), (9, 5, 3), (8, 6, 3), (8, 3, 3, 3), (7, 7, 3), (7, 5, 5), (6, 6, 5), (6, 5, 3, 3), and (5, 3, 3, 3, 3). Hence, in this case, there always exists some  $i \in \{1, \dots, r\}$  with  $\gcd(\lambda_i, 3) = 1$  and  $u_i \in \{1, 2(\leftrightarrow 1), 4(\leftrightarrow 1 \text{ or } 5), 5, 7, 8, 11, 14, 17\}$ .

Hence, we conclude that there is always an extension  $L/k$  with  $[L : k] \in \{1, 5, 7, 8, 11, 14, 17\}$  and  $\varphi_L$  isotropic.

*Summary of the procedure.* To summarise, the general procedure for any positive integers  $d, n \geq 2$  with  $\gcd(d, n) = 1$  is the following.

- (1) If  $\varphi$  is isotropic, we are done. Assume that  $\varphi$  is anisotropic over  $k$  and that  $\varphi_K$  is isotropic for some simple extension  $K/k$  of degree  $n := [K : k] \geq 2$  coprime to  $d$ .
- (2) Let  $f$  be the (irreducible) minimal polynomial of  $K/k$ , so that  $\deg(f) = n$ .
- (3) There is some  $0 \neq r \in V[t]$  with  $\deg(r) < n$  and  $0 \neq \varphi(r) = fg$ , for some  $g \in k[t]$  with  $0 < \deg(g) < n(d-1)$  and  $\deg(g) \in S_{d,n}$ , since  $\deg(\varphi(r)) = d \deg(r)$ .
- (4) Let  $g = g^* \prod_{i=1}^r p_i^{\lambda_i}$  be the factorisation of  $g$  into irreducible polynomials over  $k$ , where  $g^*$  is the leading coefficient of  $g$  and the  $p_i$ 's are distinct monic irreducible polynomials of degree  $u_i := \deg(p_i)$ . Then  $\deg(g) = \sum_{i=1}^r u_i \lambda_i \in S_{d,n}$ .
- (5) Let  $u_{\max} \in S_{d,n}$  be the largest element; it can be shown that  $u_{\max} = nd - n - d$  (see the proof of Proposition 4.6). For any  $u \in S_{d,n}$ , any partition  $(a_1, \dots, a_t)$  of  $u$  into positive integers is a subpartition of  $u_{\max}$ .
- (6) Let  $(a_1, \dots, a_r)$  be a partition of  $u_{\max}$  into positive integers. For each  $a_i$  with  $\gcd(a_i, d) = 1$ , writing  $a_i = u_i \lambda_i$  yields that  $u_i$  can be any positive divisor of  $a_i$ ; if  $u_i \mid a_i$  and  $n \nmid u_i$ , then we have found a  $p_i \nmid f$  (since  $f$  is irreducible and  $\deg(p_i) = u_i \neq n = \deg(f)$ ) appearing in the factorisation of  $fg = \varphi(r)$  with exponent  $\lambda_i$  coprime to  $d$ . By Lemma 2.6, any such  $p_i$  yields a field  $L := k[t]/(p_i(t))$  with  $\gcd([L : k], d) = 1$ ,  $n \nmid [L : k]$  and  $\varphi_L$  isotropic.

**Remark 3.10.** If there exists a partition  $(a_1, \dots, a_r)$  of  $u_{\max}$  into positive integers with  $\gcd(a_i, d) > 1$  for all  $i = 1, \dots, r$ , then unfortunately we cannot get any new information from the procedure. Moreover, if there exists a partition  $(a_1, \dots, a_r)$  of  $u_{\max}$  into positive integers such that, for any  $a_i$  with  $\gcd(a_i, d) = 1$ , we have that  $n \mid a_i$ , then unfortunately we cannot get any new information in this case as well, because the existence of such a partition implies that  $n$  could possibly divide  $[L : k]$  and that possibly  $K \subset L$ .

- (7) Hence, by considering all the possible partitions of  $u_{\max}$  into positive integers, if the situations described in Remark 3.10 do not occur, then we know that there exists some  $L/k$  with  $\gcd([L : k], d) = 1$ ,  $n \nmid [L : k]$ , and  $\varphi_L$  isotropic, where  $[L : k]$  is in the set of all possible degrees found by considering all the partitions of  $u_{\max}$ .

