



Vanishing Ideals of Projective Spaces over Finite Fields and a Projective Footprint Bound

Beelen, Peter; Datta, Mrinmoy; Ghorpade, Sudhir R.

Published in:

Acta Mathematica Sinica, English Series

Link to article, DOI:

[10.1007/s10114-018-8024-7](https://doi.org/10.1007/s10114-018-8024-7)

Publication date:

2019

Document Version

Peer reviewed version

[Link back to DTU Orbit](#)

Citation (APA):

Beelen, P., Datta, M., & Ghorpade, S. R. (2019). Vanishing Ideals of Projective Spaces over Finite Fields and a Projective Footprint Bound. *Acta Mathematica Sinica, English Series*, 35(1), 47-63.
<https://doi.org/10.1007/s10114-018-8024-7>

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Vanishing Ideals of Projective Spaces over Finite Fields and a Projective Footprint Bound

Peter BEELEN

*Department of Applied Mathematics and Computer Science, Technical University of Denmark,
DK 2800, Kgs. Lyngby, Denmark
E-mail: pabe@dtu.dk*

Mrinmoy DATTA

*Department of Applied Mathematics and Computer Science, Technical University of Denmark,
DK 2800, Kgs. Lyngby, Denmark
Current address: Department of Mathematics and Statistics,
UiT-The Arctic University of Norway, N-9037, Tromsø, Norway
E-mail: mrinmoy.dat@gmail.com*

Sudhir R. GHORPADE

*Department of Mathematics, Indian Institute of Technology Bombay, Powai, Mumbai 400076, India
E-mail: srg@math.iitb.ac.in*

Abstract We consider the vanishing ideal of a projective space over a finite field. An explicit set of generators for this ideal has been given by Mercier and Rolland. We show that these generators form a universal Gröbner basis of the ideal. Further we give a projective analogue for the so-called footprint bound, and a version of it that is suitable for estimating the number of rational points of projective algebraic varieties over finite fields. An application to Serre's inequality for the number of points of projective hypersurfaces over finite fields is included.

Keywords Finite field, projective space, algebraic variety, vanishing ideal, Gröbner basis, footprint bound, projective hypersurface

MR(2010) Subject Classification 14G15, 13P10, 11T06, 11G25, 14G05

1 Introduction

Let \mathbb{F}_q be the finite field with q elements and let $\overline{\mathbb{F}}_q$ denote an algebraic closure of \mathbb{F}_q . We are primarily interested in the problem of determining or estimating the number of \mathbb{F}_q -rational points of an affine or projective variety \mathcal{X} defined over \mathbb{F}_q . When \mathcal{X} is known to be irreducible (over $\overline{\mathbb{F}}_q$) and better still, nonsingular, then there are good estimates that arise from deeper methods in algebraic geometry, including the known validity of the Weil conjectures and related

Received January 29, 2018, accepted June 29, 2018

Peter Beelen was supported by the Danish Council for Independent Research (Grant No. DFF-4002-00367). Mrinmoy Datta was supported by the Danish Council for Independent Research (Grant No. DFF-6108-00362), and he is currently supported by the Research Council of Norway (Project No. 280731). Sudhir Ghorpade is partially supported by IRCC Award grant 12IRAWD009 from IIT Bombay

results such as the Grothendieck–Lefschetz trace formula. These estimates typically involve topological data such as the genus (when \mathcal{X} is a smooth projective curve) or more generally, the ℓ -adic Betti numbers. The estimates are particularly good when \mathcal{X} is a complete intersection. Simplest among such general estimates is the Lang–Weil inequality, which still requires \mathcal{X} to be (absolutely) irreducible with a given embedding in a projective space, and the knowledge of the dimension and degree of \mathcal{X} . One may refer to [15] for a brief survey of these aspects.

What if \mathcal{X} is not necessarily irreducible? A reducible d -dimensional algebraic variety can have many more \mathbb{F}_q -rational points than any irreducible d -dimensional algebraic variety, and the geometric estimates such as those mentioned above are not immediately applicable. A recent result of Couvreur [8] does provide a way out, but still it requires the knowledge of dimensions as well as degrees of the irreducible components. A more elementary approach that relies on simpler attributes of varieties such as the number of defining equations and their degrees may be desirable for practical applications. The simplest among such results is the bound due to Ore (1933) for the number of \mathbb{F}_q -rational points of affine hypersurfaces of degree d defined over \mathbb{F}_q . It states that if $\mathcal{Z} = Z(f)$ is the zero-set in $\mathbb{A}^m(\overline{\mathbb{F}}_q)$ of a nonzero polynomial $f \in \mathbb{F}_q[x_1, \dots, x_m]$ of degree $\leq d$, then

$$|\mathcal{Z}(\mathbb{F}_q)| \leq dq^{m-1}.$$

The bound dq^{m-1} is a good bound in the sense that it is attained when $d \leq q$. An analogous good bound for projective hypersurfaces was conjectured by Tsfasman and proved by Serre [22] and, independently, Sørensen [23] in 1991. It states that if $\mathcal{X} = V(F)$ is the zero-set in $\mathbb{P}^m(\overline{\mathbb{F}}_q)$ of a homogeneous polynomial $F \in \mathbb{F}_q[x_0, x_1, \dots, x_m]$ of degree d , then

$$|\mathcal{X}(\mathbb{F}_q)| \leq dq^{m-1} + p_{m-2}, \quad (1)$$

where for $j \in \mathbb{Z}$, by p_j we denote $|\mathbb{P}^j(\mathbb{F}_q)|$, i.e., $p_j := q^j + q^{j-1} + \dots + q + 1$ if $j \geq 0$, while we set $p_j := 0$ if $j < 0$.

In the case of affine algebraic varieties, say $\mathcal{Z} = Z(f_1, \dots, f_r)$ in $\mathbb{A}^m(\overline{\mathbb{F}}_q)$, where $f_1, \dots, f_r \in \mathbb{F}_q[x_1, \dots, x_m]$, there is an attractive alternative for determining or estimating the number of \mathbb{F}_q -rational points of \mathcal{Z} . Namely, instead of the high dimensional variety \mathcal{Z} , we consider the zero-dimensional variety $\mathcal{Z}_q = Z(f_1, \dots, f_r, x_1^q - x_1, \dots, x_m^q - x_m)$ in $\mathbb{A}^m(\overline{\mathbb{F}}_q)$ and observe that $|\mathcal{Z}(\mathbb{F}_q)| = |\mathcal{Z}_q|$. In algebraic terms (and using the superscript “ a ” to indicate the affine setting), instead of the ideal $I^a = \langle f_1, \dots, f_r \rangle$ of the polynomial ring $\overline{\mathbb{F}}_q[x_1, \dots, x_m]$, we consider the larger ideal $I_q^a := I^a + \Gamma_q^a$, where $\Gamma_q^a := \langle x_1^q - x_1, \dots, x_m^q - x_m \rangle$ is the vanishing ideal of $\mathbb{A}^m(\mathbb{F}_q)$. Now it is a general fact that if k is an arbitrary algebraically closed field and J^a is an ideal of $k[x_1, \dots, x_m]$ whose zero-set $Z(J^a)$ in $\mathbb{A}^m(k)$ is finite, then

$$|Z(J^a)| \leq |\Delta(J^a)| \quad \text{with equality if } J^a \text{ is a radical ideal}, \quad (2)$$

where $\Delta(J^a)$ is the *footprint* of J^a , defined (with respect to a fixed monomial order on the set \mathbb{M}^a of all monomials in x_1, \dots, x_m) by

$$\Delta(J^a) := \{\mu \in \mathbb{M}^a : \mu \neq \text{lm}(f) \text{ for any } f \in J^a \text{ with } f \neq 0\},$$

where for any nonzero polynomial $f \in k[x_1, \dots, x_m]$, by $\text{lm}(f)$ we denote the *leading monomial* of f (with respect to the fixed monomial order). It is customary to refer to (2) as the *footprint bound*. A proof of (2), can be found, e.g., in [1, Thm. 8.32].

In case a Gröbner basis of J^a , say $\{f_1, \dots, f_s\}$, can be found, then clearly, $\Delta(J^a) = \{\mu \in \mathbb{M}^a : \text{lm}(f_i) \nmid \mu \text{ for } i = 1, \dots, s\}$. What makes the case of $k = \overline{\mathbb{F}}_q$ and $J^a = I_q^a = I^a + \Gamma_q^a$ particularly nice is that the usual generators $x_1^q - x_1, \dots, x_m^q - x_m$ form a Gröbner basis of Γ_q^a (since their leading monomials are pairwise coprime; see, e.g., [7, Ch. 2, Section 9]), and regardless of what the ideal I^a is, I_q^a is always a radical ideal, (and, in fact, the vanishing ideal of $Z(I^a)(\mathbb{F}_q)$), thanks to a classical result of Terjanian [24]. Thus, in this case (2) specializes to the \mathbb{F}_q -footprint formula:

$$|\mathcal{Z}(\mathbb{F}_q)| = |\Delta(I_q^a)|, \quad \text{where } \mathcal{Z} := Z(I^a). \quad (3)$$

In practice, it is more convenient to consider the well-known notion of the reduction \overline{f} of a nonzero polynomial $f \in \overline{\mathbb{F}}_q[x_1, \dots, x_m]$ (see, e.g., [20, Ch. 2] or [2, Section II]) and observe that $\Delta(I_q^a) = \overline{\Delta}(I^a)$, where for any subset T^a of $\overline{\mathbb{F}}_q[x_1, \dots, x_m]$, we define

$$\overline{\Delta}(T^a) := \{\mu \in \mathbb{M}^a : \mu = \overline{\mu} \text{ and } \text{lm}(\overline{f}) \nmid \mu \text{ for all } f \in T^a \text{ with } \overline{f} \neq 0\}.$$

In particular, if $\{f_1, \dots, f_r\}$ is any set of generators of I^a , then

$$|\mathcal{Z}(\mathbb{F}_q)| \leq |\overline{\Delta}(f_1, \dots, f_r)|, \quad \text{where } \mathcal{Z} := Z(I^a) = Z(f_1, \dots, f_r). \quad (4)$$

We shall refer to (4) as the *affine \mathbb{F}_q -footprint bound*. Some early references for footprint bounds such as these, and especially their applications to coding theory, are the works of Høholdt [19], Fitzgerald and Lax [11], and Geil and Høholdt [12].

