COMBINATORICA
Akadémiai Kiadó — Springer-Verlag

COMBINATORICA 9 (3) (1989) 315—320

PLANAR FUNCTIONS OVER FINITE FIELDS

L. RÓNYAI and T. SZŐNYI

Received March 15, 1988

Let $p>2$ be a prime. A function $f: GF(p)\to GF(p)$ is planar if for every $a\in GF(p)^*$, the function $f(x+a)-f(x)$ is a permutation of $GF(p)$. Our main result is that every planar function is a quadratic polynomial. As a consequence we derive the following characterization of desarguesian planes of prime order. If P is a projective plane of prime order p admitting a collineation group of order p^2, then P is the Galois plane $PG(2,p)$. The study of such collineation groups and planar functions was initiated by Dembowski and Ostrom [3] and our results are generalizations of some results of Johnson [8].

We have recently learned that results equivalent to ours have simultaneously been obtained by Y. Hiramine and D. Gluck.

Introduction

The following construction comes from the theory of flat affine planes (see [10]) and was extended to the finite case by Dembowski and Ostrom [3]:

Consider a function $f: GF(q)\to GF(q)$ and denote by $\tilde{f}$ the graph of f in the affine plane $AG(2,q)$ over $GF(q)$. Construct a new incidence structure (for the definitions, see [2]) $I(f)=(P,B,\in)$ in which the points (elements of P) are the points of $AG(2,q)$, the blocks (elements of B) are the translates of $\tilde{f}$ together with the vertical lines of $AG(2,q)$ and the incidence is the usual 'element of' relation.

Definition 1. A function $f: GF(q)\to GF(q)$ is called planar iff the new incidence structure $I(f)$ is an affine plane.

Remark 1. Planar functions over an arbitrary field K can be defined similarly.

The simplest example of a planar function is the quadratic polynomial $f: x\mapsto x^2$. One can easily see that this function is planar over a field K iff char $K\neq 2$. Moreover the new affine plane $I(x^2)$ can be coordinatized over K (see [3]). Very recently Johnson [8] proved that over a prime field a function $x\mapsto x^j$ is planar iff $j=2$. As the construction of Dembowski and Ostrom [3] is closely related to planes of order q admitting abelian collineation groups of order q^2, this result of Johnson yields some characterization theorems for the affine Galois planes of prime order. For a detailed description of this relationship we refer to Johnson [8]. The aim of this paper is to study planar functions over finite fields. Our main theorem on the uniqueness of planar functions over prime fields will be proven in Section 2.

AMS subject classification (1980): 05 B 25, 11 T 21, 51 E 15

Our proof needs some algebraic number theory. More precisely we use some properties of cyclotomic fields and Gauss sums. Similar arguments were used to difference sets by Yamamoto [13].

Theorem 1. *Let $p>2$ be a prime and f a planar function over $GF(p)$. Then f is a quadratic polynomial.*

In Section 1 some preliminary results are stated. Furthermore we study those planar functions for which the plane $I(f)$ is a translation plane (see Propositions 2, 3). By the above-mentioned connection with collineation groups our main theorem has the following corollary.

Theorem 2. *Let $p>2$ be a prime and P be a projective plane of order p admitting a collineation group of order p^2. Then P is the Galois plane $PG(2,p)$.*

Proof. It is well known that there are no proper translation planes of prime order (cf. [2], [12]), so Theorem 2 follows immediately from [8, Lemma (2.6)] and our Theorem 1. ∎

Additional results on collineations of planes of prime order can be found in Goncalves and Ho [5].

1. Preliminaries

First we recall some results of Dembowski and Ostrom [3] on the structure of $I(f)$ if f is a planar function.

Result 1. (a) (cf. Lemma 12 of [3])
f is a planar function iff
$x\mapsto f(x+u)-f(x)$ is a permutation for every fixed $u\neq 0$.
(b) (cf. Theorem 6 and Corollary 2 of [3])
If f is planar then $I(f)$ can be coordinatized by a commutative cartesian system.
(c) (cf. Theorem 2 of [3] or [12, App. 5])
The plane $I(f)$ admits an orthogonal polarity interchanging the ideal line and the ideal point of vertical lines.

These results have several easy but interesting consequences. Propositions 1—3 are not necessary for the proof of Theorem 1, but contain some nice properties of $I(f)$.