#### 4. ALGORITHMS TO COMPUTE THE BOUND $B(d, n)$ IN THEOREM 3.1

Let  $d$  be an odd prime. Let  $u \in S_{d,n}$ . Consider a partition  $u = a_1 + \dots + a_r$  in positive integers. following the proof of the Theorem 3.1, one can extract a way to read the possible degrees of  $L/k$  with  $\varphi_L$  isotropic and  $\gcd([L : k], nd) = 1$ , given that  $\varphi$  is anisotropic and there exists some  $K/k$  with  $[K : k] = n$  prime,  $\gcd(n, d) = 1$ , and  $\varphi_K$  isotropic. For each  $a_i$ , if  $a_i > 1$  and  $\gcd(a_i, d) = 1$ , then write  $a_i = n^{\epsilon_i} a'_i$ , where  $\epsilon_i \geq 0$  and  $\gcd(a'_i, n) = 1$ . If  $a'_i > 1$ , then a set of some potential degrees of  $[L : k]$  with  $\varphi_L$  isotropic and  $\gcd([L : k], nd) = 1$  is

$$\{m \in \mathbb{Z}_{\geq 2} : m \mid a'_i\}.$$

In any other case, it is easy to check that if we write  $a_i = \lambda_i u_i$ , then, for any possible choices of positive integers  $\lambda_i$  and  $u_i$ , we have that either  $\gcd(u_i, nd) > 1$ , or  $\gcd(\lambda_i, d) > 1$ , or  $u_i = 1$ .

This suggests the following algorithm to compute  $B(d, n)$ .

**Algorithm 4.1.** Let  $d$  be an odd prime and  $n$  a prime with  $\gcd(d, n) = 1$ .

- (1) Compute the unique integer  $n^* \in \{1, \dots, d-1\}$  such that  $n^* \equiv -n \pmod{d}$ .
- (2) Define the set  $S_{d,n} := \{n^* + jd : j \in \mathbb{Z}_{\geq 0} \text{ and } n^* + jd < (d-1)n\}$ .
- (3) Let  $u \in S_{d,n}$ . Let

$$\mathcal{P}(u) := \{(a_1, \dots, a_r) : u = a_1 + \dots + a_r \text{ and } a_i \in \mathbb{Z}_{>0} \forall i = 1, \dots, r\}$$

be the set of all the partitions of  $u$  into a sum of positive integers and let

$$\mathcal{P}_{>1}(u) := \{(a_1, \dots, a_r) \in \mathcal{P}(u) : a_i > 1 \forall i = 1, \dots, r\}.$$

If  $\mathcal{P}_{>1}(u) = \emptyset$ , we let  $B(u) = 1$ . Otherwise, for each partition  $(a_1, \dots, a_r) \in \mathcal{P}_{>1}(u)$ , if there exists some  $i = 1, \dots, r$  with  $\gcd(a_i, d) = 1$ , we write  $a_i = n^{\epsilon_i} a'_i$  for  $\epsilon_i \geq 0$  and  $\gcd(a'_i, n) = 1$  and we let

$$B((a_1, \dots, a_r)) := \text{lcm} \{a'_i : \gcd(a_i, d) = 1\};$$

otherwise, we let  $B((a_1, \dots, a_r)) = 1$ . We then let

$$B(u) := \text{lcm}_{(a_1, \dots, a_r) \in \mathcal{P}_{>1}(u)} \{B((a_1, \dots, a_r))\}.$$

- (4) Finally, we let  $B(d, n) := \text{lcm}_{u \in S_{d,n}} \{B(u)\}$ .

**Remark 4.2.** If  $\varphi$  is a diagonal-full form of degree  $d$  on a finite dimensional vector space  $V$  over a field  $k$  and  $\varphi$  is anisotropic but there exists some  $K/k$  with  $[K : k] = n$  prime,  $\gcd(n, d) = 1$ , and  $\varphi_K$  isotropic, then the proof of the main theorem shows that  $B(d, n) > 1$  and that there is a field  $L/k$  with  $\gcd([L : k], nd) = 1$  and  $\varphi_L$  isotropic such that  $[L : k] \mid B(d, n)$ .

Since computing partitions is computationally expensive, we also give another, apparently less refined, algorithm to compute some integer  $\tilde{B}(d, n)$  coprime to both  $d$  and  $n$  such that  $B(d, n) \mid \tilde{B}(d, n)$  (and with equality for many, possibly all, instances of  $n$  and  $d$ ), where  $B(d, n)$  is the integer computed by Algorithm 4.1.

**Algorithm 4.3.** Let  $d$  be an odd prime and  $n$  a prime with  $\gcd(d, n) = 1$ .

- (1) Compute the unique integer  $n^* \in \{1, \dots, d-1\}$  such that  $n^* \equiv -n \pmod{d}$ .
- (2) Define the set  $S_{d,n} := \{n^* + jd : j \in \mathbb{Z}_{\geq 0} \text{ and } n^* + jd < (d-1)n\}$ .
- (3) Pick the largest element  $u_{\max} \in S_{d,n}$ . In fact,  $u_{\max} = dn - n - d$ , as shown in the proof of Proposition 4.6. If  $u_{\max} \neq 1$ , we let

$$\mathfrak{P}_{d,n} := \{p^r : p \leq u_{\max} \text{ is prime, } \gcd(p, nd) = 1, r \text{ is greatest s.t. } p^r \leq u_{\max}\},$$

otherwise we let  $\mathfrak{P}_{d,n} := \{1\}$ .

