BULL. AUSTRAL. MATH. SOC. 05B05
VOL. 11 (1974), 1-4.

A family of supplementary difference sets

Emma Lehmer

This note exhibits a family of m - (v, k, λ) supplementary difference sets with parameters $v = 2mf + 1$, where $v = p$ is a prime and f is odd, $k = mf$ and $\lambda = m(mf-1)/2$. These sets are composed of a union of cosets of $2m$-th power residues of p .

A supplementary difference set m - (v, k, λ) is a system of m sets of k elements each such that if the differences between the elements of each set are taken modulo v then each non-zero difference appears λ times in the whole system; [2].

The difference set $2 - \left(p, \frac{p-1}{2}, \frac{p-3}{2}\right)$ was discussed by Szekeres [1], who proved that if C_0, C_1, C_2, C_3 are the four cosets of quartic residues, then the sets

$$S_0 : \{C_0, C_1\} \quad \text{and} \quad S_1 : \{C_0, C_3\}$$

are a pair of supplementary sets if $p \equiv 3 \pmod 8$.

Wallis and Whiteman [3] proved a similar theorem for cosets of octic residues which states that the sets

$$S_0 : \{C_0, C_1, C_2, C_3\}, S_1 : \{C_0, C_1, C_2, C_7\}$$
$$S_2 : \{C_0, C_1, C_6, C_7\}, S_3 : \{C_0, C_5, C_6, C_7\}$$

form a supplementary difference set $4 - \left(p, \frac{p-1}{2}, p-3\right)$ provided $p \equiv 9 \pmod{16}$.

Received 19 February 1974.

https://doi.org/10.1017/S0004972700043550 Published online by Cambridge University Press

It is the purpose of this note to show that these two results generalize into the following theorem.

THEOREM. *Let* $p = 2mf + 1$ *be a prime. Let* f *be odd and let* g *be a primitive root modulo* p. *Define the cosets of* $2m$*-th power residues by*

$$C_i = \{g^{2m\nu+i} \pmod p\}, \quad i = 0, 1, \ldots, 2m-1, \quad \nu = 0, 1, \ldots, f-1 .$$

Let

$$i_j = j + m\varepsilon_j, \text{ where } \varepsilon_0 = 0, \quad \varepsilon_j = 0 \text{ or } 1 .$$

Then for every choice of ε_j *the system of* m *sets*

$$S_n : \left\{C_{i_0-i_n}, C_{i_1-i_n}, \ldots, C_{i_{m-1}-i_n}\right\}, \quad n = 0, 1, \ldots, m-1 ,$$

is a supplementary difference set $m - (v, k, \lambda)$, *where*

$$v = p = 2mf + 1, \quad k = (p-1)/2 = mf, \quad \lambda = m(mf-1)/2 \quad (f \text{ odd}).$$

Proof. Denote as usual by (u, v) the number of solutions (ν, μ) of the congruence

$$g^{2m\mu+u} + 1 \equiv g^{2m\nu+v} \pmod p .$$

Since f is odd we have

$$(u, v) = (v+m, u+m) . \tag{1}$$

Let $\delta_t = g^{2m\tau+t}$ be an element of the set C_t. The number of times that δ_t is the difference between elements of two cosets of the set S_n is the number of solutions (μ, ν) of the congruence

$$g^{2m\mu+i-n+m(\varepsilon_i-\varepsilon_n)} - g^{2m\nu+j-n+m(\varepsilon_j-\varepsilon_n)} \equiv g^{2m\tau+t} \pmod p ,$$

which by (1) is

$$(j-n-t+m(\varepsilon_j-\varepsilon_n), \; i-n-t+m(\varepsilon_i-\varepsilon_n)) .$$

