1 Introduction

In this paper, we will discuss a method for generating difference sets from groups of a specific form, first suggested by R. L. McFarland [1] and later improved by J. F. Dillon [2]. We will also consider the construction of inequivalent difference sets from the same group.

Definition 1.1. *Let $q = p^n$ be some prime power, then the* elementary abelian group *of order q is isomorphic to*

$$\overbrace{\mathbb{Z}_p \times \mathbb{Z}_p \times ... \times \mathbb{Z}_p}^{n\ times}$$

2 Constructing McFarland's Difference Sets

In McFarland's paper, he proposes that difference sets exist with parameters

$$v = q^{s+1}\left(\frac{q^{s+1}-1}{q-1}+1\right), k = q^s\frac{q^{s+1}-1}{q-1}, n = q^{2s}, \text{ and } \lambda = q^s\frac{q^s-1}{q-1} \tag{1}$$

where q is a prime power and s is an integer in a group $G = E \times K$ where E is an Elementary Abelian Group of order q^{s+1} and K is any group of order $\dfrac{q^{s+1}-1}{q-1}+1$.

Suppose we have a finite field F of order q and a vector space V of dimension $s+1$ over F. Let $H_1, H_2, \ldots, H_r$ be all the hyperplanes (i.e. subspaces of dimension s). We wish to count the number of hyperplanes in order to find r. Instead of counting the number of hyperplanes, we can count the number of one dimensional subspaces (since each hyperplane is the orthogonal complement of a one dimensional subspace).

Consider the one dimensional subspace generated by an arbitrary vector. We can scale this vector by any non-zero element in F to obtain another non-zero vector in our subspace. Thus each one-dimensional subspace contains $q-1$ non-zero vectors. There are a total of $q^{s+1}-1$ non-zero elements in V. Thus the total number of one dimensional subspaces (and the number of hyperplanes) is:

$$r = \frac{q^{s+1}-1}{q-1}$$

We are now going to change how we think about V. Let E be the additive group of V. Remember that V has finite dimension and F is a finite field, so V contains a finite number of vectors. Thus we can think about these vectors as elements of a group. Note that E satisfies definition 1.1, so it is an Elementary Abelian Group. Also note that $H_1, H_2, \ldots, H_r$ are subgroups of E.

Let K be any group of order $r+1$. Let $e_1, e_2, \ldots, e_r \in E$ and $k_1, k_2, \ldots, k_r \in K$. Consider the different cosets $H_i + e_i$. In the group $G = E \times K$, we claim that the set

$$D = \{(H_i + e_i, k_i)\} | i = i, \ldots, r\}$$

is a difference set. Before we attempt to show that D is a difference set, let's consider the following lemmas.

Lemma 2.1. $\displaystyle\sum_{i=1}^{r} H_i = q^s 1_E + \frac{q^s-1}{q-1}E$

Proof. Recall that $H_1, H_2, \ldots, H_r$ are *all* the hyperplanes contained in V. Thus, thinking of these as subgroups, they contain all the elements of E. Since the identity is contained in each group exactly one time, we have a total of r copies of the identity. Now consider two non-identity elements of E.

We know there is an automorphism that interchanges these two elements. However, this also permutes the hyperplanes. Thus each non-identity element is repeated an equal number of times. A counting argument reveals that the total number of times the non-identity elements are repeated are $\frac{q^s-1}{q-1}$. Thus, we find that

$$\sum_{i=1}^{r} H_i = r1_E + \frac{q^s-1}{q-1}[E - 1_E] = q^s 1_E + \frac{q^s-1}{q-1}E$$

□

Lemma 2.2. $H_i^2 = q^s H_i$

Proof. Recall that $H_i \cdot H_i = \{a \cdot b | a, b \in H_i\}$ (for all possible combinations of a and b). Fix $a_1 \in H_i$. Since H_i is a group, $\{a_1 \cdot b | b \in H_i\} = H_i$ since multiplying by a_1 simply permutes the group elements. In computing $H_i \cdot H_i$, we let a_1 run through all possible elements in H_i. Thus we reproduce each group element $|H_i|$ times. Recalling that $|H_i| = q^s$, we find:

$$H_i^2 = H_i \cdot H_i = |H_i| H_i = q^s H_i$$

□

Lemma 2.3. $K^2 = (r+1)K$

Proof. Following the same logic in Lemma 2.2, we find that $K^2 = |K|K$. Since $|K| = r+1$, we find $K^2 = (r+1)K$. □

