BULL. AUSTRAL. MATH. SOC. 05B10
VOL. 13 (1975), 343-348.

Nonexistence of certain supplementary difference sets

Nicholas Wormald

This paper finds restrictions on the parameters of supplementary difference sets in any group G with a subgroup of index 2, which therefore includes all cyclic groups of even orders. As a corollary to the main theorem, we have that if $S_1, \ldots, S_r$ are $r - \{2v; k_1, \ldots, k_r; 2\lambda\}$ supplementary difference sets in such a group, then not all of $v, k_1, \ldots, k_r, \lambda$ are odd; also $\left(\sum_{i=1}^{r} k_i\right) - 2\lambda$ is the sum of r squares.

Let $S_1, \ldots, S_r$ be subsets of G, a finite abelian group of order v written in additive notation. Suppose for each i that $S_i = \{s_{i,j} : 1 \le j \le k_i\}$ where k_i is the size of S_i. Suppose there is a natural number, λ say, such that for each non-zero element g of G, there are precisely λ ordered triples (i, m, n) such that

$$g = s_{i,m} - s_{i,n} .$$

Then we say that the sets $S_1, \ldots, S_r$ are $r - \{v; k_1, \ldots, k_r; \lambda\}$ *supplementary difference sets.*

We see that we are interested here in the number of times that elements of G occur as the difference between elements of subsets of G. Thus we are interested in sets of elements where an element may appear more than once. Henceforth we use square brackets to denote collections of

Received 4 August 1975. Communicated by Dr Jennifer R.S. Wallis.

elements where the elements may be repeated; for example the collection $[0, 0, 0, 1, 1, 2]$.

Suppose we have $r - \{v; k_1, \ldots, k_r; \lambda\}$ supplementary difference sets. Then we see by counting differences two different ways, that the parameters satisfy

$$\lambda(v-1) = \sum_{i=1}^{r} k_i(k_i-1) \quad . \tag{1}$$

Note that if v is even then λ must also be, because $k_i(k_i-1)$ is always even. We may write further conditions on the parameters of supplementary difference sets in certain groups G as follows:

THEOREM 1. *Suppose the abelian group G has a subgroup H of index 2 . Let $o(G) = 2v$, and suppose $S_i \subseteq G$, $|S_i| = k_i$ for $1 \leq i \leq r$, where $S_1, \ldots, S_r$ are $r - \{2v; k_1, \ldots, k_r; 2\lambda\}$ supplementary difference sets. Then there are positive integers a_i, b_i for each i , satisfying the following:*

$$a_i + b_i = k_i \quad \textit{for every} \quad i \ , \tag{2}$$

$$\sum_{i=1}^{r} 2a_i b_i = 2\lambda v \ , \tag{3}$$

$$\sum_{i=1}^{r} (a_i-1)a_i + (b_i-1)b_i = 2\lambda(v-1) \quad . \tag{4}$$

Proof. First some notation. Let $S \subseteq G$. We denote by ΔS the collection of differences between elements of S ; that is,

$$\Delta S = [s_1-s_2 : s_1 \neq s_2; \ (s_1, s_2) \in S \times S] \quad .$$

Now, call $g \in G$ even if $g \in H$, and odd otherwise. In particular, if G is a cyclic group of even order, this will correspond to the even and odd powers of a generator of G . Since G is abelian, H is normal in G , so the above idea of odd and even obeys the usual rule of $x - y$ being even if and only if both x and y are even, or both are odd.

We now prove the theorem. Let $S_1, \ldots, S_r$ be as in the statement of

https://doi.org/10.1017/S000497270002459X Published online by Cambridge University Press

the theorem. Suppose for each i that the number of odd elements of G in S_i is a_i, and the number of even elements is b_i. We now define the collection S to be the adjunction of all collections ΔS_i for each i, written $S = \sum_{i=1}^{r} \Delta S_i$. Then since $S_1, \ldots, S_r$ are supplementary difference sets, we have that S is 2λ copies of $[G\backslash\{0\}]$. However, since $0 \in H$, $G\backslash\{0\}$ contains v odd elements and $v - 1$ even elements, so S contains $2\lambda v$ odd elements and $2\lambda(v-1)$ evens. We next count these elements in a different way.

The number of odd elements in ΔS_i is $2a_i b_i$, since every time x is odd and y even, or x even and y odd, $x - y$ is odd, and otherwise it is even.

Similarly the number of even elements in ΔS_i is $a_i(a_i-1) + b_i(b_i-1)$, this being the number of ordered pairs $(x, y) \in S_i \times S_i$ such that $x \neq y$, and x and y are either both odd or both even.

Thus the total number of odd elements in $\sum_{i=1}^{r} \Delta S_i$ is $\sum_{i=1}^{r} 2a_i b_i$, and the number of even elements is

$$\sum_{i=1}^{r} a_i(a_i-1) + b_i(b_i-1) .$$

We equate these numbers with those calculated earlier for S, and we see that the a_i's and b_i's satisfy equations (3) and (4). They satisfy equation (2) since every element of G is either odd or even. This finishes the theorem.

COROLLARY 1. *If $S_1, \ldots, S_r$ are as described in the theorem, then not all of $v, k_1, \ldots, k_r, \lambda$ are odd.*

Proof. Suppose $k_1, \ldots, k_r$ are all odd. We know from the theorem that we have a_i, b_i $(1 \leq i \leq r)$ satisfying (2), (3), and (4). By equation (2) we know that for each i, not both a_i and b_i are odd (or

https://doi.org/10.1017/S000497270002459X Published online by Cambridge University Press

k_i would be even) and thus $a_i b_i$ is even for each i. Thus the left hand side of equation (3) is divisible by 4, so λv must be even, implying not both v and λ are odd.

