Contemporary Mathematics
Volume **738**, 2019
https://doi.org/10.1090/conm/738/14876

A note on Nullstellensatz over finite fields

Sudhir R. Ghorpade

Abstract. We give an expository account of Nullstellensatz-like results when the base field is finite. In particular, we discuss the vanishing ideal of the affine space and of the projective space over a finite field. As an application, we include an alternative proof of Ore's inequality for the number of points of affine hypersurfaces over finite fields.

1. Introduction

Hilbert's Nullstellensatz, or Hilbert's Zero Point Theorem, is a classical result of fundamental importance in commutative algebra and algebraic geometry. This result is only valid when the base field is $\mathbb{C}$, the field of complex numbers, or more generally an algebraically closed field. In fact, when the base field is $\mathbb{C}$, it can be viewed as a remarkable generalization of the Fundamental Theorem of Algebra. There are two versions, commonly known as Weak Nullstellensatz and Strong Nullstellensatz, which can be stated as follows.

Weak Nullstellensatz: Let k be an algebraically closed field. If I is a nonunit ideal of the polynomial ring $k[X_1, \ldots, X_n]$, then I has a 'zero', i.e., there exists $(\alpha_1, \ldots, \alpha_n) \in k^n$ such that $f(\alpha_1, \ldots, \alpha_n) = 0$, for each $f \in I$.

This result is usually deduced from the assertion, also referred to as a Nullstellensatz, that every maximal ideal of $k[X_1, \ldots, X_n]$ is of the form $(X_1 - \alpha_1, \ldots, X_n - \alpha_n)$ for some $\alpha_1, \ldots, \alpha_n \in k$, provided of course k is algebraically closed. On the other hand, the Weak Nullstellensatz together with a well-known "trick of Rabinowitsch", implies the following version.

Strong Nullstellensatz: Let k be an algebraically closed field and let $f_1, \ldots, f_m$ be any polynomials in $k[X_1, \ldots, X_n]$. If $f \in k[X_1, \ldots, X_n]$ is such that f vanishes at every common zero in k^n of $f_1, \ldots, f_m$, then

$$f^r = g_1 f_1 + \cdots + g_m f_m \quad \text{for some } g_1, \ldots, g_m \in k[X_1, \ldots, X_n] \text{ and } r \geq 0.$$

The above statement is close to the original version of the theorem as it appears in Hilbert's 1893 paper [**11**, §3] on the complete systems of invariants. Hilbert calls this a *third general theorem in the theory of algebraic functions, continuing*

2010 *Mathematics Subject Classification.* 14G15, 11T06, 13B25, 11G25, 14G05.

Key words and phrases. Nullstellensatz, finite field, vanishing ideal, affine space, projective space, footprint.

Partially supported by the DST-RCN grant INT/NOR/RCN/ICT/P-03/2018 from the Dept. of Science & Technology, Govt. of India, MATRICS grant MTR/2018/000369 from the Science and Engg. Research Board, Govt. of India, and IRCC Award grant 12IRAWD009 from IIT Bombay.

©2019 American Mathematical Society

This is a free offprint provided to the author by the publisher. Copyright restrictions may apply.

Theorems I and III of his 1890 paper [**10**, §I, III] on the theory of algebraic forms. These latter theorems being what we now call Hilbert's basis theorem and Hilbert's syzygy theorem. A translation into English of Hilbert's papers on invariant theory is now available (cf. [**12**]) and one can access more easily the writings of a master. Nowadays, (Strong) Nullstellensatz is more commonly stated in the language of vanishing ideals of affine algebraic varieties and we recall this version in § 2.1 below. We also recall analogous result for projective varieties that one calls Projective Nullstellensatz. Most modern textbooks on commutative algebra contain a proof of Hilbert's Nullstellensatz, and we refer to Eisenbud's book [**8**] which has five different proofs, and to [**1**, **17**, **19**, **24**] for a sampling of alternative proofs. See also the article by Goel, Patil and Verma [**9**] in this volume and the older article by Laksov [**15**] where some variations of Hilbert's Nullstellensatz are discussed.

A trivial consequence of Strong Nullstellensatz is that if k is an algebraically closed field and if $f \in k[X_1, \ldots, X_n]$ vanishes on all of k^n, then f is the zero polynomial. We will refer to it as **Very Weak Nullstellensatz**, or in short, **VWN**. To deduce it from Strong Nullstellensatz, it suffices to take $m = 1$ and f_1 to be the zero polynomial. The VWN is, in fact, valid if k is any infinite field, and can be proved easily using induction on n and noting that a polynomial in one variable of degree d with coefficients in a field k has at most d roots in k.

On the other hand, even the VWN is not true if the base field is finite, say the finite field $\mathbb{F}_q$ with q elements. Indeed, there are nonzero polynomials such as $X_i^q - X_i$ that vanish on all of $\mathbb{F}_q^n$. Nonetheless one has the following result, which may be viewed as an analogue of (Very Weak) Nullstellensatz over finite fields.

Affine $\mathbb{F}_q$-Nullstellensatz: Let $f \in \mathbb{F}_q[X_1, \ldots, X_n]$ and let Γ_q denote the ideal of $\mathbb{F}_q[X_1, \ldots, X_n]$ generated by $X_1^q - X_1, \ldots, X_n^q - X_n$. Then:

(i) f vanishes at every point of $\mathbb{F}_q^n$ if and only if $f \in \Gamma_q$.

