Cyclic affine planes and Paley difference sets

K.T. Arasu*
Department of Mathematics and Statistics, Wright State University, Dayton, OH 45435, USA

Alexander Pott
Mathematisches Institut der Universität Gießen, Arndtstraße 2, 6300 Gießen, Germany

Received 22 November 1991
Revised 14 January 1992

Abstract

The existence of a cyclic affine plane implies the existence of a Paley type difference set. We use the existence of this difference set to give the following condition on the existence of cyclic affine planes of order $n$:

If $n - 8 \mod 16$ then $n - 1$ must be a prime. We discuss the structure of the Paley type difference set constructed from the plane.

One of the famous unsolved problems in finite geometry is to prove or disprove the conjecture that the order of a finite projective plane must be a power of some prime $p$. It seems that we are still far away from an answer to this question. In the following we will refer to it as the prime power conjecture (PPC). We can expect to be able to say more if we assume that the plane has some symmetry properties, i.e., admits a certain type of automorphism group. A lot of work has been done on projective planes admitting a quasiregular collineation group, i.e., a group acting in such a way that the stabilizer of each point and line is a normal subgroup. A classification of planes admitting quasiregular collineation groups $G$ with $|G| > (n^2 + n + 1)/2$ was given by Dembowski and Piper [5]. Let us assume that the quasiregular group is abelian. Then in one case of the Dembowski–Piper classification the prime power conjecture is trivially satisfied, namely in the case of translation and dual translation planes. In two cases of the Dembowski–Piper...
classification the PPC is solved if \( n \) is even: These are the cases (b) (which is due to Ganley [7], a simplified proof given by Jungnickel [11]) and (f), again due to Ganley [8]. Cases (a) and (d) correspond to difference sets and affine difference sets. The following is known about the existence of difference sets and affine difference sets.

**Result 1.** Let \( D \) be an abelian difference set or an abelian affine difference set of order \( n \equiv 0 \mod 2 \). Then \( n = 2 \), \( 4 \) or \( n \equiv 0 \mod 8 \).

(The proof of this result spreads over several papers. The papers [2, 12] are just two of these but they are sufficient for a proof of Result 1.) To some extent the investigation of difference sets and affine difference sets is analogous (multiplier theorems, number theory, etc). But the proof of the result above for the classical difference set case and the affine case is quite different. To be more precise: the conclusion \( n \equiv 0 \mod 2 \) implies \( n = 2 \) or \( n \equiv 0 \mod 4 \) can be proved in a similar fashion, however the conclusion \( n \equiv 0 \mod 8 \) needs different arguments. In the affine case the idea is to construct a difference set of Paley type with parameters \((4m - 1, 2m - 1, m - 1)\) where \( n = 4m \) is the order of the affine difference set (hence if \( n \neq 2 \) the order has to be divisible by 4). We hope that a more thorough investigation of these Paley type difference sets would yield more necessary conditions on the existence of affine difference sets of even order. As a first step we will prove the following.

**Theorem 2.** Let \( D \) be a cyclic affine difference set of order \( n \equiv 8 \mod 16 \). Then \( n - 1 \) must be a prime and each prime divisor of \( n \) is a square modulo \( n - 1 \).

Before we start proving this theorem we want to recall the basic definitions and introduce some notation. An affine difference set of order \( n \) is an \( n \)-subset of a group \( G \) (where \( |G| = n^2 - 1 \)) with the following property: There exists a normal subgroup \( N \triangleleft G, |N| = n - 1 \), such that each element \( g \in G \setminus N \) has exactly one representation \( g = d - d' \) with elements \( d, d' \) in \( D \). The existence of such a difference set is equivalent to the existence of a projective plane admitting a quasiregular collineation group of type (d) in the classification of Dembowski and Piper. We call the difference set abelian or cyclic if \( G \) has the respective property. Desarguesian planes admit (cyclic) affine difference sets and planes with such a cyclic group are therefore called cyclic affine planes. For a construction we refer the reader to [3], a first systematic investigation is in [10].

