On the Finite Field Nullstellensatz

E. Ballico

Dipartimento di Matematica
Università di Trento, 38050 Povo (TN), Italy
ballico@science.unitn.it

A. Cossidente

Dipartimento di Matematica
Università della Basilicata, 85100 Potenza, Italy
cossidente@unibas.it

Abstract

Let $X \subset \mathbf{P^n}$ be an irreducible projective variety defined over the finite field $\mathbf{F_q}$. We will say that X satisfies the property $FFN(k,q)$ (Finite Field Nullstellensatz of degree k over $\mathbf{F_q}$) if every homogeneous polynomial over $\mathbf{F_q}$ of degree k on $\mathbf{P^n}$ vanishing on $X(\mathbf{F_q})$ vanishes on X, that is, it vanishes at all points of X defined over the algebraic closure of $\mathbf{F_q}$. We study when $FFN(k,q)$ holds true for the Veronese embeddings of $\mathbf{P^m}$, the Segre varieties, the minimal degree rational scrolls and the linearly normal embeddings of smooth curves.

1 Introduction

Following [1], [5], [6], we give the following definition.

Definition 1.1 *Fix positive integers k and q, with q a power of a prime. Let $X \subset \mathbf{P^n}$ be an irreducible projective variety defined over the finite field $\mathbf{F_q}$.*

We will say that X satisfies $FFN(k,q)$ (Finite Field Nullstellensatz of degree k over $\mathbf{F_q}$) if every homogeneous polynomial over $\mathbf{F_q}$ of degree k on $\mathbf{P^n}$ vanishing on $X(\mathbf{F_q})$ vanishes on X, namely, it vanishes at all points of X defined over the algebraic closure of $\mathbf{F_q}$.

We stress that the truth of property $FFN(k,q)$ for a subvariety X of $\mathbf{P^n}$ does not depend on the choice of a system of homogeneous coordinates of $\mathbf{P^n}$, that is, it is not changed if we apply to X an invertible projective transformation defined over $\mathbf{F_q}$.

Since any projective space over $\mathbf{F_q}$ is the union of $q+1$ hyperplanes defined over $\mathbf{F_q}$, the property $FFN(k,q)$ is false for every proper subvariety X, if $k \geq q+1$.

The property $FFN(k,q)$ is true if X is a projective space embedded as a linear space, see [6, Ex. 1.1] and references therein.

The property $FFN(q-1,q)$ was proved for "most" quadric hypersurfaces in [1] (see [1, Theorem 2.11] for a more precise result), for Hermitian varieties in [5] and for Grassmannians in [6, Theorem 2].

Here, we will study the Veronese embeddings of a projective space (see Theorem 2.1), the Segre varieties (see Theorem 2.2) and the minimal degree scrolls (see Theorem 2.3). For the definitions (and more results) on the Veronese embeddings, Segre varieties and minimal degree scrolls, the reader is referred to the books [4] and [3].

The last section is devoted to a generalization of the property $FFN(k,q)$ to curves.

2 The main results

We start with proving the following theorem on Veronese varieties.

Theorem 2.1 *Fix positive integers d, m, k and q, with q a power of a prime. Let $X \subset \mathbf{P^n}$, $n := ((m+d)!/(m!d!)) - 1$, be the Veronese embedding of degree d of $\mathbf{P^m}$. Then X satisfies $FFN(k,q)$ if and only if $dk \leq q$.*

Proof. Call $z_0, \ldots, z_m$ the homogeneous coordinates in $\mathbf{P^m}$, and $x_0, \ldots, x_n$ the homogeneous coordinates in $\mathbf{P^n}$, such that each x_j represents a different degree d monomial in the variables $z_0, \ldots, z_m$.

First assume $dk < q$ and let $F(x_0, \ldots, x_n)$ be a homogeneous polynomial of degree k in $n+1$ variables defined over $\mathbf{F_q}$, and vanishing on $X(\mathbf{F_q})$.

