

LINEAR SYSTEM OF HYPERSURFACES PASSING THROUGH A GALOIS ORBIT

SHAMIL ASGARLI, DRAGOS GHIOCA, AND ZINOVY REICHSTEIN

ABSTRACT. Let d and n be positive integers, and E/F be a separable field extension of degree $m = \binom{n+d}{n}$. We show that if $|F| > 2$, then there exists a point $P \in \mathbb{P}^n(E)$ which does not lie on any degree d hypersurface defined over F . In other words, the m Galois conjugates of P impose independent conditions on the m -dimensional F -vector space of degree d forms in x_0, x_1, \dots, x_n . As an application, we determine the maximal dimension of an F -linear system \mathcal{L} of hypersurfaces such that every F -member of \mathcal{L} is irreducible over F .

1. INTRODUCTION

Consider the vector space V of all degree d homogeneous forms in $n + 1$ variables with coefficients in a field F . An elementary counting argument shows that $m := \dim(V) = \binom{n+d}{n}$. Each point of $\mathbb{P}(V)$ can be identified with a projective hypersurface in \mathbb{P}^n defined over F . It is well known that if F is an infinite field, l points of $\mathbb{P}^n(F)$ in general position impose linearly independent conditions on hypersurfaces of degree d , provided that $l \leq m$; cf. Lemma 3. In particular, for points P_1, \dots, P_m of \mathbb{P}^n in general position, there is no hypersurface of degree d which passes through all of them.

Now suppose F is an arbitrary field (possibly finite) and E/F is a separable field extension of degree m . Can we choose $P \in \mathbb{P}^n(E)$ so that the m Galois conjugates of P impose independent conditions on degree d hypersurfaces in \mathbb{P}^n ? In other words, is there always a $P \in \mathbb{P}^n(E)$ which does not lie on any degree d hypersurface defined over F ? Our main result gives an affirmative answer to this question under a mild restriction on F .

Theorem 1. *Let $d, n \in \mathbb{N}$, and E/F be a separable field extension of degree $m := \binom{n+d}{n}$ where $|F| > 2$. Then there exists a point $P \in \mathbb{P}^n(E)$ such that P does not lie on any hypersurface of degree d defined over F .*

Theorem 1 can be restated as follows: there exist $a_0, a_1, \dots, a_n \in E$ such that the m elements $a_0^{i_0} a_1^{i_1} \cdots a_n^{i_n}$ of E are linearly independent over F . Here i_0, i_1, \dots, i_n range over non-negative integers such that $i_0 + i_1 + \dots + i_n = d$. Note that in the case, where $n = 1$, this assertion specializes to the Primitive Element Theorem for the separable field extension E/F .

As an application of Theorem 1, we prove a sharp result regarding the linear systems of hypersurfaces whose \mathbb{F}_q -members are all irreducible. Recall that a linear system $\mathcal{L} = \langle F_0, F_1, \dots, F_r \rangle$ consists of hypersurfaces defined by $c_0 F_0 + \dots + c_r F_r = 0$ where c_i are scalars. By definition, \mathbb{F}_q -members of \mathcal{L} are those hypersurfaces where

2020 *Mathematics Subject Classification.* Primary 14N05; Secondary 14J70, 14G15.
Key words and phrases. linear system, hypersurface, finite fields, irreducibility.

the coefficients c_i all live in \mathbb{F}_q . A linear system \mathcal{L} of hypersurfaces will be called \mathbb{F}_q -irreducible if every \mathbb{F}_q -member of \mathcal{L} is irreducible over \mathbb{F}_q . The following theorem determines the maximum size of an \mathbb{F}_q -irreducible linear system.

Theorem 2. *Let $q > 2$, $d, n \in \mathbb{N}$, and $r := \binom{n+d}{n} - \binom{n+d-1}{n} - 1 = \binom{n+d-1}{n-1} - 1$.*

- (1) *For $t > r$, no t -dimensional \mathbb{F}_q -irreducible linear system of degree d exists.*
- (2) *There exists an r -dimensional \mathbb{F}_q -irreducible linear system of degree d .*

Computer experiments with specific values of n and d suggest that the assertion of Theorem 1 may be true when $|F| = 2$, even though our proof does not go through in this case. If the assumption that $|F| > 2$ can be dropped in Theorem 1, then the assumption that $q > 2$ can be dropped in Theorem 2.

The remainder of this paper is structured as follows. In Section 2 we use a general position argument to prove Theorem 1 under the assumption that F is infinite. In the case where F is finite, the concept of general position no longer applies. Here we employ a point-counting argument. The strategy behind this counting argument is outlined in Section 3, and is carried out in Sections 4 and 5. In Section 6 we deduce Theorem 2 from Theorem 1 and present two examples.

Acknowledgements. The second and third authors are supported by NSERC Discovery grants RGPIN-2018-03690 for D. Ghioca and RGPIN-2023-03353 for Z. Reichstein.

2. PROOF OF THEOREM 1 IN THE CASE, WHERE F IS INFINITE

The following lemma is well known; we include a short proof for the sake of completeness.

