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 $x_0, x_1, \ldots, x_n$. As an application, we determine the maximal dimensions of linear systems $\mathcal{L}_1$ and $\mathcal{L}_2$ of hypersurfaces in $\mathbb{P}^n$ over a finite field F, where every F-member of $\mathcal{L}_1$ is reducible and every F-member of $\mathcal{L}_2$ is irreducible.

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

$$\dim(V) = \binom{n+d}{n}.$$

Let us denote this number by m. An F-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 $l \leqslant m$; cf. Lemma 2.1. In particular, for points $P_1, \ldots, P_m$ of $\mathbb{P}^n$ in general position, no hypersurface of degree d passes through all of them.

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 1.1. *Let d and n be positive integers, and E/F be a separable field extension of degree $m := \binom{n+d}{n}$. Assume that $|F| > 2$. 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 1.1 can be restated as follows: there exist $a_0, a_1, \ldots, a_n \in E$ 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 $i_0, i_1, \ldots, i_n$ range over non-negative integers such that $i_0 + i_1 + \ldots + i_n = d$. Note that in the case, where $n = 1$, this assertion specializes to the Primitive Element Theorem for the separable field extension E/F.

2020 *Mathematics Subject Classification.* Primary 14N05; Secondary 14J70, 14G15.

Key words and phrases. linear system, hypersurface, finite fields, irreducibility.

As an application of Theorem 1.1, we determine the maximal dimensions of linear systems $\mathcal{L}_1$ and $\mathcal{L}_2$ of hypersurfaces in $\mathbb{P}^n$ over a finite field F, where every F-member of $\mathcal{L}_1$ is reducible and every F-member of $\mathcal{L}_2$ is irreducible. Our main result in this direction is Theorem 1.3 below. Before stating it, we recall some terminology.

Let F be a field. An F-linear system $\mathcal{L}$ of degree d hypersurfaces in $\mathbb{P}^n$ is a linear subspace of such hypersurfaces defined over F. By the no-name lemma [Sha94, Appendix 3], $\mathcal{L}$ has a basis $f_0, f_1, \dots, f_r$ such that each f_i is defined over F. Members of $\mathcal{L}$ are then hypersurfaces in $\mathbb{P}^n$ of the form $c_0 f_0 + \dots + c_r f_r = 0$ where $c_0, \dots, c_r$ are scalars. Members of $\mathcal{L}$ corresponding to $c_0, \dots, c_r \in F$ are called *F-members*. The *dimension* of $\mathcal{L}$ is r (the projective dimension).

Given a property $\mathcal{P}$ of algebraic hypersurfaces defined over a finite field $\mathbb{F}_q$, it is natural to ask the following.

Question 1.2. What is the largest dimension of a linear system $\mathcal{L}$ of degree d hypersurfaces in $\mathbb{P}^n$ such that every $\mathbb{F}_q$-member of $\mathcal{L}$ satisfies $\mathcal{P}$?

In our previous paper [AGR23], we addressed Question 1.2 when $\mathcal{P}$ is the property of being smooth. In the paper [AGY23], the first two authors and Chi Hoi Yip addressed Question 1.2 when $\mathcal{P}$ is the property of being non-blocking[1]. Parts (a) and (b) of Theorem 1.3 below answer Question 1.2 when $\mathcal{P}$ is the property of being reducible, and parts (c) and (d) when $\mathcal{P}$ is the property of being irreducible.

Theorem 1.3. *Let $d \geqslant 2$ and $n \geqslant 1$ be integers, $m := \binom{n+d}{n}$, $r := \binom{n+d-1}{n}$, and $\mathbb{F}_q$ be a finite field of order $q > 2$. Then*

(a) there exists an $(r-1)$-dimensional $\mathbb{F}_q$-linear system $\mathcal{L}_{\text{red}}$ of degree d hypersurfaces in $\mathbb{P}^n$ such that every $\mathbb{F}_q$-member of $\mathcal{L}_{\text{red}}$ is reducible over $\mathbb{F}_q$.

(b) Every $\mathbb{F}_q$-linear system $\mathcal{L}$ of dimension $\geqslant r$ has an $\mathbb{F}_q$-member which is irreducible over $\mathbb{F}_q$.

(c) There exists an $(m-1-r)$-dimensional $\mathbb{F}_q$-linear system $\mathcal{L}_{\text{irr}}$ of degree d hypersurfaces in $\mathbb{P}^n$ such that every $\mathbb{F}_q$-member of $\mathcal{L}_{\text{irr}}$ is irreducible over $\mathbb{F}_q$.

(d) Every $\mathbb{F}_q$-linear system $\mathcal{L}$ of dimension $\geqslant m-r$ has an $\mathbb{F}_q$-member which is reducible over $\mathbb{F}_q$.