Proposition 1. *If f is a planar function over K, then char $K\neq 2$.*

Proof. If f is a planar function over K then, by Result 1(a), the equation $f(x+u)-f(x)=v$ has a solution x_0. If char $K=2$, then $u+x_0$ $(\neq x_0)$ is an other solution which is impossible by (1). ∎

Proposition 2. *If $I(f)$ is a translation plane then it can be coordinatized by a commutative semifield.*

Proof. As the translation plane $I(f)$ is selfdual by Result 1 (c), it suffices to consider those planes which can be coordinatized by a semifield. But then Result 1 (c) and [4, Theorem 3] give that the plane can be coordinatized by a commutative semifield. ∎

Proposition. 3. *If P is a translation plane with respect to the line l_0 which can be coordinatized by a commutative semifield, then there exists a planar function f such that $P\setminus l_0$ is isomorphic to $I(f)$.*

Proof. Let Q be the commutative semifield coordinatizing P. Then Q is isomorphic to $(GF(q), +, *)$, where $+$ is the usual addition of the field $GF(q)$. The lines of $P\setminus l_0$ have the equation $x=c$ or $y=a*x+b$, while the translates of f have the equation $y=f(x+a)+b$. Take $f(x)=x*x$ and consider the $1-1$ mapping

$$\begin{cases} x\Phi = x \\ y\Phi = y+x*x. \end{cases}$$

Φ transforms the line $y=a*x+b$ into the point-set $y=x*x+a*x+b$ but this is just the line $y=(x+a/2)*(x+a/2)+b-(a/2)*(a/2)$ of $I(x*x)$. So Φ is indeed an isomorphism between P and $I(x*x)$. ∎

For the next statement, which is the cornerstone of the proof of Theorem 1, we need a little algebraic number theory. Let $p>2$ be a prime and $\eta\in\mathbf{C}$ be a primitive p^{th} root of unity. The following result summarizes some well-known properties of the p^{th} cyclotomic field $\mathbf{Q}(\eta)$. (As usual $\mathbf{C}$ denotes the field of complex, $\mathbf{Q}$ denotes the field of rational numbers, $\mathbf{Z}$ denotes the ring of integers.)

Result 2. (a) $\dim_{\mathbf{Q}} \mathbf{Q}(\eta)=p-1$ and $1, \eta, \eta^2, \ldots, \eta^{p-2}$ is a basis of $\mathbf{Q}(\eta)$ over $\mathbf{Q}$.

(b) The ring of integers of $\mathbf{Q}(\eta)$ is $O=\mathbf{Z}[\eta]$.

(c) If $\xi\in O$ and ξ is a root of unity, then $\xi=\pm\eta^i$ for some integer $i\in\mathbf{Z}$.

(d) The ideal $(p)\lhd O$ has the prime factorization $(p)=(1-\eta)^{p-1}$ and $(1-\eta)=(1-\eta^{-1})$.

(e) Let $g_j=\sum_{a=0}^{p-1}\left(\frac{a}{p}\right)\eta^{aj}$ be the quadratic Gauss sum mod p. Here $\left(\frac{a}{p}\right)$ is the Legendre symbol mod p, i.e.

$$\left(\frac{a}{p}\right)=\begin{cases} +1 & \text{if } a \text{ is a quadratic residue mod } p \\ -1 & \text{if } a \text{ is a quadratic non-residue mod } p \\ 0 & \text{if } a\equiv 0 \pmod p. \end{cases}$$

Then $g_j\in O$ and $g_j\bar{g}_j=p$.

(f) (Kronecker's theorem). Let α be an algebraic integer such that for every algebraic conjugate α' of α we have $|\alpha'|\leqq 1$. Then α is a root of unity. Facts (a)—(d) can be found in Ireland and Rosen [7, Chapter 13], (e) in [7, Chapter 6] and (f) is in Borevich and Shafarevich [1, pp. 104—105].

Proposition 4. *Let $z=\sum_{i=0}^{p-1} k_i\eta^i$, $k_i\in\mathbf{Z}$ be an element of $\mathbf{C}$ such that $\sum_{i=0}^{p-1} k_i=p$ and $z'\bar{z}'=p$ for every algebraic conjugate z' of z. Then $|k_i|<3$ for $0\leqq i<p$. More precisely, there exist an integer j and a* sign $e\in\{+1, -1\}$ *such that*

$$k_i-1=e\left(\frac{i-j}{p}\right) \text{ for } 0\leqq i<p.$$

Proof. Clearly we have $z, \bar{z}\in O$. $z\bar{z}=p$ implies that (z) divides (p), therefore $(z)=(1-\eta)^j$ for a positive integer j. The complex conjugation is an automorphism of O, so