One of the most general estimates known for the number of \mathbb{F}_q -rational points of affine algebraic varieties defined over \mathbb{F}_q is a result of Pellikaan [18] that gives, in fact, the maximum possible value $e_r^A(d, m)$ of $|\mathcal{Z}(\mathbb{F}_q)|$, where $\mathcal{Z} = Z(f_1, \dots, f_r)$ and $\{f_1, \dots, f_r\}$ vary over sets of r linearly independent polynomials of degree $\leq d$ in $\mathbb{F}_q[x_1, \dots, x_m]$. Recent works such as [13] and [3] have shown that it is possible to derive results like these, and even more general results, by a careful study of footprints and shadows¹⁾, together with some nontrivial combinatorial results such as the Kruskal–Katona theorem and its variants. On the other hand, the corresponding projective problem of the determination of the maximum number $e_r(d, m)$ of $|\mathcal{X}(\mathbb{F}_q)|$, where $\mathcal{X} = V(F_1, \dots, F_r)$ and $\{F_1, \dots, F_r\}$ vary over sets of r linearly independent homogeneous polynomials of degree d in $\mathbb{F}_q[x_0, x_1, \dots, x_m]$ is still open, in general, although there has been some recent progress (see, e.g., [4, 9, 10]).

Motivated by the above considerations, we begin in this paper the investigation of the \mathbb{F}_q -rational points of projective varieties $\mathcal{X} = V(\mathcal{I})$ by associating to \mathcal{X} a zero-dimensional variety \mathcal{X}_q and developing suitable analogues of the footprint bound. The first question to be asked is an explicit determination of the ideal $\Gamma_q = I(\mathbb{P}^m(\mathbb{F}_q))$ and its Gröbner basis. The first part is answered by Mercier and Rolland [21], where it is shown that the homogeneous polynomials $x_i^q x_j - x_i x_j^q$, for $0 \leq i < j \leq m$, generate Γ_q . We supplement this by showing that the above generators themselves form a universal Gröbner basis of Γ_q . More importantly, we systematically develop a useful notion of projective reduction (for monomials, and more generally, polynomials), that provides canonical representatives for the cosets in $\overline{\mathbb{F}}_q[x_0, \dots, x_m]/\Gamma_q$. A projective analogue of the footprint bound (2) is easily obtained using the theory of Hilbert functions. However, unlike in the affine case, the ideal $\mathcal{I}_q := \mathcal{I} + \Gamma_q$ of $\overline{\mathbb{F}}_q[x_0, x_1, \dots, x_m]$ need

1) The notion of shadow is complementary to that of footprint.

not be a radical ideal even if \mathcal{I} is a radical ideal. Nonetheless, we prove a projective analogue of the \mathbb{F}_q -footprint formula (3) using a classical result of Macaulay. This is then used to derive a *projective \mathbb{F}_q -footprint bound* analogous to (4), and, as an application, we deduce Serre's inequality (1) from it. In a forthcoming work [5], it will be shown how the basic results in this paper can be combined with techniques from extremal combinatorics to obtain newer results concerning the determination of $e_r(d, m)$.

After this work was completed, we became aware of the works of Carvalho, Neumann and Lopez [6] and of González-Sarabia et al. [16]. In [6], the so-called projective nested cartesian codes are studied, and they obtain a Gröbner basis for the vanishing ideal of the set X of points in $\mathbb{P}^m(\mathbb{F}_q)$ having homogeneous coordinates in $A_0 \times \cdots \times A_m$, where A_0, \dots, A_m are subsets of \mathbb{F}_q satisfying a certain "nested condition". The case $A_0 = \cdots = A_m = \mathbb{F}_q$ corresponds to $X = \mathbb{P}^m(\mathbb{F}_q)$ that we consider here. Moreover, they determine the minimum distance of the corresponding codes, which amounts to a generalization of Serre's inequality shown here as an illustration of projective \mathbb{F}_q -footprint bound. However, they restrict to graded lexicographic order, and the methods are different. In [16], the so-called generalized minimum distance functions are studied and their Lemma 3.4 is related to our projective \mathbb{F}_q -footprint formula (Theorem 3.7 of this paper). Again, the formulation and methods of proof are quite different.

2 Projective Reduction and Fermat Polynomials

Let q be a prime power and let m be a positive integer (which are kept fixed throughout the paper). It is well known that an algebraic closure $\overline{\mathbb{F}}_q$ of the finite field \mathbb{F}_q with q elements is explicitly given by $\bigcup_{j \geq 1} \mathbb{F}_{q^j}$ and thus we will assume that algebraic field extensions of \mathbb{F}_q are subfields of this algebraic closure. Let x_0, x_1, \dots, x_m be independent indeterminates over $\overline{\mathbb{F}}_q$, and let

$$\mathbb{M} := \text{the set of all monomials in } x_0, x_1, \dots, x_m.$$

Moreover, for any nonnegative integer e , let

$$\mathbb{M}_e := \{\mu \in \mathbb{M} : \deg \mu = e\}.$$

For a monomial $\mu = x_0^{a_0} \cdots x_m^{a_m}$ in \mathbb{M} , we let $\text{supp}(\mu) := \{i \in \{0, 1, \dots, m\} : a_i > 0\}$.

2.1 Projective Reduction

The projective analogue of the classical notion of reduction of a polynomial that was alluded to in Introduction is the following.

Definition 2.1 *Let $\mu \in \mathbb{M}$. If $\mu = 1$, then we define $\overline{\mu} := 1$. If $\mu \neq 1$, then there is a unique $\ell \in \mathbb{Z}$ with $0 \leq \ell \leq m$ such that $\mu = x_0^{a_0} \cdots x_\ell^{a_\ell}$ for some nonnegative integers a_0, \dots, a_ℓ with $a_\ell > 0$. For $0 \leq i \leq \ell - 1$, let $\overline{a}_i \in \{0, 1, \dots, q - 1\}$ be the unique integer such that $\overline{a}_i = a_i$ if $0 \leq a_i \leq q - 1$, while $\overline{a}_i \equiv a_i \pmod{q - 1}$ and $1 \leq \overline{a}_i \leq q - 1$ if $a_i \geq q$. We then define*

$$\overline{\mu} := x_0^{\overline{a}_0} \cdots x_{\ell-1}^{\overline{a}_{\ell-1}} x_\ell^{a_\ell + \sum_{i=0}^{\ell-1} a_i - \overline{a}_i}.$$

It is clear that the monomial $\overline{\mu}$ is uniquely determined by μ . We let

$$\overline{\mathbb{M}} := \{\mu \in \mathbb{M} : \overline{\mu} = \mu\} \quad \text{and for any } e \geq 0, \quad \overline{\mathbb{M}}_e := \{\mu \in \overline{\mathbb{M}} : \deg \mu = e\}.$$

The map $\mu \mapsto \bar{\mu}$ of $\mathbb{M} \rightarrow \overline{\mathbb{M}}$ extends by linearity to polynomials. More precisely, if k is an algebraic field extension of \mathbb{F}_q and $f \in k[x_0, \dots, x_m]$, then there are unique nonzero scalars $c_1, \dots, c_N \in k$ and distinct monomials $\mu_1, \dots, \mu_N \in \mathbb{M}$ such that

$$f = c_1\mu_1 + \dots + c_N\mu_N \quad \text{and we define} \quad \bar{f} := c_1\bar{\mu}_1 + \dots + c_N\bar{\mu}_N.$$

Note that \bar{f} is uniquely determined by f . Moreover, using the empty sum convention, if f is the zero polynomial, then so is \bar{f} . We call \bar{f} the projective reduction of f . We say that f is projectively reduced if $\bar{f} = f$. Two polynomials in $k[x_0, x_1, \dots, x_m]$ are said to be projectively equivalent if they have the same projective reduction.

Some elementary properties of projective reduction are summarized below.

Proposition 2.2 *Let k be an algebraic field extension of \mathbb{F}_q .*

(i) *The map $f \mapsto \bar{f}$ of $k[x_0, \dots, x_m] \rightarrow k[x_0, \dots, x_m]$ is a k -linear homomorphism (of vector spaces) and it maps homogeneous polynomials of degree e to homogeneous polynomials of degree e , where e is any nonnegative integer.*

(ii) *The map in (i) is idempotent, i.e., $\overline{\bar{f}} = \bar{f}$ for all $f \in k[x_0, \dots, x_m]$.*

(iii) *$\overline{fg} = \bar{f}\bar{g}$ for all $f, g \in k[x_0, \dots, x_m]$.*

Proof Both (i) and (ii) are obvious from the definition once we note that $\deg \bar{\mu} = \deg \mu$ and $\overline{\bar{\mu}} = \bar{\mu}$ for all $\mu \in \mathbb{M}$. Moreover, (iii) follows from k -linearity once we verify directly that $\overline{\mu\nu} = \bar{\mu}\bar{\nu}$ for any $\mu, \nu \in \mathbb{M}$. \square

Let us define $\overline{\mathbb{M}}^{(0)} := \{x_0^a : a \geq 0\}$ and for $1 \leq \ell \leq m$,

$$\overline{\mathbb{M}}^{(\ell)} := \{x_0^{a_0} \cdots x_\ell^{a_\ell} : 0 \leq a_i < q \text{ for } 0 \leq i < \ell \text{ and } a_\ell > 0\}.$$

Then for any nonnegative integer e , we have the disjoint union decompositions:

$$\overline{\mathbb{M}} = \coprod_{\ell=0}^m \overline{\mathbb{M}}^{(\ell)} \quad \text{and} \quad \overline{\mathbb{M}}_e = \coprod_{\ell=0}^m \overline{\mathbb{M}}_e^{(\ell)}, \quad \text{where } \overline{\mathbb{M}}_e^{(\ell)} := \overline{\mathbb{M}}^{(\ell)} \cap \overline{\mathbb{M}}_e. \quad (5)$$

It is not difficult to obtain a general formula for the cardinality of $\overline{\mathbb{M}}_e$ for any $e \geq 0$, but this will not concern us here. For now on, we note that if $e \geq m(q-1) + 1$, then for $0 \leq \ell \leq m$, the elements of $\overline{\mathbb{M}}_e^{(\ell)}$ are precisely the monomials of the form $x_0^{a_0} \cdots x_{\ell-1}^{a_{\ell-1}} x_\ell^{e-a_0-\dots-a_{\ell-1}}$, where $a_0, \dots, a_{\ell-1}$ vary arbitrarily in $\{0, 1, \dots, q-1\}$ and the exponent of x_ℓ is > 0 due to the condition on e . Hence

$$|\overline{\mathbb{M}}_e^{(\ell)}| = q^\ell \quad \text{and consequently,} \quad |\overline{\mathbb{M}}_e| = \sum_{\ell=0}^m q^\ell = p_m \quad \text{for all } e \geq m(q-1) + 1.$$