When the finite field $\mathbb{F}_q$ is replaced by its algebraic closure $\overline{\mathbb{F}_q}$ or any other algebraically closed field, parts (a) and (b) of Theorem 1.3 remain valid, whereas the dimensions in parts (c) and (d) get reduced by n; see Proposition 8.1. In particular, part (c) fails when $\mathbb{F}_q$ is replaced by an algebraically closed field.

Computer experiments with specific values of n and d suggest that the assertion of Theorem 1.1 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 1.1, then the assumption that $q > 2$ can be dropped in Theorem 1.3.

The remainder of this paper is structured as follows. In Section 2, we use a general position argument to prove Theorem 1.1 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

[1]Here a hypersurface X in $\mathbb{P}^n$ defined over $\mathbb{F}_q$ is called *blocking* if $X \cap L$ has an $\mathbb{F}_q$-point for every line $L \subset \mathbb{P}^n$ defined over $\mathbb{F}_q$ and *non-blocking* otherwise.

a point-counting argument. The strategy behind this counting argument is outlined in Section 3, and is carried out in Sections 4, 5 and 6. In Section 7 we deduce Theorem 1.3 from Theorem 1.1. In Section 8 we prove a variant of Theorem 1.3 with $\mathbb{F}_q$ replaced by an algebraically closed field.

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. We are grateful to anonymous referees whose comments and questions helped us improve the exposition.

Data availability statement. No data sets were used or generated in the course of this research.

Conflict of interest statement. All authors have no conflicts of interest.

2. Proof of Theorem 1.1 in the case of infinite fields

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

Lemma 2.1. *Let F be an infinite 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, $\dim(V_i) \geqslant m - i$, 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

$$V_i \subsetneq V_{i-1} \tag{2.1}$$

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 $\dim(V_{i-1}) \geqslant m - i + 1 > 0$, 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 $f_i(P_i) \neq 0$. A point P_i with this property exists since F is an infinite field. 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 2.1. □

Proposition 2.2. *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 $\mathbb{A}^{n+1}_F(E) \simeq \mathbb{A}^{(n+1)m}_F$ defined over F with the following property: For any field extension F'/F, $E' = E \otimes_F F'$, a point $a = (a_0 : \ldots : a_n) \in \mathbb{P}^n(E')$ 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 $a = (a_0 : a_1 : \ldots : a_n) \in \mathbb{P}^n(E)$ 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 $\{b_1, \ldots, b_n\}$ is an F-basis of E. Write

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

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

$$a_i = y_{i,1} b_1 + \ldots + y_{i,m} b_m, \tag{2.3}$$

where each $y_{i,j} \in F$. Using formulas (2.2), for every $s = 1, \ldots, m$, we can express $M_s(a)$ in the form $M_s(a) = p_{s,1} b_1 + \ldots + p_{s,m} b_m$, 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 $a' = (a'_0 : \ldots : a'_m) \in \mathbb{P}^n(E')$, where $a'_i = \alpha_{i,1} b_1 + \ldots + \alpha_{i,m} b_m \in E'$ for each $i = 0, 1, \ldots, n$. By our construction, $H(\alpha_{i,j}) = 0$ if and only if $M_1(a'), \ldots, M_m(a')$ are linearly dependent over F', and the proposition follows. □

Remark 2.3. In the case, where E/F is a separable field extension of degree m, we can give an alternative description of H as follows. Denote the normal closure of E over F by E^{norm}, the Galois group $\text{Gal}(E^{\text{norm}}/F)$ by G, and the Galois group $\text{Gal}(E^{\text{norm}}/E)$ by G_0. Note that $[G : G_0] = [E : F] = m$.

It is easy to see that there exists a homogeneous polynomial

$$P_{d,n} \in \mathbb{Z}[x_{ij} \,|\, i = 1, \ldots, m \quad \text{and} \quad j = 0, 1, \ldots, n]$$

such that m points $(x_{i0} : \ldots : x_{in})$ of $\mathbb{P}^n$, where $i = 1, \ldots, m$, all lie on the same hypersurface of degree d if and only if $P_{d,n}(x_{ij}) = 0$. Then given a point $A = (a_0, \ldots, a_n)$ in $\mathbb{A}_E^{n+1}$, we set $H(A) = P_{d,n}(\sigma_1(A), \ldots, \sigma_m(A))$, where $\sigma_1, \ldots, \sigma_m$ are representatives of the m left cosets of G_0 in G.

Conclusion of the proof of Theorem 1.1, 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 2.2. We claim that H is not identically 0.

Once this claim is established, Theorem 1.1 readily follows from Proposition 2.2; 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 $E' := F' \times \ldots \times F'$ (m times). In particular, we can take F' to be an algebraic closure of F.

