On the Number of Points of a Hypersurface in Finite Projective Space (after J.-P. Serre)

Koen Thas
Ghent University
Department of Pure Mathematics and Computer Algebra
Krijgslaan 281, S22, B-9000 Ghent, Belgium
E-mail: kthas@cage.UGent.be

Abstract

In J.-P. Serre's *Lettre à M. Tsfasman* [3], an interesting bound for the maximal number of points on a hypersurface of the n-dimensional projective space $\mathbf{PG}(n,q)$ over the Galois field $\mathbf{GF}(q)$ with q elements is given. Using essentially the same combinatorial technique as in [3], we provide a bound which is relative to the maximal dimension of a subspace of $\mathbf{PG}(n,q)$ which is completely contained in the hypersurface. The lower that dimension, the better the bound. Next, by using a different argument, we derive a bound which is again relative to the maximal dimension of a subspace of $\mathbf{PG}(n,q)$ which is completely contained in the hypersurface. If that dimension increases for the latter case, the bound gets better.
As such, the bounds are complementary.

Keywords: Hypersurface, finite projective spaces, combinatorial bounds.
MSC 2000: 14J70, 05B25, 51E20.

Notation

- In this note, $\mathbf{PG}(n,q)$ is the n-dimensional projective space over the Galois field $\mathbf{GF}(q)$ with q elements.

- $p_n = \frac{q^{n+1}-1}{q-1}$ is the number of points of $\mathbf{PG}(n,q)$; in particular, $p_{-1} = 0$.

- $\Phi(X_0, X_1, \ldots, X_n) = \Phi$ is a homogeneous nonzero polynomial of degree $d \leq q+1$, with coefficients in $\mathbf{GF}(q)$ (so Φ defines a *hypersurface* in $\mathbf{PG}(n,q)$; in particular, for $n=2$, Φ defines an *algebraic curve*), and S is the set of $\mathbf{GF}(q)$-rational points of Φ.
- $|S| = N$.

1 Serre's Bound

With the notation of the previous section, J.-P. Serre proves the following

Theorem 1.1 (J.-P. Serre [3]) *We have that*

$$N \leq dq^{n-1} + p_{n-2}.$$

Consider the projective space $\mathbf{PG}(n,q)$, and define $F(n,k,q)$, $0 \leq k \leq n$, $k \in \mathbb{N}$, by

$$F(n,k,q) = \sum_{i=k}^{n-2} q^i \frac{p_{n-1}}{p_i p_{i+1}}$$

if $k \in \{1, 2, \ldots, n-2\}$, and $F(n,k,q) = 0$ if $k = 0$ or $k \geq n-1$.

In this note we will prove that

Theorem 1.2

$$N \leq dq^{n-1} + p_{n-2} + (d-(q+1))F(n,k,q),$$

where $k \leq n-1$ is the maximal dimension of a $\mathbf{PG}(k,q) \subset \mathbf{PG}(n,q)$ which is completely contained in S.

The lower k, the better the result. When $k=0$, Theorem 1.2 is essentially covered by Theorem 3.1.
Note that

$$F(n,k,q) = \sum_{i=k}^{n-2} q^i \frac{p_{n-1}}{p_i p_{i+1}} = \sum_{i=k}^{n-2} (q^{n-2-i} + \frac{p_{n-3-i}}{p_{i+1}})(1 - \frac{p_{i-1}}{p_i}) > q^{n-k-2} - \frac{1}{q},$$

for $1 \leq k \leq n-2$.

Substituting in Theorem 1.2 yields

$$N \leq dq^{n-1} + p_{n-2} + (d - (q+1))q^{n-k-2}.$$

(Recall that $N \in \mathbb{N}$, and that $1 \leq d \leq q+1$.)

The second main theorem is

Theorem 1.3 *Suppose Φ is a homogeneous polynomial of degree $d \leq q$ with coefficients in $\mathbf{GF}(q)$. Let S be its set of $\mathbf{GF}(q)$-rational points in $\mathbf{PG}(n,q)$, $n \geq 2$, and suppose that Π_{m-1} is a subspace of $\mathbf{PG}(n,q)$ of maximal dimension which is contained in S, $m-1 \leq n-2$. Then*

$$N = |S| \leq dq^{n-1} + p_{n-2} + (d - (q+1))q^{m-1}.$$

The bound gets better if m increases.

