Atti Accademia Nazionale dei Lincei

Classe Scienze Fisiche Matematiche Naturali

Rendiconti

James William Peter Hirschfeld

A curve over a finite field, the number of whose points is not increased by a quadratic extension of the field, and sub-Hermitian forms

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8, Vol. **42** (1967), n.3, p. 365–367.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1967_8_42_3_365_0>

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Accademia Nazionale dei Lincei, 1967.

Geometria. — *A curve over a finite field, the number of whose points is not increased by a quadratic extension of the field, and sub-Hermitian forms.* Nota di JAMES W. P. HIRSCHFELD, presentata (*) dal Socio B. SEGRE.

RIASSUNTO. — Mediante semplici considerazioni geometriche si dimostra che la curva espressibile nel piano uguagliando a zero la somma delle potenze $(q+1)^{me}$ delle coordinate contiene lo stesso numero di punti sui campi di Galois di ordinate q^2 e q^4, numero dato precisamente da q^3+1. Il risultato viene poi esteso (da B. Segre) a forme sub-hermitiane arbitrarie.

Hermitian forms over finite fields have been the subject of recent papers by Segre [3] and Bose and Chakravarti [1]. For a suitable coordinate system, a Hermitian form in $PG(r, p^{2k})$—the projective geometry of r dimensions over the Galois field $GF(p^{2k})$—with index of singularity t can be written as

$$x_0\bar{x}_0 + \cdots + x_{r-t}\bar{x}_{r-t} = 0 \tag{1}$$

where $\tau : x \to \bar{x} = x^{p^k}$ is the only involutory automorphism of $GF(p^{2k})$; the form is non-singular if, and only if, $t = 0$. In particular, the non-singular Hermitian curve H in the plane $PG(2, p^{2k})$ has equation

$$x_0^{p^k+1} + x_1^{p^k+1} + x_2^{p^k+1} = 0. \tag{2}$$

The curve H contains $p^{3k}+1$ points, [3] p. 44. Every line of the plane is either tangent to H with (p^k+1)-point contact or meets H in exactly p^k+1 distinct points of the plane. Furthermore, Weil [4] has shown that the total number N of points on any algebraic curve satisfies the inequalities

$$L = q+1-(n-1)(n-2)\sqrt{q} \le q+1-2g\sqrt{q} \le N \le$$
$$\le q+1+2g\sqrt{q} \le q+1+(n-1)(n-2)\sqrt{q} = U$$

where n is the order and g the genus of the curve. For $q = p^{2k}$ and $n = p^k+1$, $U = p^{3k}+1$; so, as Segre ([3] p. 44) observed, the Hermitian curve H attains the upper limit U of Weil's estimate.

Segre [2] has also considered the number of points on primals in $PG(r, q)$ with equations of the form

$$a_0 x_0^n + \cdots + a_r x_r^n = 0 \tag{3}$$

where n divides $q-1$. In particular, the number of points on $x_0^3+x_1^3+x_2^3=0$ over $GF(q)$, where $q = p^h$, h is even and $p \equiv -1 \pmod 3$, is shown ([2] p. 242) to be $q+1-2(-1)^{h/2}\sqrt{q}$; therefore, both over GF(4), the Her-

(*) Nella seduta dell'11 marzo 1967.

mitian case, and over GF(16), the curve has 9 points. This phenomenon is repeated for the curve $x_0^4 + x_1^4 + x_2^4 = 0$ over GF(q), where $q = q^h$, h is even and $p \equiv 3 \pmod 4$, which is shown ([2] p. 247) to have $q + 1 - 6(-1)^{h/2}\sqrt{q}$ points; thus, over GF(9), the Hermitian case, and over GF(81), the curve has 28 points.

The object of this Note is to show that the curve H′ with equation (2) in the plane PG$(2, p^{4k})$ has exactly $p^{3k} + 1$ points, as H does, i.e. all the points of H′ lie in a subplane PG$(2, p^{2k})$.

Firstly, it seems reasonable to call the curve H′ in the plane PG$(2, p^{4k})$ *sub-Hermitian*. It may be remarked that, if the proposed result is true, the number of points on H′ attains the lower limit L of Weil's estimate, i.e. for $q = p^{4k}$ and $n = p^k + 1$, $L = p^{3k} + 1$.

