3-1990

# A Note on Intersection Numbers of Difference Sets

K. T. Arasu

James A. Davis
*University of Richmond*, jdavis@richmond.edu

Dieter Jungnickel

Alexander Pott



Recommended Citation
Arasu, K. T., James A. Davis, Dieter Jungnickel, and Alexander Pott. "A Note on Intersection Numbers of Difference Sets." *European Journal of Combinatorics* 11, no. 2 (March 1990): 95-98. doi: 10.1016/S0195-6698(13)80061-3.

# A Note on Intersection Numbers of Difference Sets

K. T. ARASU, JAMES DAVIS, DIETER JUNGNICKEL AND ALEXANDER POTT

We present a condition on the intersection numbers of difference sets which follows from a result of Jungnickel and Pott [3]. We apply this condition to rule out several putative (non-abelian) difference sets and to correct erroneous proofs of Lander [4] for the non-existence of (352, 27, 2)- and (122, 37, 12)-difference sets.

## 1. INTRODUCTION

We refer the reader to [2] and [6] for background information on difference sets. In [3] the following generalization of a classical existence test due to Mann [5] was proved.

THEOREM 1 (Jungnickel and Pott). *Let $D$ be a $(v, k, \lambda)$-difference set with $v > k$ in $G$. Furthermore, let $u \neq 1$ be a divisor of $v$, let $U$ be a normal subgroup of index $u$ of $G$, put $H = G/U$ and assume that $H$ is abelian and has exponent $u^*$. Finally, let $p$ be a prime not dividing $u^*$ and assume that $tp^f \equiv -1 \bmod u^*$ for some numerical $G/U$-multiplier $t$ of $D$ and a suitable non-negative integer $f$. Then the following hold:*
(i) *$p$ does not divide the square-free part of $n = k - \lambda$, say $p^{2j} \parallel n$ (where $j \geq 0$);*
(ii) *$p^j \leq v/u$;*
(iii) *if $u > k$, then $p^j \mid k$.*

In this note we point out further consequences of Theorem 1, which is implicit in the proof given in [3]. We shall then apply this result to rule our a few hypothetical difference sets, in particular correcting erroneous non-existence proofs presented by Lander for some abelian (352, 27, 2)- and all the abelian (112, 37, 12)-difference sets.

## 2. INTERSECTION NUMBERS

Let $D$ be a $(v, k, \lambda)$-difference set in $G$, let $U$ be a normal subgroup of index $u$ of $G$, and write $H = G/U$. For $x \in H$, denote by $s_x$ the number of $d \in D$ satisfying $d + U = x$. The $u$ numbers $s_x$ $(x \in H)$ are called the intersection numbers of $D$ relative to $U$. It is well known and easy to see that they satisfy the following two equations (see, e.g., [1]):

$$\sum_{x\in H} s_x = k, \qquad \sum_{x\in H} (s_x)^2 = k - \lambda + \lambda \frac{v}{u}. \tag{1, 2}$$

We shall now state the following supplement to Theorem 1.

THEOREM 2. *With the same assumptions as in Theorem 1, one has the following results:*
(i) *If $p^{2j} \parallel n$, then all intersection numbers of $D$ relative to $U$ are congruent modulo $p^j$, say $s_x = y \bmod p^j$ for all $x \in H$.*
(ii) *One has $yu \equiv k \bmod p^j$; if we choose $y_0$ as the smallest non-negative solution of this congruence, we also have $y_0 u \leq k$.*

PROOF. Identify $D$ with the element

$$D = \sum_{d\in D} d$$



0195-6698/90/020095 + 04 $02.00/0 

of the group ring $\mathbb{Z}G$, and write $D'$ for the image of $D$ under the canonical epimorphism

$$\Theta\colon \mathbb{Z}G \to \mathbb{Z}(G/U) = \mathbb{Z}H.$$

In the proof of Theorem 1 given in [3], it is shown that $D'$ has the form

$$D' = p^j A + yH \tag{3}$$

for a suitable $A \in \mathbb{Z}H$ and a suitable integer $y$. This proves the validity of (i). Observing that $|H| = u$ and

$$D' = \sum_{x \in H} s_x x,$$

we see that (1) and (3) imply $yu \equiv k \bmod p^j$. Now let $y_0$ be the smallest non-negative solution of this congruence. Then clearly $s_x \geqslant y_0$ for all $x \in H$, since the intersection numbers are non-negative. This implies

$$k = \sum_x s_x \geqslant u y_0. \quad \square$$

We remark that the abelian case of Theorem 2 is similar to Theorem 4.19 of Lander [4]. Alternative proofs for both Theorems 1 and 2 (using a result of Lander [4] on self-orthogonal reversible codes, see also [7]) are given in [6]. We now present a few applications.

