Arab Gulf J. Scient. Res., Math. Phys. Sci., **A7** (1), pp. 21-28 (1989)

On the Geometry of Affine Difference Sets of Even Order

Dieter Jungnickel[*]

Mathematisches Institut, Justus-Liebig-Universität Giessen
Arndtstr. 2, D-6300 Giessen, F.R. Germany

ABSTRACT. Let A be an affine plane of even order which admits a representation by an affine difference set D in an abelian group G (relative to N), say $G = H \oplus N$. We discuss various hyperovals of A related to this representation: $(-D+y) \cup \{\infty\}$ is an oval with nucleus y (assuming w.l.o.g. $D = 2D$), and the sets $H + n$ ($n \in N$) (which form a partition of $A \setminus \{\infty\}$) are ovals with common nucleus ∞. In case $A = AG(2,2^a)$, all these ovals are in fact conics (for which we give explicit equations). In particular, the points of $AG(2,2^a) \setminus \{(0,0)\}$ can be partitioned into $2^a - 1$ conics with common nucleus (0,0); moreover, there are commuting cyclic groups H and N such that H acts regularly on each of these conics whereas N acts regularly on the set of all these conics.

1. Introduction and General Results

Let G be a group of order $n^2 - 1$, and let N be a normal subgroup of order $n - 1$. An n-subset D of G is called an *affine difference set* of *order n* (relative to N) if the following condition holds:

(1) $\{d - d' : d, d' \in D,\ d \neq d'\} = G \setminus N$,

i.e. if each $g \in G \setminus N$ has a unique representation as a difference $g = d - d'$ for suitable $d, d' \in D$. Then the incidence structure

$$\text{dev } D = (G, \{D+g;\ g \in G\}, \in)$$

is a *biaffine plane* of order n admitting G as a normal Singer group, *cf.* Jungnickel

[*] During the time of this research, the author was a Visiting Professor at the University of Waterloo. He would like to thank this institution for its hospitality and NSERC for financial assistance under grant # IS-0367.

(1987a). If one adjoins to dev D a further point ∞ and new lines $(N+g) \cup \{\infty\}$ (where g runs over a system of coset representatives of N), one obtains an affine plane $\mathbf{A} = \mathbf{A}(D)$; *cf.* Hoffman (1952). It was proved by Bose (1942) that the Desarguesian affine plane AG (2,q) always can be represented in this way, using a cyclic affine difference set. Hoffman (1952) was the first author to study *cyclic affine planes, i.e.* affine planes admitting a representation by a cyclic affine difference set. In spite of much work, his *prime power conjecture* (stating that cyclic affine difference sets exist only for prime power order) remains still unresolved, though it is verified for orders up to 5000 (*cf.* Ko and Ray-Chaudhuri (1981)). We mention Arasu and Jungnickel (1988), Jungnickel (1988a,b), Ko and Ray-Chaudhuri (1981,1982) and Pott (1988) as examples of recent work on existence conditions for both (cyclic and general) affine difference sets.

In the present note, G is always assumed to be abelian and n is even. We also assume (w.l.o.g.) that D is fixed under the "multiplier" 2 (*cf.* Hoffman (1952)), *i.e.* that D = 2D. Then the sets $B_y = (-D+y) \cup \{y\}$ $(y \in G)$ are ovals of the affine plane $\mathbf{A}(D)$ with common nucleus ∞, see Jungnickel (1986, 1987a). (We refer the reader to Hirschfeld (1979) or Hughes and Piper (1973) for ovals and hyperovals in (affine or projective) planes). Thus, we obtain $n^2 - 1$ hyperovals $H_y = B_y \cup \{\infty\}$ through ∞. (If n is odd, one may still show that the sets $(-D+y) \cup \{\infty\} = C_y$ are ovals of $\mathbf{A}$). In the case $\mathbf{A} = AG(2,2^a)$ we shall see that the hyperovals H_y are regular: more precisely, the ovals C_y are in fact conics. In the odd order case, the corresponding result is clear from the theorem of Segre (1955). Note that always the sets $-D + y$ induce a biaffine geometry dev $(-D)$ isomorphic to dev D; thus we may obtain an isomorphic copy of the classical biaffine plane of order q by using $q^2 - 1$ conics of AG(2,q) from each of which one point is omitted.

These results are in analogy to the resuls on the geometry of planar difference sets (see Beth, Jungnickel and Lenz (1985) for background on difference sets) obtained by Jungnickel and Vedder (1984). If D is a planar abelian difference set of order n in G, then the sets $-D + y$ $(y \in G)$ are ovals of D which induce a projective plane dev$(-D)$ isomorphic to dev D. In the classical case dev D = PG(2,q), these ovals are always conics. Such systems of $q^2 + q + 1$ conics of PG(2,q) forming an isomorphic plane have found some interest also in studying the geometry of $GF(q^3)$, see Sherk (1986). More generally, the connections between "divisible semiplanes", "arcs" and "relative difference sets" (of which the projective and affine cases discussed above are particular examples) are studied by Jungnickel (1987a).