2.2 Fermat Polynomials and the Division Algorithm

Define

$$\Phi_{ij} := x_i^q x_j - x_i x_j^q \quad \text{for } 0 \leq i < j \leq m.$$

Following [10], we call these the *Fermat polynomials*. We shall denote by Φ the ordered $\binom{m+1}{2}$ -tuple $(\Phi_{00}, \Phi_{01}, \dots, \Phi_{0m}, \Phi_{12}, \dots, \Phi_{m-1,m})$. Suppose k is an algebraic field extension of \mathbb{F}_q . The ideal of $k[x_0, \dots, x_m]$ generated by $\{\Phi_{ij} : 0 \leq i < j \leq m\}$ will be denoted by $\Gamma_q(k)$. Let us fix a monomial order \succ on the set \mathbb{M} of all monomials in x_0, \dots, x_m in such a way that

$$x_0 \succ x_1 \succ \dots \succ x_m.$$

For $0 \neq f \in \overline{\mathbb{F}}_q[x_0, \dots, x_m]$, we denote by $\text{lm}(f)$ the *leading monomial* of f , i.e., the largest monomial (with respect to \preceq) appearing in f with a nonzero coefficient. For example, $\text{lm}(\Phi_{ij}) = x_i^q x_j$ for $0 \leq i < j \leq m$. Given any $I \subseteq k[x_0, \dots, x_m]$, we will denote by $\text{LT}(I)$ the ideal of $k[x_0, \dots, x_m]$ generated by $\{\text{lm}(f) : f \in I \text{ with } f \neq 0\}$. This may be referred to as the *leading term ideal* of I (with respect to \preceq). Let us recall that if $\phi = (\phi_1, \dots, \phi_s)$ is an ordered s -tuple of nonzero polynomials in $k[x_0, \dots, x_m]$, then any $f \in k[x_0, \dots, x_m]$ can be written as $f = f_1 \phi_1 + \dots + f_s \phi_s + g$ for some $f_1, \dots, f_s, g \in k[x_0, \dots, x_m]$ such that no monomial appearing in g with a nonzero coefficient is divisible by any of $\text{lm}(\phi_1), \dots, \text{lm}(\phi_s)$. Here g is uniquely determined by f and the ordered tuple ϕ . We call g the *remainder* of f upon division by ϕ , and we write $f \rightarrow_\phi g$ to indicate this. Note that one arrives at g and f_1, \dots, f_s by a specific *division algorithm* that is guaranteed to terminate in a finite number of steps, and thus we can and will speak of the first step of this algorithm for division of f by ϕ ([7, Ch. 2]).

Here is a connection between Fermat polynomials and projective reduction.

Proposition 2.3 *Let $\mu \in \mathbb{M}$. Then $\mu \rightarrow_\Phi \overline{\mu}$. Two monomials in \mathbb{M} have the same remainder upon division by Φ if and only if they are projectively equivalent.*

Proof If $\mu = 1$, then $\overline{\mu} = 1$ and clearly $\mu \rightarrow_\Phi \overline{\mu}$. Suppose $\mu = x_0^{a_0} \dots x_\ell^{a_\ell}$ for some nonnegative integers a_0, \dots, a_ℓ with $a_\ell > 0$. We define the *weight* of μ as follows.

$$\text{wt}(\mu) = \sum_{i=0}^{\ell-1} (a_i - \overline{a}_i) q^{m-i}, \quad \text{where } \overline{a}_i \text{ are as in Definition 2.1.}$$

Note that $\text{wt}(\mu) \geq 0$. Moreover, $\text{wt}(\mu) = 0$ if and only if μ is projectively reduced.

Claim 1 $\mu \rightarrow_\Phi \nu$ for some projectively reduced monomial $\nu \in \overline{\mathbb{M}}$.

We prove the claim by induction on $\text{wt}(\mu)$. First, suppose $\text{wt}(\mu) = 0$, i.e., $\mu = \overline{\mu}$. Then $0 \leq a_i \leq q-1$ for all $i = 0, \dots, \ell-1$. Since $\text{lm}(\Phi_{ij}) = x_i^q x_j$ with $i < j$, it follows that none of the leading monomials of Φ_{ij} divides μ . Hence $\mu \rightarrow_\Phi \mu = \overline{\mu}$.

Now suppose $\text{wt}(\mu) > 0$, and the claim holds for monomials of weight smaller than $\text{wt}(\mu)$. Then μ is not projectively reduced. Let i be the smallest index such that $a_i > q-1$. Note that $i < \ell$, since μ is not projectively reduced. Further let j be the smallest index such that $i < j \leq \ell$ and $a_j > 0$.

Then the first step of the division algorithm for the division of μ by Φ will be the reduction

$$\mu \rightarrow \mu - \frac{\mu}{x_i^q x_j} \Phi_{ij} = \mu', \quad \text{where } \mu' := x_i^{a_i-q+1} x_j^{a_j+q-1} \prod_{\substack{0 \leq s \leq \ell \\ s \neq i, s \neq j}} x_s^{a_s}. \quad (6)$$

However,

$$\text{wt}(\mu') = \text{wt}(\mu) - (q-1)(q^{m-i} - q^{m-j}) < \text{wt}(\mu).$$

Thus Claim 1 follows from the induction hypothesis.

Claim 2 If $\mu \rightarrow_\Phi \nu$ for some $\nu \in \overline{\mathbb{M}}$, then $\nu = \overline{\mu}$.

To prove this claim, note that if μ is transformed to μ' by the first step of the division algorithm, then from (6), we see that $\text{supp}(\mu) = \text{supp}(\mu')$ and moreover, if $\mu' = x_0^{a'_0} \dots x_\ell^{a'_\ell}$ for some nonnegative integers a'_0, \dots, a'_ℓ , then

$$a_i \equiv a'_i \pmod{q-1} \quad \text{and} \quad a_i = 0 \iff a'_i = 0 \quad \text{for } 0 \leq i \leq \ell. \quad (7)$$

Likewise if in the next step of the division algorithm, μ' is transformed to some μ'' in \mathbb{M} , then $\text{supp}(\mu') = \text{supp}(\mu'')$ and the exponents of μ'' will satisfy conditions similar to that in (7). It follows that if $\mu \rightarrow_{\Phi} \nu$, then $\nu = x_0^{b_0} \cdots x_{\ell}^{b_{\ell}}$ for some nonnegative integers b_0, \dots, b_{ℓ} that satisfy (7) with a'_i replaced by b_i . Since ν is projectively reduced, this implies that $\nu = \bar{\mu}$, is desired.

The proposition now follows directly from the above two claims. \square

Corollary 2.4 *Let k be an algebraic extension of \mathbb{F}_q and let $f \in k[x_0, \dots, x_m]$. Then $f \rightarrow_{\Phi} \bar{f}$. Moreover $\bar{f} = 0$ if and only if $f \in \Gamma_q(k)$.*

Proof Let us first prove that $f \rightarrow_{\Phi} \bar{f}$. Write $f = c_1\mu_1 + \cdots + c_N\mu_N$, with μ_1, \dots, μ_N distinct monomials in \mathbb{M} and c_1, \dots, c_N nonzero elements of k . We define

$$\text{wt}(f) := \text{wt}(\mu_1) + \cdots + \text{wt}(\mu_N),$$

where for $\mu \in \mathbb{M}$, $\text{wt}(\mu)$ is as in the proof of Proposition 2.3. Then f is projectively reduced if and only if $\text{wt}(f) = 0$. Hence if $\text{wt}(f) = 0$, there is nothing to prove.

Now suppose that $\text{wt}(f) > 0$. Equation (6) implies that a single step in the division algorithm will replace a monomial occurring in f by a projectively equivalent monomial of lower weight. Hence if $\text{wt}(f) > 0$, the first step of the division algorithm will replace f by a polynomial g satisfying $\bar{g} = \bar{f}$ and $\text{wt}(g) < \text{wt}(f)$. By induction, the first assertion in the corollary follows.

We now prove the second assertion. To this end, note that since $f \rightarrow_{\Phi} \bar{f}$, in case $\bar{f} = 0$, it follows from the division algorithm that f is in the ideal generated by $\{\Phi_{ij} : 0 \leq i < j \leq m\}$, i.e., $f \in \Gamma_q(k)$. Conversely if $f \in \Gamma_q(k)$, then we can write $f = \sum_{i < j} f_{ij}\Phi_{ij}$ for some $f_{ij} \in k[x_0, \dots, x_m]$. Using parts (i) and (iii) of Proposition 2.2, we see that

$$\bar{f} = \sum_{i < j} \overline{f_{ij}\Phi_{ij}} = \sum_{i < j} \overline{f_{ij}} \overline{\Phi_{ij}} = 0,$$

where the last equality follows since $\overline{\Phi_{ij}} = x_i x_j^q - x_j^q x_i = 0$ for $0 \leq i < j \leq m$. This completes the proof. \square

2.3 Vanishing Ideal of $\mathbb{P}^m(\mathbb{F}_q)$

Let k be a field. Recall that the *vanishing ideal* over k of a subset \mathcal{X} of $\mathbb{P}^m(k)$ is the ideal $I(\mathcal{X})$ of $k[x_0, x_1, \dots, x_m]$ generated by the homogeneous polynomials in $k[x_0, x_1, \dots, x_m]$ that vanish at every point of \mathcal{X} . The following result was proved by Mercier and Rolland [21, Thm. 2.1].

Theorem 2.5 *The vanishing ideal over \mathbb{F}_q of $\mathbb{P}^m(\mathbb{F}_q)$ is $\Gamma_q(\mathbb{F}_q)$, i.e., it is the ideal of $\mathbb{F}_q[x_0, \dots, x_m]$ generated by the Fermat polynomials $x_i^q x_j - x_i x_j^q$ ($0 \leq i < j \leq m$).*

We observe that this can be used to deduce a more general result.