(ii) Let $f_1, \ldots, f_m$ be polynomials in $\mathbb{F}_q[X_1, \ldots, X_n]$. If f vanishes at every common zero of $f_1, \ldots, f_m$ in $\mathbb{F}_q^n$, then

$$f = g_1 f_1 + \cdots + g_m f_m + \gamma \quad \text{for some } g_1, \ldots, g_m \in \mathbb{F}_q[X_1, \ldots, X_n] \text{ and } \gamma \in \Gamma_q.$$

Note that (i) is a special case of (ii) and also that in (ii), one doesn't have to take a power of f (unlike in Strong Nullstellensatz). In other words, if I is an ideal of $\mathbb{F}_q[X_1, \ldots, X_n]$, then $I + \Gamma_q$ is automatically a radical ideal of $\mathbb{F}_q[X_1, \ldots, X_n]$. The above result is not new and goes back at least to Terjanian [**23**]. An excellent account is available in the article (in French) of Joly [**13**]; see also Delsarte, Goethals, and MacWilliams[**7**, § 1]. A more modern reference is Kreuzer and Robbiano [**14**, § 6.2A]. However, in the experience of the author, the result is not as widely known as it should be. Moreover, an analogue of (i) in the projective case that gives an explicit description of homogeneous polynomials that vanish on all of $\mathbb{P}^n(\mathbb{F}_q)$, appears to be known to even fewer algebraists. This is of a relatively recent vintage and may be attributed to Mercier and Rolland [**18**] (see also Remark 3.4). We thus provide in this article a self-contained account of these Nullstellensatz-like results in the setting of finite fields. Our proof of the projective analogue of (i) above uses the notion of projective reduction developed in [**3**] and is a little simpler than the original proof of Mercier and Rolland. We will also point out that a straightforward analgoue of (ii) in the projective case is not possible. In the affine case, the Affine $\mathbb{F}_q$-Nullstellensatz can be useful to deduce the so called affine $\mathbb{F}_q$-footprint bound for estimating the number of $\mathbb{F}_q$-rational points of affine algebraic

This is a free offprint provided to the author by the publisher. Copyright restrictions may apply.

varieties defined over $\mathbb{F}_q$. We outline this and show how such a bound can be used to deduce a classical inequality for the number of points of affine hypersurfaces defined over $\mathbb{F}_q$.

As indicated in the abstract, this is an expository article, and we have made an attempt to keep it fairly self-contained. The results given here are not new, but are somewhat scattered in the literature not all of which is easily available in English. The proofs given here of some of the results (especially in Section 3) appear to be simpler and more natural than those available elsewhere in the literature.

2. The Affine Case

In the first subsection, we set up some basic notation and recall preliminaries about affine varieties. The notion of reduced polynomials is discussed in the next subsection and a couple of auxiliary results are proved here. These are then used in § 2.3 to prove the result described in the Introduction as the Affine $\mathbb{F}_q$- Nullstellensatz, and, in fact, a slightly more general version of it. Finally, in § 2.4, we give an application to a classical inequality due to Ore. Our exposition in subsections 2.2 and 2.3 closely follows Joly [**13**, Ch. 2], while the proof of Lemma 2.6 in § 2.3 is adapated from Carvalho's notes [**4**, § 3].

2.1. Preliminaries. Let k be a field and let n be a nonnegative integer. Also, let $S := k[X_1, \ldots, X_n]$ be the ring of polynomials in n variables $X_1, \ldots, X_n$ with coefficients in k. We denote by $\mathbb{A}_k^n$ (or simply, $\mathbb{A}^n$ if the reference to k is clear from the context) the space of n-tuples of elements of k. Given any $I \subseteq S$, we let

$$\mathsf{Z}(I) := \{\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{A}_k^n : f(a_1, \ldots, a_n) = 0 \text{ for all } f \in I\}.$$

Given a subfield F of k, we call a subset Z of $\mathbb{A}_k^n$ an *affine algebraic variety* defined over F if $Z = \mathsf{Z}(I)$ for some $I \subseteq F[X_1, \ldots, X_n]$. This is equivalent to saying that $Z = \mathsf{Z}(I)$ for some ideal I of S generated by finitely many polynomials in $F[X_1, \ldots, X_n]$. If Z is an affine algebraic variety defined over F and if K is a field extension of F such that K is a subfield of an algebraic closure $\overline{k}$ of k (so that F, K and k are subfields of $\overline{k}$), then we denote by $Z(K)$ the set of K-rational points of Z, i.e., $Z(K) := \{\mathbf{a} \in \mathbb{A}_K^n : f(\mathbf{a}) = 0 \text{ for all } f \in I\}$. Given a subset Z of $\mathbb{A}_k^n$, we let

$$\mathsf{I}(Z) := \{f \in S : f(\mathbf{a}) = 0 \text{ for all } \mathbf{a} \in Z\},$$

and we note that $\mathsf{I}(Z)$ is an ideal of S; it is called the *vanishing ideal* of Z. It is not difficult to see that if Z is an affine algebraic variety defined over k, then $\mathsf{Z}(\mathsf{I}(Z)) = Z$. On the other hand, Strong Nullstellensatz can be stated as follows.

$$\mathsf{I}(\mathsf{Z}(I)) = \sqrt{I} \quad \text{if } k \text{ is algebraically closed and } I \text{ is any ideal of } S. \tag{2.1}$$

By considering an ideal I of S such that $\mathsf{Z}(I) = \emptyset$, we obtain the Weak Nullstellensatz, whereas by considering the special case $\mathsf{Z}(I) = \mathbb{A}_k^n$, we can deduce the VWN. As noted in the Introduction, the latter is valid (and rather easily proved) more generally when k is an infinite field that is not necessarily algebraically closed.

2.2. Reduction. Fix a finite field $\mathbb{F}_q$ with q elements (so that q is a prime power) and an algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$ (in fact, we can take $\overline{\mathbb{F}}_q$ to be $\cup_{n\geq 1}\mathbb{F}_{q^n}$). Let k be a subfield of $\overline{\mathbb{F}}_q$ containing $\mathbb{F}_q$ (or equivalently, k is an algebraic extension of $\mathbb{F}_q$). As before, let $S := k[X_1, \ldots, X_n]$.

A polynomial $f \in S$ is said to be *reduced* if $\deg_{X_i} f \leq q-1$ for each $i = 1, \ldots, n$. The set of all reduced polynomials in S will be denoted by $\mathfrak{R}$. Clearly, $\mathfrak{R}$ is a vector

This is a free offprint provided to the author by the publisher. Copyright restrictions may apply.

space over k and the monomials $X_1^{i_1} \cdots X_n^{i_n}$, where $0 \le i_j \le q-1$ for $j = 1, \ldots, n$, form a k-basis of $\mathfrak{R}$. In particular, $\dim \mathfrak{R} = q^n$. Note that if $n = 0$, then $\mathfrak{R} = S = k$.