To prove the result, take non-homogeneous coordinates $(X, Y) = (x_1/x_0, x_2/x_0)$ in the plane and a point (A, B) on H′. Thus, H′ has equation

$$X^{p^k+1} + Y^{p^k+1} + 1 = 0 \tag{4}$$

and the tangent at (A, B) has equation

$$A^{p^k} X + B^{p^k} Y + 1 = 0\,; \tag{5}$$

this tangent meets H′ where

$$X^{p^k+1} - A^{p^{2k}} X^{p^k} - A^{p^k} X + A^{p^k(p^k+1)} = 0,$$

i.e.

$$(X - A)^{p^k} (X - A^{p^{2k}}) = 0\,.$$

Substituting in (5), we obtain that the tangent meets the curve p^k times at (A, B) and once at $(A^{p^{2k}}, B^{p^{2k}})$. If it is not true that both $A^{p^{2k}} = A$ and $B^{p^{2k}} = B$, then the two points are different. In this case, the tangent to H′ at $(A^{p^{2k}}, B^{p^{2k}})$ meets the curve p^k times at the point of contact and once at $(A^{p^{4k}}, B^{p^{4k}})$, which, the field being GF(p^{4k}), is our original point (A, B). Thus, the tangent to H′ at (A, B) is the same as the tangent at $(A^{p^{2k}}, B^{p^{2k}})$ and meets H′ at least $2p^k$ times, giving a contradiction. Therefore, both $A^{p^{2k}} = A$ and $B^{p^{2k}} = B$, the tangent at (A, B) has $(p^k + 1)$–point contact with H′, every point of H′ lies in a subplane PG$(2, p^{2k})$ and the number of points on (2) is the same in PG$(2, p^{4k})$ as in PG$(2, p^{2k})$, viz. $p^{3k} + 1$.

The sub-Hermitian curve H′ differs from the Hermitian curve H in that the PG$(2, p^{2k})$ containing H has $p^{3k} + 1$ lines which are 1–secant to H and $p^{4k} - p^{3k} + p^{2k}$ lines which are $(p^k + 1)$–secant to H, whereas PG$(2, p^{4k})$ has these lines as well as a further $p^{7k} - p^{5k} + p^{4k} - p^{2k}$ lines which are 1–secant to H′ and $p^{8k} - p^{7k} + p^{5k} - p^{4k}$ lines which do not meet H′ at all.

Professor Segre has pointed out to me the following extension (including also an alternative proof) of the results above.

Let $H = H^t_{r,q}$ (*) be any Hermitian form of $S_{r,q}$, having the speciality index $t\,(\geq 0)$. If P denotes an arbitrary point of the quadratic extension S_{r,q^2} of $S_{r,q}$, but not of $S_{r,q}$, then the conjugate P′ of P in that extension is again a point of S_{r,q^2}, but not of $S_{r,q}$. The points P, P′ are distinct and their join is a line of $S_{r,q}$, l say; hence (B. Segre [3], § 29), either (i) l lies on H, or (ii) l meets H in $\sqrt{q}+1$ distinct points of $S_{r,q}$, or (iii) l meets H in a single point of $S_{r,q}$ to be counted $\sqrt{q}+1$ times.

It follows that, if the above point P (and so also its conjugate point P′) lies on the quadratic extension H* of H, then (since H and H* have the same order $\sqrt{q}+1$) (i) necessarily must occur. Therefore,

The points of the sub-Hermitian form H* *are precisely those of the corresponding Hermitian form* H *and the points* P *of the lines* l *of* H, *if any, which are defined over the ground field* GF(q^2) *of* H*, *but not over* GF(q).

The numbers of points of either type are immediately obtainable from Segre [3], §§ 30–33, after having remarked that each of these lines l contains $(q^2+1)-(q+1)=q(q-1)$ points P, while each P lies on just one l. In particular, if $t=0$, $r=2$, no such line l (hence no such point P) exists, and so the only points of H* are now those of H.

BIBLIOGRAPHY.

[1] BOSE R. C. and CHAKRAVARTI I. M., *Hermitian varieties in a projective space* PG(N, q^2), «Canad. J. Math.», *18*, 1161–1182 (1966),

[2] SEGRE B., *Arithmetische Eigenschaften von Galois–Raümen I*, «Math. Ann.», *154*, 195–256 (1964).

[3] SEGRE B., *Forme e geometrie hermitiane, con particolare riguardo al caso finito*, «Ann. Mat. Pura Appl.», *70*, 1–202 (1965).

[4] WEIL A., *Sur les courbes algébriques et les variétés qui s'en déduisent*, Hermann, Paris 1948.

(*) We use the notation of [3].