Corollary 2.6 *Let k be an algebraic extension of \mathbb{F}_q . Then the vanishing ideal over k of the set $\mathbb{P}^m(\mathbb{F}_q)$ of all \mathbb{F}_q -rational points of $\mathbb{P}^m(k)$ is $\Gamma_q(k)$.*

Proof Let I denote the vanishing ideal of $\mathbb{P}^m(\mathbb{F}_q)$ over k . Clearly, $\Gamma_q(k) \subseteq I$. To prove the other inclusion, suppose $f \in I$. Then f is a finite sum of the form

$$f = \sum c_{i_0 i_1 \dots i_m} x_0^{i_0} x_1^{i_1} \cdots x_m^{i_m} \quad \text{where the coefficients } c_{i_0 i_1 \dots i_m} \text{ are in } k.$$

Since this is a finite sum, there is a positive integer e such that $\mathbb{F}_{q^e} \subseteq k$ and all the coefficients are in \mathbb{F}_{q^e} . Now let $\{\alpha_1, \dots, \alpha_e\}$ be a \mathbb{F}_q -basis of \mathbb{F}_{q^e} . Then

$$c_{i_0 i_1 \dots i_m} = \sum_{j=1}^e c_{i_0 i_1 \dots i_m}^{(j)} \alpha_j \quad \text{for some } c_{i_0 i_1 \dots i_m}^{(j)} \in \mathbb{F}_q.$$

Consequently, $f = \sum_{j=1}^e f_j \alpha_j$ for some $f_j \in \mathbb{F}_q[x_0, x_1, \dots, x_m]$. Since $f(P) = 0$ for all $P \in \mathbb{P}^m(\mathbb{F}_q)$, we see that $f_j(P) = 0$ for all $P \in \mathbb{P}^m(\mathbb{F}_q)$ and $j = 1, \dots, e$. Hence f_j is in the vanishing ideal of $\mathbb{P}^m(\mathbb{F}_q)$ over \mathbb{F}_q , and so by Theorem 2.5, $f_j \in \Gamma_q(\mathbb{F}_q)$ for each $j = 1, \dots, e$. Consequently, $f \in \Gamma_q(k)$. \square

Remark 2.7 An argument similar to the proof of Corollary 2.6 will show that $\Gamma_q(\mathbb{F}_q) = \Gamma_q(k) \cap \mathbb{F}_q[x_0, \dots, x_m]$. In other words, the vanishing ideal of $\mathbb{P}^m(\mathbb{F}_q)$ over \mathbb{F}_q is the contraction of the vanishing ideal of $\mathbb{P}^m(\mathbb{F}_q)$ over k to $\mathbb{F}_q[x_0, \dots, x_m]$. An alternative proof of Corollary 2.6 that is independent of Theorem 2.5, can be found in Section 3.3 of the expository article [14].

Recall that a *universal Gröbner basis* of an ideal I in a polynomial ring over a field is a subset of I that is a Gröbner basis of I with respect to any term order.

Theorem 2.8 *Let k be an algebraic extension of \mathbb{F}_q and let I be the vanishing ideal of $\mathbb{P}^m(\mathbb{F}_q)$ over k . Then the set $\{\Phi_{ij} : 0 \leq i < j \leq m\}$ of Fermat polynomials is a reduced Gröbner basis of I , and also a universal Gröbner basis of I .*

Proof We know from Corollary 2.6 that the Fermat polynomials generate I . Moreover, for any $i, j, r, s \in \mathbb{Z}$ with $0 \leq i < j \leq m$ and $0 \leq r < s \leq m$, it is clear that the S -polynomial $S(\Phi_{ij}, \Phi_{rs})$ is in the ideal $\Gamma_q(k)$. Hence by Corollary 2.4, $S(\Phi_{ij}, \Phi_{rs}) \rightarrow_{\Phi} 0$. So it follows from Buchberger's criterion [7, Ch. 2, Section 6] that $\{\Phi_{ij} : 0 \leq i < j \leq m\}$ forms a Gröbner basis of I . Further, $\text{lm}(\Phi_{ij}) = x_i^q x_j$ is clearly not divisible by any of the monomials appearing in Φ_{rs} whenever $i, j, r, s \in \mathbb{Z}$ are such that $0 \leq i < j \leq m$, $0 \leq r < s \leq m$, and $(i, j) \neq (r, s)$. Thus, we see that $\{\Phi_{ij} : 0 \leq i < j \leq m\}$ is a reduced Gröbner basis of I . To see that this set is also a universal Gröbner basis, it suffices to note that thus far, we had put no condition on the term order \preceq , except that the variables are ordered as $x_0 \succ x_1 \succ \dots \succ x_m$. Changing the order on the variables amounts to considering the Fermat polynomials Φ_{ij} with the variables permuted. But any such permutation of variables will leave the set $\{\Phi_{ij} : 0 \leq i < j \leq m\}$ invariant, except for a sign change in some of the Φ_{ij} 's. Thus we see that $\{\Phi_{ij} : 0 \leq i < j \leq m\}$ is a Gröbner basis of I with respect to any term order. \square

Corollary 2.9 *Let k be an algebraic extension of \mathbb{F}_q and let I be the vanishing ideal of $\mathbb{P}^m(\mathbb{F}_q)$ over k . Then $\{x_i^q x_j : 0 \leq i < j \leq m\}$ is a Gröbner basis of $\text{LT}(I)$.*

Proof By Theorem 2.8, $\{\Phi_{ij} : 0 \leq i < j \leq m\}$ is a Gröbner basis of I . Also, $\text{lm}(\Phi_{ij}) = x_i^q x_j$ for $0 \leq i < j \leq m$. So $\{x_i^q x_j : 0 \leq i < j \leq m\}$ generates $\text{LT}(I)$. Moreover, it is easily seen that $S(x_i^q x_j, x_r^q x_s) = 0$ for any $i, j, r, s \in \mathbb{Z}$ with $0 \leq i < j \leq m$ and $0 \leq r < s \leq m$. Thus, from Buchberger's criterion, it follows that $\{x_i^q x_j : 0 \leq i < j \leq m\}$ is a Gröbner basis of $\text{LT}(I)$. \square

We end this section with the following useful consequences of the determination of Gröbner bases of the vanishing ideals of projective spaces over finite fields.

Corollary 2.10 *Let k be an algebraic extension of \mathbb{F}_q and let I be the vanishing ideal of $\mathbb{P}^m(\mathbb{F}_q)$ over k . Then every element of $k[x_0, \dots, x_m]/I$ can be uniquely written as $f + I$, where*

f is a projectively reduced polynomial. Moreover, every element of $k[x_0, \dots, x_m]/\text{LT}(I)$ can also be uniquely written as $f + \text{LT}(I)$, where f is a projectively reduced polynomial.

Proof Let $f \in k[x_0, \dots, x_m]$. By Corollary 2.4 and Corollary 2.6, $f - \bar{f} \in \Gamma_q(k) = I$. Hence $f + I(\mathbb{P}^m(\mathbb{F}_q)) = \bar{f} + I(\mathbb{P}^m(\mathbb{F}_q))$. Moreover, if f, g are two projectively reduced polynomials such that $f - g \in I$, then Corollary 2.6, Corollary 2.4 and Proposition 2.2 imply that $f - g = \overline{f - g} = 0$. This proves the first assertion.

For the second assertion, note that if $\mu \in \mathbb{M}$ is not projectively reduced, then μ is divisible by $x_i^q x_j$ for some $i, j \in \mathbb{Z}$ with $0 \leq i < j \leq m$, and thus $\mu \in \text{LT}(I)$. This shows that every coset in $k[x_0, \dots, x_m]/\text{LT}(I)$ can be written as $f + \text{LT}(I)$ for some projectively reduced polynomial f . Moreover, if f, g are two distinct projectively reduced polynomials such that $f - g \in \text{LT}(I)$, then by Corollary 2.9, $\text{lm}(f - g)$ is divisible by an element of $\{x_i^q x_j \mid 0 \leq i < j \leq m\}$. But this is impossible, since $f - g \neq 0$ and $f - g$ is a linear combination of projectively reduced monomials. \square

3 Projective Footprint Bound

We let \mathbb{N} denote the set of all nonnegative integers. For a parameter e varying in the set \mathbb{N} , we shall write “for all $e \gg 0$ ” to mean “for all large enough e ”, that is to say for all $e \in \mathbb{N}$ that are larger than or equal to some fixed $e_0 \in \mathbb{N}$.

3.1 Hilbert Functions and Projective Footprints

Let k be a field. Note that the polynomial ring $k[x_0, \dots, x_m]$ is a graded k -algebra. For any $e \in \mathbb{N}$, its e^{th} graded component $k[x_0, \dots, x_m]_e$ consists of homogeneous polynomials of degree e (including the zero polynomial), and it is a vector space over k of dimension $\binom{m+e}{e}$. If \mathcal{J} is a homogeneous ideal of $k[x_0, \dots, x_m]$, then $\mathcal{J} = \bigoplus_{e \geq 0} \mathcal{J}_e$, where $\mathcal{J}_e := \mathcal{J} \cap k[x_0, \dots, x_m]_e$ for $e \in \mathbb{N}$. The *Hilbert function* of $k[x_0, \dots, x_m]/\mathcal{J}$ is the map

$$h_{\mathcal{J}} : \mathbb{N} \rightarrow \mathbb{N} \quad \text{defined by} \quad h_{\mathcal{J}}(e) := \dim_k k[x_0, \dots, x_m]_e / \mathcal{J}_e \quad \text{for } e \in \mathbb{N}.$$

It is well known that there is a polynomial $\chi_{\mathcal{J}} \in \mathbb{Q}[t]$ such that

$$h_{\mathcal{J}}(e) = \chi_{\mathcal{J}}(e) \quad \text{for all } e \gg 0.$$

Clearly $\chi_{\mathcal{J}}$ is uniquely determined by \mathcal{J} and it is called the *Hilbert polynomial* of \mathcal{J} . Note that if \mathcal{I} is a homogeneous ideal of $k[x_0, \dots, x_m]$ such that $\mathcal{J} \subseteq \mathcal{I}$, then

$$h_{\mathcal{I}}(e) \leq h_{\mathcal{J}}(e) \quad \text{for all } e \in \mathbb{N} \quad \text{and hence} \quad \chi_{\mathcal{I}}(e) \leq \chi_{\mathcal{J}}(e) \quad \text{for all } e \gg 0. \quad (8)$$

The following result is classical. A proof can be gleaned, for instance, from [7, Section 3 of Ch. 8 and 9] and [17, Section 7 of Ch. 1].

Theorem 3.1 *Let k be an algebraically closed field and let \mathcal{J} be a homogeneous ideal of $k[x_0, \dots, x_m]$, and $\mathcal{X} = V(\mathcal{J})$ be the corresponding projective variety consisting of all $P \in \mathbb{P}^m(k)$ such that $F(P) = 0$ for all homogeneous $F \in \mathcal{J}$. Then:*

(i) (Projective Nullstellensatz) *If $V(\mathcal{J})$ is empty, then $\sqrt{\mathcal{J}} \supseteq \langle x_0, x_1, \dots, x_m \rangle$, whereas if $\mathcal{X} = V(\mathcal{J})$ is nonempty, then $I(\mathcal{X}) = \sqrt{\mathcal{J}}$.*

(ii) *Suppose \mathcal{X} is nonempty and $\mathcal{I} = I(\mathcal{X})$. Then $\deg \chi_{\mathcal{I}} = \deg \chi_{\mathcal{J}} = \dim \mathcal{X}$, where $\dim \mathcal{X}$ denotes the dimension of \mathcal{X} as a projective algebraic variety. Moreover if $d = \dim \mathcal{X}$*

and we write $\chi_{\mathcal{I}}(t) = a_0 t^d + \dots + a_d$, then $\deg \mathcal{X} = d!a_0$, where $\deg \mathcal{X}$ denotes the degree of \mathcal{X} , and this is a positive integer with the property that if $\mathcal{I} = \langle F \rangle$ for some homogeneous $F \in k[x_0, \dots, x_m]$, then $\deg \mathcal{X} = \deg F$, whereas if \mathcal{X} is a finite set, then $\deg \mathcal{X} = |\mathcal{X}|$.