Under the hypotheses of Theorem 1.3, a combination of the main results will then lead to

$$N < dq^{n-1} + p_{n-2} + (d - (q+1))(q^{m-1} + q^{n-m-1} - 1).$$

Remark 1.4 Each of the main results is obtained by using elementary combinatorial methods from projective geometry; the Hasse-Weil bound [1, 2, 6, 7] is *not* used.

2 Proof of Theorem 1.2

We do not consider the case $d = q+1$, as in that case $p_n = dq^{n-1} + p_{n-2}$. So $d \leq q$. The proof is by induction on n. We assume that $n \geq 2$ as the case $n = 1$ is easy. Let $F_1, F_2, \ldots, F_r$ be the different linear factors of Φ over $\mathbf{GF}(q)$, and suppose that $\Pi_1, \Pi_2, \ldots, \Pi_r$ are the hyperplanes of $\mathbf{PG}(n,q)$ which correspond to $F_1, F_2, \ldots, F_r$, respectively. Then $U = \bigcup_{i=1}^{r} \Pi_i$ is contained in S. We assume that $S \neq \emptyset$, as that case is trivial. We distinguish two cases.

(i) $U = S$ AND $r \geq 1$. In that case, $k = n-1$, so $F(n,k,q) = 0$. See, e.g., J.-P. Serre [3] for this case.

(ii) $U \neq S$ OR Φ HAS NO LINEAR FACTORS OVER $\mathbf{GF}(q)$. Let p be a point of S which is not in U. If then Π is a hyperplane of $\mathbf{PG}(n,q)$ containing p, then the restriction of Φ to Π is not identically zero. Hence we can apply the Induction Hypothesis on $S \cap \Pi$ to obtain that

$$|S \cap \Pi| \leq dq^{n-2} + p_{n-3} + (d - (q+1))F(n-1, k', q),$$

where k' is the maximal dimension of a $\mathbf{PG}(k',q)$ which is completely contained in $S \cap \Pi$. Now we count in two ways the number θ of point-hyperplane pairs (p',Π') for which p' is a point of $S \setminus \{p\}$ and Π' is a hyperplane containing p and p'. Clearly we have that

$$\theta = (N-1)p_{n-2}.$$

Now fix a hyperplane Π'' containing p; then there are at most $dq^{n-2} + p_{n-3} + (d-(q+1))F(n-1,k_m,q) - 1$ points contained in $(S \cap \Pi'') \setminus \{p\}$, where k_m is the maximal k^* for which there is a hyperplane Π^* of $\mathbf{PG}(n,q)$ containing p, so that $S \cap \Pi^*$ contains a $\mathbf{PG}(k^*,q)$ (note that $r \leq r'$ implies that $F(n,r,q) \geq F(n,r',q)$). Hence

$$\theta \leq p_{n-1}(dq^{n-2} + p_{n-3} + (d-(q+1))F(n-1,k_m,q) - 1).$$

Thus we obtain that

$$N \leq 1 + \frac{p_{n-1}}{p_{n-2}}[dq^{n-2} + p_{n-3} + (d-(q+1))F(n-1,k_m,q) - 1],$$

and direct computations lead to

$$N \leq dq^{n-1} + p_{n-2} + (d-(q+1))F(n,k_m,q).$$

It is now clear that

$$(d-(q+1))F(n,k_m,q) \leq (d-(q+1))F(n,k,q),$$

where k is the maximal dimension of a $\mathbf{PG}(k,q) \subset \mathbf{PG}(n,q)$ which is completely contained in S. The theorem follows. ■

Notation. In the rest of this note, we denote by $F(n,q)$ the following.

$$F(n,q) = \frac{p_{n-1}}{p_1} + F(n,1,q).$$

Clearly,

$$F(n,q) > \frac{p_{n-1}}{p_1} + q^{n-3} - \frac{1}{q} (> q^{n-2} + q^{n-3} - \frac{1}{q}).$$

3 An Interesting Corollary

There is an interesting corollary of the proof of Theorem 1.2:

Theorem 3.1 *Suppose Φ is a homogeneous polynomial of degree $d \leq q+1$ with coefficients in* **GF**(q). *Let S be the set of* **GF**(q)*-rational points in* **PG**(n,q), $n \geq 2$, *and suppose the following property is satisfied:*

(L) There is no line in **PG**(n,q) which is completely contained in S.