Example 1. Let $G$ be any group of order 56 with a normal subgroup $U$ of order 8, i.e. of index $u = 7$. Then $G$ cannot contain a $(56, 11, 2)$-difference set. To see this, assume otherwise and take $p = 3$ and note $3^3 \equiv -1 \bmod 7$. The conditions of Theorem 1 are all satisfied, in particular $p^2 \,\|\, n$, i.e. $j = 1$. But then Theorem 2 implies $7y_0 \leqslant 11$, where $y_0$ is the smallest non-negative solution of the congruence $7y \equiv 11 \bmod 3$. Thus $y_0 = 2$, and we obtain the contradiction $14 \leqslant 11$. This rules out all abelian $(56, 11, 2)$-difference sets, a well known result (cf. [4]); but it also excludes non-abelian groups (e.g., we may take $G = \mathbb{Z}_7 \times H$, where $H$ is one of the two non-abelian groups of order 8, or we may take any semi-direct product $\mathbb{Z}_7 \cdot H$).

Example 2. Let $G$ be any group of order 204 with a normal subgroup of order 12, i.e. of index $u = 17$. Then $G$ cannot contain a $(204, 29, 4)$-difference set. Here we take $p = 5$ and note $5^8 \equiv -1 \bmod 17$. We have $5^2 \,\|\, n$, i.e. $j = 1$. So Theorem 2 gives $17y_0 \leqslant 29$, where $y_0$ is the smallest non-negative solution of the congruence $17y \equiv 29 \bmod 5$. But $y_0 = 2$ and thus we obtain the contradiction $34 \leqslant 29$. Again, this excludes all abelian groups of order 206 (which is known, see [4]) but also non-abelian examples.

Example 3. Let $G$ be a group of order 352 with a normal subgroup $U$ of index $u = 8$ and assume that $H = G/U$ is $EA(8)$ (and thus $u^* = 2$). Then $G$ cannot contain a $(352, 27, 2)$-difference set. Here we choose $p = 5$ and note $5 \equiv -1 \bmod 2$. We have $p^2 \,\|\, n$, so $j = 1$. By Theorem 2, we obtain $8y_0 \leqslant 27$, where $y_0$ is the smallest non-negative solution of $8y \equiv 27 \bmod 5$. Thus $y_0 = 4$, a contradiction. Again, this rules out both abelian and non-abelian examples.

Example 4. No abelian group of order 112 contains a $(112, 37, 12)$-difference set.

We first consider the groups $\mathbb{Z}_7 \times \mathbb{Z}_8 \times \mathbb{Z}_2$, $\mathbb{Z}_7 \times (\mathbb{Z}_4)^2$, $\mathbb{Z}_7 \times \mathbb{Z}_4 \times (\mathbb{Z}_2)^2$ and $\mathbb{Z}_7 \times (\mathbb{Z}_2)^4$. To prove the non-existence in these cases we select a subgroup $U$ of order 4 such that the exponent of $G/U$ is 14 (this is possible in the groups that are under consideration). Note that $5^3 \equiv -1 \bmod 14$ and $5^2 \,\|\, 25 = n$; thus Theorem 1 shows that $5 \leqslant |U| = 4$, a contradiction. We cannot use this argument to rule out the existence of difference sets in the cyclic case. But then we can take a subgroup $U$ or order 8 and index 14, thus the exponent of $G/U$ is again 14. Then the assumptions of Theorem 2 are fulfilled, with $j = 1$. The smallest positive solution of $14y \equiv 37 \bmod 5$ is $y_0 = 3$. Then Theorem 2(ii) gives the contradiction $42 \leqslant 37$.

