Canad. Math. Bull. Vol. **23** (3) 1980

ON THE NUMBER OF ZEROS OVER A FINITE FIELD OF CERTAIN SYMMETRIC POLYNOMIALS

BY
P. V. CECCHERINI* AND J. W. P. HIRSCHFELD

1. **Introduction.** A variety of applications depend on the number of solutions of polynomial equations over finite fields. Here the usual situation is reversed and we show how to use geometrical methods to estimate the number of solutions of a non-homogeneous symmetric equation in three variables.

2. **The main equation.** Write $K=GF(q)$, the finite field of order q. Let F in $K[T]$ be any polynomial of degree $m\geq 2$, and form the following symmetric polynomial in $K[X, Y, Z]$:

$$L_F=L(X, Y, Z)=F(X)(Y-Z)+F(Y)(Z-X)+F(Z)(X-Y).$$

We wish to estimate the number of solutions over K of the equation $L=0$.

Without loss of generality, we may assume that $m<q$, since if $F(T)=G(T)$ mod (T^q-T), then $L_F=0$ and $L_G=0$ are equivalent equations over K.

In any case, $L=0$ has at least $3q^2-2q$ solutions over K, namely the triples (x, y, z) with some pair of coordinates equal: these are the *trivial* solutions. Further, if $L=0$ has a non-trivial solution, then it has at least six: the given one as well as those obtained by permuting the coordinates.

$PG(n,q)$ is projective space of n dimensions over K. A *k-arc* in $PG(2,q)$ is a set of k points no three of which are collinear.

Lemma 1. *$L=0$ has only trivial solutions over K if and only if $\bar{\mathcal{K}}=\{(1, t, F(t))\mid t\in K\}$ is a q-arc in $PG(2,q)$.*

Proof. The determinant with successive rows $(1, X, F(X))$, $(1, Y, F(Y))$, $(1, Z, F(Z))$ is equal to $-L$. So (x, y, z) is a non-trivial solution of $L=0$ if and only if $(1, x, F(x))$, $(1, y, F(y))$, $(1, z, F(z))$ are three distinct collinear points of $\bar{\mathcal{K}}$. □

Corollary. *If $m=\deg F=2$, then $L=0$ has only trivial solutions over K.*

Proof. If $m=2, \mathcal{K}=\bar{\mathcal{K}}\cup\{(0,0,1)\}$ is the set of points in $PG(2,q)$ of the irreducible conic with equation $x_0x_2=x_0^2F(x_1/x_0)$, whence $\bar{\mathcal{K}}$ is a q-arc. □

To invert this corollary, we need the following.

Received by the editors September 7, 1978 and in revised form May 22, 1979
* Section 4 of GNSAGA, CNR.

LEMMA 2. *Let F in $K[T]$ have degree m with $2 \le m \le q-1$. If the curve $\mathscr{C}$ with equation $x_0^{m-1}x_2 = x_0^m F(x_1/x_0)$ coincides in $PG(2,q)$ with an irreducible conic, then $m=2$.*

Proof. Let $F(T) = A_0 + A_1 T + A_2 T^2 + \cdots + A_{q-1}T^{q-1}$ and $G(T) = F(T) - A_0 - A_1 T$. Then $\mathscr{K} = \{(1, t, F(t)) \mid t \in K\} \cup \{(0,0,1)\}$ is a conic if and only if $\mathscr{K}' = \{(1, t, G(t)) \mid t \in K\} \cup \{(0,0,1)\}$ is: for, the projectivity given by $x_0' = x_0$, $x_1' = x_1$, $x_2' = -A_0x_0 - A_1x_1 + x_2$ transforms $\mathscr{K}$ into $\mathscr{K}'$. Suppose therefore that the points of $\mathscr{C}$ form the set $\mathscr{K}'$.