Lemma 3. *Let F be a field, d and n be positive integers, and $m = \binom{n+d}{n}$. Then there exist $P_1, \dots, P_m \in \mathbb{P}^n(F)$ such that no degree d hypersurface in \mathbb{P}^n passes through P_1, \dots, P_m .*

Proof. Let $V_0 = H^0(\mathbb{P}^n, \mathcal{O}(d))$ be the m -dimensional vector space space of all degree d forms in x_0, \dots, x_n and $V_i \subset V$ be the subspace of forms vanishing at P_1, \dots, P_i . Clearly $V_i \subseteq V_{i-1}$ for any choice of P_1, \dots, P_i . Requiring forms to vanish on each P_i imposes one linear condition; hence, $\dim(V_i) \geq m - i$, again for any choice of P_1, \dots, P_i . We claim that for a suitable choice of P_1, \dots, P_m , we have

$$(2.1) \quad V_i \subsetneq V_{i-1}$$

for every $i = 1, 2, \dots, m$ or equivalently, $\dim(V_i) = m - i$. In particular, for this choice of P_1, \dots, P_m , we will have $\dim(V_m) = 0$, and the lemma will follow.

We will choose P_1, \dots, P_i so that (2.1) holds, by induction on $i \in \{1, \dots, m\}$. Indeed, assume P_1, \dots, P_{i-1} have been chosen. Since $\dim(V_{i-1}) \geq m - i + 1 > 0$, there exists a non-zero element $f_i \in V_{i-1}$. We will now choose $P_i \in \mathbb{P}^n(F)$ so that $f_i(P_i) \neq 0$. The existence of P_i with this property is obvious if F is an infinite field. If F is finite, say $F = \mathbb{F}_q$ and $E = \mathbb{F}_{q^m}$ for some prime power q , then the existence of P_i such that $f_i(P_i) \neq 0$ follows from the fact that the minimal degree of a hypersurface defined over \mathbb{F}_q and passing through every \mathbb{F}_{q^m} -point in \mathbb{P}^n is $q^m + 1$ (see [MR98]), and $q^m + 1 > m > d$. For this choice of P_i , $f \in V_{i-1} \setminus V_i$, and (2.1) follows. This completes the proof of the claim and thus of Lemma 3. \square

Proposition 4. *Let d and n be positive integers and E/F be a commutative algebra of degree $m = \binom{n+d}{n}$ over F . View E as an m -dimensional vector space over F . Then there is a homogeneous polynomial function H on the affine space $\mathbb{A}_F(E^{n+1}) \simeq \mathbb{A}_F^{(n+1)m}$ defined over F with the following property: For any field extension F'/F , $E' = E \otimes_F F'$, a point $a = (a_0 : \dots : a_n) \in \mathbb{P}^n(E')$ lies on a hypersurface of degree d defined over F' if and only if $H(a_0, a_1, \dots, a_n) = 0$.*

Proof. Let M_1, \dots, M_m be distinct monomials of degree d in x_0, \dots, x_n . Clearly $a = (a_0 : a_1 : \dots : a_n) \in \mathbb{P}^n(E)$ lies on a hypersurface of degree d in \mathbb{P}^n defined over F if and only if $M_1(a), \dots, M_m(a)$ are linearly dependent over F .

Suppose $\{b_1, \dots, b_m\}$ is an F -basis of E . Write

$$(2.2) \quad b_i b_j = \sum_{h=1}^n c_{ij}^h b_h,$$

where the structure constants c_{ij}^h lie in F . Using the basis b_1, \dots, b_m we can identify E with F^m as an F -vector space (not necessarily as an algebra). Set

$$(2.3) \quad a_i = y_{i,1} b_1 + \dots + y_{i,m} b_m,$$

where each $y_{i,j} \in F$. Using formulas (2.2), for every $s = 1, \dots, m$, we can express $M_s(a)$ in the form $M_s(a) = p_{s,1} b_1 + \dots + p_{s,m} b_m$, where each $p_{s,t}$ is a homogeneous polynomial of degree d in $y_{i,j}$ with coefficients in F . By abuse of notation, we will denote these polynomials by $p_{s,t}(y_{i,j})$.

Now, view $y_{i,j}$ as independent $(n+1)m$ variables, as i ranges from 0 to n and j ranges from 1 to m . Set

$$H(y_{i,j}) = \det \begin{pmatrix} p_{1,1}(y_{i,j}) & p_{1,2}(y_{i,j}) & \cdots & p_{1,m}(y_{i,j}) \\ p_{2,1}(y_{i,j}) & p_{2,2}(y_{i,j}) & \cdots & p_{2,m}(y_{i,j}) \\ \vdots & \vdots & \ddots & \vdots \\ p_{m,1}(y_{i,j}) & p_{m,2}(y_{i,j}) & \cdots & p_{m,m}(y_{i,j}) \end{pmatrix}.$$

For any field extension F'/F , an F' -point $(\alpha'_{i,j}) \in \mathbb{A}_F^{(n+1)m}$ represents a point $a' = (a'_0 : \dots : a'_n) \in \mathbb{P}^n(E')$, where $a'_i = \alpha_{i,1} b_1 + \dots + \alpha_{i,m} b_m \in E'$ for each $i = 0, 1, \dots, n$. By our construction, $H(\alpha_{i,j}) = 0$ if and only if $M_1(a'), \dots, M_m(a')$ are linearly dependent over F' , and the proposition follows. \square

Conclusion of the proof of Theorem 1, assuming F is an infinite field. Let $H(y_{i,j})$ be the homogeneous polynomial function on $\mathbb{A}_F(E^n) \simeq \mathbb{A}_F^{(n+1)m}$ defined over F whose existence is asserted by Proposition 4. We claim that H is not identically 0.

Once this claim is established, Theorem 1 readily follows from Proposition 4; since F is an infinite field, we can specialize each x_{ij} to some $c_{ij} \in F$ so that $H(c_{ij}) \neq 0$.

