ELSEVIER

Journal of Statistical Planning and
Inference 62 (1997) 63–67

journal of
statistical planning
and inference

A multiplier theorem for projections of affine difference sets

Alexander Pott*, Dirk Reuschling, Bernhard Schmidt

Institut für Mathematik der Universität Augsburg, Universitätsstraße 14 86135 Augsburg, Germany

Received 15 August 1994; revised 3 March 1995

Abstract

It is shown that every abelian relative $(m,n,m-1,(m-2)/n)$-difference set admits $m-1$ as a multiplier.

1. Relative difference sets and multipliers

A *relative* (m,n,k,λ)-*difference set* in a finite group G of order mn relative to a normal subgroup N of order n is a subset R of G such that every element of $G\setminus N$ is represented exactly λ times as a difference $r-r'$ with $r,r'\in R$, and no nonidentity element of N has such a representation. For instance, the set $\{0,1,3\}$ is a relative $(4,2,3,1)$-difference set in the cyclic group of order 8. If $n=1$ we call the relative difference set a *difference set* (in the usual sense). The investigation of (relative) difference sets is of interest in view of the connection to symmetric designs, in particular to projective planes: A difference set G is equivalent to a symmetric design admitting G as a point regular automorphism group, see Beth et al. (1986). If $\lambda=1$, this design is called a projective plane. Relative $(n,n,n,1)$- and $(n+1,n-1,n,1)$-difference sets correspond to projective planes admitting quasiregular collineation groups of type (b) and (d) in the classification of Dembowski and Piper (1967). We call relative difference sets with parameters $(n+1,n-1,n,1)$ *affine difference sets.* We refer the reader to the recent survey (Pott, 1996) for more information on relative difference sets.

Let R be a difference set with parameters (m,n,k,λ) relative to N and let φ be the canonical epimorphism from G onto G/U, where U is a normal subgroup of G contained in N. If $|U|=u$, it is easy to see that $\varphi(R)$ is a relative $(m,n/u,k,u\lambda)$-difference set in G/U relative to N/U. We call $\varphi(R)$ the projection of R. If $U=N$, the image of R is a difference set in the usual sense having parameters $(m,k,n\lambda)$. We

* Corresponding author.

0378-3758/97/$17.00
PII S0378-3758(96)00169-3

can therefore "classify" relative difference sets according to the underlying difference sets: Our relative difference sets are "extensions" of difference sets.

The affine difference sets and the $(n,n,n,1)$-difference sets are extensions of (trivial) $(n+1,n,n-1)$- and (n,n,n)-difference sets. Difference sets with these parameters exist in any group (take the group itself or the group minus an arbitrary element). Although these difference sets are quite trivial, the "lifting" problem is not at all trivial. On the existence side, it is known that cyclic affine difference sets of order n exist whenever n is a prime power (see Bose, 1942), therefore we have the following result:

Result 1. *If n is a prime power, then there exist cyclic relative $(n+1,(n-1)/u,n,u)$-difference sets for every divisor u of $n-1$.*

It is sometimes conjectured that the converse of this result is also true. Several partial results in this direction can be found in Delsarte et al. (1971) and Jungnickel (1992): It is shown that for certain values of n and u, no relative difference sets with parameters $(n+1,(n-1)/u,n,u)$ can exist. Multipliers play an important role in the proofs of such non-existence results: If G is a multiplicatively written abelian group then a group automorphism τ of G is called a *multiplier* of R if and only if there exists an element $g \in G$ such that

$$\tau(R) := \{\tau(r) : \ r \in R\}$$

is a translate $Rg := \{rg : r \in R\}$ of R. If τ is of the special form $g \to g^t$, we say that t is a *numerical* multiplier. It is the content of so-called *multiplier theorems* to provide sufficient conditions for the existence of multipliers depending on the parameters of (putative) difference sets. The following result extends a multiplier theorem in Elliott and Butson (1966) (the version quoted here is contained in Arasu and Xiang (1996)).