LEMMA 2.1. *If $f \in \mathfrak{R}$ is such that $f(\mathbf{a}) = 0$ for all $\mathbf{a} \in \mathbb{A}^n(\mathbb{F}_q)$, then f is the zero polynomial. In other words, $\mathfrak{R} \cap \mathsf{I}(\mathbb{A}^n(\mathbb{F}_q)) = \{0\}$.*

PROOF. The case when $n = 0$ is trivial. Suppose $n > 0$ and the result holds for polynomials in $n-1$ variables. Let $f \in \mathfrak{R}$ be such that $f(\mathbf{a}) = 0$ for all $\mathbf{a} \in \mathbb{A}^n(\mathbb{F}_q)$. Since f is reduced, we can write $f = f(X_1, \ldots, X_n)$ as

$$f = f_0 X_n^{q-1} + f_1 X_n^{q-2} + \cdots + f_{q-1} \quad \text{where } f_i \in k[X_1, \ldots, X_{n-1}] \text{ for } i = 0, 1, \ldots, q-1.$$

Now for any fixed $(a_1, \ldots, a_{n-1}) \in \mathbb{A}^{n-1}(\mathbb{F}_q)$, the polynomial $f(a_1, \ldots, a_{n-1}, X_n)$ in $k[X_n]$ has degree $\le q-1$ and has at least q roots in k. Hence it must be the zero polynomial. Consequently, $f_i(a_1, \ldots, a_{n-1}) = 0$ for all $i = 0, 1, \ldots, q-1$ and $(a_1, \ldots, a_{n-1}) \in \mathbb{A}^{n-1}(\mathbb{F}_q)$. So by the induction hypothesis, each f_i is the zero polynomial, and therefore, so is f. □

Now let us define $\Gamma_q(k)$ to be the ideal of $S = k[X_1, \ldots, X_n]$ generated by $X_1^q - X_1, \ldots, X_n^q - X_n$. Clearly, $\Gamma_q(k) \subseteq \mathsf{I}(\mathbb{A}^n(\mathbb{F}_q))$, and so Lemma 2.1 implies that

$$\mathfrak{R} \cap \Gamma_q(k) = \{0\}. \tag{2.2}$$

LEMMA 2.2. *Every $f \in S$ can be uniquely written as $f = g + \gamma$ for some $g \in \mathfrak{R}$ and $\gamma \in \Gamma_q(k)$. In other words, $S = \mathfrak{R} \oplus \Gamma_q(k)$.*

PROOF. The uniqueness is clear from (2.2) since both $\mathfrak{R}$ and $\Gamma_q(k)$ are clearly vector spaces over k. To prove the existence, it suffices to take f to be a monomial, say $f = X_1^{i_1} \cdots X_n^{i_n}$. If f is not reduced, then $i_j \ge q$ for some $j \in \{1, \ldots, n\}$. Note that

$$X_j^{i_j} = X_j^{i_j - q}(X_j^q - X_j + X_j) \equiv X_j^{i_j - (q-1)} (\text{mod } \Gamma_q(k)).$$

Hence $f \equiv X_1^{i_1} \cdots X_{j-1}^{i_{j-1}} X_j^{i_j-(q-1)} X_{j+1}^{i_{j+1}} \cdots X_n^{i_n} (\text{mod } \Gamma_q(k))$. Continuing in this way, we see that $f \equiv g (\text{mod } \Gamma_q(k))$ for some reduced monomial g. □

2.3. Affine $\mathbb{F}_q$-Nullstellensatz. We will continue to use the notation and terminology in § 2.1 and § 2.2. The Affine $\mathbb{F}_q$-Nullstellensatz stated in the Introduction is a special case of the theorem below with $k = \mathbb{F}_q$, where $Z(\mathbb{F}_q)$ coincides with $Z(I)$.

THEOREM 2.3. *Let k be an algebraic extension of $\mathbb{F}_q$. Then:*

(i) $\mathsf{I}(\mathbb{A}^n(\mathbb{F}_q)) = \Gamma_q(k)$.

(ii) *If Z is an affine algebraic variety in $\mathbb{A}_k^n$ defined over $\mathbb{F}_q$ and $Z = \mathsf{Z}(I)$ for some ideal I of S generated by polynomials in $\mathbb{F}_q[X_1, \ldots, X_n]$, then*

$$\mathsf{I}(Z(\mathbb{F}_q)) = I + \Gamma_q(k).$$

PROOF. (i) The inclusion $\Gamma_q(k) \subseteq \mathsf{I}(\mathbb{A}^n(\mathbb{F}_q))$ is obvious. To prove the reverse inclusion, suppose $f \in \mathsf{I}(\mathbb{A}^n(\mathbb{F}_q))$. By Lemma 2.2, we can write $f = g + \gamma$ for some $g \in \mathfrak{R}$ and $\gamma \in \Gamma_q(k)$. But then $g = f - \gamma$ vanishes on $\mathbb{A}^n(\mathbb{F}_q)$ and so by Lemma 2.1, $g = 0$. Thus $f \in \Gamma_q(k)$.

(ii) Let I be an ideal of S generated by polynomials in $\mathbb{F}_q[X_1, \ldots, X_n]$ and let $Z = \mathsf{Z}(I)$. Evidently, $I + \Gamma_q(k) \subseteq \mathsf{I}(Z(\mathbb{F}_q))$. To prove the reverse inclusion, first note that by Hilbert basis theorem, $I = \langle f_1, \ldots, f_r \rangle$ for some $f_1, \ldots, f_r \in \mathbb{F}_q[X_1, \ldots, X_n]$. Let us consider

$$g := 1 - \left(1 - f_1^{q-1}\right) \cdots \left(1 - f_r^{q-1}\right) \quad \text{and} \quad h := 1 - g.$$

This is a free offprint provided to the author by the publisher. Copyright restrictions may apply.