Therefore the number of times $N_n(\delta_t)$ that δ_t is the difference between elements of S_n is

https://doi.org/10.1017/S0004972700043550 Published online by Cambridge University Press

$$(2) \qquad N_n(\delta_t) = \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} \left(j-n-t+m(\varepsilon_j-\varepsilon_n),\ i-n-t+m(\varepsilon_i-\varepsilon_n)\right) = N_{n+m}(\delta_t)$$

by (1). Similarly, since the sum is symmetric in i and j, it remains unaltered if ε_n is changed and is therefore a function of $n + t$. Hence

$$(3) \qquad N_n(\delta_t) = N_{n+r}(\delta_{t-r}) \ , \quad r = 0, 1, \ldots, 2m-1 \ .$$

Hence the total number of times $N(\delta_t)$ that δ_t is a difference in all the m sets S_n is

$$N(\delta_t) = \sum_{n=0}^{m-1} N_n(\delta_t) = \sum_{n=0}^{m-1} N_{n+r}(\delta_{t-r}) = \sum_{\nu=r}^{m-1+r} N_\nu(\delta_{t-r}) = \sum_{n=0}^{m-1} N_n(\delta_{t-r})$$

by (2) and is therefore not a function of t, which proves the theorem.

Putting $n = 2$ and $n = 4$ gives the theorems of Szekeres and Wallis and Whiteman. For $n = 1$ we get the well known result that the $(p-1)/2$ quadratic residues modulo $p \equiv 3 \pmod 4$ form an ordinary difference set with $\lambda = (p-3)/4$.

For $m = 3$ the theorem seems to give a new result, [2], namely:

COROLLARY 1. *If* $p \equiv 7 \pmod{12}$ *is a prime then a* $3 - \left\{p, \frac{p-1}{2}, \frac{3(p-3)}{4}\right\}$ *supplementary difference set is given by*

$$S_0 : \{C_0, C_1, C_2\},\ S_1 : \{C_0, C_1, C_5\},\ S_2 : \{C_0, C_4, C_5\}$$

where C_i *are the cosets of sextic residues.*

For $m = 3$ the only other set S which satisfies the conditions of the theorem is $S : \{C_0, C_2, C_4\}$, which is the ordinary difference set of quadratic residues modulo p.

In general there are 2^{m-1} choices of the ε_i and hence of possible sets S. If m is a prime, then $2^{m-1} \equiv 1 \pmod m$ and we have an ordinary difference set and $(2^{m-1}-1)/m$ supplementary difference sets. Thus the number $n(m)$ of supplementary difference sets covered by the theorem increases very rapidly. In fact

https://doi.org/10.1017/S0004972700043550 Published online by Cambridge University Press

m	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$n(m)$	1	1	1	2	3	5	9	16	29	51	93	170	315	585	1092

We note that $n(4) = 2$, but the second set obtained by the theorem can be transformed into the Wallis-Whiteman set by a change of primitive root. Also $n(8)$ can be reduced from 16 to 4 if changes of primitive root are allowed. For m a prime there is at least one supplementary difference set which is independent of the primitive root. Simply choose for S_0 the union of C_0 with those cosets C_i for which i is prime to $2m$. Since all the primitive roots must be in these cosets, S_0 does not depend on the primitive root and therefore the other sets of the system must permute among themselves with a change of primitive root. This singles out an invariant set from the $n(m)$ sets when m is a prime.

It is obvious that every element of C_0 is a multiplier of every supplementary difference set made up of cosets as it leaves every S_n unaltered. A broader definition of multipliers which permute the sets might be useful.

References

[1] G. Szekeres, "Cyclotomy and complementary difference sets", *Acta Arith.* 18 (1971), 349-353.

[2] Jennifer Wallis, "On supplementary difference sets", *Aequationes Math.* 8 (1972), 242-257.

[3] Jennifer Wallis and Albert Leon Whiteman, "Some classes of Hadamard matrices with constant diagonal", *Bull. Austral. Math. Soc.* 7 (1972), 233-249.

Berkeley,
California,
USA.