Result 2. *Let R be a relative (m,n,k,λ)-difference set in an abelian group G of exponent v^* relative to N. Let t be an integer relatively prime to v^* and let k_1 be a divisor of k. We assume that t is a multiplier of the underlying $(m,k,n\lambda)$-difference set. Let $k_1 = p_1{}^{e_1} \cdots p_s{}^{e_s}$ be the prime factorization of k_1 and $k_2 := k_1/gcd(v^*,k_1)$. For each p_i, we define*

$$q_i = \begin{cases} p_i & \textit{if } p_i \textit{ does not divide } v^*. \\ l_i & \textit{if } v^* = p_i{}^r u_i,\ (p_i,u_i)=1. \textit{ Here } l_i \textit{ is an integer} \\ & \textit{such that } (l_i,p_i)=1 \textit{ and } l_i \equiv p_i{}^f \bmod u_i. \end{cases}$$

For each i, we assume the existence of an integer f_i and a multiplier s_i such that $s_i q_i{}^{f_i} \equiv t \bmod v^*$. If $k_2 > \lambda$, then t is a multiplier of R.

We refer the reader to the literature for multiplier theorems for ordinary difference sets (which have to be known in order to apply this result). However, if R is a lifting of a trivial difference set D, then all integers relatively prime to the group order are multipliers of D. This is exactly the case which will be considered and it is in this situation not necessary to know multiplier theorems for difference sets in the usual sense.

Multipliers are a very useful tool for nonexistence proofs of difference sets, in particular in connection with the following result (see Elliott and Butson, 1966).

Result 3. *Let R be a relative (m,n,k,λ)-difference set where k is relatively prime to mn. Then there is a translate Rg of R which is fixed by all multipliers.*

2. The theorem

We will focus on the case where the parameters of the relative difference set have the form $(m,n,m-1,(m-2)/n)$.

Theorem 4. *Let R be a relative $(m,n,m-1,(m-2)/n)$-difference set in an abelian group G relative to N. Then $m-1$ is always a numerical multiplier of R.*

Proof. For convenience, we write G multiplicatively. By replacing R by a translate Rg, $g \in G$, if necessary, we can assume $R \cap N = \emptyset$. We set

$$t = \left(\prod_{h\in N} h\right)^{(m-2)/n}.$$

Note that $\prod_{h\in N} h$ is an involution or 1, hence $t^2 = 1$.

For $g \in G \setminus N$, let $\gamma(g)$ be the unique element of R in Ng. Let r be an arbitrary element of R and define

$$t' := \prod_{\substack{r_1,r_2\in R\\ r_1r_2^{-1}\in Nr}} r_1r_2^{-1}.$$

We are now going to calculate t' in two ways. From the definition of a relative difference set it is immediate that

$$t' = tr^{m-2}.$$

On the other hand, we have

$$t' = \prod_{\substack{r'\in R\\ r'\neq r}} r'\gamma(r^{-1}r')^{-1} = r^{-1}\gamma(r^{-1})$$

as $\gamma(r^{-1}r')$ ranges over $R \setminus \{\gamma(r^{-1})\}$ if r' ranges over $R \setminus \{r\}$. Hence

$$r^{m-1} = r^{m-2}r = t't^{-1}r = \gamma(r^{-1})t$$

for all $r \in R$. Thus $R^{(m-1)} = tR$. □

We note that this theorem is already contained in (Delsarte et al. 1971) for the cyclic case and $n = 2$.

3. Applications

We will first show that our multiplier theorem does not follow from Result 2:

Example 5. Result 2 shows that 9, 17 and 25 are multipliers of every abelian (16, 2, 15, 7)-RDS: We take $k_1 = 15$, $p_1 = 3$, $p_2 = 5$. Then $9 \equiv 3^2 \equiv 5^6 \mod 32$ and $25 \equiv 5^2 \equiv 3^6 \mod 32$ as required. But it is not possible to get the multipliers 3 and 5 using Result 2 since no power of 3 is congruent $5 \bmod 32$ and no power of 5 is congruent $3 \bmod 32$. But our theorem shows that 3 and 5 actually are multipliers of every abelian relative (16,2,15,7)-difference set using the multiplier 15 in Result 2: We have $3 \equiv 3 \mod 32$ and $3 \equiv 15 \cdot 5^7 \mod 32$.

We can generalize this example and obtain the following corollary:

Corollary 6. *Let R be an abelian relative $(m, n, m-1, (m-2)/n)$-difference set. If $m-1 = p^i q^j$ is the product of two prime powers, then p^i and q^j are both multipliers of R.*

Proof. Let k be the order of q modulo mn (note that p and q are relatively prime to mn). Then we use Result 2 with $k_1 = m-1$. We have

$$p^i \equiv p^i \mod mn,$$
$$p^i \equiv (m-1) \cdot q^{k-j} \mod mn$$

which proves the corollary. □

This corollary generalizes a result in (Delsarte et al., 1971).