If $N = |S|$, then we have that

$$N \leq dq^{n-1} + p_{n-2} + (d-(q+1))F(n,q).$$

Proof. As in Section 2, we may assume w.l.o.g. that $d \leq q$. Again the proof goes by induction on n. We start with supposing that $n = 2$. Then $F(2,q) = 1$, and by considering Property (L), the theorem follows from J. A. Thas [4]. Now suppose that $n \geq 3$. Suppose F_i, Π_j, U, etc. are as in the proof of Theorem 1.2. We also assume that $S \neq \emptyset$ to avoid triviallity. Then clearly $U \neq S$ (Case (ii) of the proof of Theorem 1.2). In fact, $U = \emptyset$. Let p be a point of S. If Π is a hyperplane of **PG**(n,q) containing p, then the restriction of Φ to Π is not identically zero. As Property (L) holds for the restriction of Φ to Π, we can apply the Induction Hypothesis on $S \cap \Pi$ to obtain that

$$|S \cap \Pi| \leq dq^{n-2} + p_{n-3} + (d-(q+1))F(n-1,q).$$

Now we count in two ways the number θ of point-hyperplane pairs (p', Π') for which p' is a point of $S \setminus \{p\}$ and Π' is a hyperplane containing p and p'. Then $\theta = (N-1)p_{n-2}$.
Fix a hyperplane Π'' containing p; then there are at most $dq^{n-2} + p_{n-3} + (d-(q+1))F(n-1,q) - 1$ points contained in $(S \cap \Pi'') \setminus \{p\}$. Hence

$$\theta \leq p_{n-1}(dq^{n-2} + p_{n-3} + (d-(q+1))F(n-1,q) - 1).$$

Thus we obtain that

$$N \leq 1 + \frac{p_{n-1}}{p_{n-2}}[dq^{n-2} + p_{n-3} + (d-(q+1))F(n-1,q) - 1],$$

and hence

$$N \leq dq^{n-1} + p_{n-2} + (d-(q+1))F(n,q).$$

■

Remark 3.2 The function $F(n,q)$ can be adapted in the obvious way to functions $F'(n,q)$ for which $F'(n,q) \geq F(n,q)$ for all n and q, and so that in the previous theorem $F(n,q)$ can be replaced by $F'(n,q)$, if the bound

$$N \leq dq + d - q$$

for the number N of points on a plane algebraic curve in $\mathbf{PG}(2, q)$ of degree d with no linear components (i.e., for $d \leq q$ the case $n = 2$ with the assumption of Property (L)) is improved. See e.g. J. A. Thas [5] for such improvements.

4 A Second Approach

We now obtain

Theorem 4.1 *Suppose Φ is a homogeneous polynomial of degree $d \leq q$ with coefficients in $\mathbf{GF}(q)$. Let S be the set of $\mathbf{GF}(q)$-rational points of Φ in $\mathbf{PG}(n, q)$, $n \geq 2$, and suppose that Π_{m-1} is a $\mathbf{PG}(m-1, q) \subset \mathbf{PG}(n, q)$ which is contained in S. Suppose that $S \neq \mathbf{PG}(n, q)$, and that no hyperplane of $\mathbf{PG}(n, q)$ which contains Π_{m-1}, is contained in S. Then*

$$N = |S| \leq dq^{n-1} + p_{n-2} + (d - (q+1))q^{m-1}.$$

Proof. Suppose that $S \neq \mathbf{PG}(n, q)$, and that Π_{m-1} is a $\mathbf{PG}(m-1, q) \subset \mathbf{PG}(n, q)$ which is contained in S. Suppose that no hyperplane of $\mathbf{PG}(n, q)$ containing Π_{m-1} is contained in S. Then there is a $\mathbf{PG}(m, q) = \Pi_m$ containing Π_{m-1} which is not contained in S. Now count in two ways the number of point-hyperplane pairs (p, Π) for which $p \subset \Pi$, where p is a point of $S \setminus \Pi_m$, $\Pi_{m-1} \subset \Pi$, and where $\Pi_m \not\subset \Pi$. If $\alpha = |\Pi_m \cap S|$ and $\beta = |\Pi_{m-1} \cap S| = p_{m-1}$, then

$$(N - \alpha)q^{n-m-1} \leq q^{n-m}(N' - \beta),$$

with N' the theoretical upper bound for the number of points of S in a hyperplane of $\mathbf{PG}(n, q)$ for which Φ is not identically zero, so

$$N \leq qN' - q\beta + \alpha = qN' - qp_{m-1} + \alpha.$$

Applying Theorem 1.1 (and remarking that we are not necessarily in Case (ii) of the proof of that theorem for Π_m), we obtain

$$N \leq q(dq^{n-2} + p_{n-3}) - qp_{m-1} + dq^{m-1} + p_{m-2}.$$

The theorem follows. ■

Hence the following very general theorem.

