THE DIFFERENCE BETWEEN CONSECUTIVE MEMBERS OF A DIFFERENCE SET (mod v)

E. SPENCE

ABSTRACT. Let $\mathcal{D} = \{d_1, d_2, \dots, d_k\}$ be a difference set (mod v) so that for any $d \not\equiv 0 \pmod{v}$ there are exactly λ pairs (d_i, d_j) , $d_i, d_j \in \mathcal{D}$ such that $d_i - d_j \equiv d \pmod{v}$. Suppose further that $0 \leq d_1 < d_2 < \dots < d_k < v$ and write $d_{k+1} = v + d_1$. The following two results are proved:

- (i) $\sum_{i=1}^k (d_{i+1} - d_i)^2 = O((v^2/k) \log k)$,
- (ii) $\max_{1 \leq i \leq k} (d_{i+1} - d_i) = O(v/\sqrt{k})$.

1. Introduction. A set $\mathcal{D} = \{d_1, d_2, \dots, d_k\}$ of k integers is said to be a *difference set modulo v* if for any $d \not\equiv 0 \pmod{v}$ there are exactly λ pairs (d_i, d_j) , $d_i, d_j \in \mathcal{D}$ such that $d_i - d_j \equiv d \pmod{v}$. By counting all possible pairs (d_i, d_j) in two ways it is clear that the parameters v , k and λ satisfy

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

For an excellent account of the present state of knowledge of difference sets see [1]. The most well-known difference sets are the *Singer difference sets* with parameters $v = (q^{n+1} - 1)/(q - 1)$, $k = (q^n - 1)/(q - 1)$, $\lambda = (q^{n-1} - 1)/(q - 1)$ where $n \geq 2$ and q is a power of a prime [6], and the *Hadamard difference sets* with parameters $v = p$, $k = \frac{1}{2}(p-1)$, $\lambda = \frac{1}{4}(p-3)$, where p is a prime congruent to 3 (mod 4).

It is clear that if $\mathcal{D} = \{d_1, d_2, \dots, d_k\}$ is a difference set modulo v it may be assumed that $0 \leq d_i < v$ and that $d_i < d_{i+1}$. This condition will be taken to hold throughout the remaining discussion.

Write $d_{k+1} = v + d_1$ so that the integers $d_1, d_2, \dots, d_{k+1}$ lie in an interval of length v . The problem that is the purpose of this paper is to discuss the estimation, in terms of v , k and λ of

- (i) $\sum_{i=1}^k (d_{i+1} - d_i)^2$, and
- (ii) $\max_{1 \leq i \leq k} (d_{i+1} - d_i)$.

Received by the editors September 5, 1972.

AMS (MOS) subject classifications (1970). Primary 05B10; Secondary 05A20.

Key words and phrases. Difference set (mod v).

Copyright © 1974, American Mathematical Society

Using methods due to Hooley [3] and Erdős and Turán [2] the following results will be proved:

$$(iii) \sum_{i=1}^k (d_{i+1} - d_i)^2 = O((v^2/k) \log k),$$

$$(iv) \max_{1 \leq i \leq k} (d_{i+1} - d_i) = O(v/\sqrt{k}).$$

A trivial lower bound for (iii) is v^2/k obtained by using Cauchy's inequality, while $\max_{1 \leq i \leq k} (d_{i+1} - d_i)$ is clearly greater than or equal to v/k . Because of the discrepancy between the upper and lower bounds obtained and since (iii) can certainly be improved for a particular class of Hadamard difference sets (as will be mentioned later), it is felt that the estimates obtained may possibly be improved.

2. An upper bound for $\sum_{i=1}^k (d_{i+1} - d_i)^2$. Let

$$f(m) = 1 \quad \text{if } m \equiv d_i \pmod{v} \text{ for some } d_i \in \mathcal{D}, \\ = 0 \quad \text{otherwise,}$$

and for any positive integer h let $F(m, h)$ be defined by $F(m, h) = \sum_{n=m}^{m+h-1} f(n)$. If $d_i \in \mathcal{D}$ then d_i , or an integer congruent to $d_i \pmod{v}$, lies in exactly h of the intervals $[0, h[$, $[1, h+1[$, $\dots$, $[v-1, v+h-1[$ and hence

$$(2) \quad \sum_{m=0}^{v-1} F(m, h) = hk.$$

Similarly, $F(m, h)(F(m, h) - 1)$ is the number of ordered pairs (d_i, d_j) , $d_i, d_j \in \mathcal{D}$ with $m \leq d_i, d_j < m+h$ (where integers congruent $\pmod{v}$ are identified) and each such pair (d_i, d_j) lies in $h - |d_i - d_j|$ of the intervals $[0, h[$, $[1, h+1[$, $\dots$, $[v-1, v+h-1[$. Hence

$$\begin{aligned} \sum_{m=0}^{v-1} F(m, h)(F(m, h) - 1) &= 2 \sum_{t=1}^h \sum_{\substack{d_i - d_j \equiv t \pmod{v}; \\ d_i, d_j \in \mathcal{D}}} (h - t) \\ &= 2\lambda \sum_{t=1}^h (h - t) = \lambda h(h - 1). \end{aligned}$$