Using Proposition 2.2, we can rephrase the above observation as follows: to prove the existence of a point $a = (a_0 : a_1 : \ldots : a_n) \in \mathbb{P}^n(E)$ 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 $a' = (a'_0 : \ldots : a_n) \in \mathbb{P}^n(E')$ 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 2.1 with $F = F'$. □

3. Proof strategy for Theorem 1.1 in the finite field case

From now on, we will assume that $F = \mathbb{F}_q$ and $E = \mathbb{F}_{q^m}$ are finite fields. This section outlines a strategy for a proof of Theorem 1.1 in this case. We begin by proving Theorem 1.1 under the assumption $q > d$, which greatly simplifies our counting argument.

Proposition 3.1. *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 1.1, 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 3.1. Observe that $\deg(\mathcal{H}) = d(q^{m-1} + \ldots + q + 1)$. Since $q > d$, we have

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

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, Théorème 2.1]. We conclude that $\mathcal{H}$ is not space-filling in $\mathbb{P}^n(\mathbb{F}_{q^m})$, and the proposition follows. □

When $d \geqslant q$, 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

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

due to Cafure and Matera [CM06, Theorem 5.2]. When X is geometrically reducible, we will use Serre's estimate [Ser91, Théorème],

$$|X(\mathbb{F}_q)| \leqslant dq^{m(n-1)} + q^{m(n-2)} + \cdots + q^m + 1. \tag{3.2}$$

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 $t \to 0$, as $d \to \infty$ 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 3.2. *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:*

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

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

We will prove Proposition 3.2 in Section 5, then use it to complete the proof of Theorem 1.1 in Section 6. In Section 4 we gather several elementary inequalities involving binomial coefficients, which will be used in our proofs.

4. Combinatorial bounds

Throughout this section, we let $q, d \geqslant 3$ and $n \geqslant 2$ be integers. For each i between 0 and d, set

$$N_i = \binom{n+d}{d} - \binom{n+i}{n} - \binom{n+d-i}{n}. \tag{4.1}$$

Lemma 4.1. *Assume $2(i+1) \leqslant d$. Then*

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

Proof. (a) Using Pascal's identity recursively, we rewrite $N_{i+1} - N_i$ as

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

The above sum has $(d-i) - (i-1) = d - 2i + 1 \geqslant 1$ terms by our assumption on i. Moreover, each term $\geqslant 1$, so the sum is $\geqslant d - 2i + 1$, as desired.

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

$$N_{i+1} - N_1 = (N_{i+1} - N_i) + (N_i - N_{i-1}) + \ldots + (N_2 - N_1) \geqslant N_2 - N_1 \geqslant d - 3, \tag{4.2}$$

as desired. ☐

Lemma 4.2. *Let* $u_1 := \sum_{i=1}^{\lfloor d/2 \rfloor} q^{-N_i}$*, where* N_i *is as in* (4.1)*. Then*

(a) $u_1 \leqslant \frac{29}{27} q^{2-d}$ *if* $n = 2$*,* $q \geqslant 3$ *and* $d \geqslant 6$*.*

(b) $u_1 \leqslant \frac{3}{2} q^{-\frac{n(n+d-1)}{2}+n+1}$ *for all* $n \geqslant 3$*,* $q \geqslant 3$*, and* $d \geqslant 3$*.*

Proof. We first estimate N_1 from below. Note that we assume $n \geqslant 2$ throughout.

$$\begin{aligned} N_1 &= \binom{n+d-1}{n-1} - \binom{n+1}{n} = \binom{n+d-1}{d} - \binom{n+1}{1} \\ &= \frac{(n+d-1)(n+d-2)\cdots(n+1)n}{d!} - (n+1) \\ &= (n+d-1)\cdot\left(\frac{n+d-2}{d}\right)\cdots\left(\frac{n+1}{3}\right)\cdot\frac{n}{2} - (n+1) \qquad (4.3) \\ &\geqslant \frac{(n+d-1)n}{2} - (n+1). \end{aligned}$$

Using this estimate in combination with Lemma 4.1(b), we obtain:

$$\begin{aligned} u_1 \leqslant & q^{-N_1} \cdot \sum_{i=1}^{\lfloor d/2 \rfloor} q^{-(N_i - N_1)} \leqslant q^{-N_1}\left(1 + \sum_{i=2}^{\lfloor d/2 \rfloor} q^{-(d-3)}\right) \\ & \leqslant q^{-N_1}\left(1 + \left(\frac{d}{2} - 1\right) q^{3-d}\right) \leqslant q^{-\frac{(n+d-1)n}{2}+(n+1)}\left(1 + \left(\frac{d}{2} - 1\right) q^{3-d}\right). \end{aligned}$$

An elementary computation shows that for integers $d \geqslant 6$ and $q \geqslant 3$, the expression $\left(1 + \left(\frac{d}{2} - 1\right) q^{3-d}\right)$ is at most $\frac{29}{27}$. (This maximal value is attained when $q = 3$ and $d = 6$.) This completes the proof of part (a).