Lemma 2.4. $H_i H_j = q^{s-1} E$ *if* $i \neq j$

Proof. Again, recall that $H_i H_j = \{a \cdot b | a \in H_i, b \in H_j\}$. For any $e \in H$, there exists $a \in H_j$ and $b \in H_j$ such that $e = ab$ (note that $e \in H_i H_j$). For e to be in $H_i H_j$, e must be in the form $e = (ah)(bh^{-1})$ where $h \in H_i \cap H_j$. Since $i \neq j$, we find that the dimension of $H_i \cap H_j$ is $s-1$. Thus there are a total of q^{s-1} elements h. This means that in $H_i H_j$ each element is repeated q^{s-1} times. Thus,

$$H_i H_j = q^{s-1} E$$

□

Lemma 2.5. *Let* $k, k_1, k_2, \ldots, k_r$ *be all the elements of* K*. Then,*

$$\sum_{i \neq j} k_i^{-1} k_j = q\frac{q^s-1}{q-1}[K - 1_K]$$

Proof. First note that given the elements defined above,

$$\sum_{i \neq j} k_i^{-1} k_j + \sum_{i=1}^{r} k_i^{-1} k_i = (K - k^{-1})(K - k)$$

$$\begin{aligned}
\sum_{i \neq j} k_i^{-1} k_j &= (K - k^{-1})(K - k) - \sum_{i=1}^{r} k_i^{-1} k_i \\
&= K^2 - 2K + 1_K - rK \\
&= (r+1)K - 2K - (r-1)1_K \text{ by Lemma 2.3} \\
&= (r-1)K - (r-1)1_K \\
&= (r-1)(K - 1_K) \\
&= q\frac{q^s-1}{q-1}[K - 1_K]
\end{aligned}$$

Thus $\sum_{i\neq j} k_i^{-1}k_j = q\frac{q^s-1}{q-1}[K-1_K]$. □

Theorem 2.6. *The set $D = \{(H_i + e_i, k_i)\}|i = 1, \ldots, r\}$ is a difference set with parameters given in 1.*

Proof. First note that with $G = E \times K$, we find that

$$|G| = |E||K| = v = q^{s+1}(r+1) = q^{s+1}\left(\frac{q^{s+1}-1}{q-1}+1\right)$$

$$|D| = |H_i|r = k = q^s r = q^s\left(\frac{q^{s+1}-1}{q-1}\right)$$

Note that we can equivalently define D as $D = \sum_{i=1}^{r} H_i e_i k_i$. To prove that D is a difference set, and to find the remaining parameters, recall that $D^{-1}D = n1_G + \lambda G$.

$$\begin{aligned}
D^{-1}D &= \left(\sum_i H_i e_i^{-1} k^{-1}\right)\left(\sum_j H_j e_j k_j\right) \\
&= \sum_i H_i^2 1_K + \sum_{i\neq j} H_i H_j e_i^{-1} e_j k_i k_j \text{ noting that } E \text{ is Abelian} \\
&= q^s \sum_i H_i 1_K + q^{s-1}\sum_{i\neq j}(E e_i^{-1} e_j)(k_i^{-1}k_j) \text{ by Lemma 2.2 and 2.4} \\
&= q^s\left[q^s 1_E + \left(\frac{q^s-1}{q-1}\right)E\right]1_K + q^{s-1}E\sum_{i\neq j} k_i^{-1}k_j \text{ by Lemma 2.1} \\
&= q^s\left[q^s 1_E + \left(\frac{q^s-1}{q-1}\right)E\right]1_K + q^s E\frac{q^s-1}{q-1}[K-1_K] \text{ by Lemam 2.5} \\
&= q^{2s}1_E 1_K + q^s\frac{q^s-1}{q-1}E1_K + Eq^s\frac{q^s-1}{q-1}K - Eq^s\frac{q^s-1}{q-1}1_K \\
&= q^{2n}1_E 1_K + q^s\frac{q^s-1}{q-1}EK \\
&= q^{2s}1_G + q^s\frac{q^s-1}{q-1}G
\end{aligned}$$

Thus we find that D is a difference set with parameters given in (1). □

3 Dillon's Extension of McFarland's Work

We will again let q be a prime power, and examine the elementary Abelian group (1.1) E of order q^{s+1}. We will once again look at the hyperplanes, defined identically as in McFarland's work. We notice that in the integral group ring, ZG, we have

$$\sum_{i=1}^{r} H_i = r1_E + \left(\frac{q^s-1}{q-1}\right)(E - 1_E) \tag{2}$$

Let G be a group of order $v = q^{s+1}(r+1)$ such that E is a normal subgroup of G. Now, let us partition G into its cosets of E

$$G = g_1E + g_2E + ... + g_{r+1}E$$

If we look at the factor group G/E we note that $g_1E, g_2E, ...g_rE$ forms a trivial difference set with parameters $(r+1, r, r-1, 1)$. Analogously in ZG

$$\sum_{i,j=1}^{r} g_i g_j^{-1} E = E + (r-1)G \\ = rE + (r-1)(G-E) \tag{3}$$

Let our proposed difference set, D, be the subset of G given by

$$D = g_1H_1 + ... + g_rH_r$$

We note that

$$DD^{-1} = \sum_{i,j=1}^{r} g_i H_i H_j g_j^{-1} \\ = q^s \sum_{i=1}^{r} g_i H_i g_i^{-1} + q^{s-1} \sum_{i,j=1, i\neq j}^{r} g_i g_j^{-1} E$$