To prove the claim, it suffices to show that $H(c_{ij}) \neq 0$, for some choice of c_{ij} in a larger field F' containing F . Let us choose F' so that F' splits E/F , i.e., $E \otimes_F F'$ isomorphic to $E' := F' \times \dots \times F'$ (m times). In particular, we can take F' to be an algebraic closure of F .

Using Proposition 4, we can rephrase the above observation as follows: in order to prove the existence of a point $a = (a_0 : a_1 : \dots : a_n) \in \mathbb{P}^n(E)$ with the property that it does not lie of any hypersurface of degree d defined over F , it suffices to prove the existence of a point $a' = (a'_0 : \dots : a'_n) \in \mathbb{P}^n(E')$ which does not lie on

any hypersurface of degree d defined over F' . To finish the proof, observe that the existence of a' with this property is equivalent to Lemma 3 with $F = F'$. \square

3. PROOF OF THEOREM 1 IN THE CASE, WHERE F IS FINITE: THE OVERALL STRATEGY

From now on, we will assume that $F = \mathbb{F}_q$ and $E = \mathbb{F}_{q^m}$ are finite fields. The purpose of this section is to outline a strategy for a proof of Theorem 1 in this case. We begin by proving Theorem 1 under an additional assumption, $q > d$, which greatly simplifies our counting argument.

Proposition 5. *Let q be a prime power, $d, n \in \mathbb{N}$ and $m := \binom{n+d}{n}$. Assume $q > d$. Then there exists a point $P \in \mathbb{P}^n(\mathbb{F}_{q^m})$ such that P does not lie on any hypersurface of degree d defined over \mathbb{F}_q .*

Note that here $q = 2$ is allowed, unlike in Theorem 1, but only in the (trivial) case, where $d = 1$. For the remainder of the paper,

$\mathcal{H} \subset \mathbb{P}^n$ will denote the union of all hypersurfaces of degree d defined over \mathbb{F}_q .

Proof of Proposition 5. Observe that $\deg(\mathcal{H}) = d(q^{m-1} + \dots + q + 1)$. Since $q > d$, we have

$$\deg(\mathcal{H}) \leq (q-1)(q^{m-1} + \dots + q + 1) = q^m - 1$$

On the other hand, the degree of a space-filling hypersurface in $\mathbb{P}^n(\mathbb{F}_{q^m})$ defined over \mathbb{F}_q is at least $q^m + 1$; see, e.g., [MR98]. We conclude that \mathcal{H} is not space-filling in $\mathbb{P}^n(\mathbb{F}_{q^m})$, and the proposition follows. \square

When $d \geq q$, we will need a more delicate argument to show that \mathcal{H} does not contain every \mathbb{F}_{q^m} -point of \mathbb{P}^n . We will estimate the number of \mathbb{F}_{q^m} -points on \mathcal{H} , with the goal of showing that this number is strictly smaller than the number of \mathbb{F}_{q^m} -points in \mathbb{P}^n . To estimate the number of \mathbb{F}_{q^m} -points on \mathcal{H} , we will subdivide the hypersurfaces $X \subset \mathbb{P}^n$ of degree d defined over \mathbb{F}_q into two classes:

- a) X is geometrically irreducible (that is, irreducible over $\overline{\mathbb{F}_q}$), or
- b) X is geometrically reducible.

When $X \subset \mathbb{P}^n$ is geometrically irreducible, we will use the inequality

$$(3.1) \quad |X(\mathbb{F}_{q^m})| \leq (q^{m(n-1)} + \dots + q^m + 1) + (d-1)(d-2)q^{m(n-3/2)} + 5d^{13/3}q^{m(n-2)},$$

due to Cafure and Matera [CM06]. When X is geometrically reducible, we will use Serre's estimate [Ser91],

$$(3.2) \quad |X(\mathbb{F}_q)| \leq dq^{m(n-1)} + q^{m(n-2)} + \dots + q^m + 1.$$

Note that both of these are polynomial bounds in q of degree $m(n-1)$. However, the one in Case b) is asymptotically weaker, because the leading term $q^{m(n-1)}$ comes with coefficient 1 in (3.1) and with coefficient d in (3.2). To get a strong upper bound on the number of \mathbb{F}_{q^m} -points on \mathcal{H} , we need to make sure that Case b) does not occur too often. In other words, if we let t denote the fraction of hypersurfaces in \mathbb{P}^n over \mathbb{F}_q of fixed degree d which are *not* geometrically irreducible, then our first task is to bound t from above. Note that t depends on q , d and n .

Poonen showed that $t \rightarrow 0$, as $d \rightarrow \infty$ and q and n remain fixed; see [Poo04, Proposition 2.7]. This is not enough for our purposes. We will refine the inequalities from the proof of [Poo04, Proposition 2.7] to establish the following upper bound on t .

Proposition 6. *Let t denote the fraction of hypersurfaces in \mathbb{P}^n of degree d over \mathbb{F}_q that are geometrically reducible. Assume that one of the following conditions holds:*

- $n = 2$, $d \geq 6$ and $q \geq 3$; or
- $n \geq 3$, $d \geq 3$ and $q \geq 3$.

Then $(d-1)tq \leq 2$.

We will prove this proposition in the next section, then use it to complete the proof of Theorem 1 in Section 5.

4. PROOF OF PROPOSITION 6

Following Poonen [Poo04, Proof of Proposition 2.7], we will write

$$(4.1) \quad t = t_1 + t_2$$

and estimate t_1 and t_2 separately. Here

- t_1 is the proportion of hypersurfaces of degree d in \mathbb{P}^n defined over \mathbb{F}_q , which are reducible over \mathbb{F}_q , and
- t_2 is the proportion of hypersurfaces of degree d in \mathbb{P}^n defined over \mathbb{F}_q , which are irreducible over \mathbb{F}_q but reducible over \mathbb{F}_{q^e} for some integer $e > 1$, dividing d .

