Atti Accademia Nazionale dei Lincei

Classe Scienze Fisiche Matematiche Naturali

Rendiconti

Stanley E. Payne

A Complete Determination of Translation Ovoids in Finite Desarguian Planes

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8, Vol. **51** (1971), n.5, p. 328–331.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1971_8_51_5_328_0>

Geometria. — *A Complete Determination of Translation Ovoids in Finite Desarguian Planes.* Nota di STANLEY E. PAYNE, presentata (*) dal Socio B. SEGRE.

RIASSUNTO. — Riattaccandosi ad un recente lavoro di B. Segre ed U. Bartocci [7], si determinano tutte le ovali di traslazione di un piano di Galois di caratteristica due col dimostrare che, denotando con α una permutazione addittiva di un campo F di Galois d'ordine 2^e, affinché $x \to x^\alpha \cdot x^{-1}$ permuti gli elementi non nulli di F, occorre che α sia della forma $x \to cx^{2^i}$, con c elemento non nullo di F e m.c.d. $(i, e) = 1$.

I. INTRODUCTION

Let Π be a finite projective plane of order q. An ovoid Ω of Π is a set of $q + 1$ points no three of which are collinear. Through each point of Ω there is a unique *tangent* line, incident with no other point of Ω, and the concept of ovoid generalizes that of nondegenerate conic. It turns out that by a well-known Theorem of Segre [5] the two concepts are equivalent for desarguian planes of odd order. On the other hand, it is still an open problem to determine all the ovoids in desarguian planes of order $q = 2^e$. It is the purpose of this Note to completely determine the so-called translation ovoids (defined below) in this case.

Let F be the finite field with $q = 2^e$ elements, and let Π be the desarguian plane coordinatized by F in the usual ternary ring fashion (cfr. [1]). Let Ω be an ovoid of Π. In this case the $q + 1$ tangents of Ω are known to meet at a point N of Π called the *nucleus* of Ω (cfr. B. Segre [6], p. 157, Corollary, or [2]). By choosing coordinates for Π in a suitable manner we may assume that $\Omega = \{(c, c^\alpha) \mid c \in F\} \cup \{(\infty)\}$ and $N = (0)$, where α is a permutation of the elements of F satisfying

$$0^\alpha = 0 \tag{1}$$

$$1^\alpha = 1 \tag{2}$$

$$\frac{c_0^\alpha - c_1^\alpha}{c_0 - c_1} \neq \frac{c_0^\alpha - c_2^\alpha}{c_0 - c_2}, \quad \text{for distinct} \quad c_0, c_1, c_2 \in F. \tag{3}$$

If α satisfies (3) and is additive, i.e. $(x + y)^\alpha = x^\alpha + y^\alpha$ for $x, y \in F$, then the resulting ovoid Ω is said to be a *translation* ovoid. In that case $0^\alpha = 0$, and by adjusting α by a scalar multiple we may assume (2) is satisfied. Henceforth in this paper we assume that translation ovoids Ω (" ovali di

(*) Nella seduta del 13 novembre 1971.

traslazione " in the terminology of [7]) are given by α which satisfy (2). Note also that for additive α (3) may be restated as

(3)′ α is an additive permutation of F such that $x \to x^{\alpha} \cdot x^{-1}$ permutes the nonzero elements of F.

As a consequence of the Dedekind Independence Theorem (cfr. [3], p. 32), each additive map $\alpha : F \to F$ has a unique representation of the form

$$\alpha : x \to \sum_{i=0}^{e-1} a_i x^{2^i}, \qquad a_i \in F . \tag{4}$$

For $a_0 , a_1 , \cdots , a_{e-1} \in F$, define the matrix

$$\{a_0 , a_1 , \cdots , a_{e-1}\} = \begin{pmatrix} a_0 & a_1 & \cdots & a_{e-1} \\ a_{e-1}^2 & a_0^2 & \cdots & a_{e-2}^2 \\ \vdots & & & \\ a_1^{2^{e-1}} & a_2^{2^{e-1}} & , \cdots , & a_0^{2^{e-1}} \end{pmatrix} . \tag{5}$$

Hence if $\{a_0 , a_1 , \cdots , a_{e-1}\} = (b_{ij})_{1 \le i \le e}^{1 \le j \le e}$ then $b_{ij} = a_{[j-i]}^{2^i}$, where in $a_{[k]}$, $[k]$ indicates k is to be reduced modulo e to one of 0 , 1 , $\cdots$, e — 1.