Similarly, when $q \geqslant 3$ and $d \geqslant 3$, the maximal value of the expression $\left(1 + \left(\frac{d}{2} - 1\right) q^{3-d}\right)$ is $\frac{3}{2}$. (This maximal value is attained when $q = 3$ and $d = 3$). This completes the proof of part (b). □

Lemma 4.3. *For each divisor* $e > 1$ *of* d*, set* $M_e := \binom{d+n}{n} - e \cdot \binom{d/e+n}{n}$*. Then*

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

for any $n \geqslant 2$*,* $q \geqslant 3$*,* $d \geqslant 3$*. Here* $e \mid d$*, where* $e > 1$*.*

Proof. 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 $S_1, S_2, \ldots, S_e$ 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 $1 \leqslant i < j \leqslant e$. Choose elements $a \in T_i$ and $b \in T_j$ and consider n-subsets of S 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 $1 \leqslant k \leqslant e$. 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 $1 \leqslant k \leqslant e$. Consequently,

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

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 in the conclusion of Lemma 4.3. □

We will also need the following lower bound for the integers M_e defined in Lemma 4.3.

Lemma 4.4. *If $n \geqslant 2$ and $d, q \geqslant 3$, then for each divisor $e > 1$ of d, we have:*

$$M_e \geqslant \frac{1}{4} \binom{n}{2} d^2 - d + 1. \tag{4.4}$$

Proof. The bound from (4.4) follows from Lemma 4.3 using that

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

since $d \geqslant e \geqslant 2$. □

Lemma 4.5. *Set $u_2 := \sum_{e \mid d, e > 1} q^{-M_e}$. If $n \geqslant 2$, $q \geqslant 3$, $d \geqslant 3$, then*

$$u_2 \leqslant (d-1) q^{-\frac{1}{4}\binom{n}{2} d^2 + d - 1}.$$

Proof. First, we note that the number of divisors e of d with $e > 1$ is at most $d-1$. Thus the sum the right hand side of $u_2 := \sum_{e|d, e>1} q^{-M_e}$ has at most $d-1$ terms. By Lemma 4.4, each term q^{-M_e} is at most $q^{-\frac{1}{4}\binom{n}{2}d^2+d-1}$. Lemma 4.5 now tells us that

$$u_2 \leqslant (d-1)q^{-\frac{1}{4}\binom{n}{2}d^2+d-1},$$

as desired. □

Finally, we set

$$v_1 := \frac{3}{2}\, q^{-\frac{(n+d-1)n}{2}+(n+1)} + (d-1)q^{-\frac{1}{4}\binom{n}{2}d^2+d-1}, \tag{4.5}$$

when $n \geqslant 3$, $q \geqslant 3$ and $d \geqslant 3$, and

$$v_2 := \frac{29}{27}\, q^{2-d} + (d-1)q^{-\frac{1}{4}d^2+d-1}, \tag{4.6}$$

when $n = 2$, $q \geqslant 3$ and $d \geqslant 6$. We will establish next upper bounds for v_2 and v_1 (in this order).

Lemma 4.6. *For $n = 2$, $q \geqslant 3$ and $d \geqslant 6$, we have $(d-1)qv_2 \leqslant 2$.*

Proof. Using (4.6), we write

$$(d-1)v_2 q = \Theta(q, d) := (d-1)\left(\frac{29}{27}q^{3-d} + (d-1)q^{-\frac{1}{4}d^2+d}\right).$$

For $d \geqslant 6$, both exponents in q^{3-d} and $q^{-\frac{1}{4}d^2+d}$ are negative. This yields $\Theta(q, d) \leqslant \Theta(3, d)$ for $q \geqslant 3$. We now view $\Theta(3, d)$ as a function of d, as d ranges over the interval $[6, \infty)$. On this interval $\Theta(3, d)$ achieves its maximum at $d = 6$. Thus, $(d-1)tq \leqslant \Theta(3, 6) \approx 1.125$. In particular, $(d-1)tq \leqslant 2$. □

Lemma 4.7. *Assume that $n \geqslant 3$, $q \geqslant 3$ and $d \geqslant 3$. Then $(d-1)v_1 q \leqslant 2$.*

Proof. We argue as in the proof of Lemma 4.6. For $n \geqslant 3$, the definition of v_1 from (4.5) implies

$$v_1 \leqslant 1.5q^{4-\frac{3}{2}(d+2)} + (d-1)q^{-\frac{3}{4}d^2+d-1}.$$

where we have substituted $n = 3$ in (4.5). Consequently,

$$(d-1)v_1 q \leqslant \Psi(q, d) := (d-1)\left(1.5q^{5-\frac{3}{2}(d+2)} + (d-1)q^{-\frac{3}{4}d^2+d}\right)$$