The next theorem is also classical and is sometimes ascribed to Macaulay. See, e.g., [7, Section 3 of Ch.9] for a proof. Henceforth we fix a monomial order \preccurlyeq on the set \mathbb{M} of all monomials in $k[x_0, \dots, x_m]$ in such a way that $x_0 \succ \dots \succ x_m$. The leading monomial $\text{lm}(F)$ of a nonzero $F \in k[x_0, \dots, x_m]$ and the leading term ideal $\text{LT}(\mathcal{J})$ of an ideal \mathcal{J} of $k[x_0, \dots, x_m]$ will be understood to be with respect to this fixed monomial order.

Theorem 3.2 *Let k be a field and let \mathcal{J} be a homogeneous ideal of $k[x_0, \dots, x_m]$. Then $h_{\mathcal{J}}(e) = h_{\text{LT}(\mathcal{J})}(e)$ and therefore $\chi_{\mathcal{J}}(e) = \chi_{\text{LT}(\mathcal{J})}(e)$ for all $e \in \mathbb{N}$.*

We define the notion of a projective footprint over an arbitrary field as follows.

Definition 3.3 *Let k be a field and let \mathcal{J} be a homogeneous ideal of $k[x_0, \dots, x_m]$. Then for any $e \in \mathbb{N}$, the set*

$$\Delta_e(\mathcal{J}) := \{\mu \in \mathbb{M}_e : \mu \neq \text{lm}(F) \text{ for all homogeneous } F \in \mathcal{J} \text{ with } F \neq 0\}$$

is called the projective footprint of \mathcal{J} in degree e .

Theorem 3.4 (Projective Footprint Bound) *Let k be an algebraically closed field and let \mathcal{J} be a homogeneous ideal of $k[x_0, \dots, x_m]$, such that the corresponding projective variety $\mathcal{X} = V(\mathcal{J})$ is a finite subset of $\mathbb{P}^m(k)$. Then for all $e \gg 0$,*

$$|V(\mathcal{J})| \leq |\Delta_e(\mathcal{J})| \quad \text{with equality if } \mathcal{J} \text{ is a radical ideal.} \quad (9)$$

Proof If \mathcal{X} is empty, then the inequality in (9) holds trivially for all $e \in \mathbb{N}$; if, in addition, \mathcal{J} is a radical ideal, then by part (i) of Theorem 3.1, $\Delta_e(\mathcal{J})$ is empty for all $e \geq 1$ and so the equality holds in this case. Now suppose \mathcal{X} is nonempty. Let $\mathcal{I} = I(\mathcal{X})$ be the vanishing ideal of $\mathcal{X} = V(\mathcal{J})$ over k . Since \mathcal{X} is finite, $\dim \mathcal{X} = 0$ and by part (ii) of Theorem 3.1, both $\chi_{\mathcal{I}}$ and $\chi_{\mathcal{J}}$ are constant polynomials and $\chi_{\mathcal{I}} = |\mathcal{X}|$. On the other hand, since \mathcal{J} is a homogeneous ideal of $k[x_0, \dots, x_m]$, it is easily seen that $\Delta_e(\mathcal{J}) = \{\mu \in \mathbb{M}_e : \mu \notin \text{LT}(\mathcal{J})\}$. Now $\text{LT}(\mathcal{J})$ is a monomial ideal and it is well known (and easily deduced, e.g., from the division algorithm) that $\{\mu + \text{LT}(\mathcal{J}) : \mu \in \mathbb{M}_e, \mu \notin \text{LT}(\mathcal{J})\}$ is a k -basis of $(k[x_0, \dots, x_m]/\text{LT}(\mathcal{J}))_e$, which implies:

$$h_{\text{LT}(\mathcal{J})}(e) = |\Delta_e(\mathcal{J})| \quad \text{for all } e \in \mathbb{N} \quad \text{and so} \quad \chi_{\text{LT}(\mathcal{J})}(e) = |\Delta_e(\mathcal{J})| \quad \text{for all } e \gg 0.$$

Thus in view of (8) and Theorem 3.2, we obtain

$$|V(\mathcal{J})| = \chi_{\mathcal{I}}(e) \leq \chi_{\mathcal{J}}(e) = \chi_{\text{LT}(\mathcal{J})}(e) = |\Delta_e(\mathcal{J})| \quad \text{for all } e \gg 0,$$

and the equality clearly holds if $\mathcal{I} = \mathcal{J}$, i.e., if \mathcal{J} is a radical ideal. \square

Remark 3.5 The above proof of Theorem 3.4 together with Projective Nullstellensatz shows that if k is algebraically closed and \mathcal{J} a homogeneous ideal of $k[x_0, \dots, x_m]$ such that $V(\mathcal{J})$ is finite, then $\chi_{\mathcal{J}}$ and $\chi_{\sqrt{\mathcal{J}}}$ are constant polynomials and

$$\chi_{\sqrt{\mathcal{J}}} = |V(\mathcal{J})| \quad \text{and} \quad \chi_{\mathcal{J}} = |\Delta_e(\mathcal{J})| \quad \text{for all } e \gg 0.$$

3.2 Projective \mathbb{F}_q -Footprint Formula

Let k be an algebraic closure of \mathbb{F}_q . By Corollary 2.6, the vanishing ideal over k of $\mathbb{P}^m(\mathbb{F}_q)$ is given by

$$I(\mathbb{P}^m(\mathbb{F}_q)) = \Gamma_q(k) := \langle x_i^q x_j - x_i x_j^q : 0 \leq i < j \leq m \rangle \subseteq k[x_0, \dots, x_m].$$

If \mathcal{J} is a homogeneous ideal of $k[x_0, \dots, x_m]$ and if $\mathcal{X} = V(\mathcal{J})$ is the corresponding projective algebraic variety in $\mathbb{P}^m(k)$, then we let

$$\mathcal{J}_q := \mathcal{J} + \Gamma_q(k) \quad \text{and} \quad \mathcal{X}_q := V(\mathcal{J}_q).$$

Clearly, \mathcal{J}_q is a homogeneous ideal of $k[x_0, \dots, x_m]$ and $\mathcal{X}_q(k) = V(\mathcal{J}_q) = \mathcal{X}(\mathbb{F}_q)$.

Example 3.6 Suppose $m = 1$ and $F(x_0, x_1) := x_0^q x_1 - x_0 x_1^q + x_0^{q+1}$. Consider the homogeneous ideal $\mathcal{J} := \langle F(x_0, x_1) \rangle$ of $k[x_0, x_1]$. Observe that $\mathcal{J} = \sqrt{\mathcal{J}}$. To see this, note that $k[x_0, x_1]$ is a UFD and F does not have a multiple root in $\mathbb{P}^1(k)$. Indeed, $F(x_0, x_1) = x_0 G(x_0, x_1)$ where $G(x_0, x_1) := x_0^{q-1} x_1 - x_1^q + x_0^q$ does not have $[0 : 1]$ as a root and also no multiple root of the form $[1 : a]$ since the derivative with respect to x_1 of $G(1, x_1)$ is never zero. On the other hand, $\mathcal{J}_q = \mathcal{J} + \langle x_0^q x_1 - x_0 x_1^q \rangle$ contains x_0^{q+1} , but does not contain x_0 (since every nonzero element of \mathcal{J}_q has degree $\geq q + 1$). Thus \mathcal{J}_q is not a radical ideal even though \mathcal{J} is a radical ideal.

In light of this example, the following result seems noteworthy.

Theorem 3.7 (Projective \mathbb{F}_q -Footprint Formula) *Let k be an algebraic closure of \mathbb{F}_q . Also, let \mathcal{J} be a homogeneous ideal of $k[x_0, \dots, x_m]$ and $\mathcal{X} = V(\mathcal{J})$ the corresponding projective algebraic variety in $\mathbb{P}^m(k)$. Then*

$$|\mathcal{X}(\mathbb{F}_q)| = |\Delta_e(\mathcal{J}_q)| \quad \text{for all } e \gg 0.$$

Proof We have noted that $\mathcal{X}(\mathbb{F}_q) = \mathcal{X}_q = V(\mathcal{J}_q)$. Let $\mathcal{I} := I(\mathcal{X}_q) = \sqrt{\mathcal{J}_q}$. In view of Remark 3.5, both $\chi_{\mathcal{J}_q}$ and $\chi_{\mathcal{I}}$ are constant polynomials and

$$\chi_{\mathcal{I}} = |\mathcal{X}(\mathbb{F}_q)| \quad \text{and} \quad \chi_{\mathcal{J}_q} = |\Delta_e(\mathcal{J}_q)| \quad \text{for all } e \gg 0.$$

Thus it suffices to show that $\chi_{\mathcal{I}} = \chi_{\mathcal{J}_q}$. To this end, let $\{G_1, \dots, G_r\}$ be a Gröbner basis of \mathcal{I} such that each G_i is a homogeneous polynomial in $k[x_0, \dots, x_m]$. Let $d_i := \deg G_i$ for $i = 1, \dots, r$. Choose a large enough positive integer s such that

$$G_i \text{ has all its coefficients in } \mathbb{F}_{q^s} \quad \text{and} \quad G_i^{q^s} \in \mathcal{J}_q \quad \text{for each } i = 1, \dots, r.$$