We now return to the affine case. Thus let D = 2D be once again an abelian affine difference of even order n in G, relative to N. Since $n - 1$ and $n + 1$ are coprime, G splits as $G = H \oplus N$, where H is the subgroup of order $n + 1$ of G. Recent results of Arasu and Jungnickel (1988) imply that $\mathbf{A} = \mathbf{A}(D)$ contains another class of hyperovals naturally associated with D. In proving a new non-existence result (*i.e.*, that n is divisible by 8 for n $\neq$ 2,4 and that there exists a Hadamard difference set in N), a crucial step was the following result:

For each y $\in$ N, the number of elements h $\in$ H with (h,y) $\in$ D is either exactly 2 or 0, *cf.* the proof of Theorem 2 in Arasu and Jungnickel (1988). This obviously implies that $|(H+y) \cap (D+x)| \in \{0,2\}$ for all x $\in$ G and all y $\in$ N. In other words, the cosets H + y of H are also ovals of **A;** the tangents of H + y are the new lines $(N+g) \cup \{\infty\}$, and the nucleus of H + y is ∞. (This result in fact still holds if N is abelian but H is non-abelian. However, no examples of this situation are known). We shall see later that the ovals H + y are in fact again conics for **A** = $AG(2,2^a)$. We now summarize our discussion:

1.1. *Theorem*

Let D = 2D be an abelian affine difference set of even order n in G = H$\oplus$N (relative to N). Then one has the following:

(i) The sets $-D + y$ (y $\in$ G) form a biaffine plane isomorphic to dev D, and the sets $B_y = (-D+y) \cup \{y\}$ are ovals of the affine plane **A** = **A**(D) with common nucleus ∞.

(ii) The sets H + y (y $\in$ N) are n $-$ 1 pairwise disjoint ovals of **A** with common nucleus ∞. The group N acts regularly on each of these ovals, and the group H acts regularly on the set of all ovals H + y.

The existence of the ovals described in (ii) seems intuitively a severe restriction on **A** which lends some evidence to the following conjecture:

1.2 *Conjecture*

Let D be an abelian affine difference set of even order n in G. Then the affine plane **A** = **A**(D) is Desarguesian and G is cyclic.

With the purpose of better understanding the geometric situation described in Theorem 1.1, we shall now consider the classical case **A** = $AG(2,2^a)$ and show - as already mentioned - that all the ovals encountered from studying affine difference sets are then in fact conics. As the work of Sherk (1986) indicates, sets of conics with properties similar to those considered here (or in the projective case, *cf.* Jungnickel and Vedder (1984)) may also be of some intrinsic geometric interest.

2. The Classical Case

Let **A** = AG(2,q) where $q = 2^a$. We may represent the points of **A** by the elements of $GF(q^2)$. (We assume the reader to be familiar with the basic theory of finite fields; *e.g.* Lidl and Niederreiter (1983).) We can choose an irreducible polynomial of the form $x^2 + x + d$ over GF(q) to define $GF(q^2)$ (since the mapping $x \to x^2 - x$ on GF(q) is not injective, for $0 = 0^2 + 0 = 1^2 + 1$, and thus not surjective). Let α be a root of this polynomial, *i.e.*

(2) $\alpha^2 = \alpha + d$.

We shall use the basis $(1,\alpha)$ of $GF(q^2)$ over GF(q); thus the points of **A** are the elements $x + y\alpha$ ($x,y \in GF(q)$). Consider the line L with equation $y = 1$, *i.e.* the line $\{x+\alpha : x \in GF(q)\}$, and note that L is fixed under squaring:

(3) $(x+\alpha)^2 = (x^2+d) + \alpha$.

Now the Singer group G of the biaffine plane $\mathbf{D} = \mathbf{A}\backslash\{(0,0)\}$ is induced by the linear mappings

$$\gamma_b\colon z \to bz \quad (z \in GF(q))$$

for $b \in GF(q^2)^*$ and is, of course, cyclic. If ω is a generator of $GF(q^2)^*$, we may identify the point ω^i ($i = 0,\ldots,q^2-2$) of D with the element $i \in \mathbf{Z}_{q^2-1}$. Then the "exponents" of the elements of L form an affine difference set D in $\mathbf{Z}_{q^2-1}$ which, because of (3), is fixed by the multiplier 2. (Note that $x + \alpha = \omega^i$ implies $(x+\alpha)^2 = \omega^{2i}$).