We have $\Psi(q, d) \leqslant \Psi(3, d)$ for $q \geqslant 3$. Viewing $\Psi(3, d)$ as a function of d and letting d range over the interval $[3, \infty)$, we see that $\Psi(3, d)$ achieves its maximum on this interval when $d = 3$. Thus, $(d-1)tq \leqslant \Psi(3, 3) \approx 0.257$. In particular, $(d-1)v_1 q \leqslant 2$, as desired. □

5. Proof of Proposition 3.2

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

$$t = t_1 + t_2 \tag{5.1}$$

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 5.1. *(a) Assume $n = 2$, $q \geqslant 3$ and $d \geqslant 6$. Then $t_1 \leqslant \dfrac{29}{27} q^{2-d}$.*

(b) Assume $n \geqslant 3$, $q \geqslant 3$, and $d \geqslant 3$. Then $t_1 \leqslant \dfrac{3}{2} q^{-\frac{n(n+d-1)}{2}+n+1}$.

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

$$t_1 \leqslant \sum_{i=1}^{\lfloor d/2 \rfloor} q^{-N_i}, \tag{5.2}$$

where $N_i = \binom{n+d}{d} - \binom{n+i}{n} - \binom{n+d-i}{n}$, as in (4.1). Parts (a) and (b) now follow from Lemma 4.2(a) and (b), respectively. (Note that the right hand side of the inequality (5.2) is denoted by u_1 in the statement of Lemma 4.2.) ☐

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

Lemma 5.2. *Let $n \geqslant 2$, $q \geqslant 3$, $d \geqslant 3$, we have $t_2 \leqslant (d-1) q^{-\frac{1}{4}\binom{n}{2}d^2+d-1}$.*

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

$$t_2 \leqslant \sum_{e \mid d, e>1} q^{-M_e} \tag{5.3}$$

where $M_e = \binom{d+n}{n} - e\binom{d/e+n}{n}$. The desired conclusion now follows from Lemma 4.5. (Note that the right hand side of the inequality (5.3) is denoted by u_2 in the statement of Lemma 4.5.) ☐

We are finally ready to finish the proof of Proposition 3.2.

Proof of Proposition 3.2. Writing $t = t_1 + t_2$, as in (5.1) and using Lemma 5.1 and Lemma 5.2, we obtain

$$t \leqslant \frac{3}{2} q^{-\frac{(n+d-1)n}{2}+(n+1)} + (d-1) q^{-\frac{1}{4}\binom{n}{2}d^2+d-1}$$

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

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

when $n = 2$, $q \geqslant 3$ and $d \geqslant 6$. Note that the right hand sides of these inequalities are precisely the quantities v_1 and v_2 from (4.5) and (4.6). The desired conclusion,

$$(d-1)rq \leqslant 2,$$

now follows from Lemmas 4.7 and 4.6, respectively. □

6. Conclusion of the proof of Theorem 1.1

The case when F is infinite is examined in Section 2. Thus we will assume that $F = \mathbb{F}_q$ and $E = \mathbb{F}_{q^m}$ are finite fields. The case where $q > d$ is handled in Proposition 3.1. Hence, from now on, we assume that $q \leqslant d$.

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 $q^{m-1} + ... + q + 1 = \dfrac{q^m - 1}{q-1}$, there are exactly $t\left(\dfrac{q^m-1}{q-1}\right)$ 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:

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

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

$$\begin{aligned}(1 + (d-1)t)q^{m(n-1)} + q^{m(n-2)} + ... + q^m + 1 \\ + (d-1)(d-2)q^{m(n-3/2)} + 5d^{13/3}q^{m(n-2)}.\end{aligned} \tag{6.1}$$

By Proposition 3.2, we have

$$(d-1)t \leqslant \frac{2}{q}, \tag{6.2}$$

for all $n \geqslant 3$, $d \geqslant 3$ and $q \geqslant 3$, or $n = 2$, $q \geqslant 3$ and $d \geqslant 6$. Since we already know that Theorem 1.1 holds when $q > d$ (see Proposition 3.1), we may assume that the inequality (6.2) 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 (6.1).

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

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

In order to verify this inequality, we first note that

$$q^{m(n-2)} + \cdots + q^m + 1 = \frac{q^{m(n-1)} - 1}{q^m - 1} < \frac{q^{m(n-1)}}{q^m - 1} < \frac{q^{m(n-1)}}{1000q}, \tag{6.3}$$

since $q \geqslant 3$ and $m \geqslant (d+2)(d+1)/2 \geqslant 10$ because $d \geqslant 3$. Employing (6.3), we see that the left-hand side of the inequality in the Claim is less than

$$(d-1)(d-2)q^{m(n-3/2)} + \frac{q^{m(n-1)-1}}{1000} + 5d^{13/3}q^{m(n-2)}. \tag{6.4}$$

Dividing the expression from (6.4) 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 $q \geqslant 3$ and $m \geqslant (d+2)(d+1)/2$, while $d \geqslant 3$. This completes the proof of the Claim.