Lemma 7. $t_1 \leq \frac{29}{27}q^{2-d}$ when $n = 2$, $q \geq 3$ and $d \geq 6$, while $t_1 \leq 1.5 \cdot q^{-\frac{n(n+d-1)}{2}+n+1}$ for all $n \geq 3$, $q \geq 3$, and $d \geq 3$.

Proof. Following the proof of [Poo04, Proposition 2.7], we obtain:

$$(4.2) \quad t_1 \leq \sum_{i=1}^{\lfloor d/2 \rfloor} q^{-N_i},$$

where

$$N_i = \binom{n+d}{d} - \binom{n+i}{n} - \binom{n+d-i}{n}$$

Claim: For each $1 \leq i \leq \lfloor d/2 \rfloor - 1$

- (a) $N_{i+1} - N_i \geq d - 2i - 1$, and
- (b) $N_{i+1} - N_1 \geq d - 3$.

To prove part (a), we use Pascal's identity to rewrite $N_{i+1} - N_i$ as

$$\begin{aligned} N_{i+1} - N_i &= \binom{n+d-i-1}{n-1} - \binom{n+i}{n-1} \\ &= \sum_{j=0}^{d-i} \binom{n-2+j}{n-2} - \sum_{j=0}^{i+1} \binom{n-2+j}{n-2} \\ &= \sum_{j=i+2}^{d-i} \binom{n-2+j}{n-2} \end{aligned}$$

Each term in the above sum is ≥ 1 (note also that $d-i \geq i+2$ since $i \leq \lfloor d/2 \rfloor - 1$); thus $N_{i+1} - N_i \geq d - 2i - 1$, as claimed in part (a).

To prove part (b), write $N_{i+1} - N_1 = (N_{i+1} - N_i) + (N_i - N_{i-1}) + \dots + (N_2 - N_1)$. Part (a) tells us that each term in this sum is non-negative, and the last term, $N_2 - N_1$, is $\geq d - 3$. Thus

$$(4.3) \quad N_{i+1} - N_1 = (N_{i+1} - N_i) + (N_i - N_{i-1}) + \dots + (N_2 - N_1) \geq N_2 - N_1 \geq d - 3.$$

This completes the proof of the Claim.

Next we estimate N_1 from below:

$$(4.4) \quad \begin{aligned} N_1 &= \binom{n+d-1}{n-1} - \binom{n+1}{n} = \binom{n+d-1}{d} - \binom{n+1}{1} \\ &= \frac{(n+d-1)(n+d-2) \cdots (n+1)n}{d!} - (n+1) \\ &= (n+d-1) \cdot \left(\frac{n+d-2}{d}\right) \cdots \left(\frac{n+1}{3}\right) \cdot \frac{n}{2} - (n+1) \\ &\geq \frac{(n+d-1)n}{2} - (n+1). \end{aligned}$$

Substituting (4.3) and (4.4) into the inequality (4.2), we deduce that

$$t_1 \leq q^{-N_1} \left(1 + \left(\frac{d}{2} - 1\right) q^{3-d}\right) = q^{-\frac{(n+d-1)n}{2} + (n+1)} \left(1 + \left(\frac{d}{2} - 1\right) q^{3-d}\right)$$

An elementary computation shows that for integers $d \geq 6$ and $q \geq 3$ (which corresponds to the case $n = 2$), the expression $(1 + (\frac{d}{2} - 1) q^{3-d})$ is at most $\frac{29}{27}$ (which is achieved when $q = 3$ and $d = 6$). Similarly, when $n \geq 3$, we need to find the maximum of the expression $(1 + (\frac{d}{2} - 1) q^{3-d})$ when $q \geq 3$ and $d \geq 3$; the maximum equals 1.5 and is attained when $q = 3$ and $d = 3$.

Thus,

$$\begin{aligned} t_1 &\leq \frac{29}{27} \cdot q^{2-d} \text{ when } n = 2, \text{ while} \\ t_1 &\leq 1.5 \cdot q^{-\frac{(n+d-1)n}{2} + (n+1)} \text{ when } n \geq 3, \end{aligned}$$

as desired. \square

Next, we prove a lower bound on the proportion t_2 of hypersurfaces which are irreducible but not geometrically irreducible.

Lemma 8. *Let $n \geq 2$, $q \geq 3$, $d \geq 3$, we have $t_2 \leq (d-1)q^{-\frac{1}{4}\binom{n}{2}d^2+d-1}$.*

Proof. It is shown in the proof of [Poo04, Proposition 2.7] that

$$(4.5) \quad t_2 \leq \sum_{e|d, e>1} q^{-M_e}$$

where $M_e = \binom{d+n}{n} - e \binom{d/e+n}{n}$. Our first task is to provide a lower bound on M_e .

Claim 1. Assume $n \geq 2$, $q \geq 3$, $d \geq 3$ and $e | d$, where $e > 1$. Then

$$M_e \geq \binom{e}{2} \binom{n}{2} \left(\frac{d}{e}\right)^2 - e + 1.$$

Proof of Claim 1. Let $S = T \cup F$, where T and F are disjoint sets of cardinality d and n , respectively. The binomial coefficient $\binom{d+n}{n}$ counts the number of n -subsets of S .