It is clear that $g, h \in \mathbb{F}_q[X_1, \ldots, X_n]$ and $g \in I$. Moreover,

$$g(\mathbf{a}) = \begin{cases} 0 & \text{if } \mathbf{a} \in Z(\mathbb{F}_q) \\ 1 & \text{if } \mathbf{a} \in \mathbb{A}^n(\mathbb{F}_q) \setminus Z(\mathbb{F}_q) \end{cases} \quad \text{and} \quad h(\mathbf{a}) = \begin{cases} 1 & \text{if } \mathbf{a} \in Z(\mathbb{F}_q) \\ 0 & \text{if } \mathbf{a} \in \mathbb{A}^n(\mathbb{F}_q) \setminus Z(\mathbb{F}_q). \end{cases}$$

Now let $f \in \mathsf{I}(Z(\mathbb{F}_q))$. Then $fg \in I$ and $fh \in \mathsf{I}(\mathbb{A}^n(\mathbb{F}_q))$. Since $g + h = 1$, we see from (i) above that $f = fg + fh \in I + \Gamma_q(k)$. Thus $\mathsf{I}(Z(\mathbb{F}_q)) = I + \Gamma_q(k)$. □

REMARK 2.4. An immediate corollary of part (ii) of the above theorem is that for any ideal I of S generated by polynomials in $\mathbb{F}_q[X_1, \ldots, X_n]$, the ideal $I + \Gamma_q(k)$ is a radical ideal. This particular fact can also be deduced from Seidenberg's Lemma given in Article 92 of [**21**].

2.4. Application to Affine Hypersurfaces over Finite Fields. Let k be an arbitrary field and as before, let S denote the polynomial ring $k[X_1, \ldots, X_n]$. Also, let $\mathcal{M}$ denote the set of all monomials in S (including the constant monomial 1). Fix a monomial order on $\mathcal{M}$, i.e., a total order $\preccurlyeq$ on $\mathcal{M}$ satisfying (i) $1 \preccurlyeq \mu$ for all $\mu \in \mathcal{M}$ and (ii) $\mu_1 \preccurlyeq \mu_2 \Rightarrow \nu\mu_1 \preccurlyeq \nu\mu_2$ for all $\mu_1, \mu_2, \nu \in \mathcal{M}$. For $0 \neq f \in S$, let $\mathrm{in}_{\preccurlyeq}(f)$ denote the largest monomial (w.r.t. $\preccurlyeq$) appearing in f with a nonzero coefficient; this is called the *leading monomial* or the *initial monomial* of f (w.r.t. $\preccurlyeq$). For any subset I of S, define the *footprint* of I to be the set $\Delta(I)$ of all monomials in $\mathcal{M}$ that are not divisible by the leading monomials of any nonzero element of I, i.e.,

$$\Delta(I) := \{\mu \in \mathcal{M} : \mathrm{in}_{\preccurlyeq}(f) \nmid \mu \text{ for all } f \in I \text{ with } f \neq 0\}.$$

If $I \subseteq S$ is finite, say $I = \{f_1, \ldots, f_r\}$, then we may write $\Delta(I)$ as $\Delta(f_1, \ldots, f_r)$.

The following result due to Buchberger is classical and is easily derived from the division algorithm (w.r.t. $\preccurlyeq$) in S. See, for example, Prop. 1 in Ch. 5, § 3 of [**5**].

PROPOSITION 2.5. $\{\mu + I : \mu \in \Delta(I)\}$ is a k-basis of S/I for any ideal I of S.

We can use this and a variant of Lagrange interpolation to derive a useful bound for the number of $\mathbb{F}_q$-rational points of affine algebraic varieties defined over $\mathbb{F}_q$.

LEMMA 2.6 (Affine $\mathbb{F}_q$-Footprint Bound). *Let k be an algebraic extension of $\mathbb{F}_q$ and let I be an ideal of $S := k[X_1, \ldots, X_n]$ generated by some nonzero polynomials $f_1, \ldots, f_r \in \mathbb{F}_q[X_1, \ldots, X_n]$. Also let $Z = \mathsf{Z}(I)$ denote the corresponding affine algebraic variety in $\mathbb{A}^n_k$ defined over $\mathbb{F}_q$. Then*

$$|Z(\mathbb{F}_q)| \leq \left|\overline{\Delta}(f_1, \ldots, f_r)\right|,$$

where $\overline{\Delta}(f_1, \ldots, f_r) := \{\mu \in \mathcal{M} : \mu \text{ is reduced and } \mathrm{in}_{\preccurlyeq}(f_i) \nmid \mu \text{ for } i = 1, \ldots, r\}$.

PROOF. If $Z(\mathbb{F}_q)$ is empty, then there is nothing to prove. Thus, assume that $Z(\mathbb{F}_q)$ is nonempty. Let $I_q := I + \Gamma_q(k)$. Clearly, $Z(I_q) = Z(\mathbb{F}_q)$. Hence $Z(I_q)$ is a nonempty finite subset of $\mathbb{A}^n_k$; in particular, $I_q \neq S$. Write $Z(I_q) = \{\mathbf{a}_1, \ldots, \mathbf{a}_m\}$, where $\mathbf{a}_i \neq \mathbf{a}_j$ for $1 \leq i < j \leq m$. Write $\mathbf{a}_i = (a_{i1}, \ldots, a_{in})$ for $i = 1, \ldots, m$. Fix $i \in \{1, \ldots, m\}$. Then for each $j \in \{1, \ldots, m\}$ with $j \neq i$, there is $t_j \in \{1, \ldots, n\}$ such that $a_{it_j} \neq a_{jt_j}$. Consider

$$p_i(X_1, \ldots, X_n) = \prod_{\substack{1 \leq j \leq m \\ j \neq i}} \frac{X_{t_j} - a_{jt_j}}{a_{it_j} - a_{jt_j}}.$$

This is a free offprint provided to the author by the publisher. Copyright restrictions may apply.