(4) We let

$$\tilde{B}(d, n) := \prod_{a \in \mathfrak{P}_{d, n}} a = \begin{cases} 1 & \text{if } dn - n - d = 1 \\ \prod_{\substack{p \text{ prime:} \\ p \leq dn - n - d, \\ \gcd(p, dn) = 1}} p^{\lfloor \log_p(dn - n - d) \rfloor} & \text{if } dn - n - d > 1. \end{cases}$$

**Proposition 4.4.** *Let  $d$  be an odd prime and  $n$  a prime with  $\gcd(d, n) = 1$ . Let  $B(d, n)$  and  $\tilde{B}(d, n)$  be the positive integers given by Algorithm 4.1 and Algorithm 4.3, respectively. Then  $B(d, n) \mid \tilde{B}(d, n)$ . If, moreover, either of the conditions*

- (1)  $n$  is odd;
- (2)  $n = 2$  and  $d \equiv 1 \pmod{4}$ ;
- (3)  $n = 2$ ,  $d \equiv 3 \pmod{4}$  and  $d \neq 2^s + 3$  for any  $s \in \mathbb{N}$ ;

*holds, then  $B(d, n) = \tilde{B}(d, n)$ .*

*Proof.* In the construction of  $B(d, n)$ , for each  $u \in S_{d, n}$  and each partition  $(a_1, \dots, a_r) \in \mathcal{P}(u)$ , we have that, for any  $a_i$  with  $\gcd(a_i, d) = 1$  and  $a_i > 1$ ,

$$a'_i \leq u \leq u_{\max}.$$

Hence, for any such  $a_i$ , if  $p$  is a prime with  $p \mid a'_i$ , then  $p \leq u_{\max}$  and  $\gcd(p, nd) = 1$ . Moreover, if  $p^\epsilon \parallel a'_i$  and if  $r$  is the largest positive integer such that  $p^r \leq u_{\max}$ , then  $p^\epsilon \mid p^r$ . Hence, for any such  $a_i$ , we have that

$$a'_i \mid \tilde{B}(d, n).$$

from the definition of  $B(d, n)$ , it is then clear that  $B(d, n) \mid \tilde{B}(d, n)$ .

To show equality, we just note that if  $(a_1, \dots, a_r)$  is a partition of  $u \in S_{d, n}$  and  $u \neq u_{\max}$ , then  $(a_1, \dots, a_r, Nd)$  is a partition for  $u_{\max}$ , for some positive integer  $N$ . Moreover, in the algorithm for  $B(d, n)$ , it is easy to see that  $B((a_1, \dots, a_r)) = B((a_1, \dots, a_r, dN))$ . Hence, in the notation of the algorithm for  $B(d, n)$ , we have

$$B(d, n) = \text{lcm}\{B(u_{\max})\}.$$

We now show that  $\tilde{B}(d, n) \mid B(d, n)$ . If  $u_{\max} = 1$ , the claim is clear. So suppose that  $u_{\max} > 1$ . Let  $p^r \in \mathfrak{P}_{d, n}$ , so that  $p \leq u_{\max}$  is a prime with  $\gcd(p, nd) = 1$  and  $r$  is the largest such that  $p^r \leq u_{\max}$ . It suffices to prove that there is a partition  $(a_1, \dots, a_m)$  of  $u_{\max}$  with  $a_i = p^r$  for some  $i$  and  $a_j > 1$  for all  $j = 1, \dots, m$ . Write

$$u_{\max} = p^r + t,$$

for some non-negative integer  $t$ . We claim that  $t \neq 1$ , so that  $(p^r, t)$  is a partition of  $u_{\max}$  with all the entries strictly greater than 1. Suppose, for a contradiction, that  $t = 1$ , that is,  $u_{\max} = p^r + 1$ . Since we know that  $u_{\max} = nd - d - n$ , we have

$$nd - d - n = p^r + 1.$$

We notice that  $nd - n - d$  is always odd (since  $d$  is odd), and so the only way that  $p^r$  can also be odd is if  $p = 2$ . Hence,

$$nd - d - n = 2^r + 1. \tag{4.1}$$

But if  $n$  is odd or if  $n = 2$  and  $d \equiv 1 \pmod{4}$ , then  $nd - d - n \equiv 3 \pmod{4}$ , so the only way that the above equation can hold is if  $r = 1$ , that is, if

$$nd - d - n = 3,$$

which is equivalent to  $d = \frac{n+3}{n-1} = 1 + \frac{4}{n-1}$ . If  $(d, n) = (5, 2)$ , then one can check directly that  $B(5, 2) = \tilde{B}(5, 2)$ . If  $n = 2$  and  $d > 5$ , then we get a contradiction. If  $n$  is odd, then  $n \geq 5$ , so we get a contradiction to the fact that  $d \geq 3$ .