We now want to compute the coordinates of the points in $-D$ relative to the basis $(1,\alpha)$. Using (2) one checks that

$$(x+\alpha)(1+x+\alpha) = x^2 + x + d \quad (x \in GF(q));$$

thus the inverse of $x + \alpha \in GF(q^2)^*$ is

(4) $$(x+\alpha)^{-1} = \frac{x+1}{x^2+x+d} + \frac{1}{x^2+x+d}\,\alpha$$

Hence

(5) $$-D \triangleq \{\frac{x+1}{N} + \frac{\alpha}{N} : x \in GF(q)\},$$

where $N = x^2 + x + d$. Put $\frac{x+1}{N} = \zeta$ and $\frac{1}{N} = \eta$ and note

$$\eta + 1 = \frac{1+N}{N} = \frac{x^2+x+d+1}{N}$$

Thus

$$\eta(\eta+1) = \frac{x^2+x+d+1}{N^2} = \zeta^2 + \zeta\eta + (d+1)\eta^2,$$

and thus the point set corresponding to $-D$ satisfies the equation

$$(6) \quad d\eta^2 + \zeta^2 + \zeta\eta + \eta = 0.$$

Note that the origin $\infty = (0,0)$ also satisfies equation (6). Hence the oval C_0 belonging to $-D$ is indeed the conic with equation (6). It is clear, then, that all C_y are conics, since they form the orbit of C_0 under the group G. (In fact, the conics in the orbit of the subgroup $H \cong GF(q)^*$ of G are given by the equations $d\eta^2 + \zeta^2 + \zeta\eta + c\eta = 0$, $c \in GF(q)^*$. We omit determining the equations for the remaining conics). Thus we have proved:

2.1 *Theorem*

Let $\mathbf{A} = AG(2,q)$ where q is even. Then $\mathbf{A}$ can be represented by a cyclic affine difference set D fixed under the multiplier 2 for which the oval $C_0 = -D \cup \{\infty\}$ is the conic with equation (6).

We note that Theorem 2.1 remains in fact true for every field of characteristic 2 which admits field extensions of degree 2. A similar discussion is possible for fields of characteristic $\neq 2$. In view of Segre's Theorem, however, this is only interesting in the infinite case. We have therefore preferred to only give the case of characteristic 2.

We now turn our attention to the subgroup H of order $q + 1$ of $GF(q^2)^*$. In order to conveniently represent H, we have to exercise a little more care in choosing the irreducible polynomial $x^2 + x + d$. In fact, we want the root α of this polynomial to have order a multiple of $q + 1$ in $GF(q^2)^*$. It is possible to choose a *primitive* polynomial of the form x^2+x+d over GF(q); *i.e.*, its root α has order q^2-1 in $GF(q^2)^*$. This is a special case of a considerably more general result of Jungnickel and Vanstone (1988). We remark in passing that the existence of some primitive polynomial of degree 2 over GF(q) together with a result of Jungnickel (1987b) could be used to give an elementary proof for the existence of a polynomial x^2+x+d with root α which has order a multiple of $q+1$.

Using an irreducible polynomial of either of the types discussed above, we can easily represent H; If $o(\alpha) = c(q+1)$, then $H = <\alpha^c> = <\alpha^{q-1}>$, since c divides $q - 1$ and since $|H| = q+1$ and $(0-1)/c$ are coprime. We shall now show that H is a conic of $\mathbf{A}$.

As α^q is the second root of $x^2 + x + d = 0$, we have $\alpha^q = 1 + \alpha$ and thus $\beta = \alpha^{q-1} = 1 + \frac{1}{\alpha} = \frac{d+1}{d} + \frac{\alpha}{d}$; the last equality holds as $(\alpha+1)d = (d+1+\alpha)\alpha$ by (2). Hence

$$(7)\quad H = \{1,\beta, \ldots, \beta^q\} = \{(\frac{d+1}{d} + \frac{\alpha}{d})^i \colon i = 0,\ldots,q\}.$$

We now claim that H is the conic with equation

$$(8)\quad \zeta^2 + d\eta^2 + \zeta\eta = 1.$$

Clearly, $1 = 1 + 0\alpha$ satisfies (8). In view of (7) it is therefore sufficient to prove that (8) holds for

$$\zeta' + \eta'\alpha = (\zeta+\eta\alpha)\beta = (\zeta + \frac{\zeta}{d} + \eta) + (\eta + \frac{\zeta}{d})\alpha$$

whenever it holds for $\zeta + \eta\alpha$. This is easily checked. Obviously then the cosets of H are just the conics with equations

$$(9)\quad \zeta^2 + d\eta^2 + \zeta\eta = c \ (c \in GF(q)^*).$$

Thus we have the following result:

2.2 *Theorem*

Let **A** = AG(2,q), where q is even. Then the conics with equations (9) are pairwise disjoint and have the same nucleus (*i.e.*, the origin (0,0)). Moreover, **A** admits a representation by a cyclic affine difference set in $G = H \oplus N$ such that the following holds:

(i) The conics with equation (9) are the cosets of H in G.
(ii) H acts regularly on each conic given by (9).
(iii) N acts regularly on the set of $q - 1$ conics given by (9).