The polynomials $p_1, \ldots, p_m \in \mathbb{F}_q[X_1, \ldots, X_n]$ thus obtained have the property that $p_i(\mathbf{a}_j) = \delta_{ij}$ for $i, j = 1, \ldots, m$. Moreover, $I_q = I(Z(\mathbb{F}_q))$, by part (ii) of Theorem 2.3. Hence if $\sum_{j=1}^{m} \lambda_j p_j \in I_q$ for some $\lambda_1, \ldots, \lambda_m \in k$, then by evaluating at $\mathbf{a}_i$, we obtain $\lambda_i = 0$ for $i = 1, \ldots, m$. It follows that $\{p_1 + I_q, \ldots, p_m + I_q\}$ is a k-linearly independent subset of S/I_q. Thus, by Proposition 2.5, we see that

$$|Z(\mathbb{F}_q)| = m \leq \dim_k S/I_q = |\Delta(I_q)| \leq |\Delta(f_1, \ldots, f_r, X_1^q - X_1, \ldots, X_n^q - X_n)|\,.$$

Finally, since $\mathrm{in}_{\preccurlyeq}(X_i^q - X_i) = X_i^q$ for each $i = 1, \ldots, n$, it is clear that $\mu \in \mathcal{M}$ is reduced if and only if $\mathrm{in}_{\preccurlyeq}(X_i^q - X_i) \nmid \mu$ for all $i = 1, \ldots, n$. This readily implies that $\Delta(f_1, \ldots, f_r, X_1^q - X_1, \ldots, X_n^q - X_n) = \overline{\Delta}(f_1, \ldots, f_r)$. □

As a corollary, we shall deduce an inequality that according to [**16**, p. 320], goes back at least to Ore (1922) and provides an effective bound on the number of $\mathbb{F}_q$-rational points of an affine hypersurface defined over $\mathbb{F}_q$ in terms of its degree. It can also be viewed as a multivariable generalization of the elementary fact that a univariate polynomial of degree d with coefficients in a field has at most d roots in that field. The generalization is of course possible when the base field is finite.

Corollary 2.7 (Ore's Inequality). Let $f \in \mathbb{F}_q[X_1, \ldots, X_n]$ be a nonzero polynomial of degree d and let $Z = Z(f)$ be the corresponding variety in $\mathbb{A}_k^n$, where k is any algebraic extension of $\mathbb{F}_q$. Then

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

Proof. The inequality is trivial if $d \geq q$ because then $dq^{n-1} \geq |\mathbb{A}^n(\mathbb{F}_q)| \geq |Z(\mathbb{F}_q)|$. Assume that $d < q$. This implies, in particular, that f is reduced. Fix a monomial order $\preccurlyeq$ on the set $\mathcal{M}$ of all monomials in $S := k[X_1, \ldots, X_n]$, and write $\mathrm{in}_{\preccurlyeq}(f) = X_1^{i_1} \cdots X_n^{i_n}$, where $i_1, \ldots, i_n$ are nonnegative integers such that $i_1 + \cdots + i_n \leq d$. Note that $0 \leq i_j \leq d \leq q - 1$ for $j = 1, \ldots, n$. By Lemma 2.6,

$$|Z(\mathbb{F}_q)| \leq |\overline{\Delta}(f)| = \left|\{\mu \in \mathcal{M} : \mu \text{ is reduced and } X_1^{i_1} \cdots X_n^{i_n} \nmid \mu\}\right|.$$

Now a monomial $\mu = X_1^{j_1} \cdots X_n^{j_n}$ is reduced and is divisible by $X_1^{i_1} \cdots X_n^{i_n}$ if and only if $i_t \leq j_t \leq q - 1$ for all $t = 1, \ldots, n$. The number of such monomials is therefore $(q - i_1) \cdots (q - i_n)$. An easy induction on n shows that

$$(q-i_1)\cdots(q-i_n) \geq q^n - (i_1 + \cdots + i_n)q^{n-1} \quad \text{whenever } 0 \leq i_j < q \text{ for } j = 1, \ldots, n.$$

Since the number of reduced monomials in $\mathcal{M}$ is clearly q^n, it follows that

$$|Z(\mathbb{F}_q)| \leq |\overline{\Delta}(f)| \leq q^n - \left(q^n - dq^{n-1}\right) = dq^{n-1},$$

where we have used the fact that $i_1 + \cdots + i_n \leq d$. □

3. Projective Version

In this section, we will try to develop projective analogues of the results in the first three subsections of Section 2. Our treatment will, in fact, be very parallel to that in §2.1-2.3.

This is a free offprint provided to the author by the publisher. Copyright restrictions may apply.

3.1. Preliminaries. Let k be a field. The projective n-space over k will be denoted by $\mathbb{P}^n_k$ and it is the set of equivalence classes of elements of the set $k^{n+1} \setminus \{\mathbf{0}\}$ w.r.t. the equivalence relation $\sim$ given by proportionality, i.e., for all $\mathbf{a} = (a_0, a_1, \ldots, a_n)$ and $\mathbf{b} = (b_0, b_1, \ldots, b_n)$ in $k^{n+1} \setminus \{\mathbf{0}\}$,

$$\mathbf{a} \sim \mathbf{b} \iff \text{there is } \lambda \in k \text{ such that } a_i = \lambda b_i \text{ for all } i = 0, 1, \ldots, n.$$

We may denote by $[a_0 : a_1 : \cdots : a_n]$ the equivalence class of $(a_0, a_1, \ldots, a_n)$ in $k^{n+1} \setminus \{\mathbf{0}\}$. We let $\mathcal{S}$ be the polynomial ring $k[X_0, X_1, \ldots, X_n]$ in $n+1$ variables. Given a subset $\mathcal{I}$ of $\mathcal{S}$ consisting of homogeneous polynomials, we let

$$\mathsf{V}(\mathcal{I}) := \{[a_0 : a_1 : \cdots : a_n] \in \mathbb{P}^n_k : f(a_0, a_1, \ldots, a_n) = 0 \text{ for all } f \in \mathcal{I}\}.$$

