JOURNAL OF COMBINATORIAL THEORY, Series A 25, 62–67 (1978)

A Summary of Noncyclic Difference Sets, $k < 20$

ROBERT E. KIBLER

Department of Defense, Fort George G. Meade, Maryland 20755

Communicated by the Managing Editors

Received September 30, 1975

This note contains a list of (v, k, λ) difference sets in noncyclic groups, for $k < 20$.

We begin with the usual definition of a cyclic difference set. In the cyclic group Z_v of v elements, with the usual additive notation, a set D of k distinct elements from Z_v is called a *difference set* if each nonzero element of Z_v occurs exactly λ times in the set $D - D = \{d_i - d_j : d_i, d_j \in D\}$. Since $D - D$ contains $k(k-1)$ nonzero elements, a necessary condition for D to be a difference set is $k(k-1) = \lambda(v-1)$.

If instead of Z_v we consider a group G with v elements (now written multiplicatively), the condition for a set D of k distinct elements to be a difference set is that each nonidentity element of G occurs exactly λ times in the set $DD^{-1} = \{d_i d_j^{-1} : d_i, d_j \in D\}$. We write $n = k - \lambda$.

If D is a difference set in G then the set $E = Dg$ is also a difference set (for $g \in G$) because $EE^{-1} = \{d_i g g^{-1} d_j^{-1} : d_i, d_j \in D\} = DD^{-1}$. Also if α is an automorphism of G then $F = D^\alpha = \{d_i^\alpha : d_i \in D\}$ is again a difference set since $FF^{-1} = \{d_i^\alpha (d_j^\alpha)^{-1} : d_i, d_j \in D\} = \{(d_i d_j^{-1})^\alpha : d_i, d_j \in D\}$. We say that two difference sets D, D' are equivalent if there exists an automorphism α of G and an element $g \in G$ such that $D' = D^\alpha g$. If for some pair (α, g) we have $D = D^\alpha g$ then the pair is called a *multiplier* of the difference set. Clearly the multipliers of a fixed difference set form a group.

While much is known about difference sets in the cyclic case [1], little systematic work has been done for noncyclic groups.

A difference set gives rise, under translation by group elements, to a symmetric balanced incomplete block design [3]. By the theorem of Bruck *et al.* [3, p. 107], such a design can exist only if (1) v is even and n is a square or (2) v is odd and $z^2 = nx^2 + (-1)^{(v-1)/2} \lambda y^2$ has a solution in integers x, y, z not all zero.

It is shown in [2] that condition (1), each nonidentity element of G occurs exactly λ times in DD^{-1}, is equivalent to condition (2), each nonidentity element of G occurs exactly λ times in $D^{-1}D$.

0097-3165/78/0251-0062\$02.00/0

In the same paper it is shown that if H is a homomorphic image of G under θ, $[G : H] = w$, and if for $h \in H$ we denote by $N(h)$ the number of $d \in D$ such that $d\theta = h$ then we have

$$\sum_h N(h) = k,$$

$$\sum_h N(h)^2 = n + \lambda w,$$

and

$$\sum_h N(h)\, N(gh) = \lambda w \qquad \text{for} \quad g \neq 1.$$

With this theorem as our principal tool we have enumerated the noncyclic difference sets for $k < 20$. Some of our possible parameter sets were eliminated by [4].

The most interesting cases are $(v, k, \lambda) = (16, 6, 2)$ and $(36, 15, 6)$, where the variety of groups available provides a wealth of examples. Aside from these two cases we have only the following examples:

1.	(21, 5, 1)	$a^7 = b^3 = 1, ba = a^2b$	$1, a, a^3, b, a^2b^2$
2.	(57, 8, 1)	$a^{19} = b^3 = 1, ba = a^7b$	$1, a, a^3, a^8, b, a^4b, a^{13}b, a^{18}b^2$
3.	(57, 8, 1)	$a^{19} = b^3 = 1, ba = a^7b$	$1, a, a^3, a^8, b, a^5b^2, a^9b^2, a^{18}b^2$
4.	(45, 12, 3)	$a^{15} = b^3 = 1, ba = ab$	$1, a^2, a^3, a^4, a^7, a^{12}, b, a^8b, a^{14}b, b^2, a^9b^2, a^{13}b^2$
5.	(45, 12, 3)	$a^{15} = b^3 = 1, ba = ab$	$1, a^2, a^3, a^7, a^9, a^{12}, b, a^4b, a^8b, b^2, a^{13}b^2, a^{14}b^2$
6.	(27, 13, 6)	$a^3 = b^3 = c^3$, abelian	$1, a, a^2, b, ab, b^2, c, ac, bc, ac^2, a^2bc^2, b^2c^2, a^2b^2c^2$
7.	(27, 13, 6)	$a^9 = b^3 = 1, ba = a^4b$	$1, a, a^2, a^4, a^5, a^7, b, ab, a^2b, a^5b, a^5b^2, a^6b^2, a^8b^2$
8.	(27, 13, 6)	$a^9 = b^3 = 1, ba = a^4b$	$1, a, a^2, a^4, a^5, a^7, b, a^5b, a^8b, a^2b^2, a^4b^2, a^5b^2, a^6b^2$
9.	(40, 13, 4)	$a^5 = b^8 = 1, ba = a^4b$	$1, a, a^2, b, a^3b, ab^2, a^3b^2, a^4b^2, ab^4, ab^5, a^2b^5, ab^6, a^4b^7$
10.	(183, 14, 1)	$a^{61} = b^3 = 1, ba = a^{13}b$	$1, a, a^3, a^{20}, a^{26}, a^{48}, a^{57}, b, a^8b, a^{18}b, a^{29}b, a^{17}b^2, a^{32}b^2, a^{44}b^2$
11.	(183, 14, 1)	$a^{61} = b^3 = 1, ba = a^{13}b,$	$1, a, a^3, a^{20}, a^{26}, a^{48}, a^{57}, b, a^{12}b, a^{46}b, a^9b^2, a^{17}b^2, a^{27}b^2, a^{38}b^2$
12.	(273, 17, 1)	$a^{13} = b^7 = c^3 = 1, ba = ab, ca = a^3c, cb = b^2c$	$a, b, a^2b, a^4b^2, a^{11}b^2, a^5b^4, a^{10}b^4, a^4c, a^9bc, a^{12}bc, a^2b^2c, a^6b^2c, a^{10}b^4c, a^{11}b^4c, b^3c^2, b^5c^2, b^6c^2$

13. (273, 17, 1) $a^{13}=b^7=c^3=1, ba=ab$ $a, b, a^2b, a^4b^2, a^{11}b^2, a^5b^4, a^{10}b^4,$
$ca=a^{12}c, cb=bc$ $a^4c, a^9bc, a^{12}bc, a^2b^2c, a^6b^2c,$
$a^{10}b^4c, a^{11}b^4c, b^3c^2, b^5c^2, b^6c^2$

The multiplier group is trivial in example 4; it is Z_3 for examples 1, 2, 3, 7, 8, 10, and 11; for examples 9, 12, 13, and 5 it is Z_4, Z_6, Z_6, and Z_8, respectively. The multiplier group of example 6 is noncyclic of order 39. Examples 7 and 8 are due to Alltop [9]; except for #13, the examples with $\lambda = 1$ were given in [2, p. 475]. Example 6 is well known [2, p. 480]. Examples 4 and 5 appear in [5, p. 9].