Partition T as $T = T_1 \cup T_2 \cup \cdots \cup T_e$, where $|T_i| = d/e$ for each i , and set $S_i = T_i \cup F$. Note that $|S_i| = (d/e) + n$; hence, the binomial coefficient $\binom{d/e+n}{n}$ counts the number of n -subsets of S_i . It is also clear that the number of *common* n -subsets of S_i and S_j for $i \neq j$ is exactly 1, namely the n -set F . Thus, the total number of n -subsets arising from S_1, S_2, \dots, S_e is exactly:

$$e \cdot \left(\binom{d/e+n}{n} - 1 \right) + 1 = e \cdot \binom{d/e+n}{n} - e + 1$$

Next, we construct additional n -subsets of S that are not contained in any S_k . Fix integers $1 \leq i < j \leq e$. Choose elements $a \in T_i$ and $b \in T_j$ and consider an n -subset of S containing both a and b . Any such subset is of the form

$$\{a, b\} \cup E$$

for some $(n-2)$ -subset E of F . By our construction $\{a, b\} \cup E$ is not contained in S_k for any $1 \leq k \leq e$. The number of subsets of the form $\{a, b\} \cup E$ is equal to $(d/e) \cdot (d/e) \cdot \binom{n}{n-2}$ once i and j are fixed, because there are d/e ways to choose a in T_i , d/e ways to choose b in T_j , and $\binom{n}{n-2} = \binom{n}{2}$ ways to choose an $(n-2)$ -subset E of F . Varying (i, j) among the $\binom{e}{2}$ choices, we get a total contribution of

$$\binom{e}{2} \binom{n}{2} \left(\frac{d}{e} \right)^2$$

many distinct n -subsets of S that do not arise as n -subsets of S_k for any $1 \leq k \leq e$. Consequently,

$$\binom{d+n}{n} - \left(e \cdot \binom{d/e+n}{n} - e + 1 \right) \geq \binom{e}{2} \binom{n}{2} \left(\frac{d}{e} \right)^2,$$

leading to the lower bound

$$M_e = \binom{d+n}{n} - e \cdot \binom{d/e+n}{n} \geq \binom{e}{2} \binom{n}{2} \left(\frac{d}{e} \right)^2 - e + 1,$$

as claimed. \square

Claim 2: $M_e \geq \frac{1}{4} \binom{n}{2} d^2 - d + 1$

To deduce this bound from Claim 1, note that

$$\binom{e}{2} \binom{n}{2} \left(\frac{d}{e} \right)^2 - e + 1 \geq \left(\frac{1}{2} - \frac{1}{2e} \right) \binom{n}{2} d^2 - d + 1 \geq \frac{1}{4} \binom{n}{2} d^2 - d + 1$$

since $d \geq e \geq 2$.

To complete the proof of Lemma 8, we note that the number of divisors e of d with $e > 1$ is at most $d-1$. Thus the right hand side of (4.5) has at most $d-1$ terms. By Claim 2, each term q^{-M_e} is at most $q^{-\frac{1}{4} \binom{n}{2} d^2 + d - 1}$. This yields the inequality

$$t_2 \leq (d-1) q^{-\frac{1}{4} \binom{n}{2} d^2 + d - 1}$$

of Lemma 8. \square

We are now ready to finish the proof of Proposition 6. Writing $t = t_1 + t_2$, as in (4.1) and using Lemma 7 and Lemma 8, we obtain

$$(4.6) \quad t \leq 1.5 \cdot q^{-\frac{(n+d-1)n}{2}+(n+1)} + (d-1)q^{-\frac{1}{4}\binom{n}{2}d^2+d-1}$$

when $n \geq 3$, $q \geq 3$ and $d \geq 3$, while

$$(4.7) \quad t \leq \frac{29}{27} \cdot q^{2-d} + (d-1)q^{-\frac{1}{4}d^2+d-1},$$

when $n = 2$, $q \geq 3$ and $d \geq 6$. We will consider the cases, where $n = 2$ and $n \geq 3$ separately.

Claim 1: For $n = 2$, $q \geq 3$ and $d \geq 6$, we have $(d-1)tq \leq 2$.

Indeed, when $n = 2$, the inequality (4.6) specializes to

$$t \leq \frac{29}{27}q^{2-d} + (d-1)q^{-\frac{1}{4}d^2+d-1}.$$

Consequently,

$$(d-1)tq \leq \Theta(q, d) := (d-1) \left(\frac{29}{27}q^{3-d} + (d-1)q^{-\frac{1}{4}d^2+d} \right).$$

For $d \geq 6$, both exponents in q^{3-d} and $q^{-\frac{1}{4}d^2+d}$ are negative. This yields $\Theta(q, d) \leq \Theta(3, d)$ for $q \geq 3$. On the domain $d \geq 6$, the one-variable function $\Theta(3, d)$ achieves its maximum when $d = 6$. Thus, $(d-1)tq \leq \Theta(3, 6) \approx 1.125$. In particular, $(d-1)tq \leq 2$. This proves Claim 1.

Claim 2. For $n \geq 3$, $q \geq 3$ and $d \geq 3$, we have $(d-1)tq \leq 2$.