Combining the Claim with the inequality (6.2), the quantity in (6.1) 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 $\#\mathcal{H}(\mathbb{F}_{q^m})$.

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

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

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

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

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

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

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

This last inequality $q^2 - 2q - 3 \geqslant 0$ is valid for all $q \geqslant 3$. Therefore, we have established Theorem 1.1 with $F = \mathbb{F}_q$ and $E = \mathbb{F}_{q^m}$, for all triples (n, q, d) with $n \geqslant 2$, $q \geqslant 3$, $d \geqslant 1$, 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 1.1 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 $P \in \mathbb{P}^2(\mathbb{F}_{q^m})$ such that P does not lie on any degree d hypersurface defined over $\mathbb{F}_q$. Here $m = \binom{n+d}{n}$.

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 $\mathbb{F}_5$. □

7. Proof of Theorem 1.3

We will first construct the linear systems $\mathcal{L}_{\mathrm{red}}$ and $\mathcal{L}_{\mathrm{irr}}$ in parts (a) and (c), then use them to prove parts (b) and (d). We will use the notation from the statement of Theorem 1.3 throughout this section: d and n are positive integers,

$$m := \binom{n+d}{n} \qquad \text{and} \qquad r := \binom{n+d-1}{n}.$$

(a) We take $\mathcal{L}_{\mathrm{red}}$ to be the linear system of hypersurfaces of degree d in $\mathbb{P}^n$ containing a fixed hyperplane H. Let us say, H is the hyperplane given by $x_0 = 0$. Then $\mathcal{L}_{\mathrm{red}}$ consists of polynomials of the form $x_0 F(x_0, x_1, \ldots, x_n)$, where $F(x_0, x_1, \ldots, x_n)$ is a polynomial of degree $d-1$ in $x_0, x_1, \ldots, x_n$. (Note that we are using the assumption that $d \geqslant 2$ to conclude that any polynomial of this form is reducible.) The dimension of $\mathcal{L}_{\mathrm{red}}$ is thus equal to the dimension of the linear system of homogeneous polynomials $F(x_1, \ldots, x_n)$ of degree $d-1$ in $x_1, \ldots, x_n$. In other words, $\dim(\mathcal{L}_{\mathrm{red}}) = r - 1$.

(c) We apply Theorem 1.1 for degree $d-1$ hypersurfaces in $\mathbb{P}^n$. Note that as we replace d by $d-1$ in Theorem 1.1, m gets replaced by r. We obtain a point $P \in \mathbb{P}^n(\mathbb{F}_{q^r})$ 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 $S = \{P_1, \cdots, P_r\}$ be the orbit of P under $\mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$, where $P_1 = P$. 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 $\dim V_S \geqslant m - r$. Pick linearly independent forms $f_0, f_1, ..., f_{m-1-r} \in V_S$ and consider the $(m-1-r)$-dimensional linear system $\mathcal{L}_{\mathrm{irr}} = \langle f_0, f_1, ..., f_{m-1-r} \rangle$ of degree d hypersurfaces.

It remains to show that each $\mathbb{F}_q$-member of $\mathcal{L}_{\mathrm{irr}}$ is irreducible over $\mathbb{F}_q$. Indeed, assume the contrary: we factor f as $f = g \cdot h$, where $g, h \in \mathbb{F}_q[x_0, \ldots, x_n]$ are homogeneous polynomials of degree at most $d-1$. Since $f(P) = 0$, we have $g(P) = 0$ or $h(P) = 0$. This leads to a contradiction, because P does not lie on a hypersurface in $\mathbb{P}^n$ of degree at most $d-1$ defined over $\mathbb{F}_q$. Thus, every $\mathbb{F}_q$-member of $\mathcal{L}_{\mathrm{irr}}$ is irreducible over $\mathbb{F}_q$.

(b) Suppose $\mathcal{L}$ is a linear system of hypersurfaces of degree d in $\mathbb{P}^n$ of dimension r. Then $\mathcal{L}$ and $\mathcal{L}_{\mathrm{irr}}$ intersect non-trivially in $\mathbb{P}^{m-1}$. An $\mathbb{F}_q$-member of $\mathcal{L}$ corresponding to the $\mathbb{F}_q$-point of intersection is irreducible over $\mathbb{F}_q$.

(d) Similarly, if $\mathcal{L}$ is a linear system of hypersurfaces of degree d in $\mathbb{P}^n$ of dimension $\geqslant m - r$, then $\mathcal{L}$ and $\mathcal{L}_{\mathrm{red}}$ intersect non-trivially in $\mathbb{P}^{m-1}$. An $\mathbb{F}_q$-member of $\mathcal{L}$ corresponding to an $\mathbb{F}_q$-point of intersection is reducible over $\mathbb{F}_q$. □

8. A variant of Theorem 1.3 over an algebraically closed field

In this section we prove a variant of Theorem 1.3, where the finite field $\mathbb{F}_q$ is replaced by an algebraically closed field F. As we mentioned in the Introduction, parts (a) and (b) of Theorem 1.3 remain valid in this setting, whereas the dimensions in parts (c) and (d) get reduced by n.