The (16, 6, 2) Case

There are 14 groups. The cyclic and dihedral groups have no difference set. The other groups with their difference sets are:

(A) Abelian. $a^8 = b^2 = 1$ [7]

1. $1, a, a^2, a^4, ab, a^6b$
2. $1, a, a^2, a^5, b, a^6b$

(B) Abelian. $a^4 = b^4 = 1$

3. $1, a, a^2, b, ab^2, a^2b^3$ [6, p. 68–69; 7, p. 336]
4. $1, a, a^2, b, b^3, a^3b^2$
5. $1, a, b, a^2b, ab^2, a^2b^2$

(C) Abelian. $a^4 = b^2 = c^2 = 1$

6. $1, a, a^2, b, c, a^3bc$ [5]
7. $1, a, a^2, ab, ac, a^3bc$ [6, p. 68–69; 7, p. 336]

(D) Abelian. $a^2 = b^2 = c^2 = d^2 = 1$

8. $1, a, b, c, d, abcd$ [2]

(E) $a^4 = b^2 = c^2 = 1, bab = a^3, ac = ca, bc = cb$

9. $1, a, a^2, b, ac, a^2bc$
10. $1, a, b, a^2b, c, a^3c$

(F) $a^4 = c^2 = 1, b^2 = a^2, ba = a^3b, ac = ca, bc = cb$

11. $1, a, a^2, b, c, abc$
12. $1, a, a^2, b, ac, a^2bc$

(G) $a^4 = 1, b^2 = a^2 = c^2, ba = a^3b, ac = ca, bc = cb$

13. $1, a, a^2, b, ac, bc$
14. $1, a, b, ab, c, a^2c$

(H) $a^4 = b^2 = 1, ba = ab, c^2 = b, ca = a^3bc$

15. $1, a, a^2, ab, c, a^2bc$
16. $1, a, a^2, ab, ac, a^3bc$
17. $1, a, b, a^3b, ac, a^3c$
18. $1, a, a^2, a^3b, ac, abc$

(I) $a^4 = b^4 = 1, ba = a^3b$

19. $1, a, a^2, b, ab^2, a^2b^3$
20. $1, a, a^2, b, b^3, a^3b^2$
21. $1, a, b, a^2b, b^2, a^3b^2$

(J) $a^8 = 1, b^2 = a^2, ba = a^5b$

22. $1, a, a^2, a^5, ab, a^7b$
23. $1, a, a^3, a^4, b, a^2b$

(K) $a^8 = 1, b^2 = a^4, ba = a^3b$

24. $1, a, a^2, a^5, b, a^2b$
25. $1, a, a^3, a^4, ab, a^3b$

(L) $a^8 = 1, b^2 = a^4, ba = a^7b$

26. $1, a, a^2, a^5, b, a^2b$
27. $1, a, a^3, a^4, b, a^2b$

The multiplier groups of these sets are: Z_2, set 1; $Z_2 \oplus Z_2$, sets 2, 13, 24, 25, 26, 27; $Z_2 \oplus Z_2 \oplus Z_2$, sets 6, 9, 15, 16, 19, 20, 21, 22, 23; $Z_2 \oplus$ octic, sets 3, 10, 12, 17, 18; $Z_2 \oplus Z_3$, sets 11, 14; $Z_2 \oplus S_4$, set 7; S_6, set 8. The multiplier group G of set 4 is of order 24 generated by $a^6 = b^6 = 1$, $a^3 = b^3$, $ab = b^2a^2$. The multiplier group of set 5 is $G + Gc$ with $c^2 = 1$, $ca = a^5c$, $cb = a^2bc$.

The block designs generated by these sets are nearly all isomorphic. The only exceptions are set 1 which is distinct from all the others and the isomorphic pair of set 11 and set 14. Thus all three (16, 6, 2) designs are generated by appropriate difference sets.

THE (36, 15, 6) CASE

There are 14 groups. Of these, five have cyclic 3-Sylow subgroups and no difference set. The nine groups having noncyclic 3-Sylow subgroups with their difference sets are:

(I) cyclic 2-Sylow subgroup: $a^3 = b^3 = c^4 = 1$, $ab = ba$

(A) $ca = ac$, $cb = bc$ [7]