$(\bar{z})=\overline{(1-\eta)}^j=(1-\eta^{-1})^j=(1-\eta)^j$, hence $j=(p-1)/2$. Essentially the same argument shows that $(g_k)=(1-\eta)^{(p-1)/2}$ and thus $(g_k)=(z)$. (For the definition of g_j see Result 2 (e).) So there exists a unit $u\in O$ such that $z=g_1u$. Using (e) we obtain that $|u'|=1$ for every algebraic conjugate u' of u, hence by (f) and (c) we have $u=e\eta^j$ where $e\in\{+1,-1\}$ and j is an integer. By (a) the only linear dependence over $\mathbf{Q}$ among the elements $1, \eta, \ldots, \eta^{p-1}$ is $\sum_{i=0}^{n-1}\eta^i=0$ and thus

$$(1)\qquad \sum_{i=0}^{p-1} a_i\eta^i=\sum_{i=0}^{p-1} b_i\eta^i \quad\text{and}\quad \sum_{i=0}^{p-1} a_i=\sum_{i=0}^{p-1} b_i \quad (a_i, b_i\in\mathbf{Q})$$

imply that $a_i=b_i$ for every i. The relation $z=g_1u=g_1e\eta^j$ means that

$$(2)\qquad \sum_{i=0}^{p-1}(k_i-1)\eta^i=e\eta^j\sum_{i=0}^{p-1}\left(\frac{i}{p}\right)\eta^i=e\sum_{i=0}^{p-1}\left(\frac{i}{p}\right)\eta^{i+j}=e\sum_{l=0}^{p-1}\left(\frac{l-j}{p}\right)\eta^l.$$

Applying the previous observation to (2) the statement follows. ∎

Finally, our proof requires the use of the famous theorem of Segre [11] on ovals of Galois planes of odd order. For the basic facts about conics and ovals we refer to [6] and [12].

Result 3. (a) (Segre's theorem [11].) Let q be odd and A be a set of $q+1$ points of the projective Galois plane $PG(2, q)$ no three of which are collinear. Then A is a conic (i.e. A can be described by a quadratic equation).

(b) If q is odd and f: $GF(q)\to GF(q)$ is a function such that the graph $\tilde{f}$ of f has no three collinear points in $AG(2, q)$, then f is a quadratic polynomial (i.e. $f(x)=ax^2+bx+c$).

Adding the ideal point of vertical lines to $\tilde{f}$ we get a set of $q+1$ points no three of which are collinear. This is a conic having one ideal point the ideal point of vertical lines, hence its equation is $y=ax^2+bx+c$ (in affine coordinates). Thus (b) is an easy consequence of (a).

2. Proof of Theorem 1

In the first part of the proof we deduce the fundamental relation (3) (see below) using characters of abelian groups. This relation can be obtained by elementary counting arguments as well, see Remark 3.

Let χ be a character of the additive group $G=(GF(p), +)\times(GF(p), +)$ (i.e. χ is a homomorphism from G into the multiplicative group of complex numbers) and f: $GF(p)\to GF(p)$ be a planar function. Let

$$z=z(\chi, f)=\sum_{x\in GF(p)}\chi((x, f(x)))$$

and express the product $z\bar{z}$.

$$z\bar{z}=\sum_{x\in GF(p)}\chi((x, f(x)))\overline{\sum_{y\in GF(p)}\chi((y, f(y)))}=\sum_{x,y\in GF(p)}\chi((x-y, f(x)-f(y))).$$

As f is a planar function, the pairs (a, b) with $a\neq 0$ can be obtained in the form $(a, b)=(x-y, f(x)-f(y))$ once (c.f. Section 1 Result 1 (a)), the pairs $(0, b)$ with

$b\neq 0$ cannot be obtained and finally (0, 0) occurs p times. Thus if χ is a non-principal character (i.e. there exists a $g\in G$ such that $\chi(g)\neq 1$), then

$$z\bar{z} = \sum_{\substack{x,y\in GF(p)\\ x\neq y}} \chi((x-y, f(x)-f(y)))+p = \sum_{\substack{a,b\in GF(p)\\ a\neq 0}} \chi(a, b)+p = p.$$

Now let χ_0 be a non-principal character of $(GF(q), +)$ and extend χ_0 to G in the natural way by $\chi((u, v))=\chi_0(v)$. Obviously χ is a non-principal character of G. In this case

$$z = \sum_{x\in GF(p)} \chi((x, f(x))) = \sum_{x\in GF(p)} \chi_0(f(x)) = \sum_{j\in GF(p)} k_j\chi_0(j),$$

where k_j is the number of solutions of $f(x)\equiv j \pmod p$. Moreover

$$\sum_{j=0}^{p-1} k_j = p.$$

If $\xi=\chi_0(1)$ (which is a p^{th} root of unity), then $\chi_0(j)=\xi^j$ and the equation $z\bar{z}=p$ gives

$$\sum_{j=0}^{p-1} k_j\xi^j \overline{\sum_{j=0}^{p-1} k_j\xi^j} = p. \tag{3}$$

As χ_0 can be chosen arbitrarily, (3) holds for every p^{th} root of unity $\xi\neq 1$. In other words, equation (3) remains true for every algebraic conjugate z' of z. But this is exactly the situation described in Proposition 4, thus $k_j=0$, 1 or 2 for each j. Geometrically this means that the horizontal lines meet $\tilde{f}$ in at most two points. If f is planar then, by Result 1 (a), $f(x)-ax$ is also planar for every fixed $a\in GF(p)$. Repeating the same argument for the function $f(x)-ax$ we infer that the lines with slope a meet $\tilde{f}$ in at most two points. Thus the graph $\tilde{f}$ of f has no three collinear points and Result 3 (b) gives that $f(x)=ax^2+bx+c$, proving our main theorem. ∎