A fundamental result of Segre and Bartocci [7] is that the map α given in (4) is nonsingular if and only if $\{a_0 , a_1 , \cdots , a_{e-1}\}$ is. Furthermore, the determinant $|\{a_0 , a_1 , \cdots , a_{e-1}\}|$ always equals zero or 1, and α satisfies (3)′ if and only if $a_0 = 0$ and

$$|\{\lambda , a_1 \cdots a_{e-1}\}| = \lambda^{2^e - 1} + 1 , \tag{6}$$

where λ is an indeterminate. By taking a careful look at the coefficients of λ^j, $1 \le j < 2^e$, we will show that only one a_i may be nonzero so that, assuming (2), α must be of the form $\alpha : x \to x^{2^i}$. But $x \to x^{2^i} \cdot x^{-1} = x^{2^i - 1}$ permutes the nonzero elements of F if and only if 2^i — 1 and 2^e — 1 are relatively prime which is if and only if i and e are relatively prime. This solves the Problem (though not the General Problem) of [4]. For additional remarks and references we recommend [7].

II. Proof of Main Result

Put $f(\lambda) = |\{\lambda , a_1 , \cdots , a_{e-1}\}|$. Then $f(\lambda)$ is clearly a monic polynomial of degree $2^0 + 2^1 + \cdots + 2^{e-1} = 2^e$ — 1. Furthermore, the coefficient of λ^t, $0 \le t \le 2^e$ — 1, is calculated as follows. Let $t = \sum_{i=1}^{e} t_i 2^{i-1}$, where $t_i = 0$ or 1. Suppose $t_{i_1} , \cdots , t_{i_k}$ are precisely those t_i's equal to 1. Then the coefficient of λ^t in $f(\lambda)$ is $\sum_{\sigma} b_{1\sigma(1)} b_{2\sigma(2)} \cdots b_{e\sigma(e)}$, where $b_{ij} = a_{[j-i]}^{2^i}$ and the

summation is extended over those permutations σ which fix $i_1, \cdots, i_k$ and move all other elements of $\{1, \cdots, e\}$.

An alternate description of the coefficient of λ^t is easily derived from the one just given. Suppose $j_1, j_2, \cdots, j_r$ are the complementary indices to $i_1, \cdots i_k$, i.e. $t_{j_1}, \cdots, t_{j_r}$ are precisely the t_i's equal to zero in the binary representation of t. Let M_t be the $r \times r$ principal minor obtained from $\{\lambda, a_1, \cdots, a_{e-1}\}$ by selecting the rows and columns with indices $j_1, \cdots, j_r$ and then putting $\lambda = 0$. Then $|M_t|$ is the coefficient on λ^t. Hence for $1 < t < 2^e - 1$, $|M_t|$ must be zero for α to satisfy (3)'. We state this as a separate Lemma.

LEMMA 1. *Let* $\alpha : x \to \sum_{i=1}^{e-1} a_i x^{2^i}$, $a_i \in F$, *be a nonsingular mapping of* F. *Let* $B = (b_{ij})$, *where* $b_{ij} = a_{[j-i]}^{2^i}$, $1 \leq i, j \leq e$, *and* a_0 *is interpreted as zero. Then* α *satisfies* (3)' (*and hence* (3)) *if and only if each* $k \times k$ *principal minor of* B *is singular,* $1 < k < 2^e - 1$.

LEMMA 2. *Let* $i_1, \cdots, i_k$ *be any* k *elements from among* $1, \cdots, e$, $2 \leq k < e$. *Then* $a_{[i_2-i_1]} \cdot a_{[i_3-i_2]} \cdots a_{[i_k-i_{k-1}]} \cdot a_{[i_1-i_k]} = 0$.