Finally, we will use our multiplier theorem in order to show that -1 is never a multiplier of a relative $(m, n, m-1, (m-2)/n)$-difference set.

Corollary 7. *A relative $(m, n, m-1, (m-2)/n)$-difference set where n is odd cannot admit -1 as a multiplier.*

Proof. First of all note that G has to be abelian since otherwise the map $x \rightarrow x^{-1}$ is not a group automorphism. We may assume that R is fixed both by the multiplier $m-1$ and the multiplier -1. We choose $x \in R$. Since R is fixed by multipliers, we know that x^{-1} and x^{m-1} are also elements of R. But then $x^{m-1}(x^{-1})^{-1} = x^m$ has a "difference" representation with elements of R. Since $x^m \in N$, this is only possible if $x^m = 1$. But it is of course possible to choose x in such a way that its order is not a divisor of m: Otherwise $G \setminus N$ contains only elements y with $y^m = 1$, which is absurd if n is odd. □

Now let us look at the case that n is even. We may assume $n = 2$ using a projection argument. Note that the projection of a relative difference set R has (at least) the same multipliers as R. We will show that a relative $(m, 2, m-1, (m-2)/2)$-difference set cannot admit -1 as a multiplier. To see this, we use two results from the literature. The first is contained in Arasu et al. (1990), the second one in Jungnickel (1990):

Result 8. *Let R be an abelian $(m, n, m-1, (m-2)/n)$-difference set in G relative to N with $R = R^{(-1)}$. Then $(m-2)/n$ has to be even.*

Result 9. *Let R be an abelian $(m, n, m-1, (m-2)/n)$-difference set in G relative to N where n is even. Then N is not a direct factor of G.*

Result 8 shows that $m \equiv 2 \bmod 4$ and Result 9 implies that the Sylow 2-subgroup of G has to be cyclic of order 4 if G contains a relative $(m, 2, m-1, (m-2)/2)$-difference set with multiplier -1. As in the proof of Corollary 7, we may assume that $x^m = 1$ if $x \in R$ which is, again, impossible (there are elements in G/N of order 4). We summarize this in the following theorem:

Theorem 10. *A relative $(m, n, m-1, (m-2)/n)$-difference set cannot admit -1 as a multiplier.*

We note that there are several wrong proofs of this theorem in the literature (Arasu and Ray Chaudhuri, 1985; Arasu et al., 1995; Jungnickel, 1992).

It has been known that no abelian relative difference set can admit -1 as a multiplier if the underlying difference set is nontrivial, see Arasu et al. (1985). In view of Theorem 10, the only interesting case of relative difference sets with multiplier -1 which still has to be considered is the case of relative $(n, u, n, n/u)$-difference sets. We refer the reader to Ma (1992) for an investigation of this case.

References

Arasu, K.T., D. Jungnickel and A. Pott (1990). Divisible difference sets with multiplier -1. J. Algebra **133**, 35–62.

Arasu, K.T. and D.K. Ray Chaudhuri (1985). Divisible quotient lists and their multipliers. Congr.Numer. **49**, 321–338.

Arasu, K.T. and Q. Xiang (1995). Multiplier theorems, *J. Combin. Designs* **3**, 257–268.

Beth, T., D. Jungnickel and H. Lenz (1986). *Design Theory*. Cambridge Univ. Press, Cambridge.

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

Delsarte, P., J.M. Goethals and J.J. Seidel (1971). Orthogonal matrices with zero diagonal II. Canad. J. Math. **23**, 816–832.

Dembowski, P. and F. Piper (1967). Quasiregular collineation groups of finite projective planes. Math. Zeitschrift **99**, 53–75.

Elliott, J.E.H. and A.T. Butson (1966). Relative difference sets. *Ill. J. Math.* **10**, 517–531.

Jungnickel, D. (1990). On automorphism groups of divisible designs, II: group invariant generalized conference matrices. *Arch. Math.* **54**, 200–208.

Jungnickel, D. (1992). On affine difference sets. *Sankhyā* (A) **54**, 219–240.

Ma, S.L. (1992). Reversible relative difference sets. *Combinatorica* **12**, 425–432.

Pott, A. (1996). A survey on relative difference sets. In: K.T. Arasu, J. Dillon, K. Harada, S. Sehgal and R. Solomon, Eds., *Groups, Difference Sets and the Monster*. de Gruyter Verlag, Berlin, pp. 195–232.