Then $G_i^{q^s}(x_0, \dots, x_m) = G_i(x_0^{q^s}, \dots, x_m^{q^s})$ for $1 \leq i \leq r$. Hence if we let

$$H_{ij} := x_j(G_i^{q^s} - x_j^{d_i(q^s-1)} G_i) \quad \text{for } i = 1, \dots, r \quad \text{and} \quad j = 0, 1, \dots, m,$$

then we see that $H_{ij}(P) = 0$ for all $P \in \mathbb{P}^m(\mathbb{F}_q)$. Indeed, if $P = [a_0 : \dots : a_m]$, where $a_0, \dots, a_m \in \mathbb{F}_q$, then clearly $H_{ij}(P) = 0$ when $a_j = 0$, whereas in case $a_j = 1$, $H_{ij}(P) = G_i^{q^s}(a_0, \dots, a_m) - G_i(a_0, \dots, a_m) = G_i(a_0^{q^s}, \dots, a_m^{q^s}) - G_i(a_0, \dots, a_m) = 0$ as well. Thus by Corollary 2.6,

$$H_{ij} \in \Gamma_q(k) \quad \text{and so} \quad x_j^{d_i(q^s-1)+1} G_i \in \mathcal{J}_q \quad \text{for } i = 1, \dots, r \quad \text{and} \quad j = 0, 1, \dots, m,$$

where the last assertion follows since $\Gamma_q(k) \subseteq \mathcal{J}_q$ and $G_i^{q^s} \in \mathcal{J}_q$ for $1 \leq i \leq r$. It follows that $x_j^d G_i \in \mathcal{J}_q$ and $x_j^d \text{lm}(G_i) \in \text{LT}(\mathcal{J}_q)$ for $1 \leq i \leq r$ and $0 \leq j \leq m$, where

$$d := \max\{d_i(q^s - 1) + 1 : i = 1, \dots, r\}.$$

Hence the monomial ideal $\mathcal{M}_q := \langle x_j^d \text{lm}(G_i) : 1 \leq i \leq r, 0 \leq j \leq m \rangle$ satisfies

$$\mathcal{M}_q \subseteq \text{LT}(\mathcal{J}_q) \subseteq \text{LT}(\mathcal{I}) = \langle \text{lm}(G_i) : 1 \leq i \leq r \rangle, \quad (10)$$

where the last equality holds since $\{G_1, \dots, G_r\}$ is a Gröbner basis of \mathcal{I} . Now suppose $e \geq d(m+1) + \max\{d_1, \dots, d_r\}$. We claim that $\text{LT}(\mathcal{I})_e \subseteq (\mathcal{M}_q)_e$. To see this, let $\mu \in \mathbb{M}_e$ be such that $\mu \in \text{LT}(\mathcal{I}) = \langle \text{lm}(G_i) : 1 \leq i \leq r \rangle$. Then $\mu = \nu \text{lm}(G_i)$ for some $i \in \{1, \dots, r\}$ and $\nu \in \mathbb{M}_{e-d_i}$. Now $e - d_i \geq d(m+1)$, by our choice of e , and so $x_j^d \mid \nu$ for some $j \in \{0, 1, \dots, m\}$. Thus $\nu = x_j^d \nu'$ for some $\nu' \in \mathbb{M}$, and hence $\mu = \nu' x_j^d \text{lm}(G_i)$. This shows that $\mu \in \mathcal{M}_q$. So the claim is proved. Consequently, $h_{\mathcal{M}_q}(e) \leq h_{\text{LT}(\mathcal{I})}(e)$ for all $e \gg 0$. This implies that $\chi_{\mathcal{M}_q}$ is a constant polynomial (because $\chi_{\mathcal{I}}$ is a constant polynomial and by Theorem 3.2, $\chi_{\mathcal{I}} = \chi_{\text{LT}(\mathcal{I})}$), and moreover, $\chi_{\mathcal{M}_q} \leq \chi_{\text{LT}(\mathcal{I})}$. On the other hand, by (8) and (10), $\chi_{\text{LT}(\mathcal{I})} \leq \chi_{\text{LT}(\mathcal{J}_q)} \leq \chi_{\mathcal{M}_q}$. Thus, we obtain $\chi_{\text{LT}(\mathcal{I})} = \chi_{\text{LT}(\mathcal{J}_q)}$ and so by Theorem 3.2, $\chi_{\mathcal{I}} = \chi_{\mathcal{J}_q}$, as desired. \square

Although very simple, it may be instructive to work out the Hilbert functions in Example 3.6 so as to illustrate Theorem 3.7.

Example 3.8 Suppose $m = 1$ and $F(x_0, x_1)$ as well as \mathcal{J} and \mathcal{J}_q are as in Example 3.6. Let $\mathcal{X} := V(\mathcal{J})$. Evidently, $\mathcal{X}(\mathbb{F}_q) = \{[0 : 1]\}$ and so $|\mathcal{X}(\mathbb{F}_q)| = 1$. Also, $\mathcal{I} := \sqrt{\mathcal{J}_q} = \langle x_0 \rangle$ and thus $\{x_1^e + \mathcal{I}\}$ is a basis of $(k[x_0, x_1]/\mathcal{I})_e$; in particular, $h_{\mathcal{I}}(e) = 1$ for all $e \in \mathbb{N}$. On the other hand,

$$\mathcal{J}_q = \langle F_1, F_2 \rangle \quad \text{where} \quad F_1 := x_0^q x_1 - x_0 x_1^q \quad \text{and} \quad F_2 := x_0^{q+1}.$$

A Gröbner basis for \mathcal{J}_q is given by $\{F_1, F_2, F_3, F_4\}$, where F_1, F_2 are as above, while $F_3 := x_0^2 x_1^q$ and $F_4 := x_0 x_1^{2q-1}$. Indeed, F_3 and F_4 are in \mathcal{J}_q , and since F_2, F_3, F_4 are monomials, the S -polynomial $S(F_i, F_j)$ is 0 for $2 \leq i < j \leq 4$, whereas

$$S(F_1, F_2) = -F_3, \quad S(F_1, F_3) = -F_4, \quad \text{and} \quad S(F_1, F_4) = -x_0 x_1^{3q-2} \in \langle F_4 \rangle.$$

The Hilbert function of \mathcal{J}_q or equivalently, the cardinality of the footprint of \mathcal{J}_q in each degree, is not difficult to determine by a direct computation, and is given by

$$h_{\mathcal{J}_q}(e) = \begin{cases} e + 1 & \text{if } 0 \leq e \leq q, \\ 2q + 1 - e & \text{if } q + 1 \leq e \leq 2q - 1, \\ 1 & \text{if } e \geq 2q. \end{cases}$$

So the Hilbert function stabilizes after $e = 2q$ and $\chi_{\mathcal{J}_q} = 1 = |\Delta_e(\mathcal{J}_q)|$ for $e \geq 2q$.

3.3 Projective \mathbb{F}_q -Footprint Bound

We shall now derive a version of Theorems 3.4 and 3.7 that is useful for estimating the number of \mathbb{F}_q -rational points of projective algebraic varieties over an algebraic extension k of \mathbb{F}_q . We first note some elementary properties of the fixed monomial order \preccurlyeq on \mathbb{M} and projective reduction.

Lemma 3.9 *Let \preccurlyeq be a monomial order on \mathbb{M} for which $x_0 \succ \dots \succ x_m$. Then:*

(i) $\bar{\nu} \preccurlyeq \nu$ for all $\nu \in \mathbb{M}$.

(ii) If $F \in k[x_0, \dots, x_m]$ is such that $F \neq 0$ and $\text{lm}(F)$ is reduced, then $\bar{F} \neq 0$ and $\text{lm}(F) = \text{lm}(\bar{F})$.

Proof (i) The case $\nu = 1$ is trivial. Suppose $\nu \in \mathbb{M}$ with $\nu \neq 1$. Then $\nu = x_0^{a_0} \cdots x_\ell^{a_\ell}$ for some $a_0, \dots, a_\ell \in \mathbb{N}$ with $a_\ell > 0$. Let $\bar{a}_0, \dots, \bar{a}_{\ell-1}$ be as in Definition 2.1. Now

$$x_j \succ x_\ell \implies x_j^{a_j} \succ x_j^{\bar{a}_j} x_\ell^{a_j - \bar{a}_j} \quad \text{for } 0 \leq j < \ell \quad \text{and hence } \bar{\nu} \preceq \nu.$$

(ii) Let $0 \neq F \in k[x_0, \dots, x_m]$ be such that $\text{lm}(F)$ is reduced. Let c_1, \dots, c_N be nonzero elements of k and ν_1, \dots, ν_N be monomials in \mathbb{M} such that

$$F = c_1 \nu_1 + \cdots + c_N \nu_N \quad \text{and} \quad \nu_1 \succ \cdots \succ \nu_N.$$

Then $\text{lm}(\bar{F}) = \nu_1$ and by hypothesis, $\nu_1 = \bar{\nu}_1$. Thus, in view of (i) above,

$$\bar{F} = c_1 \bar{\nu}_1 + \cdots + c_N \bar{\nu}_N \quad \text{and} \quad \bar{\nu}_1 = \nu_1 \succ \nu_j \succ \bar{\nu}_j \text{ for } 2 \leq j \leq N.$$

It follows that $\bar{F} \neq 0$ and $\text{lm}(\bar{F}) = \bar{\nu}_1 = \nu_1 = \text{lm}(F)$. \square

We now define a variant of the projective footprint that is specific to the base field \mathbb{F}_q and uses projectively reduced monomials.

Definition 3.10 *Let k be an algebraic extension of \mathbb{F}_q and let S be a subset of $k[x_0, \dots, x_m]$. Then for any $e \in \mathbb{N}$, the set*

$$\bar{\Delta}_e(S) := \{\mu \in \bar{\mathbb{M}}_e : \text{lm}(\bar{F}) \nmid \mu \text{ for all homogeneous } F \in S \text{ with } \bar{F} \neq 0\}$$

is called the projective \mathbb{F}_q -footprint of S in degree e . Moreover, its complement

$$\bar{\nabla}_e(S) := \{\mu \in \bar{\mathbb{M}}_e : \text{lm}(\bar{F}) \mid \mu \text{ for some homogeneous } F \in S \text{ with } \bar{F} \neq 0\}$$

is called the projective \mathbb{F}_q -shadow of S in degree e . If $S = \{F_1, \dots, F_r\}$, we often write $\bar{\Delta}_e(F_1, \dots, F_r)$ and $\bar{\nabla}_e(F_1, \dots, F_r)$ for $\bar{\Delta}_e(S)$ and $\bar{\nabla}_e(S)$, respectively. Note that if S contains no homogeneous polynomial F with $\bar{F} \neq 0$, then $\bar{\Delta}_e(S) = \bar{\mathbb{M}}_e$ and $\bar{\nabla}_e(S) = \emptyset$. Also, for any $S' \subseteq k[x_0, \dots, x_m]$,

$$S \subseteq S' \implies \bar{\Delta}_e(S) \supseteq \bar{\Delta}_e(S') \quad \text{and} \quad \bar{\nabla}_e(S) \subseteq \bar{\nabla}_e(S'). \quad (11)$$

A relation between projective footprints and projective \mathbb{F}_q -footprints is as follows.

