Note

On Wilbrink's Theorem

K. T. ARASU

Department of Mathematics and Statistics, Wright State University, Dayton, Ohio 45435

Communicated by the Managing Editors

Received August 1, 1985

An easy extension of Wilbrink's Theorem on planar difference sets for higher values of λ is given. It follows that the Bruck–Ryser–Hall conjecture on the superfluousness of the "$p > \lambda$" condition (or its variations thereof) in the multiplier theorems implies Hall's conjecture on the existence of only a finite number of (v, k, λ) abelian difference sets, for the case λ odd and $k - \lambda \equiv 2 \pmod 4$. More strongly, under these conditions we can show that the corresponding designs are Hadamard, i.e., $k = 2\lambda + 1$ and $v = 2k + 1$. © 1987 Academic Press, Inc.

1. INTRODUCTION

We use all the notations of [7]. We assume familiarity with (v, k, λ) abelian difference sets (for instance, see [3, 5]). Let D be a (v, k, λ) difference set in an abelian group G. Let $n = k - \lambda$; n is said to be the order of D. Let p be a prime divisor of n and let $A = \mathbb{F}_p(G)$, the group algebra of G over $\mathbb{F}_p$. Each subset S of G is identified with the element $\sum_{x \in S} x$ of A. If $x = \sum_g \alpha_g\, g \in A$ and k is an integer, then $x^{[k]} = \sum_g \alpha_g\, g^k$.

2. EXTENDING WILBRINK'S THEOREM

THEOREM. *Let D be a (v, k, λ) difference set in an abelian group G. Let p be a prime divisor of n $(n = k - \lambda)$ such that $p^2 \nmid n$ and $p \nmid \lambda$. Suppose that p is a multiplier of D. Further suppose that D is chosen in such a way that p fixes D. Then*

$$D^{p-1} + (D^{[-1]})^{p-1} = 1 + \lambda^{p-2} G.$$

0097-3165/87 $3.00

Proof. From the definition of difference sets, we have

$$DD^{[-1]} = (k-\lambda)\,1 + \lambda G$$

and

$$\lambda(v-1) = k(k-1)$$

or

$$\lambda v = (k-\lambda)(k+\lambda-1) + \lambda^2.$$

So the following identities hold in $\mathbb{F}_p G$:

$$DD^{[-1]} = \lambda G, \qquad G^2 = vG = \lambda G,$$
$$DG = kG = \lambda G, \qquad D^{[-1]}G = \lambda G.$$

The rest of the proof follows as in Wilbrink's Theorem [7], noting that

$$(DD^{[-1]})^{p-1} = \lambda^{p-1} G^{p-1} = G^{p-1} = \lambda^{p-2} G.$$

COROLLARY. *Let D be a (v, k, λ) difference set in an abelian group G with λ odd. Suppose that $k - \lambda \equiv 2 \pmod 4$ and that 2 is a multiplier of D. Then $k = 2\lambda + 1$, and so the corresponding design is Hadamard.*

Proof. Let $p = 2$ in previous theorem. Without loss of generality, we can assume that D is fixed by the multiplier 2 (otherwise, replace D by such a translate of D). We have $D + D^{[-1]} = 1 + G$ in $\mathbb{F}_2 G$. The right-hand side of this equation has $(v-1)$ nonzero coefficients, while $D + D^{[-1]}$ can have at most $2k$ nonzero coefficients. Hence, $v - 1 \leqslant 2k$, so $v \leqslant 2k + 1$. We also have $(G + D) + (G + D^{[-1]}) = 1 + G$. Similar analysis on this equation yields $2(v-k) \geqslant v - 1$, i.e., $v \geqslant 2k - 1$. Thus $2k - 1 \leqslant v \leqslant 2k + 1$. Since v is odd, either $v = 2k - 1$ or $v = 2k + 1$. But $v = 2k - 1$ gives $k = 2\lambda$, a contradiction as k is odd. ($v = 2k - 1$ corresponds to the complementary design, of course.) Hence $v = 2k + 1 = 4\lambda + 3$, $k = 2\lambda + 1$, and D is a Hadamard difference set, as asserted.

3. CONNECTION TO WELL-KNOWN CONJECTURES

It is widely conjectured—we attribute the conjecture to Bruck, Ryser, and Hall and call it the Bruck–Ryser–Hall conjecture—that conditions of the form "$p > \lambda$" (or $n_1 > \lambda$) are unnecessary in all the known multiplier theorems. All the known proofs of multiplier theorems require this condition very heavily. If the conjecture were true, then in the above theorem and corollary, the assumption that p (or $p = 2$) is a multiplier of the difference set under consideration would be superfluous. Thus the Bruck–Ryser–Hall conjecture implies the following conjecture of Hall for λ odd and $k - \lambda \equiv 2 \pmod 4$.

Conjecture (Hall). For each fixed $\lambda > 1$, there exist only a finite number of (v, k, λ) difference sets.

4. Remarks

Some attempts were made to settle the Bruck–Ryser–Hall conjecture. The best known result in this direction is due to McFarland [6] (a generalization of his result can be found in [1, 2, 5]). Using McFarland's multiplier theorem, one can show that 2 is a multiplier of a putative (25, 9, 3) difference set. Its nonexistence would then follow from our corollary.

As another example, we can show that (79, 27, 9) difference sets do not exist. If D were such a difference set, then by Bruck's multiplier Theorem [4], since $2^1 \equiv 2 \pmod{79}$ and $3^r \equiv 2 \pmod{79}$ for some positive integer r (as 3 is a primitive root mod 79), 2 would be a multiplier of D. But $27 \neq (2)(9) + 1$, so our corollary excludes such a difference set.

Acknowledgment

The author would like to thank Professor H. A. Wilbrink for giving a valuable suggestion to improve our corollary.

References

1. K. T. Arasu, (1983). "Quotient Sets, Homomorphic Images, and Multipliers," Ph. D. dissertation, Ohio State University.
2. K. T. Arasu, and D. K. Ray-Chaudhuri, Multiplier theorem for a list, to appear.
3. Th. Beth, D. Jungnickel, and H. Lenz, "Design Theory," Bibliograph Inst., Mannheim/Wien/Zurich, 1985.
4. R. H. Bruck, Difference sets in a finite group, *Trans. Amer. Math. Soc.* **78** (1955), 464–481.
5. E. S. Lander, Symmetric Designs: An Algebraic Approch, London Math. Society Lecture Note Ser. Vol. 74, Cambridge Univ. Press, Cambridge, 1983.
6. R. L. McFarland, "On Multipliers of Abelian Difference Sets," Ph. D. dissertation, Ohio State University, 1970.
7. H. A. Wilbrink, (1985). A note on planar difference sets, *J. Combin. Theory Ser. A* **38**, 94–95.