We argue as in the proof of Claim 1. For $n \geq 3$, the inequality (4.6) implies

$$t \leq 1.5q^{4-\frac{3}{2}(d+2)} + (d-1)q^{-\frac{3}{4}d^2+d-1}.$$

where we have substituted $n = 3$ in (4.6). Consequently,

$$(d-1)tq \leq \Psi(q, d) := (d-1) \left(1.5q^{5-\frac{3}{2}(d+2)} + (d-1)q^{-\frac{3}{4}d^2+d} \right)$$

We have $\Psi(q, d) \leq \Psi(3, d)$ for $q \geq 3$. On the domain $d \geq 3$, the one-variable function $\Psi(3, d)$ achieves its maximum when $d = 3$. Thus, $(d-1)tq \leq \Psi(3, 3) \approx 0.257$. In particular, $(d-1)tq \leq 2$. This completes the proof of Claim 2 and thus of Proposition 6. \square

5. CONCLUSION OF THE PROOF OF THEOREM 1

The case when F is infinite is handled in Section 2. Thus we will assume that $F = \mathbb{F}_q$ and $E = \mathbb{F}_{q^m}$ are finite fields. Furthermore, Proposition 5 delivers the desired result when $q > d$; hence, from now on, we assume that $q \leq d$.

We follow the strategy outlined in Section 3. Recall the notation we used there:

- \mathcal{H} denotes the union of all degree d hypersurfaces in \mathbb{P}^n defined over \mathbb{F}_q , and
- t denotes the fraction of these hypersurfaces which are *not* geometrically irreducible.

Our goal is to show that there exists an \mathbb{F}_{q^m} -point in \mathbb{P}^n which does not lie on \mathcal{H} . As the total number of hypersurfaces of degree d defined over \mathbb{F}_q is $q^{m-1} + \dots + q + 1 = \frac{q^m - 1}{q - 1}$, there are exactly $t \left(\frac{q^m - 1}{q - 1} \right)$ hypersurfaces of degree d which are geometrically reducible. Using the upper bounds (3.1) and (3.2) on the number of points of a hypersurface of degree d , we obtain the following inequality:

$$\begin{aligned} \#\mathcal{H}(\mathbb{F}_{q^m}) &\leq \left(\frac{q^m - 1}{q - 1} \right) \cdot ((1 - t)((q^{m(n-1)} + \dots + q^m + 1) + (d - 1)(d - 2)q^{m(n-3/2)} \\ &\quad + 5d^{13/3}q^{m(n-2)}) + t(dq^{m(n-1)} + q^{m(n-2)} + \dots + q^m + 1)), \end{aligned}$$

where $m := \binom{n+d}{n}$. After some cancellations, we can bound the term in the parenthesis after $\frac{q^m - 1}{q - 1}$ from above by

$$(5.1) \quad \begin{aligned} &(1 + (d - 1)t)q^{m(n-1)} + q^{m(n-2)} + \dots + q^m + 1 \\ &+ (d - 1)(d - 2)q^{m(n-3/2)} + 5d^{13/3}q^{m(n-2)}. \end{aligned}$$

By Proposition 6, we have

$$(5.2) \quad (d - 1)t \leq \frac{2}{q},$$

for all $n \geq 3$, $d \geq 3$ and $q \geq 3$, or $n = 2$, $q \geq 3$ and $d \geq 6$. Since we already know that Theorem 1 holds when $q > d$ (see Proposition 5), we may assume that the inequality (5.2) holds unless (n, q, d) equals $(2, 3, 3)$, $(2, 3, 4)$, $(2, 3, 5)$, $(2, 4, 4)$, $(2, 4, 5)$ and $(2, 5, 5)$. These exceptional cases will be handled using a computer at the end of the proof; we ignore them for now. Next, we bound the lower-order terms in the expression (5.1).

Claim. If $n \geq 2$, $q \geq 3$ and $d \geq 3$, then we have

$$(d - 1)(d - 2)q^{m(n-3/2)} + (q^{m(n-2)} + \dots + q^m + 1) + 5d^{13/3}q^{m(n-2)} < q^{m(n-1)-1}$$

In order to verify this inequality, we first note that

$$(5.3) \quad q^{m(n-2)} + \dots + q^m + 1 = \frac{q^{m(n-1)} - 1}{q^m - 1} < \frac{q^{m(n-1)}}{q^m - 1} < \frac{q^{m(n-1)}}{1000q},$$

since $q \geq 3$ and $m \geq (d + 2)(d + 1)/2 \geq 10$ because $d \geq 3$. Employing (5.3), the left-hand side of the desired inequality is less than

$$(5.4) \quad (d - 1)(d - 2)q^{m(n-3/2)} + \frac{q^{m(n-1)-1}}{1000} + 5d^{13/3}q^{m(n-2)}.$$

Dividing the expression from (5.4) by $q^{m(n-1)-1}$, we can easily check

$$(d - 1)(d - 2)q^{1-m/2} + \frac{1}{1000} + 5d^{13/3}q^{1-m} < 1,$$

keeping in mind that $q \geq 3$ and $m \geq (d + 2)(d + 1)/2$, while $d \geq 3$; this completes the proof of the claim.

Combining the Claim with the inequality (5.2), we see that the quantity in (5.1) is less than

$$\left(1 + \frac{2}{q} \right) q^{m(n-1)} + q^{m(n-1)-1} < q^{m(n-1)} + 3q^{m(n-1)-1}.$$

Thus, we obtain the following upper bound on $\#\mathcal{H}(\mathbb{F}_{q^m})$.

$$\#\mathcal{H}(\mathbb{F}_{q^m}) < \left(\frac{q^m - 1}{q - 1}\right) \left(q^{m(n-1)} + 3q^{m(n-1)-1}\right)$$