Thus, for example, if G is an abelian group with a subgroup of index 2, G has no supplementary difference sets with parameters $2 - \{14; 5, 3; 2\}$ even though these parameters satisfy equation (1).

COROLLARY 2. *With $S_1, \ldots, S_r$ as in the theorem, we have that* $\left(\sum_{i=1}^{r} k_i\right) - 2\lambda$ *is a sum of r squares.*

Proof. Subtracting (3) from (4), we have

$$\sum_{i=1}^{r} \left((a_i - b_i)^2 - (a_i + b_i)\right) = -2\lambda ,$$

or

$$\left(\sum_{i=1}^{r} k_i\right) - 2\lambda = \sum_{i=1}^{r} (a_i - b_i)^2 . \tag{5}$$

Thus $\left(\sum_{i=1}^{r} k_i\right) - 2\lambda$ is a sum of r squares.

If $r = 1$ (that is, if we have a $(2v, k, 2\lambda)$ difference set), this means $k - 2\lambda$ is a square. In this case, we may deduce this condition from the Bruck-Ryser-Chowla Theorem (see [1]), since the incidence matrix of a difference set is a (r, k, λ) configuration (see [2], [3]). This condition implies, for example, that there is no $(46, 10, 2)$ difference set (that is, $1 - \{46; 10; 2\}$ supplementary difference set) in G, even though the parameters satisfy equation (1).

For $r = 2$, Corollary 2 implies $k_1 + k_2 - 2\lambda$ is a sum of 2 squares. For example, this means that in G there do not exist $2 - \{44; 6, 8; 2\}$ supplementary difference sets even though these satisfy equation (1). Similarly with $2 - \{52; 10, 4; 2\}$ and $2 - \{68; 12, 2; 2\}$.

For $r = 3$, we see that for a group G as above, there are no $3 - \{136; 10, 10, 10; 2\}$ supplementary difference sets. Similarly with

https://doi.org/10.1017/S000497270002459X Published online by Cambridge University Press

$3 - \{140; 8, 10, 12; 2\}$ supplementary difference sets in G.

Now Corollaries 1 and 2 do not utilise the full implications of the theorem, but make its use simpler in some cases. Other cases can be eliminated using equations (2) and (4) alone. The following table shows, for some values of k_i, the possible values of $a_i(a_i-1) + b_i(b_i-1)$ for which $a_i + b_i = k_i$.

Table 1

k_i	possible values of $a_i(a_i-1) + b_i(b_i-1)$
1	0
2	2, 0
3	6, 2
4	12, 4
5	20, 12, 8
⋮	⋮
17	272, 240, 212, 188, 168, 152, 140, 132, 128
⋮	⋮

If we have $2 - \{2v; k_1, k_2; 2\lambda\}$ supplementary difference sets, in a group G with a subgroup of index 2, then by equation (4), we must have $2\lambda(v-1)$ expressible as the sum of two numbers x_1 and x_2, where x_i is in the k_ith row of Table 1 (for $i = 1$ or 2). Thus, for instance, if there exist $2 - \{138; 2, 17; 2\}$ supplementary difference sets in G, we must have x_1 in the second row and x_2 in the seventeenth row of Table 1, with $x_1 + x_2 = 136$. However, we see that this is impossible, so these supplementary difference sets do not exist, even though the parameters satisfy the conditions of Corollaries 1 and 2.

Obviously the most exhaustive condition we may check is that positive integers exist satisfying (2), (3), and (4). However, it is fairly simple to check that if (1) and (2) hold, conditions (3) and (4) are equivalent, and thus by using Table 1 above, the full power of the theorem is utilised.

The method used to prove Theorem 1 may be used to prove:

https://doi.org/10.1017/S000497270002459X Published online by Cambridge University Press

THEOREM 2. *Suppose the abelian group* G *has a subgroup* H *of index* 3 . *Let* $o(G) = 3v$, *and suppose* $S_i \subseteq G$, $|S_i| = k_i$ *for* $1 \leq i \leq r$, *where* $S_1, \ldots, S_r$ *are* $r - \{3v; k_1, \ldots, k_r; \lambda\}$ *supplementary difference sets. Then there are positive integers* a_i, b_i, c_i *for each* i , *satisfying the following:*

$$a_i + b_i + c_i = k_i \quad \text{for each } i \,, \tag{6}$$

$$\sum_{i=1}^{r} a_i b_i + b_i c_i + c_i a_i = \lambda v \,, \tag{7}$$

$$\sum_{i=1}^{r} a_i(a_i-1) + b_i(b_i-1) + c_i(c_i-1) = \lambda(v-1) \,. \tag{8}$$

However, we have found no case where parameters satisfy equation (1) but are eliminated by Theorem 2. We may state similar results for groups with subgroups of larger index, but again, we have found no cases eliminated by these.

References

[1] Marshall Hall, Jr., *Combinatorial theory* (Blaisdell Publishing Co. [Ginn and Co.], Waltham, Massachusetts; Toronto, Ontario; London; 1967).

[2] Jennifer Seberry Wallis, "Hadamard matrices", *Combinatorics: Room squares, sum-free sets, Hadamard matrices*, 273–489 (Lecture Notes in Mathematics, 292. Springer-Verlag, Berlin, Heidelberg, New York, 1972).

[3] Jennifer Seberry Wallis, "Some remarks on supplementary difference sets", *Infinite and finite sets*, Vol. III, 1503–1526 (Colloquia Mathematica Societatis János Bolyai, 10. North-Holland, Amsterdam, London, 1975).

Department of Pure Mathematics,
Faculty of Arts,
Australian National University, Canberra, ACT.