References

Arasu, K.T. and **Jungnickel, D.** (1988) Affine difference sets of even order. *J. Comb. Th. (A).*, to appear.

Beth, T., Jungnickel, D. and **Lenz, H.** (1985) Design Theory. Bibliographisches Institut, Mannheim and Cambridge University Press, Cambridge.

Bose, R.C. (1942) An affine analogue of Singer's Theorem. *J. Indian Math. Soc.* **6:** 1-15.

Hirschfeld, J.W.P. (1979) Projective geometries over finite fields. Oxford University Press, Oxford.

Hoffman, A.J. (1952) Cyclic affine planes. *Canadian J. Math.* **4:** 295-301.

Hughes, D.R. and **Piper, F.C.** (1973) Projective Planes, Springer, Berlin-Heidelberg-New York.

Jungnickel, D. (1986) A note on affine difference sets. *Archiv. Math.* **47:** 279-280.

Jungnickel, D. (1987a) Divisible semiplanes, arcs and relative difference sets. *Canadian J. Math.* **39:** 1001-1024.

Jungnickel, D. (1987b) Eine Bemerkung über endliche abelsche Gruppen. *Math. Semesterber.* **34:** 116-120.

Jungnickel, D. (1988a) On automorphism groups of divisible designs, II. Group invariant generalized conference matrics. *Archiv. Math.*, to appear.

Jungnickel, D. (1988b) On affine difference sets. Submitted.

Jungnickel, D. and **Vanstone, S.A.** (1988) On primitive polynomials over finite fields. *J. Algebra*, to appear.

Jungnickel, D. and **Vedder, K.** (1984) On the geometry of planar difference sets. *European J. Comb.* **5:** 143-148.

Ko, H.P. and **Ray-Chaudhuri, D.K.** (1981) Multiplier theorems. *J. Comb. Th. (A)* **30:** 134-157.

Ko, H.P. and **Ray-Chaudhuri, D.K.** (1982) Intersection theorems for group divisible difference sets. *Discr. Math.* **39:** 37-58.

Lidl, R. and **Neiderreiter, H.** (1983) Finite fields. Addison-Wesley, Reading Mass.

Pott, A. (1988) An affine analogue of Wilbrink's theorem. *J. Comb. Th. (A), to appear.*

Segre, B. (1955) Ovals in a finite projective plane. *Canadian J. Math.* **7:** 414-416.

Sherk, F.A. (1986) The geometry of GF(q^3). *Canadian J. Math.* **38:** 672-696.

(Received 14/02/1988;
in revised 28/07/1988)

حول هندسة مجموعات الفروق الافينية ذات الرتب الزوجية

ديتر يونجنيكل

معهد الرياضيات بجامعة جستس ـ ليبج ـ جيسين ـ ألمانيا الاتحادية

لنفرض أن A مستوى أفيني ذو رتبة زوجية ويسمح بتمثيله بمجموعة فرق أفينية D في زمرة آبيلية G بالنسبة إلى N ، وليكن $G = H \oplus N$. وفي هذا البحث ندرس بيضويات فوقية متعددة للمستوى A منسوباً إلى التمثيل : $(-D+y) \cup \{\infty\}$ الذي هو بيضوي ذو نواة y وان المجموعات $H + n$ $(n \in N)$ التي تكون بتجزئة في $A/\{\infty\}$ هي بيضويات ذات نواة مشتركة ∞ . وعندما يكون $A = AG(2, 2^a)$ تكون جميع هذه البيضويات قطوعاً مخروطية تعطيها معادلات واضحة. وبصورة خاصة، من الممكن بتجزئة نقاط $AG(2,2^a)/\{(0,0)\}$ إلى $2^a - 1$ من القطوع المخروطية ذات النواة المشتركة $(0,0)$. وإضافة إلى ذلك، توجد زمر إبدالية دائرية H و N بحيث تؤثر H بصورة منتظمة على كل من هذه القطوع المخروطية، بينما تؤثر N بصورة منتظمة على مجموعة جميع هذه القطوع المخروطية .