Since the variables $x_0, \ldots, x_n$ are a basis of the vector space of all degree d homogeneous polynomials in $m+1$ variables, F defines a homogeneous polynomial G of degree dk vanishing at all points of $\mathbf{P^m}$, defined over $\mathbf{F_q}$. Since $dk \leq q$, we have $G = 0$ and hence $F|X$, the restriction of F to X, is zero.

Now, assume $dk > q$. Take a homogeneous polynomial G of degree dk on $\mathbf{P^m}$ vanishing at all points of $\mathbf{P^m}(\mathbf{F_q})$, but with $G \neq 0$. We may take as G a product of linear forms. Every monomial of degree dk in the variables $z_0, \ldots z_m$ may be represented (not uniquely) by a monomial of degree k in the variables $x_0, \ldots, x_n$.

Hence, we may associate to G a homogeneous polynomial of degree k, $F(x_0, \ldots, x_n)$, whose restriction to X induces G, and hence vanishes at each point of $X(\mathbf{F_q})$.

Since F induces G, we have $F \neq 0$, that is $FFN(k,q)$ is false for X. □

Next, we consider $FFN(k,q)$ for Segre varieties.

Theorem 2.2 *Fix positive integers q, r, s and m, with q a power of a prime, and set $m := rs + r + s$. Let $X := \mathbf{P^m} \times \mathbf{P^s} \subset \mathbf{P^n}$ be the Segre variety defined over $\mathbf{F_q}$. Then X satisfies $FFN(q,q)$.*

Proof. Let F be a homogeneous polynomial on $\mathbf{P^n}$ of degree $k \leq q$ vanishing on $X(\mathbf{F_q})$. Since any linear space defined over $\mathbf{F_q}$ satisfies $FFN(q,q)$, for every $P \in \mathbf{P^r}(\mathbf{F_q})$, it follows that the restriction of F to $\{P\} \times \mathbf{P^s}$ vanishes.

First assume $r = 1$ and F not does not vanish on X. Let S be the subvariety defined by F. We have seen that the hypersurface $S \cap X$ of X contains $q+1$ hypersurfaces of type $\{P\} \times \mathbf{P^s}$ with $P \in \mathbf{P^r}(\mathbf{F_q})$. Hence $F|X$ vanishes, as wanted.

Now, assume $r > 1$. By induction on r, we see that for every hyperplane H of $\mathbf{P^r}$ defined over $\mathbf{F_q}$, the polynomial F vanishes on $H \times \mathbf{P^s}$. This implies that $S \cap X$ is not a hypersurface of X, that is F vanishes on X. □

We conclude this section with the case of minimal degree scrolls.

Theorem 2.3 *Fix positive integers q, k, n and m, with $m < n$, $(n-m+1)k \leq q$ and q a power of a prime. Let $X \subset \mathbf{P^n}$ be a m-dimensional irreducible non-degenerate variety of minimal degree (that is, with degree $n-m+1$) defined over $\mathbf{F_q}$. Then X satisfies $FFN(k,q)$.*

Proof. If $m = 1$, then X is a normal rational curve and the result follows from Theorem 2.2.

Assume $m \geq 2$. If X is not smooth, then it is a cone (defined over $\mathbf{F_q}$) over a lower dimensional smooth minimal degree variety, say Y, spanning the linear space M, with $n-m = \dim(M) - \dim(Y) - 1$, and with as vertex a linear space V, defined over $\mathbf{F_q}$, with $\dim(V) = m - \dim(Y) - 1$. Taking a linear subspace complementary to V and defined over $\mathbf{F_q}$, we reduce to the case in which X is smooth.

Fix a degree k homogeneous polynomial F vanishing on $X(\mathbf{F_q})$. Assume $m = 2$, and take a hyperplane H defined over $\mathbf{F_q}$.