Given a subfield F of k, we call a subset V of $\mathbb{P}^n_k$ a *projective algebraic variety* defined over F if $V = \mathsf{V}(\mathcal{I})$ for some subset $\mathcal{I}$ of homogeneous polynomials in $F[X_0, X_1, \ldots, X_n]$. This is equivalent to saying that $V = \mathsf{V}(\mathcal{I})$ for some homogeneous ideal $\mathcal{I}$ of S generated by finitely many homogeneous polynomials in $F[X_0, X_1, \ldots, X_n]$. If V a projective algebraic variety defined over F and if K is a field extension of F such that K is a subfield of an algebraic closure $\overline{k}$ of k, then we denote by $V(K)$ the set of K-rational points of V, i.e.,

$$V(K) := \{[a_0 : \cdots : a_n] \in \mathbb{P}^n_K : f(a_0, \ldots, a_n) = 0 \text{ for all homogeneous } f \in \mathcal{I}\}.$$

Given a subset V of $\mathbb{P}^n_k$, the *vanishing ideal* of V is defined to be the ideal $\mathsf{I}(V)$ of $\mathcal{S}$ generated by the homogeneous polynomials in $\mathcal{S}$ that vanish at every point of V. It is not difficult to see that if V is any projective algebraic variety defined over k, then $\mathsf{V}(\mathsf{I}(V)) = V$, while the projective analogue of (2.1) is the following.

Projective Nullstellensatz: If k is algebraically closed and if $\mathcal{I}$ is any homogeneous ideal of $\mathcal{S}$, then $\sqrt{\mathcal{I}} \supseteq \langle X_0, X_1, \ldots, X_n\rangle$ if $\mathsf{V}(\mathcal{I})$ is empty, whereas $\mathsf{I}(\mathsf{V}(\mathcal{I})) = \sqrt{\mathcal{I}}$ if $\mathsf{V}(\mathcal{I})$ is nonempty.

In particular, we see that there are nonunit homogeneous ideals of $\mathcal{S}$ that have no 'zero' in $\mathbb{P}^n_k$, even when k is algebraically closed. Thus a straightforward analogue of the Weak Nullstellensatz isn't quite true for projective varieties. On the other hand, the other special case $\mathsf{V}(\mathcal{I}) = \mathbb{P}^n_k$ still yields the projective analogue of VWN, which says that if k is algebraically closed, then the only homogeneous polynomial that vanishes on all of $\mathbb{P}^n_k$ is the zero polynomial. As before, this is valid more generally (and proved rather easily) when k is any infinite field. But when k is a finite field, such a result is not true and we discuss next what happens in this case.

3.2. Projective reduction. We follow [**3**] to outline here a projective analogue of the notion of reduction that was discussed in § 2.2. In this section, let k be an algebraic extension of $\mathbb{F}_q$ and let $\mathcal{S} := k[X_0, X_1, \ldots, X_n]$. Given a nonnegative integer d, let $\mathcal{S}_d$ denote the set of homogeneous polynomials in $\mathcal{S}$ of degree d (including the zero polynomial). We will denote by $\mathbb{M}$ the set of all monomials in $\mathcal{S}$. A monomial $\mu \in \mathbb{M}$ is said to be *projectively reduced* if either $\mu = 1$ or $\mu \neq 1$ and $\deg_{X_i} \mu \leq q-1$ for $1 \leq i < \ell_\mu$, where ℓ_μ is the index of the last variable appearing in μ, i.e., $\ell_\mu := \max\{\ell \in \{0, 1, \ldots, n\} : X_\ell \mid \mu\}$. Given a nonnegative integer d, we let $\mathfrak{R}_d$ denote the set of k-linear combinations of projectively reduced monomials in $\mathbb{M}$ of degree d. Clearly $\mathfrak{R}_d$ is a finite dimensional vector space over k and its elements may be called projectively reduced homogeneous polynomials of degree d. The next two results are projective analogues of Lemmas 2.1 and 2.2.

This is a free offprint provided to the author by the publisher. Copyright restrictions may apply.

LEMMA 3.1. *Let d be a nonnegative integer. If $f \in \mathfrak{R}_d$ is such that $f(P) = 0$ for all $P \in \mathbb{P}^n(\mathbb{F}_q)$, then f is the zero polynomial. In other words, $\mathfrak{R}_d \cap \mathsf{I}(\mathbb{P}^n(\mathbb{F}_q)) = \{0\}$.*

PROOF. The case when $n = 0$ is trivial. Suppose $n > 0$ and the result holds for homogeneous polynomials of degree d in $k[X_0, X_1, \ldots, X_{n-1}]$. Let $f \in \mathfrak{R}_d \cap \mathsf{I}(\mathbb{P}^n(\mathbb{F}_q))$. By separating terms involving X_n, we can write

$$f(X_1, \ldots, X_n) = g(X_0, \ldots, X_{n-1}) + h(X_0, \ldots, X_n)$$

where $g \in k[X_0, \ldots, X_{n-1}]$ and $h \in k[X_0, \ldots, X_n]$ are homogeneous of degree d such that the last variable in each of the monomials appearing in h (with a nonzero coefficient) is X_n. Considering points $[a_0 : \cdots : a_n]$ of $\mathbb{P}^n(\mathbb{F}_q)$ such that $a_n = 0$, we deduce from the induction hypothesis that $g(X_0, \ldots, X_{n-1})$ is the zero polynomial. On the other hand, the dehomogenization $h(X_0, \ldots, X_{n-1}, 1)$ is a reduced (and not necessarily homogeneous) polynomial in $k[X_0, \ldots, X_{n-1}]$ that vanishes on $\mathbb{A}^n(\mathbb{F}_q)$. Hence by Lemma 2.1, $h(X_0, \ldots, X_{n-1}, 1)$ is the zero polynomial. Since h is a homogeneous polynomial divisible by X_n, it follows that h is also the zero polynomial. □