From (3), we know that the second of these sums is $(r-1)(G-E)$. We want $DD^{-1} = n1_G + \lambda G$, so D is a difference set if and only if

$$q^s \sum_{i=1}^{r} g_i H_i g_i^{-1} = q^s r 1_E + q^{s-1}(r-1)[E - 1_E]$$

Through algebraic manipulation we find that this is true when

$$\sum_{i=1}^{r} g_i H_i g_i^{-1} = r1_E + \frac{q^s - 1}{q-1}[E - 1_E]$$

From (2), if $H_i \to g_i H_i g_i^{-1}$ is a map that permutes the hyperplanes, then we have a sufficient condition for the above equality to hold. This establishes Dillon's main theorem

Theorem 3.1. *Let q be a prime power and let s be any positive integer. Let E be the elementary abelian group of order q^{s+1} (which we regard as a vector space of dimension $s+1$ over $GF(q)$), and let $H_1, H_2, ..., H_r$, $r = (q^{s+1}-1)/(q-1)$, be the s-dimensional subspaces of E. Let G be a group of order $q^{s+1}(r+1)$ which contains E as a normal subgroup and let $g_1, g_2, ..., g_r$ be elements of G lying in distinct cosets of E. Let $D = g_1H_1 + g_2H_2 + ... + g_rH_r$ If the coset representatives g_i should have the property that $\{g_i H_i^* g_i^{-1} : 1 \leq i \leq r\}$ is a 1-design on the point set E^*, then D is a difference set with parameters given by 1.*

$$v = q^{s+1}\left(\frac{q^{s+1}-1}{q-1} + 1\right)$$
$$k = q^s\left(\frac{q^{s+1}-1}{q-1}\right)$$
$$\lambda = q^s\left(\frac{q^s-1}{q-1}\right)$$
$$n = q^{2s}$$

Corollary 3.2. *If the subgroup E of G lies in the center of G, then D is a difference set for all choices of the coset representatives $g_1, g_2, ..., g_r$. McFarland's result is an example of this.*

4 Inequivalent Difference Sets

Definition 4.1. *Two difference sets with the same parameters are* equivalent *if one can be mapped into the other by a translation or an automorphism.*

Consider a group, G, of the familiar form $G = E \times K$. We will show that when q^s is odd, we can generate $\frac{1}{2}(q^s+1)$ pairwise inequivalent difference sets for G.

Consider a difference set for G generated using our earlier methods, broken up into two sums based on the parameter t. We define

$$D_t = \sum_{i=1}^{t}(H_i e_i, k_i) + \sum_{i=t+1}^{r}(H_i, k_i)$$

for $t = 0, 1, 2, ..., \frac{1}{2}(q^s+1)$, where $k_i \in K$ and $e_i \in E$ but $e_i \notin H_i$. It is clear that none of the terms in the left sum contain the identity, since $e_i \notin H_i$, but each term in the right some does contain the identity. If we hit D_t with the projection homomorphism given by $G = E \times K \to E$, we have

$$D_t' = \sum_{i=1}^{t} H_i e_i + \sum_{i=t+1}^{r} H_i$$

Although D_t' may no longer be a difference set, it will still prove valuable. We note that there are $r-t$ copies of the identity in the right sum. From a previous result, we know that there are at most $(q^s-1)/(q-1)+t$ copies of any non identity element in D_t'. It follows that if $t \leq \frac{1}{2}(q^s-1)$, then D_t' has a unique largest coefficient (the coefficient of the identity) of $r-t$, as

$$\begin{aligned}
\frac{q^s-1}{2} &\geq t \\
q^s &> 2t \\
\frac{q^{s+1}-q^s}{q-1} &> 2t \\
\frac{q^{s+1}-1}{q-1} - t &> \frac{q^s-1}{q-1} + t \\
r - t &> \frac{q^s-1}{q-1} + t
\end{aligned}$$

We can use this largest coefficient to differentiate between our $\frac{1}{2}(q^s+1)$ difference sets:

$$\{D_0, D_1, ..., D_{(q^s-1)/2}\}$$

Furthermore, the fact that the image of D_t under our projection homomorphism has a largest coefficient equal to $r-t$ is clearly invariant under equivalence (see 4.1). Thus, our $\frac{1}{2}(q^s+1)$ difference sets are pairwise inequivalent, as required.

5 References

(1) McFarland, Robert L. *A Family of Difference Sets in Non-cyclic Groups.* Journal of Combinatorial Theory, Series A 15, 1-10 (1973). Copyright 1973 by Academic Press, Inc. New York, NY.

(2) Dillon, J F. *Variations on a Scheme of McFarland for Noncyclic Difference Sets.* Journal of Combinatorial Theory, Series A 40, 9-21 (1985). Copyright 1985 by Academic Press, Inc. New York, NY.