Proof. The proof is by induction on k. First suppose $k = 2$, and let $t = \sum_1^e t_i 2^{i-1}$ where $t_{i_1} = t_{i_2} = 0$, and $t_j = 1$ for $j \neq i_1, i_2$. Then the coefficient of λ^t in $f(\lambda)$ is $|M_t| = a_{[i_2-i_1]}^{2^{i_1-1}} \cdot a_{[i_1-i_2]}^{2^{i_2-1}} = 0$. Hence $a_{[i]} \cdot a_{[-i]} = 0$ for all i mod e, and the Lemma holds for $k = 2$. Now let $2 < k < e$, and suppose the Lemma holds for all $k' < k$. Let $i_1, \cdots, i_k$ be any k distinct elements from among $1, \cdots, e$. Let M be the principal minor obtained from B by selecting rows and columns indexed $i_1, \cdots, i_k$, and setting $\lambda = 0$. Then $|M|$, which must be zero, is the sum of all monomials of the form $a_{[j_2-j_1]}^{2^{j_1-1}} a_{[j_3-j_2]}^{2^{j_2-1}} \cdots a_{[j_k-j_{k-1}]}^{2^{j_{k-1}-1}} a_{[j_1-j_k]}^{2^{j_k-1}}$, where $(j_1, \cdots, j_k)$ is a permutation of $i_1, \cdots, i_k$ (which by the induction hypothesis we may assume is a cycle of length k). Suppose there are two cycles $(j_1, \cdots, j_k)$, and $(j_1', \cdots, j_k')$ of $i_1, \cdots, i_k$ for which the corresponding monomials are nonzero. Without loss of generality we may suppose $j_1 = j_1'$, $j_2 \neq j_2'$, and $a_{[j_2-j_1]} \cdots a_{[j_1-j_k]} \neq 0 \neq a_{[j_2'-j_1']} \cdots a_{[j_1'-j_k']}$. Say $j_2' = j_i$ for some i, $2 < i \leq k$. Then $a_{[j_i-j_1]} \cdot a_{[j_{i+1}-j_i]} \cdots a_{[j_k-j_{k-1}]} \cdot a_{[j_1-j_k]} \neq 0$ with $j_1, j_i, j_{i+1}, \cdots, j_k$ being fewer than k (but at least two) distinct integers from among $1, \cdots, e$. This contradicts the induction hypothesis. Hence at most one of the monomials summing to zero can be nonzero and the Lemma is proved for k.

Now consider the coefficient of λ^0 which is $|B| = 1$. Expanding $|B|$ we see it is a sum of monomials of the form $a_{[j_2-j_1]}^{2^{j_1-1}} \cdots a_{[j_e-j_{e-1}]}^{2^{j_{e-1}-1}} \cdot a_{[j_1-j_e]}^{2^{j_e-1}}$ where $(j_1, \cdots, j_e)$ is a permutation of $1, \cdots, e$, which by Lemma 2 we may assume to be a cycle of length e. If two monomials are nonzero corresponding to distinct cycles $(j_1, \cdots, j_e)$ and $(j_1', \cdots, j_e')$ respectively, then Lemma 2 is

contradicted by a step similar to one used in its proof. So only one monomial can be nonzero, and of course it must be nonzero. If a_i and a_j are both nonzero, $1 \leq i < j < e$, it is easy to find two monomials nonzero. Hence α *must be of the form* $\alpha : x \to a_i x^{2^i}$. As mentioned in the introduction, such an α satisfies $(3)'$ if and only if g.c.d. $(i, e) = 1$.

REFERENCES

[1] M. HALL, Jr., *The Theory of Groups*, Macmillan, 1959.
[2] G. E. MARTIN, *On Arcs in a Finite Projective Plane*, «Canad. J. Math.», *19*, 376–393 (1967).
[3] P. J. MCCARTHY, *Algebraic Extensions of Fields*, Blaisdell 1966.
[4] S. E. PAYNE, *Linear Transformations of a Finite Field*, «American Math. Monthly», *78*, 659–660 (1971).
[5] B. SEGRE, *Ovals in a Finite Projective Plane*, «Canad. J. Math.», 7, 414–416 (1955).
[6] B. SEGRE, *Introduction to Galois geometries*, «Mem. Acc. Naz. Lincei», (8) *8*, 133–236 (1967).
[7] B. SEGRE and U. BARTOCCI, *Ovali ed altre curve nei piani di Galois di caratteristica due*, «Acta Arith.», *18*, 423–449 (1971).