REMARK. The argument in part (3) in Lander [4, pp. 212–213] for the non-existence of abelian $(352, 27, 2)$-difference sets in $\mathbb{Z}_{11} \times U$ (where $U$ is one of $\mathbb{Z}_8 \times (\mathbb{Z}_2)^2$, $(\mathbb{Z}_4)^2 \times \mathbb{Z}_2$, $\mathbb{Z}_8 \times \mathbb{Z}_4$ or $\mathbb{Z}_{16} \times \mathbb{Z}_2$) contains several mistakes. The first two of these cases are, however, ruled out by Example 3 above. We do not see how to repair the proofs of the last two cases. Thus the entries 'NO' for difference sets #98 and 99 in Table 6-1 of Lander [4] are at present not justified; these cases are still to be considered as open. Note that Example 3 also gives simpler non-existence proofs for cases #102 and 103 in Lander's table.

Lander made another obvious mistake concerning abelian $(112, 37, 12)$-difference sets (#169 in Table 6-1): Instead of investigating all the abelian $(112, 37, 12)$-difference sets in the five abelian groups of order 112 he erroneously considered abelian groups of order 122 (in which case just the cyclic group exists). Example 4 rules out the existence of these difference sets. We summarize our non-existence results as far as they affect Lander's table in the following Proposition.

PROPOSITION. *There exists no* $(352, 27, 2)$*-difference set in* $\mathbb{Z}_{11} \times \mathbb{Z}_8 \times (\mathbb{Z}_2)^2$ *and* $\mathbb{Z}_{11} \times (\mathbb{Z}_4)^2 \times \mathbb{Z}_2$. *None of the groups* $\mathbb{Z}_7 \times \mathbb{Z}_{16}$, $\mathbb{Z}_7 \times \mathbb{Z}_8 \times \mathbb{Z}_2$, $\mathbb{Z}_7 \times (\mathbb{Z}_4)^2$, $\mathbb{Z}_7 \times \mathbb{Z}_4 \times (\mathbb{Z}_2)^2$ *and* $\mathbb{Z}_7 \times (\mathbb{Z}_2)^4$ *contains a* (112, 37, 12)-difference set.

## ACKNOWLEDGMENTS

The first author's research was partially supported by NSA grant #MDA904-87-H-2018. The second author gratefully acknowledges the hospitality of Wright State University during the time of this research. The last two authors thank the University of Waterloo for its hospitality, and the third author also acknowledges the financial support of NSERC under grant #IS-0367.

## REFERENCES

1. K. T. Arasu and D. K. Ray-Chaudhuri, Multiplier theorems for a difference list, *Ars Combin.*, **22** (1986), 119–137.
2. T. Beth, D. Jungnickel and H. Lenz, *Design Theory,* Cambridge University Press, Cambridge, 1986.
3. D. Jungnickel and A. Pott, Two results on difference sets, in: *Colloquia Mathematica Societatis János Bolyai, 52. Combinatorics, Eger,* 1987, pp. 325–330.
4. E. S. Lander, *Symmetric designs: an algebraic approach,* Cambridge University Press, Cambridge, 1983.

5. H. B. Mann, Balanced incomplete block designs and abelian difference sets, *Illinois J. Math.*, **8** (1964), 252–261.
6. A. Pott, Differenzenmengen und Gruppenalgebren, Ph.D. Thesis, Justus-Liebig-Universität Giessen, 1988.
7. A. Pott, A note on self-orthogonal codes, *Discr. Math.*, **76** (1989), 283–284.

*Received 12 April 1988 and accepted 15 July 1989*

K. T. ARASU
*Department of Mathematics and Statistics,*
*Wright State University,*
*Dayton, Ohio 45435, U.S.A.*

JAMES DAVIS
*Department of Mathematics, University of Richmond,*
*Richmond, Virginia 23173, U.S.A.*

DIETER JUNGNICKEL AND ALEXANDER POTT
*Mathematisches Institut, Justus-Liebig-Universität Giessen,*
*Arndtstrasse 2, 6300 Giessen, F.R.G.*