It $\mathscr{C}$ is a conic with equation $f(x_0, x_1, x_2) = 0$, then $f(x_0, x_1, x_2) = x_1^2 + b_0x_1x_2 + b_1x_0x_2 + b_2x_0x_1$, since $(1,0,0)$ and $(0,0,1)$ are in $\mathscr{K}'$ but $(0,1,0)$ is not. Since $\mathscr{C}$ is irreducible, $b_1(b_1 - b_0b_2) \ne 0$. Now, $g(t) = f(1, t, G(t)) = 0$ for all t in K. Therefore, since degree $g(T) \le q$, we obtain that $g(T) = c(T^q - T)$ for some c in K. However,

$$\begin{aligned} g(T) &= b_2T + T^2 + b_1G(T) + b_0TG(T) \\ &= b_2T + (1 + b_1A_2)T^2 + (b_1A_3 + b_0A_2)T^3 + \cdots \\ &\quad + b_1A_r + b_0A_{r-1})T^r + \cdots + (b_1A_{q-1} + b_0A_{q-2})T^{q-1} \\ &\quad + b_0A_{q-1}T^q \quad . \end{aligned}$$

Hence

$$\begin{aligned} b_2 &= -c; \\ 1 + b_1A_2 &= 0; \\ b_1A_r + b_0A_{r-1} &= 0, \quad \text{for} \quad 3 \le r \le q-1; \\ b_0A_{q-1} &= c. \end{aligned}$$

So $A_2 = -1/b_1$, $A_3 = b_0/b_1^2, \ldots, A_r = b_0^{r-2}/(-b_1)^{r-1}, \ldots, A_{q-1} = b_0^{q-3}/(-b_1)^{q-2}$, $b_0A_{q-1} = c = -b_2$,

whence

$$(b_0/b_1)^{q-2} = b_2 .$$

If $b_0 \ne 0$, this implies that $b_1 = b_0b_2$, contradicting the irreducibility of f. So $b_0 = 0$ and $A_3 = A_4 = \cdots = A_{q-1} = c = b_2 = 0$. Thus $m = 2$. □

THEOREM 1. *When q is odd or $q=4$, $L=0$ has non-trivial solutions over K if and only if deg $F>2$.*

Proof. If deg $F = 2$, the result is that of the Corollary to Lemma 1. If $L=0$ has only trivial solutions, then, by Lemma 1, $\bar{\mathscr{K}} = \{(1, t, F(t)) \mid t \in K\}$ is a q-arc in $PG(2,q)$, whence $\mathscr{K} = \bar{\mathscr{K}} \cup \{(0,0,1)\}$ is a $(q+1)-$arc, which is an irreducible conic by Segre's theorem ([4], p. 270; [3], §8.2): for $q=4$, a 5-arc is trivially a conic. But $\mathscr{K}$ is the set of points on the curve with equation $x_0^{m-1}x_2 = x_0^mF(x_1/x_0)$. So, by Lemma 2, deg $F = 2$. □

THEOREM 2. *When q is even, there exists F with $2<\deg F\leq q-1$ such that $L=0$ has only trivial solutions if and only if $q>4$.*

Proof. Let $\mathcal{K}^*=\{(1,t,F(t))\mid t\in K\}\cup\{(0,1,0),(0,0,1)\}$. When $F(T)=T^{q-2}$, $\mathcal{K}^*$ consists of the points on the conic with equation $x_0^2=x_1x_2$ plus the meet $(1,0,0)$ of its tangents. Alternatively, when $F(T)=T^{q/2}$, $\mathcal{K}^*$ is the conic with equation $x_2^2=x_0x_1$ plus the meet $(0,0,1)$ of its tangents. In either case, for $q>4$, $\mathcal{K}^*$ is a $(q+2)-$arc with $\deg F>2$. Hence, by Lemma 1, $L=0$ has only trivial solutions. For $q=2$, there is nothing to prove. For $q=4$, the result was part of Theorem 1. □

For examples of $(q+2)$-arcs not containing a conic and the problem of their classification, see [2].