Lemma 3.11 *Let k be an algebraic extension of \mathbb{F}_q and let \mathcal{J} be a homogeneous ideal of $k[x_0, \dots, x_m]$. As before, let $\mathcal{J}_q := \mathcal{J} + \Gamma_q(k)$. Then*

$$\bar{\Delta}_e(\mathcal{J}) = \Delta_e(\mathcal{J}_q) \quad \text{for all } e \in \mathbb{N}.$$

Proof Let $e \in \mathbb{N}$ and $\mu \in \bar{\Delta}_e(\mathcal{J})$. Suppose, if possible, $\mu = \text{lm}(F)$ for some homogeneous $F \in \mathcal{J}_q$. Write $F = G + \gamma$, where $G \in \mathcal{J}$ and $\gamma \in \Gamma_q(k)$. Since \mathcal{J} and $\Gamma_q(k)$ are homogeneous ideals, we may assume without loss of generality that both G and γ are homogeneous. By Corollary 2.4, $\bar{F} = \bar{G}$. Also since $\mu = \text{lm}(F)$ is reduced, by part (ii) of Lemma 3.9, $\bar{G} \neq 0$ and $\text{lm}(\bar{G}) = \mu$, which contradicts the assumption that $\mu \in \bar{\Delta}_e(\mathcal{J})$. Thus $\bar{\Delta}_e(\mathcal{J}) \subseteq \Delta_e(\mathcal{J}_q)$.

To prove the other inclusion, first note that $1 \in \mathcal{J} \Leftrightarrow 1 \in \mathcal{J}_q$, and that both $\Delta_0(\mathcal{J}_q)$ and $\bar{\Delta}_0(\mathcal{J})$ are equal to $\{1\}$ or the empty set according as $1 \notin \mathcal{J}$ or $1 \in \mathcal{J}$. Thus $\Delta_0(\mathcal{J}_q) = \bar{\Delta}_0(\mathcal{J})$. Now let $e \in \mathbb{N}$ with $e > 0$ and $\mu \in \Delta_e(\mathcal{J}_q)$. Then there are $a_0, \dots, a_\ell \in \mathbb{N}$ with $a_\ell > 0$ such that $\mu = x_0^{a_0} \cdots x_\ell^{a_\ell}$. In case $a_j \geq q - 1$ for some $j \in \mathbb{N}$ with $j < \ell$, then

$$\text{lm}(\Phi_{j\ell}) = x_j^q x_\ell \mid \mu \quad \text{and hence} \quad \mu = \text{lm}(\phi) \quad \text{for some } \phi \in \mathcal{J}_q.$$

This shows that μ is reduced, i.e., $\mu \in \overline{\mathbb{M}}_e$. Further, if $\text{lm}(\overline{F}) \mid \mu$ for some homogeneous $F \in \mathcal{J}$ with $\overline{F} \neq 0$, then $\mu = \nu \text{lm}(\overline{F}) = \text{lm}(\nu \overline{F})$ for some $\nu \in \overline{\mathbb{M}}$. But since $F \in \mathcal{J}$ and $F - \overline{F} \in \Gamma_q(k)$, we find $\overline{F} \in \mathcal{J}_q$. Thus we obtain a contradiction to the assumption that $\mu \in \Delta_e(\mathcal{J}_q)$. This proves that $\Delta_e(\mathcal{J}_q) \subseteq \overline{\Delta}_e(\mathcal{J})$. \square

The result that was alluded to at the beginning of this subsection is now an easy consequence of the above lemma and the projective \mathbb{F}_q -footprint formula.

Theorem 3.12 (Projective \mathbb{F}_q -Footprint Bound) *Let k be an algebraic closure of \mathbb{F}_q and let F_1, \dots, F_r be any homogeneous polynomials in $k[x_0, \dots, x_m]$. Also, let $\mathcal{X} = V(F_1, \dots, F_r)$ be the corresponding projective variety in $\mathbb{P}^m(k)$. Then*

$$|\mathcal{X}(\mathbb{F}_q)| \leq |\overline{\Delta}_e(F_1, \dots, F_r)| \quad \text{for all } e \gg 0. \quad (12)$$

Proof Let \mathcal{J} be the ideal of $k[x_0, \dots, x_m]$ generated by F_1, \dots, F_r , and let $\mathcal{J}_q := \mathcal{J} + \Gamma_q(k)$. Then $\mathcal{X} = V(\mathcal{J})$. So by Theorem 3.7, Lemma 3.11 and (11), we obtain

$$|\mathcal{X}(\mathbb{F}_q)| = |\Delta_e(\mathcal{J}_q)| = |\overline{\Delta}_e(\mathcal{J})| \leq |\overline{\Delta}_e(F_1, \dots, F_r)| \quad \text{for all } e \gg 0,$$

as desired. \square

Remark 3.13 The efficacy of the bound in (12) and the ease of computing the projective \mathbb{F}_q -footprint often depends on the choice of the homogeneous polynomials F_1, \dots, F_r whose common zeros determine the \mathbb{F}_q -rational points of the projective variety \mathcal{X} . We remark that it is always possible to choose F_1, \dots, F_r such that:

- F_i is projectively reduced for each $i = 1, \dots, r$.
- $\deg F_i \leq (m+1)(q-1)$ for all $i = 1, \dots, r$.
- F_1, \dots, F_r are linearly independent (over k).
- $\text{lm}(F_1), \dots, \text{lm}(F_r)$ are distinct.

To see this, first note that since $F_i - \overline{F}_i \in \Gamma_q(k)$ for each $i = 1, \dots, r$, the \mathbb{F}_q -rational points of $V(F_1, \dots, F_r)$ and $V(\overline{F}_1, \dots, \overline{F}_r)$ coincide. Thus, replacing F_i by \overline{F}_i , we may assume that each of F_1, \dots, F_r is projectively reduced. Next, if some F_i is homogeneous of degree $\geq (m+1)(q-1) + 1$, then every monomial $\mu = x_0^{a_0} \cdots x_m^{a_m}$ appearing in F_i , we must have $a_j \geq q$ for some j (depending on μ) with $0 \leq j \leq m$. Replacing the exponent a_j by $a_j - (q-1)$ will result in a homogeneous polynomial G_i of degree $\deg F_i - q + 1$ that has exactly the same \mathbb{F}_q -rational zeros as F_i . Again if $\deg G_i \geq (m+1)(q-1) + 1$, then this process can be continued. Thus, we can assume, without loss of generality, that $\deg F_i \leq (m+1)(q-1)$ for $i = 1, \dots, r$. Further, if F_1, \dots, F_r are linearly dependent, then one of them, say F_r is a k -linear combination of others, and hence $V(F_1, \dots, F_r) = V(F_1, \dots, F_{r-1})$. Thus it is clear that we may assume F_1, \dots, F_r to be linearly independent. Finally, if two or more of the polynomials have the same leading monomials, then we can use the division algorithm to replace F_1, \dots, F_r by G_1, \dots, G_r obtained by suitable linear combinations of F_1, \dots, F_r such that $V(F_1, \dots, F_r) = V(G_1, \dots, G_r)$ and $\text{lm}(G_1), \dots, \text{lm}(G_r)$ are distinct. Note that G_1, \dots, G_r continue to possess the properties previously arranged for F_1, \dots, F_r , i.e., they are projectively reduced, linearly independent homogeneous polynomials of degree $\leq (m+1)(q-1)$.

Remark 3.14 We remark that the projective \mathbb{F}_q -footprint bound for the number of \mathbb{F}_q -rational points of a projective variety $\mathcal{X} = V(F_1, \dots, F_r)$ in $\mathbb{P}^m(k)$ is usually superior to the bound

obtained from regarding \mathcal{X} as an affine cone, say \mathcal{Z} , in $\mathbb{A}^{m+1}(k)$ and using the affine \mathbb{F}_q -footprint bound. For example, if $q = 5$, and $F_1, F_2 \in \mathbb{F}_5[x_0, x_1, x_2]$ are homogeneous polynomials of degree 5 such that $\text{lm}(F_1) = x_0^4 x_1$ and $\text{lm}(F_2) = x_0^2 x_1^3$, then for the cone $\mathcal{Z} = Z(F_1, F_2)$ in \mathbb{A}^3 , the affine \mathbb{F}_5 -footprint bound $|\overline{\Delta}(F_1, F_2)|$ works out to be 85, which implies that the number of \mathbb{F}_5 -rational points of the projective variety $\mathcal{X} = V(F_1, F_2)$ in \mathbb{P}^2 is bounded above by $(85 - 1)/(5 - 1)$, which is 21. On the other hand, for $e \gg 0$, the projective footprint bound $|\overline{\Delta}_e(F_1, F_2)|$ is 20. The details of calculations are left to the reader.

4 Serre's Inequality

In this section we will show that Serre's inequality, as stated in equation (1), is an easy consequence of the projective \mathbb{F}_q -footprint bound. To this end, we will first compute the cardinality of projective \mathbb{F}_q -shadows of all possible leading monomials of nonzero homogeneous polynomial of degree $d \leq q$. Note that since $d \leq q$ any such polynomial is necessarily projectively reduced.

Lemma 4.1 *Let $d \in \mathbb{N}$ with $1 \leq d \leq q$ and let $\nu = x_0^{b_0} \cdots x_\ell^{b_\ell} \in \mathbb{M}_d$, where $0 \leq \ell \leq m$ and $b_0, \dots, b_\ell \in \mathbb{N}$ with $b_\ell > 0$. Then*

$$|\nabla_e^q(\nu)| = (q - b_0) \cdots (q - b_{\ell-1})(1 + (q - b_\ell)p_{m-\ell-1}) \quad \text{for all } e \gg 0.$$

Proof Note that $\bar{\nu} = \nu$ and thus $\overline{\nabla}_e(\nu) = \{\mu \in \overline{\mathbb{M}}_e : \nu \mid \mu\}$ for any $e \in \mathbb{N}$. We will use the decomposition (5). First, note that if $0 \leq j < \ell$, then the variable x_ℓ does not occur with positive exponent in any of the monomials in $\overline{\mathbb{M}}_e^{(j)}$. Hence

$$\overline{\nabla}_e(\nu) \cap \overline{\mathbb{M}}_e^{(j)} = \emptyset \quad \text{and so} \quad |\overline{\nabla}_e(\nu) \cap \overline{\mathbb{M}}_e^{(j)}| = 0, \quad \text{for } 0 \leq j < \ell \quad \text{and any } e \in \mathbb{N}.$$

Next, we observe that for $e \gg 0$, a monomial $\mu = x_0^{a_0} \cdots x_\ell^{a_\ell} \in \overline{\mathbb{M}}_e^{(\ell)}$ is in $\overline{\nabla}_e(\nu)$ if and only if $b_i \leq a_i \leq q - 1$ for $i = 0, \dots, \ell - 1$ because $b_\ell \leq a_\ell$ is automatically satisfied for sufficiently large e . Hence

$$|\overline{\nabla}_e(\nu) \cap \overline{\mathbb{M}}_e^{(\ell)}| = (q - b_0) \cdots (q - b_{\ell-1}) \quad \text{for all } e \gg 0.$$