Now let us define $\Gamma_q^*(k)$ to be the ideal of $\mathcal{S}$ generated by the $\binom{n+1}{2}$ *Fermat polynomials* $X_i^q X_j - X_i X_j^q$, where $0 \le i < j \le n$. Clearly, $\Gamma_q^*(k)$ is a homogeneous ideal of $\mathcal{S}$ and $\Gamma_q^*(k) \subseteq \mathsf{I}(\mathbb{P}^n(\mathbb{F}_q))$. For any $d \ge 0$, we let $\Gamma_q^*(k)_d := \Gamma_q^*(k) \cap \mathcal{S}_d$. From Lemma 3.1, we see that

$$\mathfrak{R}_d \cap \Gamma_q^*(k)_d = \{0\} \quad \text{for every nonnegative integer } d. \tag{3.1}$$

LEMMA 3.2. *Let d be a nonnegative integer and let $f \in \mathcal{S}_d$. Then $f = g + \gamma$ for unique $g \in \mathfrak{R}_d$ and $\gamma \in \Gamma_q^*(k)_d$. Consequently, $\mathcal{S}_d = \mathfrak{R}_d \oplus \Gamma_q^*(k)_d$.*

PROOF. The uniqueness is clear from (3.1) since both $\mathfrak{R}_d$ and $\Gamma_q^*(k)_d$ are clearly vector spaces over k. To prove the existence, it suffices to take f to be a nonconstant monomial of degree d, say $f = X_0^{i_0} \cdots X_\ell^{i_\ell}$, where ℓ is the index of the last variable in f so that $i_\ell > 0$. If f is not projectively reduced, then $\ell \ge 1$ and $i_j \ge q$ for some $j \in \mathbb{Z}$ with $0 \le j < \ell$. Now observe that $X_j^{i_j} X_\ell^{i_\ell}$ can be written as

$$X_j^{i_j - q} X_\ell^{i_\ell - 1} \left(X_j^q X_\ell - X_j X_\ell^q + X_j X_\ell^q \right) \equiv X_j^{i_j - (q-1)} X_\ell^{i_\ell + (q-1)} (\text{mod } \Gamma_q^*(k)).$$

This implies that

$$f \equiv X_1^{i_1} \cdots X_{j-1}^{i_{j-1}} X_j^{i_j - (q-1)} X_{j+1}^{i_{j+1}} \cdots X_\ell^{i_\ell + (q-1)} (\text{mod } \Gamma_q^*(k)).$$

Continuing in this way, we see that $f \equiv g (\text{mod } \Gamma_q^*(k))$ for some projectively reduced monomial g of degree d. Moreover, $\gamma := f - g$ is necessarily a homogeneous polynomial in $\Gamma_q^*(k)$ of degree d. □

3.3. Vanishing Ideal of Projective Spaces over Finite Fields. We will continue to use the notation and terminology in § 3.1 and § 3.2. The following result is a slightly more general version of a theorem of Mercier and Rolland [**18**, Thm. 2.1]; in fact, it corresponds precisely to [**3**, Cor. 2.6]. The proof, however, is different from that in [**18**] or [**3**].

THEOREM 3.3. *Let k be an algebraic extension of $\mathbb{F}_q$. Then*

$$\mathsf{I}(\mathbb{P}^n(\mathbb{F}_q)) = \Gamma_q^*(k).$$

This is a free offprint provided to the author by the publisher. Copyright restrictions may apply.

PROOF. The inclusion $\Gamma_q^*(k) \subseteq \mathsf{I}(\mathbb{P}^n(\mathbb{F}_q))$ is obvious. For the reverse inclusion, let f be a homogeneous polynomial of degree d such that $f \in \mathsf{I}(\mathbb{P}^n(\mathbb{F}_q))$. By Lemma 3.2, we can write $f = g + \gamma$ for some $g \in \mathfrak{R}_d$ and $\gamma \in \Gamma_q^*(k)_d$. But then $g = f - \gamma$ vanishes on $\mathbb{P}^n(\mathbb{F}_q)$ and so by Lemma 3.1, $g = 0$. Thus $f \in \Gamma_q^*(k)$. □

REMARK 3.4. The result in Theorem 3.3 when $k = \mathbb{F}_q$ has been stated by Bayer-Fluckiger and Serre in [**2**, Lem. 7.2.4], where the proof is left to the reader. As noted earlier, a complete proof was given by Mercier and Rolland [**18**, Thm. 2.1]. Another proof that uses part (i) of Theorem 2.3 appears in the paper of Rentería and Tapia-Recillas [**20**, Prop. 8]. It may be noted that although [**20**] was published in 1997 and [**18**] in 1998, the former was received by the journal in March 1996 and the latter in January 1995. Moreover, [**18**] is included among the references of [**20**].

Unlike in the affine case, it is not true that if $\mathcal{I}$ is a homogeneous ideal of $\mathcal{S}$, then $\mathsf{I}(\mathsf{V}(\mathcal{I})) = \mathcal{I} + \Gamma_q^*(k)$. In fact, while $\mathsf{I}(\mathsf{V}(\mathcal{I}))$ is a radical ideal, the ideal $\mathcal{I} + \Gamma_q^*(k)$ need not be a radical ideal even when $\mathcal{I}$ is a radical ideal of $\mathcal{S}$. To illustrate this, we reproduce the following example from [**3**, Ex. 3.8].

EXAMPLE 3.5. Suppose $n = 1$ and $f(X_0, X_1) := X_0^q X_1 - X_0 X_1^q + X_0^{q+1}$. Consider the principal homogeneous ideal $\mathcal{I} = \langle f(X_0, X_1) \rangle$ of $k[X_0, X_1]$. Note that $\mathcal{I}$ is a radical ideal of $\mathcal{S} = k[X_0, X_1]$ because $\mathcal{S}$ 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, $\mathcal{I} + \Gamma_q^*(k) = \mathcal{I} + \langle X_0^q X_1 - X_0 X_1^q \rangle$ contains X_0^{q+1}, but does not contain X_0 (since every nonzero element of $\mathcal{I} + \Gamma_q^*(k)$ has degree $\geq q + 1$). Thus $\mathcal{I} + \Gamma_q^*(k)$ is not a radical ideal even though $\mathcal{I}$ is a radical ideal.