THEOREM 3. *Let q be odd and suppose $m=\deg F$ satisfies $2<m<(q+1-3\alpha)/2$ for some non-negative integer α. Then, for $q>(12\alpha+3)^2$, $L=0$ has at least $6(\alpha+1)$ solutions over K.*

Proof. $\mathcal{K}=\{(1,t,F(t))\mid t\in K\}\cup\{(0,0,1)\}$ is the set of the $q+1$ points of the curve $\mathcal{C}$ of order m with equation $x_0^{m-1}x_2=x_0^mF(x_1/x_0)$. By Lemma 1, it suffices to show that there exist on $\mathcal{K}$ at least $3(\alpha+1)$ distinct points $A_i, B_i, C_i\,(i=1,2,\ldots,\alpha+1)$ such that each triple of points with the same index is collinear. If $\alpha=0$, the result follows from Theorem 1. Now, let us suppose the result true for $\alpha=\beta-1\geq 0$ and prove it for $\alpha=\beta$.

Let $2<m<(q+1-3\beta)/2$ and $\sqrt{q}>12\beta+3$. Then $2<m<[q+1-3(\beta-1)]/2$ and $\sqrt{q}>12(\beta-1)+3$. By the induction hypothesis there exists a subset $\mathcal{B}$ of $\mathcal{K}$ with 3β distinct points $A_i, B_i, C_i\,(i=1,2,\ldots,\beta)$ having the required property. If there does not exist on $\mathcal{H}=\mathcal{K}\setminus\mathcal{B}$ a triple $A_{\beta+1}, B_{\beta+1}, C_{\beta+1}$ of distinct collinear points, then $\mathcal{H}$ is $(q+1-3\beta)$-arc with

$$q-\sqrt{q}/4+7/4<q+1-3\beta<q+1.$$

So $\mathcal{H}$ is contained in a unique irreducible conic ([5], p. 163; [3], §10.4) having at least $|\mathcal{H}|=q+1-3\beta>2m$ points in common with $\mathcal{C}$: this contradicts Bézout's theorem. So there exists a triple $A_{\beta+1}, B_{\beta+1}, C_{\beta+1}$ of collinear points on $\mathcal{H}$. □

3. **An extension.** The above results can be extended to the case of a polynomial F in $K[T_1, T_2]$ of degree ≥ 2 as follows. Let us denote by Σ_F the system of four equations given by

$$\operatorname{rank}\begin{bmatrix}1 & X_1 & X_2 & F(X_1,X_2)\\ 1 & Y_1 & Y_2 & F(Y_1,Y_2)\\ 1 & Z_1 & Z_2 & F(Z_1,Z_2)\end{bmatrix}<3.$$

To estimate the number of solutions $\xi=(x_1,x_2,y_1,y_2,z_1,z_2)$ of Σ_F we may suppose that $\deg_{T_i} F \le q-1 (i=1,2)$. The system Σ_F has $3q^4-2q^2$ *trivial* solutions given by ξ with some pair of (x_1, x_2), (y_1, y_2), (z_1, z_2) equal.

A *k-cap* in $PG(3, q)$ is a set of k points no three of which are collinear.

LEMMA 3. *Σ_F has only trivial solutions if and only if $\bar{\mathcal{K}} = \{(1, t_1, t_2, F(t_1, t_2)) \mid t_1, t_2 \in K\}$ is a q^2-cap of $PG(3, q)$.*

Proof. $\xi = (x_1, x_2, y_1, y_2, z_1, z_2)$ is a non-trivial solution of Σ_F if and only if $(1, x_1, x_2, F(x_1, x_2))$, $(1, y_1, y_2, F(y_1, y_2))$, $(1, z_1, z_2, F(z_1, z_2))$ are distinct collinear points of $\bar{\mathcal{K}}$. □

If $\deg F = 2$, write $F(T_1, T_2) = f_2 + f_1 + f_0$ where f_i is a form of degree i: we call f_2 the *quadratic part* of F.