We identify a subset \( A \subseteq G \) with the element \( \Sigma_{g \in A} g \) in a group ring of \( G \). To emphasize the distinction between the addition in a group ring and in the group \( G \) we switch to multiplicative notation. For \( A = \Sigma a_g \) and \( t \) any integer we define \( A^t = \Sigma a_g^t \). Then the existence of an affine difference set is equivalent to the existence of a subset \( D \subseteq G \) satisfying \( D \cdot D^{-1} = n \cdot 1_G + G - N \) where \( 1_G \) is the
identity element in $G$. A (numerical) multiplier of an abelian difference set is an integer $t$ relatively prime to $n^2 - 1$ satisfying $D^{(t)} = D \cdot g$ for some $g \in G$. We can assume w.l.o.g. that $D^{(t)} = D$ and we may even assume that $D$ is fixed under all multipliers. It is the content of Hoffman's multiplier theorem that each divisor of $n$ is a multiplier (Hoffman proved this just for the cyclic case, the abelian case is contained in [6]).

Let us consider an abelian difference set $D$ of even order $n$ in $G$ fixed under all multipliers, i.e., $D^{(t)} = D$ for all divisors of $n$. The group $G$ splits $G \cong H \times N$, $|H| = n + 1$. We apply the canonical epimorphism $G \to N$ to the group ring element $D$ and obtain an element $D_H$ satisfying $D_H D_H^{(-1)} = n + n \cdot N$. Note that the coefficient of $x$ in $D_H$ is the intersection number $|D \cap Hx|$. Since $n$ is a multiplier that acts as the identity on $N$ we have $y \in D \cap Hx \Rightarrow y^n \in D \cap Hx$. Thus each coefficient is divisible by 2 unless $y \in D \cap Hx$ is an element of $N$. But the intersection of $N$ with $D$ has cardinality at most 1 (otherwise elements $\not\equiv 1_G$ in $N$ have a 'difference' representation with elements from $D$) and hence $|D \cap N| = 0$ since $|D|$ is even. We get $(D_H/2) \cdot (D_H^{(-1)}/2) = (n/4) + (n/4) \cdot N$ proving that $n \equiv 0 \mod 4$ if $N \not\equiv 1$, i.e., if $n \not\equiv 2$. Let us call $D_H/2 := \sum_{x \in N} a_x x$. We have $\sum a_x = n/2$, $\sum (a_x)^2 = n/2$, hence $a_x = 0$ or 1 and $D_H/2$ is a $(n - 1, n/2, n/4)$-difference set in $N$ [$a(v, k, \lambda)$-difference set of order $k - \lambda$ is a $k$-subset of a group of order $\nu$ such that each nonzero element in $G$ has exactly $\lambda$ representations $d - d'$ with elements from the difference set]. Difference sets with these parameters or the complementary parameters $(n - 1, n/2 - 1, n/4 - 1)$ are called difference sets of Paley type. Now we can give a simple proof for the affine part of Result 1: the number 2 is a multiplier of the affine difference set, hence a multiplier of the Paley type difference set which has order $n/4$. But 2 is only a multiplier if 2 divides the order of the difference set or the difference set is trivial, see [13], hence $n \equiv 4 \mod 8$ implies $n \equiv 4$ (in which case the difference set is trivial with parameters $(3, 2, 1)$).

Let us look at the Paley difference set $R = D_H/2$ under the assumption $n \equiv 8 \mod 16$. Then the order of $R$ is $n/4 = 2 \mod 4$. For the complement $R'$ of this difference set the first author proved that $R' + R'^{(-1)} = 1_G + G$ in the group ring $\mathbb{GF}(2)G$ (and then of course in $ZG$, too) [1]. On the other hand, Camion and Mann [4] studied exactly these difference sets (and they called them antisymmetric). They could prove that the group $N$ cannot be cyclic unless $|N| = p \equiv 3 \mod 4$ ($p$ prime) in which case $R'$ consists of the squares or nonsquares modulo $p$. This proves our Theorem 2.