Finally, if $\ell < j \leq m$, then $\mu = x_0^{a_0} \cdots x_j^{a_j} \in \overline{\mathbb{M}}_e^{(j)}$ is in $\overline{\nabla}_e(\nu)$ if and only if $b_i \leq a_i \leq q - 1$ for $i = 0, \dots, \ell$ and $0 \leq a_i \leq q - 1$ for $i = \ell + 1, \dots, j - 1$. Hence

$$|\overline{\nabla}_e(\nu) \cap \overline{\mathbb{M}}_e^{(j)}| = (q - b_0) \cdots (q - b_\ell) q^{j-\ell-1}, \quad \text{for } \ell < j \leq m \quad \text{and any } e \in \mathbb{N}.$$

Since $\overline{\mathbb{M}}_e$ is the disjoint union of $\overline{\mathbb{M}}_e^{(0)}, \dots, \overline{\mathbb{M}}_e^{(m)}$, we conclude that

$$|\overline{\nabla}_e(\nu)| = (q - b_0) \cdots (q - b_{\ell-1}) + (q - b_0) \cdots (q - b_\ell)(1 + q + \cdots + q^{m-\ell-1})$$

and the lemma follows. \square

Proposition 4.2 (Serre's inequality) *Let $F \in \mathbb{F}_q[x_0, \dots, x_m]$ be a nonzero homogeneous polynomial of degree $d \leq q$ and let $\mathcal{X} = V(F)$. Then*

$$|\mathcal{X}(\mathbb{F}_q)| \leq dq^{m-1} + p_{m-2}.$$

Proof If \mathcal{X} is contained in a hyperplane, then $|\mathcal{X}(\mathbb{F}_q)| \leq p_{m-1} \leq dq^{m-1} + p_{m-2}$, which proves Serre's inequality. In particular, this settles the case $d \leq 1$. Therefore we now assume that $2 \leq d \leq q$ and that \mathcal{X} contains $m + 1$ points in general position. After a projective linear transformation, we may moreover assume that \mathcal{X} contains the $m + 1$ points \mathbf{e}_j ($0 \leq j \leq m$) whose homogeneous coordinates have 1 in the j^{th} position and 0 elsewhere. This implies that

the monomials of the form x_j^d ($0 \leq j \leq m$) do not occur in F . Hence there are $s, \ell, b_s, \dots, b_\ell \in \mathbb{N}$ such that

$$\nu := \text{lm}(F) = x_s^{b_s} \cdots x_\ell^{b_\ell}, \quad 0 \leq s < \ell \leq m, \quad 0 < b_s < d, \quad 0 < b_\ell < d \quad \text{and} \quad \sum_{j=s}^{\ell} b_j = d.$$

If $\ell > s + 1$, then consider $\nu_1 := x_s^{b_s} \cdots x_{\ell-2}^{b_{\ell-2}} x_{\ell-1}^{b_{\ell-1} + b_\ell}$ and note that by Lemma 4.1,

$$\begin{aligned} |\overline{\nabla}_e(\nu)| - |\overline{\nabla}_e(\nu_1)| &= N((q - b_{\ell-1})(1 + (q - b_\ell)p_{m-\ell-1}) - 1 - (q - b_{\ell-1} - b_\ell)p_{m-\ell}) \\ &= N(b_{\ell-1}b_\ell p_{m-\ell-1} + b_\ell - 1) \geq 0 \quad \text{for all } e \gg 0, \end{aligned}$$

where $N := (q - b_0) \cdots (q - b_{\ell-2})$ and we have used the fact that $p_{m-\ell} = qp_{m-\ell-1} + 1$. If $\ell > s + 2$, then we consider $\nu_2 := x_s^{b_s} \cdots x_{\ell-2}^{b_{\ell-2} + b_{\ell-1} + b_\ell}$, and in a similar way, we obtain $|\overline{\nabla}_e(\nu_1)| - |\overline{\nabla}_e(\nu_2)| \geq 0$ for all $e \gg 0$. Continuing in this way, we see that

$$|\overline{\nabla}_e(\nu)| - |\overline{\nabla}_e(x_s^{b_s} x_{s+1}^{d-b_s})| \geq 0 \quad \text{for all } e \gg 0. \quad (13)$$

Moreover, applying Lemma 4.1 once again, we obtain

$$|\overline{\nabla}_e(x_s^{b_s} x_{s+1}^{d-b_s})| = q^s (q - b_s) (1 + (q - d + b_s) p_{m-s-2}) \quad \text{for all } e \gg 0. \quad (14)$$

Now by the projective \mathbb{F}_q -footprint bound (Theorem 3.12) and the observation in Section 2.1 that $|\overline{\mathbb{M}}_e| = p_m$ for $e \gg 0$, Serre's inequality (1) is proved if we show that

$$|\overline{\nabla}_e(\nu)| \geq p_m - (dq^{m-1} + p_{m-2}) = (q - d + 1)q^{m-1} \quad \text{for all } e \gg 0. \quad (15)$$

Thus, by (13), (14) and (15), it suffices to show that the difference

$$q^s (q - b_s) (1 + (q - d + b_s) p_{m-s-2}) - (q - d + 1) q^{m-1}$$

is nonnegative. But an easy calculation shows that this difference is equal to

$$q^{m-s-1} (a_s - 1) (d - a_s - 1) + (q - a_s) (d - a_s - 1),$$

which is clearly nonnegative, since $0 < a_s < d \leq q$. \square

Since example of homogeneous polynomials of degree $d \leq q$ attaining the Serre bound (1) are easy to construct (e.g., $F(x_0, \dots, x_m) := (x_1 - a_1 x_0) \cdots (x_1 - a_d x_0)$, where a_1, \dots, a_d are distinct elements of \mathbb{F}_q), the above proposition shows that $e_1(d, m) = dq^{m-1} + p_{m-2}$ for $d \leq q$. It would be interesting if one can also determine $e_r(d, m)$ explicitly for every $r > 1$ and $d \leq q$. While this is open, in general, we refer to [5] and the references therein for some recent results in this direction.

Acknowledgements Peter Beelen would like to thank IIT Bombay where large parts of this work were carried out when he was there in January 2017 as a Visiting Professor. Sudhir Ghorpade would like to thank the Technical University of Denmark for a visit of 11 days in June 2017 when some of this work was done.

References

- [1] Becker, T., Weispfenning, V.: Gröbner Bases: A Computational Approach to Commutative Algebra, Springer-Verlag, Berlin, 1998
- [2] Beelen, P., Ghorpade, S. R., Höholdt, T.: Duals of affine Grassmann codes and their relatives. *IEEE Trans. Inform. Theory*, **58**, 3843–3855 (2012)

- [3] Beelen, P., Datta, M.: Generalized Hamming weights of affine cartesian codes. *Finite Fields Appl.*, **51**, 130–145 (2018)
- [4] Beelen, P., Datta, M., Ghorpade, S. R.: Maximum number of common zeros of homogeneous polynomial equations over finite fields. *Proc. Amer. Math. Soc.*, **146**, 1451–1468 (2018)
- [5] Beelen, P., Datta, M., Ghorpade, S. R.: A combinatorial approach to the number of solutions of systems of homogeneous polynomial equations over finite fields, arXiv:1807.01683 [math.AG]
- [6] Carvalho, C., Neumann, V. G. L., Lopez, H. H.: Projective nested cartesian codes. *Bull. Braz. Math. Soc.*, **48**, 283–302 (2017)
- [7] Cox, D., Little, J., O’Shea, D.: *Ideals, Varieties, and Algorithms*, 3rd Ed., Springer, New York, 1992
- [8] Couvreur, A.: An upper bound on the number of rational points of arbitrary projective varieties over finite fields. *Proc. Amer. Math. Soc.*, **144**, 3671–3685 (2016)
- [9] Datta, M., Ghorpade, S. R.: On a conjecture of Tsfasman and an inequality of Serre for the number of points on hypersurfaces over finite fields. *Mosc. Math. J.*, **15**, 715–725 (2015)
- [10] Datta, M., Ghorpade, S. R.: Number of solutions of systems of homogeneous polynomial equations over finite fields. *Proc. Amer. Math. Soc.*, **145**, 525–541 (2017)
- [11] Fitzgerald, J., Lax, R. F.: Decoding affine variety codes using Gröbner bases. *Des. Codes Cryptogr.*, **13**, 147–158 (1998)
- [12] Geil, O., Høholdt, T.: Footprints or generalized Bezout’s theorem. *IEEE Trans. Inform. Theory*, **46**, 635–641 (2000)
- [13] Geil, O., Martin, S.: Relative generalized Hamming weights of q -ary Reed–Muller codes. *Adv. Math. Commun.*, **11**, 503–531 (2017)
- [14] Ghorpade, S. R.: A note on Nullstellensatz over finite fields, arXiv:1806.09489 [math.AC]
- [15] Ghorpade, S. R., Lachaud, G.: Number of solutions of equations over finite fields and a conjecture of Lang and Weil, in *Number Theory and Discrete Mathematics*, pp. 269–291, Birkhäuser, Basel, 2002
- [16] González-Sarabia, M., Martínez-Bernal, J., Villarreal, R. H., et al.: Generalized minimum distance functions, arXiv.math:1707.03285v3 [math.AC]
- [17] Hartshorne, R.: *Algebraic Geometry*, Graduate Texts in Math. No. 52. Springer-Verlag, New York, 1977
- [18] Heijnen, P., Pellikaan, R.: Generalized Hamming weights of q -ary Reed–Muller codes. *IEEE Trans. Inform. Theory*, **44**, 181–196 (1998)
- [19] Høholdt, T.: On (or in) Dick Blahut’s footprint, in *Codes, Curves and Signals*, pp. 3–9, Kluwer, Norwell, MA, 1998
- [20] Joly, J. R.: Équations et variétés algébriques sur un corps fini. *Enseign. Math.*, **19**, 1–117 (1973)
- [21] Mercier, D. J., Rolland, R.: Polynômes homogènes qui s’annulent sur l’espace projectif $\mathbb{P}^m(\mathbb{F}_q)$. *J. Pure Appl. Algebra*, **124**, 227–240 (1998)
- [22] Serre, J. P.: Lettre à M. Tsfasman, Journées Arithmétiques (Luminy, 1989). *Astérisque* No. 198–200, 351–353 (1991)
- [23] Sørensen, A. B.: Projective Reed–Muller codes. *IEEE Trans. Inform. Theory*, **37**, 1567–1576 (1991)
- [24] Terjanian, G.: Sur les corps finis. *C. R. Acad. Sci. Paris Sér. A-B*, **262**, A167–A169 (1966)