COROLLARY. *If $\deg F = 2$, then Σ_F has only trivial solutions over K if and only if f_2 is irreducible.*

Proof. Consider $\mathcal{K} = \bar{\mathcal{K}} \cup \{(0, 0, 0, 1)\}$. If $F(T_1, T_2) = f_2 + a_1 T_1 + a_2 T_2 + b_0$, the projectivity given by $x_0' = x_0, x_1' = x_1, x_2' = x_2, x_3' = -b_0 x_0 - a_1 x_1 - a_2 x_2 + x_3$ transforms $\mathcal{K}$ into

$$\mathcal{K}' = \{(1, t_1, t_2, f_2(t_1, t_2)) \mid t_1, t_2 \in K\} \cup \{(0, 0, 0, 1)\}.$$

Now, $\mathcal{K}'$ is the set of points of the quadric with equation $x_0 x_3 = f_2(x_1, x_2)$. If f_2 is reducible, $\mathcal{K}'$ is a hyperbolic quadric or a cone and so contains a line. If f_2 is irreducible, $\mathcal{K}'$ is an elliptic quadric and forms a (q^2+1)-cap, whence $\bar{\mathcal{K}}$ is a q^2-cap. □

To obtain a converse to this corollary, we require the following lemmas.

LEMMA 4. *Let F in $K[T_1, T_2]$ have $\deg_{T_i} F \le q-1 (i=1,2)$. If $\deg_{T_1} F(T_1, t_2) \le 2$ and $\deg_{T_2} F(t_1, T_2) \le 2$ for all t_1, t_2 in K, then $\deg_{T_i} F \le 2 (i=1,2)$.*

Proof. Let $\deg_{T_1} F = n$ and put $F(T_1, T_2) = \sum_{i=0}^{n} T_1^i c_i(T_2)$, where $c_i \in K[T_2]$ and $c_n(T_2) \ne 0$. Since $\deg c_n \le \deg_{T_2} F \le q-1$, there exists t_2 in K such that $c_n(t_2) \ne 0$. Then $\deg_{T_1} F(T_1, t_2) = n \le 2$ by assumption. Similarly, $\deg_{T_2} F \le 2$. □

LEMMA 5. *Let F in $K[T_1, T_2]$ have degree $m > 2$ with $\deg_{T_i} F \le q-1 (i=1,2)$. If the surface $\mathcal{S}$ with equation $x_0^{m-1} x_3 = x_0^m F(x_1/x_0, x_2/x_0)$ is an elliptic quadric in $PG(3, q)$, then $m = 2$.*

Proof. The points of $\mathcal{S}$ from the set

$$\mathcal{K} = \{(1, t_1, t_2, F(t_1, t_2) \mid t_1, t_2 \in K\} \cup \{(0, 0, 0, 1)\}.$$

If $\mathcal{S}$ is an elliptic quadric then, for all s_1 in K, the set

$$\mathcal{K}_{s_1} = \{(1, s_1, t_2, F(s_1, t_2)) \mid t_2 \in K\} \cup \{(0, 0, 0, 1)\}$$

is a conic in the plane with equation $x_1 = s_1 x_0$, in which x_0, x_2, x_3 will be used as coordinates. Similarly, for all s_2 in K, the set $\mathcal{K}_{s_2} =$

$\{(1, t_1, s_2, F(t_1, s_2)) \mid t_1 \in K\} \cup \{(0,0,0,1)\}$ is a conic in the plane with equation $x_2 = s_2 x_0$, in which x_0, x_1, x_3 will be used as coordinates. By Lemma 2, $\deg F(s_1, T_2) \le 2$ for all s_1 in K and $\deg F(T_1, s_2) \le 2$ for all s_2 in K. So, by Lemma 4, $\deg_{T_1} F \le 2$ and $\deg_{T_2} F \le 2$. Therefore

$$F(T_1, T_2) = A_0 + A_1 T_1 + A_2 T_2 + A_{11} T_1^2 + A_{12} T_1 T_2 + A_{22} T_2^2 \\ + T_1 T_2 (B_1 T_1 + B_2 T_2 + C T_1 T_2).$$

We wish to show that $B_1 = B_2 = C = 0$.