Proposition 8.1. *Let $n, d \geqslant 2$ be integers, $m = \binom{n+d}{n}$, $r = \binom{n+d-1}{n}$, and F be an algebraically closed field.*

(a) There exists an $(r-1)$-dimensional F-linear system $\mathcal{M}_{\rm red}$ of degree d hypersurfaces in $\mathbb{P}^n$ such that every F-member of $\mathcal{L}_{\rm red}$ is reducible over F.

(b) Every F-linear system $\mathcal{L}$ of dimension $\geqslant r$ has an F-member which is irreducible over F.

(c) There exists an $(m-r-n-1)$-dimensional F-linear system $\mathcal{L}_{\rm irr}$ of degree d hypersurfaces in $\mathbb{P}^n$ such that every F-member of $\mathcal{L}_{\rm irr}$ is irreducible.

(d) Let $\mathcal{L}$ be an F-linear system of degree d hypersurfaces in $\mathbb{P}^n$. If $\dim(\mathcal{L}) \geqslant m-r-n$, then $\mathcal{L}$ has a reducible F-member.

Proof. (a) The construction of $\mathcal{L}_{\rm red}$ in the proof of Theorem 1.3(a) goes through over an arbitrary field.

(b) Let $\mathcal{L} = \langle f_0, \ldots, f_t \rangle$ of degree d hypersurfaces in $\mathbb{P}^n$ defined over F, Let

$$f_\lambda(x_0, \ldots, x_n) = \lambda_0 f_0 + \ldots + \lambda_t f_t$$

be the member of this system corresponding to $\lambda = (\lambda_0 : \ldots : \lambda_t) \in \mathbb{P}^t$. Assume that every F-element of $\mathcal{L}$ is reducible, that is, f_λ is a reducible polynomial in $F[x_0, \ldots, x_n]$ for every F-point $\lambda = (\lambda_0 : \ldots : \lambda_t) \in \mathbb{P}^t(F)$. Our goal is to show that $\dim(\mathcal{L}) \leqslant r-1$. Let us consider two cases.

Case 1: The generic member of $\mathcal{L}$ is irreducible. Here by the generic member we mean the member coresponding to the generic point of $\mathbb{P}^t$. Equivalently, f_λ is irreducible as a polynomial in $x_0, \ldots, x_n$ over the field $F(\lambda_0, \ldots, \lambda_t)$.

A description of the polynomials f_λ that may occur in this case can be found in Schinzel's book [Sch00, Chapter 3, Theorem 37]. It follows from this description that if $\mathrm{char}(F)$ does not divide d, then the maximal dimension of $\mathcal{L}$ is d, and is achieved by the linear system $\langle x_1^d, x_1^{d-1}x_2, x_1^{d-2}x_2^2, \ldots, x_2^d \rangle$. On the other hand, if $\mathrm{char}(F)$ divides d, then the maximal dimension of $\mathcal{L}$ is either d, attained in the same way as above) or $\binom{n+d/p}{n} - 1$. The latter is achieved by the linear system spanned by all monomials of the form $x_0^{p\,i_0} x_1^{p\,i_1} \cdots x_n^{p\,i_n}$ with $i_0 + \ldots + i_n = d/p$.

It remains to show that (i) $d \leqslant r-1$ and (ii) if $p \geqslant 2$ divides d, then $\binom{n+d/p}{n} \leqslant r$. By Pascal's identity, for a fixed d, $\binom{n+d-1}{n}$ increases with n. In particular, since $n \geqslant 2$, we have

$$\frac{(d+1)d}{2} = \binom{2+d-1}{2} \leqslant \binom{n+d-1}{n} = r.$$

Since $d \geqslant 2$, this yields $d = (d+1) - 1 \leqslant \frac{(d+1)d}{2} - 1 \leqslant r - 1$, proving (i). To prove (ii), note that $d/p \leqslant d - 1$. Thus

$$\binom{n + d/p}{n} \leqslant \binom{n+d-1}{n} = r,$$

as desired.

Case 2: The generic member of $\mathcal{L}$ is reducible. Equivalently, f_λ is reducible as a polynomial in $x_0, \ldots, x_n$ over $F(\lambda_0, \ldots, \lambda_t)$. Using Gauss' Lemma, and the fact that f_λ is homogeneous of degree 1 in $\lambda_0, \ldots, \lambda_t$, we see that

$$f_\lambda(x_0, \ldots, x_n) = g(x_0, ..., x_n) \cdot h_\lambda(x_0, ..., x_n),$$

where $g \in F[x_0, \ldots, x_n]$ is a homogeneous polynomial of degree d_1, $h_\lambda = \lambda_0 h_0 + \ldots + \lambda_t h_t$ for some homogeneous polynomials $h_0, \ldots, h_t \in F[x_0, \ldots, x_n]$ of degree $d_2 \geqslant 1$ and $d_1 + d_2 = d$. Here $h_0, \ldots, h_t$ are linearly independent over F. Thus

$$\dim(\mathcal{L}) = t \leqslant \binom{n+d_2}{n} - 1 \leqslant \binom{n+d-1}{n} - 1 = r - 1.$$

This completes the proof of part (b).