1. $1, a, a^2, b, ab, a^2b, c, bc, b^2c, c^2, abc^2, a^2b^2c^2, c^3, a^2bc^3, ab^2c^3$
2. $1, a, a^2, b, ab, a^2b, c, bc, b^2c, c^2, abc^2, a^2b^2c^2, ac^3, bc^3, a^2b^2c^3$
3. $1, a, a^2, b, ab, a^2b, c, bc, b^2c, c^2, abc^2, a^2b^2c^2, a^2c^3, abc^3, b^2c^3$
4. $1, a, a^2, b, ab, a^2b, c, bc, b^2c, ac^2, a^2bc^2, b^2c^2, a^2c^3, abc^3, b^2c^3$

(B) $ca = ac$, $cb = b^2c$

5. $1, a, a^2, b, ab, a^2b, c, abc, a^2b^2c, d, bd, b^2d, cd, a^2bcd, ab^2cd$
6. $1, a, a^2, b, ab, a^2b, c, abc, a^2b^2c, d, bd, b^2d, acd, bcd, a^2b^2cd$
7. $1, a, b, ab, b^2, ab^2, c, abc, a^2b^2c, d, ad, a^2d, cd, a^2bcd, ab^2cd$
8. $1, a, b, ab, b^2, ab^2, c, abc, a^2b^2c, d, ad, a^2d, acd, bcd, a^2b^2cd$
9. $1, a, b, a^2b, ab^2, a^2b^2, c, ac, a^2c, d, abd, a^2b^2d, cd, bcd, b^2cd$
10. $1, a, b, a^2b, ab^2, a^2b^2, c, ac, a^2c, d, abd, a^2b^2d, acd, abcd, ab^2cd$

(C) $ca = a^2c$, $cb = b^2c$

11. $1, a, a^2, b, ab, a^2b, a^2c, bc, ab^2c, c^2, bc^2, b^2c^2, c^3, a^2bc^3, ab^2c^3$

(D) $ca = bc$, $cb = a^2c$

12. $1, a, a^2, b, ab, a^2b, a^2c, bc, ab^2c, c^2, bc^2, b^2c^2, c^3, a^2bc^3, ab^2c^3$
13. $1, a, a^2, b, ab, a^2b, a^2c, bc, ab^2c, c^2, bc^2, b^2c^2, ac^3, bc^3, a^2b^2c^3$
14. $1, a, a^2, b, ab, a^2b, a^2c, bc, ab^2c, c^2, bc^2, b^2c^2, a^2c^3, abc^3, b^2c^3$
15. $1, a, a^2, b, ab, a^2b, a^2c, bc, ab^2c, ac^2, abc^2, ab^2c^2, c^3, a^2bc^3, ab^2c^3$
16. $1, a, a^2, b, ab, a^2b, a^2c, abc, b^2c, c^2, bc^2, b^2c^2, c^3, abc^3, a^2b^2c^3$

(II) noncyclic 2-Sylow subgroup: $a^3 = b^3 = c^2 = d^2 = 1$, $ab = ba$, $cd = dc$

(A) $ca = ac$, $da = ad$, $cb = bc$, $db = bd$ [7]

17. $1, a, a^2, c, a^2c, bc, a^2bc, b^2c, a^2b^2c, ad, a^2bd, b^2d, acd, bcd, a^2b^2cd$
18. $1, a, a^2, c, a^2c, bc, a^2bc, b^2c, a^2b^2c, a^2d, abd, b^2d, cd, abcd, a^2b^2cd$
19. $1, a, a^2, c, a^2c, abc, a^2bc, b^2c, ab^2c, d, bd, b^2d, cd, abcd, a^2b^2cd$

(B) $da = ad$, $db = bd$, $ca = a^2c$, $cb = b^2c$

20. $1, a, a^2, b, ab, a^2b, c, bc, b^2c, d, abd, a^2b^2d, cd, a^2bcd, ab^2cd$

(C) $ca = a^2c$, $cb = bc$, $da = ad$, $db = bd$.