In order to show that \mathcal{H} does not pass through every \mathbb{F}_{q^m} -point in \mathbb{P}^n , it is enough to show that

$$\left(\frac{q^m - 1}{q - 1}\right) \left(q^{m(n-1)} + 3q^{m(n-1)-1}\right) \leq q^{mn},$$

because $\#\mathbb{P}^n(\mathbb{F}_{q^m}) = q^{mn} + \dots + q^m + 1$. By replacing $q^m - 1$ with q^m on the left-hand-side, we claim that the stronger inequality holds:

$$q^m(q^{m(n-1)} + 3q^{m(n-1)-1}) \leq q^{mn+1} - q^{mn}.$$

After cancelling out q^{mn-1} from both sides, it remains to show,

$$q + 3 \leq q^2 - q.$$

This last inequality $q^2 - 2q - 3 \geq 0$ is valid for all $q \geq 3$. Therefore, we have established Theorem 1 with $F = \mathbb{F}_q$ and $E = \mathbb{F}_{q^m}$, for all triples (n, q, d) with $n \geq 2$, $q \geq 3$, $d \geq 1$, and $(n, q, d) \neq (2, 3, 3), (2, 3, 4), (2, 3, 5), (2, 4, 4), (2, 4, 5), (2, 5, 5)$.

We now complete the proof of Theorem 1 by a computer-assisted computation in these six exceptional cases. For each of the exceptional triples (n, q, d) , it suffices to find a single point $P \in \mathbb{P}^2(\mathbb{F}_{q^m})$ where $m = \binom{n+d}{n}$ such that P does not lie on any degree d hypersurface defined over \mathbb{F}_q .

When $(n, q, d) = (2, 3, 3)$ we write $\mathbb{F}_{3^{10}}$ as $\mathbb{F}_3[a]/(a^{10} + a^4 + a + 1)$, and check that $P = (a : a^8 : 1)$ does not lie on any cubic plane curve defined over \mathbb{F}_3 .

When $(n, q, d) = (2, 3, 4)$, we write $\mathbb{F}_{3^{15}}$ as $\mathbb{F}_3[a]/(a^{15} + a^2 - 1)$ and check that $P = (a : a^9 : 1)$ does not lie on any quartic plane curve defined over \mathbb{F}_3 .

When $(n, q, d) = (2, 3, 5)$, we write $\mathbb{F}_{3^{21}}$ as $\mathbb{F}_3[a]/(a^{21} + a^{16} - 1)$ and check that $P = (a : a^{18} : 1)$ does not lie on any quintic plane curve defined over \mathbb{F}_3 .

When $(n, q, d) = (2, 4, 4)$, we write $\mathbb{F}_{4^{15}}$ as $\mathbb{F}_4[a]/(a^{15} + a + 1)$ and check that $P = (a^3 : a^8 : 1)$ does not lie on any quartic plane curve defined over \mathbb{F}_4 .

When $(n, q, d) = (2, 4, 5)$, we write $\mathbb{F}_{4^{21}}$ as $\mathbb{F}_4[a]/(a^{21} + a^2 + 1)$ and check that $P = (a^6 : a^{11} : 1)$ does not lie on any quintic plane curve defined over \mathbb{F}_4 .

When $(n, q, d) = (2, 5, 5)$, we write $\mathbb{F}_{5^{21}}$ as $\mathbb{F}_5[a]/(a^{21} + a^{18} + a^{14} + 1)$ and check that $P = (a : a^9 : 1)$ does not lie on any quintic plane curve defined over \mathbb{F}_5 . \square

6. PROOF OF THEOREM 2

Suppose \mathcal{P} is a property of an algebraic hypersurface. For instance, \mathcal{P} could stand for “is smooth”, or “is irreducible over \mathbb{F}_q ”, or “is geometrically irreducible.” Given a finite field \mathbb{F}_q , it is natural to ask the following.

Question 9. What is the largest value of r such that there exists a dimension- r linear system \mathcal{L} of degree d hypersurfaces in \mathbb{P}^n such that every \mathbb{F}_q -member of \mathcal{L} satisfies \mathcal{P} ?

More explicitly, Question 9 asks for the largest value of r , as a function of q, n, d , such that there exists a linear system $\mathcal{L} = \langle F_0, F_1, \dots, F_r \rangle$ of (projective) dimension r with the following property: each nontrivial linear combination $c_0 F_0 + \dots + c_r F_r = 0$ with $c_i \in \mathbb{F}_q$ defines a hypersurface in \mathbb{P}^n that satisfies the property \mathcal{P} .

When \mathcal{P} represents the property of being smooth, we answered Question 9 in [AGR23] under a mild restriction on the characteristic of our field. More precisely, we proved that the maximum value of r is n whenever $\text{char}(\mathbb{F}_q) \nmid \gcd(d, n+1)$.

When \mathcal{P} represents the property of being irreducible over \mathbb{F}_q , Theorem 2 pinpoints the exact answer: the largest value of r is $\binom{n+d}{n} - \binom{n+(d-1)}{n} - 1 = \binom{n+d-1}{n-1} - 1$.

Proof of Theorem 2. (1) Let $\mathcal{L} = \langle F_0, \dots, F_t \rangle$ be a linear system of (projective) dimension $t > r$. Let V denote the vector space of all degree- d forms and consider the following subspace:

$$W = \{F \in V \mid F \text{ is divisible by } x_0\}.$$

Evidently, $\dim(V) = \binom{n+d}{n}$ and $\dim(W) = \binom{n+d-1}{n}$. Thus,

$$\dim_{\mathbb{F}_q}(W) + \dim_{\mathbb{F}_q}(\mathcal{L}) = \binom{n+d-1}{n} + t + 1 > \binom{n+d}{n}$$

due to $t > r$ and our choice of r . It follows that W and \mathcal{L} meet in a nontrivial \mathbb{F}_q -subspace inside V . In other words, \mathcal{L} contains a hypersurface defined over \mathbb{F}_q whose equation is divisible by x_0 . Therefore, \mathcal{L} is *not* an \mathbb{F}_q -irreducible linear system.