To prove (c) and (d), let $\mathcal{R}$ be the locus of reducible hypersurfaces inside the parameter space $\mathbb{P}^{m-1}$ of all degree d hypersurfaces in $\mathbb{P}^n$. Denote the dimension of $\mathcal{R}$ by s. Then every linear subspace of (projective) dimension $\geqslant m - 1 - s$ intersects $\mathcal{R}$ in $\mathbb{P}^{m-1}$; on the other hand, a linear subspace of (projective) dimension $< m - 1 - s$ in general position will *not* meet $\mathcal{R}$ in $\mathbb{P}^{m-1}$. Since F is algebraically closed, a nonempty intersection always has an F-point. In other words, the following are equivalent:

- every linear system of (projective) dimension t has a reducible F-member, and
- $t \geqslant m - 1 - s$.

It remains to show that

$$s = r + n - 1; \tag{8.1}$$

this immediately implies both (c) and (d). To prove (8.1), note that $\mathcal{R} = \bigcup_{i=1}^{\lfloor d/2 \rfloor} \mathcal{R}_i$, where $\mathcal{R}_i$ consists of reducible hypersurfaces $F(x_0, \ldots, x_n) = 0$, where $F = F_1 \cdot F_2 = 0$ and F_1, F_2 are homogeneous polynomials in $x_0, x_1, \ldots, x_n$ of degree i and $d - i$, respectively. In other words, $\mathcal{R}_i$ is the image of the map $\mathbb{P}^{m_1 - 1} \times \mathbb{P}^{m_2 - 1} \to \mathbb{P}^{m-1}$ given by $(F_1, F_2) \to F_1 \cdot F_2$ where $m_1 = \binom{n+i}{n}$, $m_2 = \binom{n+d-i}{n}$. It is easy to see that

$$\dim(\mathcal{R}_i) = \binom{n+i}{n} + \binom{n+d-i}{n} - 2.$$

The difference $\dim(\mathcal{R}_i) - \dim(\mathcal{R}_{i+1})$ is exactly the quantity $N_{i+1} - N_i$ we considered at the beginning of Section 4; see (4.1). By Lemma 4.1(a), $N_{i+1} - N_i \geqslant 0$ whenever $2(i+1) \leqslant d$. We conclude that $\dim(\mathcal{R}_i)$ assumes its maximal value when $i = 1$. In other words,

$$s = \dim(\mathcal{R}) = \dim(\mathcal{R}_1) = \binom{n+1}{n} + \binom{n+d-1}{n} - 2 = \binom{n+d-1}{n} + n - 1 = r + n - 1,$$

as claimed. □

Remark 8.2. Note that the assumption that $d \geqslant 2$ in Theorem 1.3 and Proposition 8.1 is harmless, since every hypersurface of degree 1 in $\mathbb{P}^n$ is irreducible. Moreover, over an algebraically closed field, every hypersurface of degree $d \geqslant 2$ in $\mathbb{P}^1$ is reducible. Thus the assumption that $n \geqslant 2$ in the statement of Proposition 8.1 is harmless as well.

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.

[AGY23] Shamil Asgarli, Dragos Ghioca, and Chi Hoi Yip, *Existence of pencils with nonblocking hypersurfaces*, Finite Fields Appl. **92** (2023), Paper No. 102283, 11.

[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* $\mathrm{P}^m(\mathbf{F}_q)$, J. Pure Appl. Algebra **124** (1998), no. 1-3, 227–240.

[LW54] S. Lang and A. Weil, *Number of points of varieties in finite fields*, Amer. J. Math. **76** (1954), 819–827.

[Poo04] Bjorn Poonen, *Bertini theorems over finite fields*, Ann. of Math. (2) **160** (2004), no. 3, 1099–1127.

[Sch00] Andrzej Schinzel, *Polynomials with special regard to reducibility*, Encyclopedia of Mathematics and its Applications, vol. 77, Cambridge University Press, Cambridge, 2000. With an appendix by Umberto Zannier.

[Ser91] Jean-Pierre Serre, *Lettre à M. Tsfasman*, 1991, pp. 11, 351–353 (1992). Journées Arithmétiques, 1989 (Luminy, 1989).

[Sha94] Igor R. Shafarevich, *Basic algebraic geometry. 1*, Second, Springer-Verlag, Berlin, 1994. Varieties in projective space, Translated from the 1988 Russian edition and with notes by Miles Reid.

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