21. $1, a, a^2, b, ab, a^2b, c, abc, a^2b^2c, d, bd, b^2d, cd, a^2bcd, ab^2cd$
22. $1, a, a^2, b, ab, a^2b, c, abc, a^2b^2c, d, bd, b^2d, acd, bcd, a^2b^2cd$
23. $1, a, b, ab, b^2, ab^2, c, abc, a^2b^2c, d, ad, a^2d, cd, a^2bcd, ab^2cd$
24. $1, a, b, ab, b^2, ab^2, c, abc, a^2b^2c, d, ad, a^2d, acd, bcd, a^2b^2cd$
25. $1, a, b, a^2b, ab^2, a^2b^2, c, ac, a^2c, d, abd, a^2b^2d, cd, bcd, b^2cd$
26. $1, a, b, a^2b, ab^2, a^2b^2, c, ac, a^2c, a^2d, bd, ab^2d, cd, bcd, b^2cd$

(D) $ca = a^2c,\ cb = bc,\ da = ad,\ db = b^2d$

27. $1, a, a^2, b, ab, a^2b, c, abc, a^2b^2c, d, a^2bd, ab^2d, cd, bcd, b^2cd$
28. $1, a, a^2, b, ab, a^2b, c, abc, a^2b^2c, d, a^2bd, ab^2d, a^2cd, a^2bcd, a^2b^2cd$
29. $1, a, b, a^2b, ab^2, a^2b^2, c, ac, a^2c, d, bd, b^2d, cd, abcd, a^2b^2cd$
30. $1, a, b, a^2b, ab^2, a^2b^2, c, ac, a^2c, a^2d, a^2bd, a^2b^2d, cd, abcd, a^2b^2cd$ [8]
31. $1, a, b, a^2b, ab^2, a^2b^2, c, bc, b^2c, d, ad, a^2d, cd, abcd, a^2b^2cd$
32. $1, a, b, a^2b, ab^2, a^2b^2, c, bc, b^2c, d, ad, a^2d, acd, a^2bcd, b^2cd$

(E) $cb = bc,\ db = bd,\ da = ac,\ cda = ad$

33. $1, c, d, cd, a, ca, da^2, cb, cab, cdab, cda^2b, cb^2, cab^2, dab^2, a^2b^2$
34. $1, c, d, a, cda, ca^2, cda^2, ab, dab, ca^2b, da^2b, ab^2, cab^2, a^2b^2, ca^2b^2$

Sets 2, 9, 25 have trivial multiplier group; sets 1, 3, 6, 7, 10, 18, 21, 24, 26 have group Z_2; sets 27 and 33 have Z_3; sets 4, 5, 8, 11, 16, 20, 22, 23 have group $Z_2 \oplus Z_2$; sets 29 and 32 have Z_6; sets 19, 28, 34 have S_3; the multiplier group of sets 17, 30, 31 is dihedral of order 12; that of set 14 is $Z_3 \oplus Z_3$; of sets 12 and 13 is $Z_3 \oplus S_3$; the group of set 15 is of order 36, generated by $A^3 = B^3 = C^2 = D^2 = 1$ with $BA = AB$, $CA = BC$, $DA = B^2D$, $CB = AC$, $DB = A^2D$, $DC = CD$ (*group* II.D above).

There are nine nonisomorphic block designs generated by these difference sets.

References

1. L. D. Baumert, "Cyclic Difference Sets," Springer–Verlag, New York, 1971.
2. R. H. Bruck, Difference sets in a finite group, *Trans. Amer. Math. Soc.* **78** (1955), 464–481.
3. M. Hall, Jr., "Combinatorial Theory," Blaisdell, Waltham, Mass., 1967.
4. H. B. Mann, Difference sets in elementary Abelian groups, *Illinois J. Math.* **9** (1965), 212–219.
5. R. L. McFarland, A Family of difference sets in non-cyclic groups, *J. Combinatorial Theory, Ser. A* **15** (1973), 1–10.
6. H. B. Mann, "Addition Theorems," Interscience, New York, 1965.
7. R. J. Turyn, Character sums and difference sets, *Pacific J. Math.* **15** (1965), 319–346.
8. P. Kesava Menon, On difference sets, *Proc. Amer. Math. Soc.* **13** (1962), 739–745.
9. W. O. Alltop, Non-Abelian difference sets for quadratic designs, unpublished manuscript.