Remark 2. If f is planar, then by Result 1 (a) $f(x+a)-f(x)$ is a permutation polynomial for every $a\neq 0$. If we require that $f(x+a)+f(x)$ is a permutation polynomial for every $a\in GF(p)$, then

$$\{(-x, f(x))\ x\in GF(p)\}+\{(y, f(y))\ y\in GF(p)\}$$

is a factorization of the group $G=(GF(p), +)\times(GF(p), +)$ and, by a theorem of Rédei [9, Thm. 23], f has to be linear. The idea of using additive characters of G comes from Rédei's proof.

Our proof (and the used facts from algebraic number theory) are similar to Yamamoto [13].

Remark 3. As in the proof let f be planar and k_i be the number of solutions of the congruence $f(x)\equiv i \pmod p$. Obviously

$$\sum_{i=0}^{p-1} k_i = p. \tag{4'}$$

Counting the pairs (u, v) $u \neq v$ with $f(u)=f(v)$ we get

$$(4'') \qquad \sum_{i=0}^{p-1} k_i(k_i-1) = p-1.$$

Similarly, for each fixed $h \neq 0$ counting the pairs (u, v) with $f(u)-f(v)=h$ we get

$$(4''') \qquad \sum_{i=0}^{p-1} k_i k_{i+h} = p-1.$$

Now it is easy to see that

$$\sum_{i=0}^{p-1} k_i \zeta^i \cdot \overline{\sum_{i=0}^{p-1} k_i \zeta^i} = p,$$

which is just the equation (3). The end of the proof is similar to the original one. Finally, we mention an open question about a possible generalization of Theorem 1 to $q=p^e$ $(e>1)$. If $q=p^e$ with $e>1$ then there are planar functions over $GF(q)$ of the form

$$f(x) = \sum_{i,j=0}^{e-1} a_{ij} x^{p^i+p^j}.$$

Question. Let $q=p^e$ $(e>1)$ and f be a planar function. Can f be transformed into the form

$$f(x) = \sum_{i,j=0}^{e-1} a_{ij} x^{p^i+p^j} + \sum_{k=0}^{e-1} b_k x^{p^k}$$

by a linear transformation?

References

[1] Z. I. BOREVICH and I. R. SHAFAREVICH, Number theory, *Academic Press*, New York, 1966.
[2] P. DEMBOWSKI, *Finite Geometries*, Springer-Verlag, Berlin, 1968.
[3] P. DEMBOWSKI and T. G. OSTROM, Planes of order n with collineation groups of order n^2, *Math. Zeit.*, **103** (1968), 239—258.
[4] M. GANLEY, Polarities of translation planes, *Geom. Ded.*, **1** (1972), 103—116.
[5] A. GONCALVES and C. Y. HO, On collineation groups of a projective plane of prime order, *Geom. Ded.*, **20** (1986), 357—366.
[6] J. W. P. HIRSCHFELD, *Projective Geometries over Finite Fields*, Clarendon Press, Oxford, 1979.
[7] K. IRELAND and M. ROSEN, *A classical introduction to modern number theory*, GTM 84, Springer-Verlag, Berlin 1982.
[8] N. L. JOHNSON, Projective planes of order p that admit collineation groups of order p^2, *J. of Geom.*, **30** (1987), 49—68.
[9] L. RÉDEI, *Lacunary polynomials over finite fields*, Akadémiai Kiadó, Budapest, 1973.
[10] H. SALZMANN, Topological planes, *Advances in Math.*, **2** (1967), 1—60.
[11] B. SEGRE, Ovals in a finite projective plane, *Can. J. Math.* (1955), 414—416.
[12] B. SEGRE, *Lectures on Modern Geometry*, Cremonese Roma, 1961.
[13] K. YAMAMOTO, On Jacobi Sums and Difference Sets, *J. Comb. Th.* **3** (1967), 146—181.

L. Rónyai

Department of Computer Science
The University of Chicago
Ryerson Hall, 1100 E. 58th Street
Chicago, IL 60637, USA

L. Rónyai and T. Szőnyi

Computer and Automation Institute
Hungarian Academy of Sciences
H—1502 Budapest, P. O. B. 63. HUNGARY