If  $n = 2$ ,  $d \equiv 3 \pmod{4}$  and  $d \neq 2^s + 3$  for any  $s \in \mathbb{N}$ , then we get a contradiction from (4.1).

Hence, in any of the above cases, if  $(d, n) \neq (5, 2)$ , we have that  $t \neq 1$ , and so  $p^r \mid B(d, n)$ . Hence,  $\tilde{B}(d, n) \mid B(d, n)$ , as required.  $\square$

**Remark 4.5.** In the case when  $n = 2$  and  $d = 2^s + 3$  for some  $s \geq 2$ , we have checked computationally that  $B(d, n) = \tilde{B}(d, n)$  for  $2 \leq s \leq 6$ . This seems to suggest that, perhaps,  $B(d, n) = \tilde{B}(d, n)$  in general. We also remark that the proof of Proposition 4.4 shows that, for any odd prime  $d$  and any prime  $n$ , if we write  $B(d, n) = 2^a \lambda$  with  $\gcd(\lambda, 2) = 1$  and  $\tilde{B}(d, n) = 2^b \mu$  with  $\gcd(\mu, 2) = 1$ , then  $\lambda = \mu$  and  $a \mid b$ . In other words,  $\frac{\tilde{B}(d, n)}{B(d, n)}$  is a power of 2.

**Proposition 4.6.** *For any primes  $n, d$  with  $\gcd(d, n) = 1$  we have*

$$\tilde{B}(d, n) = \tilde{B}(n, d).$$

*Proof.* Without loss of generality, we assume that  $d < n$ . By the way that  $\tilde{B}(d, n)$  and  $\tilde{B}(n, d)$  are defined, in order to show that  $\tilde{B}(d, n) = \tilde{B}(n, d)$  it suffices to show that  $\max S_{d,n} = \max S_{n,d}$ .

If  $d^* \in \{1, 2, \dots, n-1\}$  is such that  $d^* \equiv -d \pmod{n}$ , then, since  $d < n$ , we have  $d^* = n - d$ . Hence,

$$\begin{aligned} S_{d,n} &= \{n - d + jn : j \in \mathbb{Z}_{\geq 0} \text{ and } n - d + jn < (n-1)d\} \\ &= \{n - d + jn : j \in \{0, 1, \dots, d-2\}\} \end{aligned}$$

and so  $\max S_{d,n} = n - d + (d-2)n = dn - n - d$ .

On the other hand, if  $n^* \in \{1, 2, \dots, d-1\}$  is such that  $n^* \equiv -n \pmod{d}$ , then, since  $d < n$ , we can write  $n^* = \alpha d - n$  where  $\alpha$  is the unique positive integer strictly between  $\frac{n}{d}$  and  $\frac{d+n}{d}$ . Hence,

$$\begin{aligned} S_{n,d} &= \{\alpha d - n + jd : j \in \mathbb{Z}_{\geq 0} \text{ and } \alpha d - n + jd < (d-1)n\} \\ &= \{\alpha d - n + jd : j \in \{0, 1, \dots, n - \alpha - 1\}\} \end{aligned}$$

and so  $\max S_{n,d} = \alpha d - n + (n - \alpha - 1)d = dn - n - d$ , implying that  $\max S_{d,n} = \max S_{n,d}$ , as required.  $\square$

## REFERENCES

- [Cor76] D. Coray. Algebraic points on cubic hypersurfaces. *Acta Arithmetica*, 30(3):267–296, 1976.
- [EKN08] R. S. Elman, Karpenko, and A. N., Merkurjev. *The algebraic and geometric theory of quadratic forms*, volume 56. American Mathematical Society, 2008.
- [Ma21] Q. Ma. Closed points on cubic hypersurfaces. *Michigan Math. J.*, 70(4):857–868, 2021.
- [RV21] C. Rivera and B. Viray. Persistence of the Brauer-Manin obstruction on cubic surfaces. 2021. Preprint, arXiv:2111.03546.
- [Spr52] T. A. Springer. Sur les formes quadratiques d’indice zéro. *C. R. Acad. Sci. Paris*, 234:1517–1519, 1952.

THE AMERICAN UNIVERSITY OF PARIS, 5 BOULEVARD DE LA TOUR-MAUBOURG, 75007 PARIS, FRANCE  
*Email address:* fbalestrieri@aup.edu