Let $G(T_1, T_2) = F(T_1, T_2) - (A_0 + A_1 T_1 + A_2 T_2)$. The projectivity given by $x_0' = x_0$, $x_1' = x_1$, $x_2' = x_2$, $x_3' = -A_0 x_0 - A_1 x_1 - A_2 x_2 + x_3$ transforms $\mathscr{K}$ into $\mathscr{K}' = \{(1, t_1, t_2, G(t_1, t_2)) \mid t_1, t_2 \in K\} \cup \{(0,0,0,1)\}$, which is an elliptic quadric if and only if $\mathscr{K}$ is. With $m = 4$ and $F = G$, the equation of $\mathscr{S}$ is

$$x_0^3 x_3 = x_0^2 (A_{11} x_1^2 + A_{12} x_1 x_2 + A_{22} x_2^2) \\ + x_1 x_2 (B_1 x_0 x_1 + B_2 x_0 x_2 + C x_1 x_2).$$

So $\mathscr{S}$ and $\mathscr{K}'$ contain the line with equations $x_0 = x_1 = 0$, which is impossible since $\mathscr{K}'$ is a (q^2+1)-cap. So $\deg G < 4$, whence $C = 0$. If $\deg G = 3$, the equation of $\mathscr{S}$ is

$$x_0^2 x_3 = x_0 (A_{11} x_1^2 + A_{12} x_1 x_2 + A_{22} x_2^2) + x_1 x_2 (B_1 x_1 + B_2 x_2).$$

Again $\mathscr{S}$ and $\mathscr{K}'$ contain the line with equations $x_0 = x_1 = 0$. So $\deg G < 3$. Thus $B_1 = B_2 = 0$ and $\deg G = 2$. □

THEOREM 4. *For q odd or $q = 4$, Σ_F has only trivial solutions if and only if* deg *$F = 2$ and the quadratic part of F is irreducible.*

Proof. If Σ_F has only trivial solutions, then by Lemma 3, $\mathscr{K} = \bar{\mathscr{K}} \cup \{(0,0,0,1)\}$ is a (q^2+1)-cap in $PG(3, q)$, which in turn is an elliptic quadric, [1]. By Lemma 5, $\deg F = 2$ and, by the Corollary to Lemma 3, the quadratic part of F is irreducible. The converse is given by the same corollary. □

THEOREM 5. *For $q = 2^{2r+1}$, $r \ge 1$, there exists F with $2 < \deg F \le q-1$ such that Σ_F has only trivial solutions.*

Proof. Let σ be an automorphism of $K = GF(2^{2r+1})$ such that $x^{\sigma^2} = x^2$: then $x^\sigma = x^{2^{r+1}}$. With

$$F(t_1, t_2) = t_1 t_2 + t_1^\sigma + t_2^2 t_2^\sigma,$$

$\mathscr{K} = \bar{\mathscr{K}} \cup \{(0,0,0,1)\}$ is a (q^2+1)-cap (but not an elliptic quadric), [6]. So, by Lemma 3, F is a polynomial of degree >2 such that Σ_F has only trivial solutions. □

https://doi.org/10.4153/CMB-1980-046-5 Published online by Cambridge University Press

Remark. Lemmas 2 and 5 are related to the following question: can two absolutely irreducible hypersurfaces of $PG(n, q)$ of orders $\leq q-1$ have the same set of points but different equations?

References

1. A. Barlotti, *Un estensione del teorema di Segre-Kustaanheimo*, Boll. Un. Mat. Ital. **10** (1955), 96-98.

2. J. W. P. Hirschfeld, *Ovals in Desarguesian planes of even order*, Ann. Mat Pura. Appl. **102** (1975), 79–89.

3. J. W. P. Hirschfeld, *Projective geometries over finite fields*, Oxford Univ. Press, 1979.

4. B. Segre, *Lectures on modern geometry*, Cremonese, Rome, 1961.

5. B. Segre, *Introduction to Galois geometries*, Atti Accad. Naz. Lincei Mem. **8** (1967), 133–236.

6. J. Tits, *Ovoides et groupes de Suzuki*, Arch. Math. **13** (1962), 187–198.

Università di Roma,
00100 Roma, Italy;

University of Sussex,
Brighton, U.K. BN1 9QH.