(2) We apply Theorem 1 for degree $d-1$ hypersurfaces in \mathbb{P}^n . We obtain a point $P \in \mathbb{P}^n(\mathbb{F}_{q^m})$ with $m = \binom{n+d-1}{n}$ that is *not* contained in any hypersurface of degree $d-1$ defined over \mathbb{F}_q . Clearly, P is also not contained in any hypersurface of degree *at most* $d-1$. Let $P_1 := P$, and set $S = \{P_1, \dots, P_m\}$ to be the orbit of P under $\text{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$. Consider the vector space V_S of degree d forms defined over \mathbb{F}_q , which vanish at the point P (and therefore at each point of S). Since vanishing at each additional point imposes at most one new linear condition, we obtain

$$\dim V_S \geq \binom{n+d}{d} - m = \binom{n+d}{d} - \binom{n+d-1}{n} = r + 1.$$

Pick linearly independent forms $F_0, F_1, \dots, F_r \in V_S$. Consider the linear system $\mathcal{L} = \langle F_0, F_1, \dots, F_r \rangle$ of degree d hypersurfaces. We claim that each \mathbb{F}_q -member F of \mathcal{L} is irreducible over \mathbb{F}_q . Otherwise, $F = G \cdot H$ where $\deg(G) \leq d-1$ and $\deg(H) \leq d-1$. Since $F(P) = 0$, we have $G(P) = 0$ or $H(P) = 0$. Either case leads to a contradiction because P does not lie on a hypersurface of degree at most $d-1$ defined over \mathbb{F}_q . Therefore, \mathcal{L} is \mathbb{F}_q -irreducible. \square

Example 10. Consider the case $d = 4$ and $n = 2$, along with $q > 2$.

- By [AGR23], there exist $n+1 = 3$ linearly independent plane quartics $C_i = \{F_i = 0\}$ for $i = 0, 1, 2$ such that the quartic $\{a_0F_0 + a_1F_1 + a_2F_2 = 0\}$ is smooth for all $(a_0, a_1, a_2) \in (\mathbb{F}_q)^3 \setminus \{(0, 0, 0)\}$. The number 3 is maximum possible here.
- By Theorem 2, there exist $r+1 = \binom{d+2}{2} - \binom{d+1}{2} = d+1 = 5$ linearly independent plane quartics $C_i = \{F_i = 0\}$ for $i = 0, 1, 2, 3, 4$ such that the quartic $\{\sum_{i=0}^4 a_i F_i = 0\}$ is irreducible over \mathbb{F}_q for all $(a_0, a_1, a_2, a_3, a_4) \in (\mathbb{F}_q)^5 \setminus \{(0, 0, 0, 0, 0)\}$. The number 5 is maximum possible here.

Example 11. Consider the case $d = 3$ and $n = 3$, along with $q > 2$.

- By [AGR23], there exist $n+1 = 4$ linearly independent cubic surfaces $C_i = \{F_i = 0\}$ for $i = 0, 1, 2, 3$ such that the cubic $\{a_0F_0 + a_1F_1 + a_2F_2 + a_3F_3 = 0\}$ is smooth for all $(a_0, a_1, a_2, a_3) \in (\mathbb{F}_q)^4 \setminus \{(0, 0, 0, 0)\}$. The number 4 is maximum possible here.

- By Theorem 2, there exist $r + 1 = \binom{d+3}{3} - \binom{d+2}{3} = \frac{1}{2}(d^2 + 3d + 2) = 10$ linearly independent cubic surfaces $C_i = \{F_i = 0\}$ for $i = 0, 1, 2, \dots, 9$ such that the cubic $\{\sum_{i=0}^9 a_i F_i = 0\}$ is irreducible over \mathbb{F}_q for all $(a_0, \dots, a_9) \in (\mathbb{F}_q)^{10} \setminus \{(0, \dots, 0)\}$. The number 10 is maximum possible here.

REFERENCES

- [AGR23] Shamil Asgarli, Dragos Ghioca, and Zinovy Reichstein, *Linear families of smooth hypersurfaces over finitely generated fields*, Finite Fields Appl. **87** (2023), Paper No. 102169, 10.
- [CM06] Antonio Cafure and Guillermo Matera, *Improved explicit estimates on the number of solutions of equations over a finite field*, Finite Fields Appl. **12** (2006), no. 2, 155–185.
- [MR98] Dany-Jack Mercier and Robert Rolland, *Polynômes homogènes qui s’annulent sur l’espace projectif $\mathbb{P}^m(\mathbb{F}_q)$* , J. Pure Appl. Algebra **124** (1998), no. 1–3, 227–240.
- [Poo04] Bjorn Poonen, *Bertini theorems over finite fields*, Ann. of Math. (2) **160** (2004), no. 3, 1099–1127.
- [Ser91] Jean-Pierre Serre, *Lettre à M. Tsfasman*, 1991, pp. 11, 351–353 (1992). Journées Arithmétiques, 1989 (Luminy, 1989).

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE, SANTA CLARA UNIVERSITY, 500 EL CAMINO REAL, USA 95053

Email address: `sasgarli@scu.edu`

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF BRITISH COLUMBIA, VANCOUVER, BC V6T 1Z2

Email address: `dghioca@math.ubc.ca`

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF BRITISH COLUMBIA, VANCOUVER, BC V6T 1Z2

Email address: `reichst@math.ubc.ca`