REMARK 3.6. The nonavailability of a straightforward analogue of part (ii) of Theorem 2.3 in the projective case makes it harder to find a suitable analogue of the affine $\mathbb{F}_q$-footprint bound (Lemma 2.6). Nonetheless, it is shown in [**3**] how a useful projective $\mathbb{F}_q$-footprint bound can be obtained, and as an application an inequality due to Serre for the number of points of projective hypersurfaces is deduced. This inequality is, in fact, a not-so-straightforward projective analogue of Ore's inequality given in Corollary 2.7; see [**6**] for more on this.

Acknowledgements

The author is grateful to Peter Beelen and Mrinmoy Datta for some helpful conversations related to the topics in this article.

References

[1] E. Arrondo, *Another elementary proof of the Nullstellensatz*, Amer. Math. Monthly **113** (2006), no. 2, 169–171, DOI 10.2307/27641869. MR2203239

[2] E. Bayer-Fluckiger and J.-P. Serre, *Torsions quadratiques et bases normales autoduales* (French), Amer. J. Math. **116** (1994), no. 1, 1–64, DOI 10.2307/2374981. MR1262426

[3] P. Beelen, M. Datta, and S. R. Ghorpade, *Vanishing ideals of projective spaces over finite fields and a projective footprint bound*, Acta Math. Sin. (Engl. Ser.) **35** (2019), no. 1, 47–63, DOI 10.1007/s10114-018-8024-7. MR3917991

[4] C. Carvalho, Applications of results from commutative algebra to the study of certain evaluation codes, Lecture notes of CIMPA Research School on Algebraic Methods in Coding Theory, Sao Paulo, Brazil, July 2017. https://www.ime.usp.br/∼cimpars/notes/sc4_01.pdf

This is a free offprint provided to the author by the publisher. Copyright restrictions may apply.

[5] D. Cox, J. Little, and D. O'Shea, *Ideals, varieties, and algorithms*: *An introduction to computational algebraic geometry and commutative algebra*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1992. MR1189133

[6] M. Datta and S. R. Ghorpade, *On a conjecture of Tsfasman and an inequality of Serre for the number of points of hypersurfaces over finite fields*, Mosc. Math. J. **15** (2015), no. 4, 715–725, DOI 10.17323/1609-4514-2015-15-4-715-725. MR3438829

[7] P. Delsarte, J.-M. Goethals, and F. J. MacWilliams, *On generalized Reed-Muller codes and their relatives*, Information and Control **16** (1970), 403–442. MR0274186

[8] D. Eisenbud, *Commutative algebra*: *With a view toward algebraic geometry*, Graduate Texts in Mathematics, vol. 150, Springer-Verlag, New York, 1995. MR1322960

[9] K. Goel, D. P. Patil, and J. K. Verma, Nullstellensätze and applications, `arXiv:1809.02818 [math.AC]`, Sept. 2018.

[10] D. Hilbert, *Ueber die Theorie der algebraischen Formen* (German), Math. Ann. **36** (1890), no. 4, 473–534, DOI 10.1007/BF01208503. MR1510634

[11] D. Hilbert, *Ueber die vollen Invariantensysteme* (German), Math. Ann. **42** (1893), no. 3, 313–373, DOI 10.1007/BF01444162. MR1510781

[12] D. Hilbert, *Hilbert's invariant theory papers*, Lie Groups: History, Frontiers and Applications, VIII, Math Sci Press, Brookline, Mass., 1978. Translated from the German by Michael Ackerman; With comments by Robert Hermann. MR512034

[13] J.-R. Joly, *Équations et variétés algébriques sur un corps fini* (French), Enseignement Math. (2) **19** (1973), 1–117. MR0327723

[14] M. Kreuzer and L. Robbiano, *Computational linear and commutative algebra*, Springer, Cham, 2016. MR3559741

[15] D. Laksov, *Radicals and Hilbert Nullstellensatz for not necessarily algebraically closed fields*, Enseign. Math. (2) **33** (1987), no. 3-4, 323–338. MR925995

[16] R. Lidl and H. Niederreiter, *Finite fields*, 2nd ed., Encyclopedia of Mathematics and its Applications, vol. 20, Cambridge University Press, Cambridge, 1997. MR1429394

[17] J. P. May, *Munshi's proof of the Nullstellensatz*, Amer. Math. Monthly **110** (2003), no. 2, 133–140, DOI 10.2307/3647772. MR1952440

[18] D.-J. Mercier and R. Rolland, *Polynômes homogènes qui s'annulent sur l'espace projectif* $\mathrm{P}^m(\mathbf{F}_q)$ (French, with French summary), J. Pure Appl. Algebra **124** (1998), no. 1-3, 227–240, DOI 10.1016/S0022-4049(96)00104-1. MR1600301

[19] R. Munshi, Hilbert's Nullstellensatz, *Bull. Bombay Math. Colloq.* **15** (1999), 20–24.

[20] C. Rentería and H. Tapia-Recillas, *Reed-Muller codes: an ideal theory approach*, Comm. Algebra **25** (1997), no. 2, 401–413, DOI 10.1080/00927879708825862. MR1428786

[21] A. Seidenberg, *Constructions in algebra*, Trans. Amer. Math. Soc. **197** (1974), 273–313, DOI 10.2307/1996938. MR0349648

[22] G. Stengle, *A nullstellensatz and a positivstellensatz in semialgebraic geometry*, Math. Ann. **207** (1974), 87–97, DOI 10.1007/BF01362149. MR0332747

[23] G. Terjanian, *Sur les corps finis* (French), C. R. Acad. Sci. Paris Sér. A-B **262** (1966), A167–A169. MR0194416

[24] O. Zariski, *A new proof of Hilbert's Nullstellensatz*, Bull. Amer. Math. Soc. **53** (1947), 362–368, DOI 10.1090/S0002-9904-1947-08801-7. MR0020075

Department of Mathematics, Indian Institute of Technology Bombay,
Powai, Mumbai 400076, India.
Email address: `srg@math.iitb.ac.in`

This is a free offprint provided to the author by the publisher. Copyright restrictions may apply.