Theorem 4.2 *Suppose Φ is a homogeneous polynomial of degree $d \leq q$ with coefficients in* $\mathbf{GF}(q)$*. Let S be the set of* $\mathbf{GF}(q)$*-rational points of Φ in* $\mathbf{PG}(n,q)$*, $n \geq 2$, and suppose that Π_{m-1} is a subspace of* $\mathbf{PG}(n,q)$ *of maximal dimension which is contained in S, $m-1 \leq n-2$. Then*

$$N = |S| \leq dq^{n-1} + p_{n-2} + (d-(q+1))q^{m-1}.$$

Proof. Suppose Π_m is an arbitrary m-dimensional subspace of $\mathbf{PG}(n,q)$ which contains Π_{m-1}. Then Π_m is not contained in S. Also, no hyperplane of $\mathbf{PG}(n,q)$ which contains Π_{m-1}, is contained in S. Hence Theorem 4.1 applies. ■

In fact, by using the (rather messy) bound of Theorem 1.2, we can do a little better. For, suppose Φ is a homogeneous polynomial of degree $d \leq q$ with coefficients in $\mathbf{GF}(q)$. Let $S \neq \emptyset$ be its set of $\mathbf{GF}(q)$-rational points in $\mathbf{PG}(n,q)$, $n \geq 2$, and suppose that Π_{m-1} is a $\mathbf{PG}(m-1,q) \subset \mathbf{PG}(n,q)$ contained in S, and which is a subspace of $\mathbf{PG}(n,q)$ of maximal dimension which is contained in S, $m-1 \leq n-2$. Then each $\mathbf{PG}(m,q) = \Pi_m$ containing Π_{m-1} is not contained in S. Then applying the proof of Theorem 4.1, and remarking that for each hyperplane Π containing Π_{m-1} and not Π_m, the maximal dimension of its subspaces which are completely contained in S is also $m-1$ (the same holds for Π_m), we have

$$N = |S| \leq qN' - qp_{m-1} + \alpha = q(dq^{n-2} + p_{n-3} + (d-(q+1))F(n-1,m-1,q))$$

$$-qp_{m-1} + dq^{m-1} + p_{m-2} + (d-(q+1))F(m,m-1,q).$$

Hence

$$N \leq dq^{n-1} + p_{n-2} + (d-(q+1))(q^{m-1} + q\sum_{i=m-1}^{n-3} q^i \frac{p_{n-2}}{p_i p_{i+1}}),$$

where we emphasize that $m \leq n-1$. Thus

$$N < dq^{n-1} + p_{n-2} + (d-(q+1))(q^{m-1} + q^{n-m-1} - 1).$$

Acknowledgements. The author is a Postdoctoral Fellow of the Fund for Scientific Research — Flanders (Belgium).

References

[1] H. HASSE. Abstrakte Begründung der Komplexen Multiplication und Riemannsche Vermutung in Functionenkörpern, *Abh. Math. Sem. Univ. Hamburg* **10** (1934), 325–348.

[2] H. HASSE. Punti razionali sopra curva algebriche a congruenze, *Atti dei Convegni, 1939*, Reale Accademia d' Italia, Rome, 1943.

[3] J. -P. SERRE. Lettre à M. Tsfasman, *Astérisque* **198-199-200** (1991), 351–353.

[4] J. A. THAS. Elementary proofs of two fundamental theorems of B. Segre without using the Hasse-Weil theorem, *J. Combin. Theory Ser. A* **34** (1983), 381–384.

[5] J. A. THAS. Complete arcs and algebraic curves in PG$(2, q)$, *J. Algebra* **106** (1987), 451–464.

[6] A. WEIL. *Sur les Courbes Algébriques et les Variétés qui s'en Déduisent*, Hermann, Paris, 1948.

[7] A. WEIL. *Variétés Abéliennes et Courbes Algébriques*, Hermann, Paris, 1948.