Consequently

$$(3) \quad \sum_{m=0}^{v-1} F^2(m, h) = h\{\lambda(h - 1) + k\}.$$

In order to find a lower bound for the sum $\sum_{m=0}^{v-1} F^2(m, h)$ Cauchy's inequality is used and to utilize it to the full advantage we find the number of integers m , $0 \leq m < v$, such that $F(m, h) = 0$. For if this number is $v(h)$, then

$$(4) \quad \sum_{m=0}^{v-1} F^2(m, h) \geq \left\{ \sum_{m=0}^{v-1} F(m, h) \right\}^2 / (v - v(h)) = \frac{h^2 k^2}{v - v(h)},$$

by (2).

Combining (3) and (4) yields

$$(5) \quad v(h) \leq v - hk^2/(\lambda(h-1) + k) = (k - \lambda)(v - h)/(\lambda(h-1) + k).$$

Now, for $d_1 + 1 \leq m \leq v + d_1$, $F(m, h) = 0$ if and only if there exists an integer i , $1 \leq i \leq k$, such that $d_i \leq m - 1$ and $d_{i+1} \geq m + h$, which implies $d_{i+1} - d_i \geq h + 1$. Let N_r be the number of integers i with $1 \leq i \leq k$, such that $d_{i+1} - d_i = r$. Then if $d_{i+1} - d_i = r \geq h + 1$ there are $r - h$ values of m , $0 \leq m < v$, such that $d_i \leq m - 1$, $d_{i+1} \geq m + h$ and $F(m, h) = 0$ (since $F(m, h)$ is periodic in m of period v).

Hence

$$(6) \quad \begin{aligned} v(h) &= \sum_{r \geq h+1; d_{i+1}-d_i=r} (r-h) = \sum_{r \geq h+1} (r-h)N_r \\ &= N_{h+1} + 2N_{h+2} + 3N_{h+3} + \dots \end{aligned}$$

Thus (5) and (6) give

$$(7) \quad N_{h+1} + 2N_{h+2} + 3N_{h+3} + \dots \leq (k - \lambda)(v - h)/(\lambda(h-1) + k).$$

This inequality is valid also when $h = 0$, since then the left-hand side is $N_1 + 2N_2 + 3N_3 + \dots = \sum_{i=1}^k (d_{i+1} - d_i) = v$.

It is a simple exercise to show that

$$\sum_{h \geq 0} (N_{h+1} + 2N_{h+2} + \dots) = \frac{1}{2} \sum_{h \geq 1} h(h+1)N_h = \frac{1}{2} \sum_{i=1}^k (d_{i+1} - d_i)^2 + \frac{1}{2}v.$$

The series on the left-hand side of (7) is of course finite, ending with the term $(M - h)N_M$ where $M = \max_{1 \leq i \leq k} (d_{i+1} - d_i)$ (assuming that $h \leq M$). Taking a trivial estimate for M , namely v , and summing (7) from $h = 0$ to $h = v$ we obtain

$$\begin{aligned} \frac{1}{2} \sum_{i=1}^k (d_{i+1} - d_i)^2 + \frac{1}{2}v &\leq \sum_{h=0}^v \frac{(k - \lambda)(v - h)}{\lambda(h-1) + k} \leq v + \frac{(k - \lambda)v}{\lambda} \sum_{h=1}^v \frac{1}{h-1 + k/\lambda} \\ &= O\left(\frac{k - \lambda}{\lambda} v \log \frac{v-1 + k/\lambda}{k/\lambda}\right) \\ &= O\left(\frac{k - \lambda}{\lambda} v \log k\right) \quad \text{by (1).} \end{aligned}$$

Hence

$$\sum_{i=1}^k (d_{i+1} - d_i)^2 = O\left(\frac{k-\lambda}{\lambda} v \log k\right) = O\left(\frac{v^2}{k} \log k\right)$$

when (1) is used to express λ in terms of v and k .

Notes. 1. In the case of a Hadamard difference set with parameters $v = p$, $k = \frac{1}{2}(p-1)$, $\lambda = \frac{1}{4}(p-3)$, p a prime congruent to 3 (mod 4), where $\mathcal{D}$ is the set of quadratic residues (mod p) (that the quadratic residues (mod p) form a difference set (mod p) is easily shown; see, for example, [5, p. 133]), Norton [4] has obtained a much better upper bound, namely $O(v^2/k) = O(p)$. However, his method utilized deep results on character sums which are not available for general difference sets. It is perhaps also worthwhile pointing out that a Hadamard difference set (mod p) (p a prime congruent to 3 (mod 4)) is not necessarily a set of quadratic residues (mod p).