Either $X \cap H$ is a normal rational curve spanning H or $X \cap H$ is a nodal curve which is union of a line D and a normal rational curve C spanning a hyperplane H' of H, with $|C \cap D| = 1$.

If $X \cap H$ is smooth, we have that $F|H$, the restriction of F to H, vanishes by the case $m = 1$, and hence F is divided by the polynomial defining H.

We could check directly that $F|H \equiv 0$ even if $X \cap H$ is singular, but we do not need it to get $F = 0$, because there are more than k hyperplanes defined over $\mathbf{F_q}$ and with $X \cap H$ smooth.

Now, assume $m > 2$ and the result true for lower dimensional minimal degree varieties. Let H be a hyperplane defined over $\mathbf{F_q}$. It follows that $X \cap H$ is an irreducible $(m-1)$–dimensional minimal degree subvariety of H.

Hence, $F|H \equiv 0$ by the inductive hypothesis, and we obtain again $F = 0$.

3 Linearly normal smooth curves

In section 2, we considered the case of Veronese embeddings of $\mathbf{P^m}$ and of varieties containing many lines.

In this section, we will consider the case of curves, giving very strong generalizations of the $FFN(k,q)$ failure for Veronese embeddings of $\mathbf{P^1}$.

Let X be a smooth complete curve of genus $g \geq 0$ defined over $\mathbf{F_q}$. The property $FFN(k,q)$ may fail for X, because the number N of its rational points over $\mathbf{F_q}$ might be very small. We have a classical general estimate of N (Hasse–Weil theorem) and several improvements of this estimate, and hence, it is reasonable to give results on $FFN(k,q)$ for embeddings of X in terms of N.

Theorem 3.1 *Let X be a smooth complete curve of genus $g \geq 0$ defined over $\mathbf{F_q}$. Fix positive integers k, d, with $d \geq 2g+2$ and $kd+1-g > N$. Let L be a line bundle on X of degree d defined over $\mathbf{F_q}$. Let $h := X \subset \mathbf{P^n}$, $n = d-g$, be the embedding induced by the complete linear system $H^0(X,L)$. Then $FFN(k,q)$ fails for $h(X)$.*

Proof. Since $d \geq 2g+2$, by a theorem of Fujita, h is an embedding and $h(X)$ is projectively normal (see [2] for a proof in arbitrary characteristic). Since $N < kd+1-g$, there is a positive divisor $D \in |L^{\otimes k}|$ containing the sum of all points of $X(\mathbf{F_q})$.

Since $h(X)$ is projectively normal, there is a degree k hypersurface F of $\mathbf{P^n}$, with $F \cap h(X) = D$. Hence $FFN(k,q)$ fails for $h(K)$. □

Acknowledgments. This research was partially supported by M.U.R.S.T. and G.N.S.A.G.A. of C.N.R. (Italy). The authors want to thank G.E. Moorhouse for stimulating e-mail messages.

References

[1] A. Blokhuis, G.E. Moorhouse, Some p–ranks related to orthogonal spaces, J. Algebraic Combinatorics 4, (1995) 295-316.

[2] M. Green, R. Lazarsfeld, Some results on the syzygies of finite sets and algebraic curves, Compositio Math. 67, (1988) 301-314.

[3] J. Harris, *Algebraic Geometry. A First Course*, GTM 133, Springer-Verlag, New York, 1992.

[4] J.W.P. Hirschfeld, J.A. Thas, *General Galois Geometries*, Oxford University Press, Oxford, 1991.

[5] G.E. Moorhouse, Some p–ranks related to Hermitian varieties, Special issue on orthogonal arrays and affine designs, Part II, J. Statist. Plann. Inference 56, (1996) 229-241.

[6] G.E. Moorhouse, Some p–ranks related to finite geometric structures, in Mostly finite geometries (Iowa City, IA, 1996) Lecture Notes in Pure and Appl. Math. 190 Dekker, New York, (1997) 353-364.

(Received 18/11/98)