The main step in our proof is the combination of Arasu's equation with the results on antisymmetric difference sets. This is of course true for all $(4n - 1, 2n - 1, n - 1)$-difference sets with $n = 2 \mod 4$ and multiplier 2 (and not only for those obtained from an affine difference set). Further, a more careful investigation of Arasu's proof shows that the assumption $n = 2 \mod 4$ is just needed for a dimension argument (that the $\mathbb{GF}(2)$-rank of the incidence matrix is exactly $2m$). This has the following interesting consequence.
Theorem 3. Let $D$ be an abelian $(4n-1, 2n-1, n-1)$-difference set with multiplier 2. If the design associated with $D$ has GF(2)-rank $2n$ (equivalently, if the ideal generated by $D$ in $GF(2)G$ has dimension $2n$) then $4n-1$ is a power of some prime $p$. If $D$ is cyclic then $4n-1$ is a prime $p$ and $D$ consists of the squares or nonsquares modulo $p$.

A few more remarks about the Paley type difference set coming from an affine difference set are in order. If we start with a Desarguesian plane of order $2^t$ and construct an affine difference set according to Bose then the Paley type difference set corresponds to the complement of the point-hyperplane design of $PG(t-1, 2)$. For proof, we consider a generator of $GF(2^{2t})$. The affine difference set $D$ is the set of elements $\omega \in GF(2^{2t})^*$ such that $\text{trace}(\omega) = 1$ (here the trace is computed with respect to the quadratic extension $GF(2^{2t})/GF(2^t)$). The subgroup $N$ is simply $GF(2^t)^*$. The canonical epimorphism $GF(2^{2t})^* \to GF(2^t)^*$ is simply the map $\omega \mapsto \omega^{2^{-t}(2^{2t}-1)}$ (this map is the identity on $N$ and its kernel is the complement of $N$). If $\omega + \omega^{2^t} = 1$ then the trace of $\omega^{2^{-t}(2^{2t}-1)}$ (with respect to $GF(2^t)/GF(2^t)$) is

$$\text{trace}(\omega^{2^{-t} \cdot \omega^{2^{-t}-1}}) = \text{trace}(\omega \cdot \omega^{2^t}) = \text{trace}(\omega + \omega^{2^t}) = \omega + \omega^{2^t} = 1$$

(the second equality is satisfied since $\omega + \omega^{2^t} = 1$). This shows that the difference set of Paley type in $GF(2t)^*$ consists of the elements of trace 1 which is the Singer difference set (to be precise, the complement of the Singer difference set) corresponding to the point-hyperplane design of $PG(t-1, 2)$.

In order to prove that cyclic affine planes with $n \equiv 8 \mod 16$, $n > 8$, cannot exist it is enough to show that the Paley difference set consisting of squares together with 0 cannot occur as the $(n-1, n/2, n/4)$-difference set in $N$ as the projection of an affine difference set of order $n$. We hope that this approach is useful (not only for the case $n \equiv 8 \mod 16$) because of the following reason: The ‘classical’ geometric $(n-1, n/2, n/4)$-difference sets and the corresponding designs have some ‘nice’ properties, for instance the incidence matrix has very small $GF(2)$-rank [9] or equivalently the symmetric difference of 2 blocks is a block. Further, we have the Dembowski–Wagner characterization of the classical point-hyperplane design. If it is true that only the Desarguesian planes admit a cyclic affine difference set and if these are constructed as described in this paper there is a chance to prove that the $(n-1, n/2, n/4)$-difference set constructed from a putative affine difference set must have at least some of the properties of the geometric $(n-1, n/2, n/4)$-difference sets. This might give further necessary conditions on the existence of cyclic affine planes of even order.

References