2. If a really good estimate for $M = \max_{1 \leq i \leq k} (d_{i+1} - d_i)$ could be found, an improvement in the above estimate would follow. Unfortunately, the result $M = O(v/\sqrt{k})$ to be obtained in the next section is not quite good enough, since it only replaces the factor $\log k$ by $\log \sqrt{k}$ which is no improvement at all.

3. Using the inequality (7) and Hooley's method as in [3] it is possible to prove that $\sum_{i=1}^k (d_{i+1} - d_i)^\beta = O(v(v/k)^{\beta-1})$ ($1 \leq \beta < 2$) where the implied constant depends only on β . This result is best possible.

3. An upper bound for $\max_{1 \leq i \leq k} (d_{i+1} - d_i)$. The method used to estimate $\max (d_{i+1} - d_i)$ is due to Erdős and Turán [2]. As before let $\mathcal{D} = \{d_1, d_2, \dots, d_k\}$ be a difference set (mod v) and let $M = \max_{1 \leq i \leq k} (d_{i+1} - d_i)$. Since $\{d_1 + d, \dots, d_k + d\}$, with integers reduced (mod v), is also a difference set (mod v) for any integer d we may suppose that

$$(8) \quad d_k = v \quad \text{and} \quad d_k - d_{k-1} = M.$$

Let $\mathcal{D}' = \{d_1, \dots, d_{k-1}\}$ where $d_1 < d_2 < \dots < d_{k-1}$ and let h be a positive integer. Consider the $d_{k-1} + h$ intervals $I_m = [-h + m, -1 + m]$ ($1 \leq m \leq d_{k-1} + h$), and let $G(m, h)$ denote the number of integers in $\mathcal{D}'$ that lie in the interval I_m . Since each d_i occurs in exactly h intervals we have

$$(9) \quad \sum_{m=1}^{d_{k-1}+h} G(m, h) = h(k-1).$$

Also, the number of pairs (d_i, d_j) ($1 \leq i < j \leq k-1$) lying in I_m is $\frac{1}{2}G(m, h)(G(m, h) - 1)$ and hence the total number of pairs (d_i, d_j) belonging

to the same interval I_m ($1 \leq m \leq d_{k-1} + h$) is $\frac{1}{2} \sum_{m=1}^{d_{k-1}+h} G(m, h)(G(m, h) - 1)$.

However, since each positive integer $d < h$ can arise as a difference $d_i - d_j$ at most λ times, and corresponding to $d = d_i - d_j$ the pair (d_i, d_j) occurs in exactly $h - d$ intervals I_m , we have that

$$\frac{1}{2} \sum_{m=1}^{d_{k-1}+h} G(m, h)(G(m, h) - 1) \leq \lambda \sum_{d=1}^h (h - d) = \frac{1}{2} \lambda h(h - 1).$$

Moreover, using Cauchy's inequality and (9) we obtain

$$\sum_{h=1}^{d_{k-1}+h} G(m, h)(G(m, h) - 1) \geq \frac{h(k-1)\{h(k-1) - (d_{k-1} + h)\}}{d_{k-1} + h},$$

from which follows

$$(h(k-1)\{h(k-1) - (d_{k-1} + h)\})/(d_{k-1} + h) \leq \lambda h(h-1),$$

i.e.

$$d_{k-1} + h \geq h(k-1)^2/(\lambda(h-1) + k-1).$$

But $d_k - d_{k-1} = M$ by (8), and the latter inequality reduces to

$$M \leq v + h - h(k-1)^2/(\lambda(h-1) + k-1).$$

By choosing $h = [(1/\lambda)\{(k-1)\sqrt{(k-\lambda-1)} - (k-\lambda-1)\}]$ and using (1) we find that

$$M = O((k-1)\sqrt{(k-\lambda)/\lambda}) = O(v/\sqrt{k}).$$

REFERENCES

1. L. D. Baumert, *Cyclic difference sets*, Lecture Notes in Math., vol. 182, Springer-Verlag, Berlin and New York, 1971. MR 44 #97.
2. P. Erdős and P. Turán, *On a problem of Sidon in additive number theory, and on some related problems*, J. London Math. Soc. 16 (1941), 212–215. MR 3, 270.
3. C. Hooley, *On the difference of consecutive numbers prime to n* , Acta Arith. 8 (1962/63), 343–347. MR 27 #5741.
4. K. K. Norton, *On the distribution of k th power residues and non-residues modulo n* , J. Number Theory 1 (1969), 398–418. MR 40 #4223.
5. H. J. Ryser, *Combinatorial mathematics*, Carus Math. Mono., no. 14, Wiley, New York.
6. J. Singer, *A theorem in finite projective geometry and some applications to number theory*, Trans. Amer. Math. Soc. 43 (1938), 377–385.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF GLASGOW, GLASGOW G12 8QW, SCOTLAND