数理解析研究所講究録
第 344 巻 1979 年 22-25

A Family of Difference Sets having Minus One as a Multiplier.

by

Masahiko Miyamoto.

Department of Mathematics

Hokkaido University.

A construction is given for difference sets having minus one as multiplier, whose parameters are
$v=\frac{1}{2}3^{s+1}(3^{s+1}-1)$, $k=\frac{1}{2}3^{s}(3^{s+1}+1)$, $\lambda=\frac{1}{2}3^{s}(3^{s}+1)$, $n=3^{2s}$ (s even).

Let G be a finite group of order v. A subset D of order k is a difference set in G with parameters (v,k,λ,n) in case every non-identity element g in G can be expressed in exactly λ way as $g=d_1^{-1}d_2$ with $d_1,d_2 \in D$. The parameter n is defined by $n=k-\lambda$. For any integer t, let D(t) denote the image of D under the mapping $g \to g^t$, g in G. If D(t) is a translate of D, then t is called a multiplier of D.

In his paper [1], McFarland constructed difference sets and showed the first example of difference set having minus one as a multiplier whose parameters are not of the form $(v,k,\lambda,n)=(4m^2,2m^2-m,m^2-m,m^2)$. This difference set has the parameters (4000,775,150,625).

In this paper, we will show an infinite series of difference sets which have minus one as a multiplier. Recently, Spence [2] showed a family of difference set with parameters
$v=\frac{1}{2}3^{s+1}(3^{s+1}-1)$, $k=\frac{1}{2}3^{s}(3^{s+1}+1)$, $\lambda=\frac{1}{2}3^{s}(3^{s}+1)$, $n=3^{2s}$.

By modification of his argument, we will prove the following theorem.

Theorem. There exists a difference set with parameter $v=\frac{1}{2}3^{s+1}(3^{s+1}-1)$, $k=\frac{1}{2}3^{s}(3^{s+1}+1)$, $\lambda=\frac{1}{2}3^{s}(3^{s}+1)$, $n=3^{2s}$ which has minus one as a multiplier for each even integer $s \geq 2$.

Proof. Let E denote the additive group of $GF(3^{s+1})$ and K_1 denote the multiplicative group of $GF(3^{s+1})$ (s an even integer ≥ 2). Then since s is even, we have $K_1=Z_2 \times K$ for a subgroup K of odd order. Set $G=E*K$ be a semi-direct product of E by K. Then we have the following;

(I). a) $|G|=\frac{1}{2}3^{s+1}(3^{s+1}-1)$,

b) K is a cyclic subgroup of order $r=\frac{1}{2}(3^{s+1}-1)$,

c) K acts on $E^{\#}$ as fixed point free automorphisms,

and d) K permutes all hyperplanes of E transitively and no elements of $K^{\#}$ fix a hyperplane of E.

Let H be a hyperplane of E and $k_1=1, k_2, \ldots, k_r$ be the element of K. Then we will show that

$$D=(E-H)*k_1 \cup \bigcup_{i=2}^{r} (H^{\sqrt{k_i}^{-1}})*k_i$$

is a difference set in G having minus one as a multiplier, where $\sqrt{k}$ is a square of k in K, which is well defined since the order r of K is odd.

Using the group ring notation for ZE, it is readily seen that (cf. [2])

(II). $H^{\sqrt{k_1}^{-1}}+H^{\sqrt{k_2}^{-1}}+\ldots+H^{\sqrt{k_r}^{-1}}=3^{s}\cdot 1_E+\frac{1}{2}(3^{s}-1)E$,

$$H^{\sqrt{k_i^{-1}}}H^{\sqrt{k_i^{-1}}}=3^s H^{\sqrt{k_i^{-1}}},$$

$$H^{\sqrt{k_i^{-1}}}H^{\sqrt{k_j^{-1}}}=3^{s-1}E \quad (i\neq j),$$

$$(E-H)(E-H)=3^s(H+E), \quad \text{and}$$

$$(E-H)H^{\sqrt{k_i^{-1}}}=2\cdot 3^{s-1}E \quad (i\neq 1),$$

since $H^{\sqrt{k_i^{-1}}}=H^{\sqrt{k_j^{-1}}}$ if and only if $k_i=k_j$.

To verify that D is a difference set in G it is sufficient to show that $D(-1)D=n\cdot 1_G+\lambda G$, where n,λ are as above. Since the inverse of an element $h*k$ is $h^{-k}*k^{-1}$ for $h\in E$ and $k\in K$, we have

$$D(-1)=(E-H)*k_1 \cup \bigcup_{i=2}^{r}(H^{\sqrt{k_i}}*k_i^{-1}).$$

Then we can easily check $D(-1)=D$. Using (II), we have

$$\begin{aligned}
D(-1)D &=(E-H)(E-H)*k_1 +\sum_{i=2}^{r}(H^{\sqrt{k_i}}*k_i^{-1})(H^{\sqrt{k_i^{-1}}}*k_i)\\
&\quad + \underset{2\leqq i\neq j\leqq r}{}(H^{\sqrt{k_i}}*k_i^{-1})(H^{\sqrt{k_j^{-1}}}*k_j)\\
&\quad +(E-H)\sum_{j=2}^{r}H^{\sqrt{k_j^{-1}}}*k_j +(\sum_{i=2}^{r}H^{\sqrt{k_i}}*k_i^{-1})(E-H)*1_K\\
&=3^2(E+H)*1_K +\sum_{i=2}^{r}H^{\sqrt{k_i}}H^{\sqrt{k_i}}*1_K\\
&\quad +\sum_{2\leqq i\neq j\leqq r}H^{\sqrt{k_i}}H^{\sqrt{k_j^{-1}}k_i}*k_i^{-1}k_j\\
&\quad +2\cdot 3^{s-1}E*(K-1_K) +\sum_{i=2}^{r}H^{\sqrt{k_i}}(E-H)^{k_i}*k_i^{-1}\\
&= 3^2(E+H)*1_K +\sum_{i=2}^{r}3^s H^{\sqrt{k_i}}*1_K +\sum_{2\leqq i\neq j\leqq r}3^{s-1}E*k_i^{-1}k_j\\
&\quad +2\cdot 3^{s-1}E*(K-1_K) +2\cdot 3^{s-1}E*(K-1_K)\\
&=3^s E*1_K +3^s(3^s\cdot 1_E +\tfrac{1}{2}(3^s-1)E)*1_K +3^{s-1}(r+2)E*(K-1_K)
\end{aligned}$$

$$=3^{2s}\cdot 1_G + \frac{1}{2}3^s(3^s+1)E^*1_K + 3^{s-1}(\frac{1}{2}(3^{s+1}-1)+2)E^*(K-1_K)$$

$$=3^{2s}\cdot 1_G + \frac{1}{2}3^s(3^s+1)G.$$

So we have proved that D is a difference set having minus one as a multiplier.

This completes the proof of Theorem.

Reference

[1]. R.L.McFarland, A Family of Difference Sets in Non-cyclic Groups, J. Combinatorial Theory (A) 15 (1973), 1-10.

[2]. E.Spence, A Family of Difference Sets, J. Combinatorial Theory (A) 22 (1977), 103-106.