

A Brief Survey of Difference Sets, Partial Difference Sets, and Relative Difference Sets

Abstract

This paper gives an introduction to difference sets (DSs), partial difference sets (PDSs), and relative difference sets (RDSs). Included is a discussion of methods for analyzing these sets with group rings and characters, as well as their relationships with designs and graphs. Finally, we make use of the character theory to give some interesting examples.

1 Introduction

Difference sets, partial difference sets, and relative difference sets are algebraic structures with combinatorial applications. The purpose of this paper is to give the reader definitions and basic examples of these sets, as well describe their connections to some other well-known combinatorial objects. We will conclude with some examples that illustrate how character theory can be used to prove that a set is a (partial) difference set. A fairly extensive list of references is included for further reading.

Definition 1 *Let G be a finite group of order v , and let D be a subset of G with cardinality k .*

1. *D is a (v, k, λ) -difference set (DS) if the list of differences $d_1 d_2^{-1}$, $d_1, d_2 \in D$, represents every nonidentity element in G exactly λ times.*
2. *D is a (v, k, λ, μ) -partial difference set (PDS) if the list of differences $d_1 d_2^{-1}$, $d_1, d_2 \in D$, represents every nonidentity element in D exactly λ times and every nonidentity element of $G - D$ exactly μ times.*
3. *If N is a normal subgroup of G with order n , and $v = mn$, then D is an (m, n, k, λ) -relative difference set (RDS) in G relative to N if the differences $d_1 d_2^{-1}$ for $d_1, d_2 \in D, d_1 \neq d_2$ represent each nonidentity element of $G \setminus N$ exactly λ times and each element of N zero times. For this reason, N is called the forbidden subgroup.*

A DS (PDS, RDS) is called *cyclic* or *abelian* when the group G is cyclic or abelian. For more extensive information on these sets there are excellent sources for each type of set. For difference sets, the survey of Jungnickel, [8], is a good reference. Ma has written an informative survey on partial difference sets [10], and finally the text by Pott, [13], gives detailed information on relative difference sets.

The following are some small examples of each of these types of difference sets. First let $G_1 = \mathbf{Z}_7$ and $D_1 = \{1, 2, 4\}$, so D_1 is the set of nonzero quadratic residues modulo 7. Then D_1 is a $(7, 3, 1)$ -DS. As another example, consider $G_2 = \mathbf{Z}_5$ and $D_2 = \{1, 4\}$, so D_2 is the set of nonzero quadratic residues modulo 5. Then D is a $(5, 2, 0, 1)$ -PDS because $1 - 4 = 2 \notin D$ and $4 - 1 = 3 \notin D$. In general, the set of

nonzero quadratic residues in $GF(p^r)$ is a DS in the additive group if $p^r \equiv 3 \pmod{4}$ and a PDS if $p^r \equiv 1 \pmod{4}$. Finally, let $G_3 = \mathbf{Z}_4$, with $N = \{0, 2\}$ and $D_3 = \{1, 2\}$. Then D_3 is a $(2, 2, 2, 1)$ -RDS in G_3 relative to N .

2 Relationships with Character Theory

We will see that difference sets are equivalent to certain symmetric designs, while partial difference sets have connections to strongly regular graphs. Because of these connections, and the resulting applications to error-correcting codes, difference sets are widely studied objects. We will consider some of these relationships in the following section.

In this section, we develop a theorem that relates partial difference sets to character sums. We also state two theorems, relating difference sets and relative difference sets to character sums. We will then use those theorems in Section 4.

Often DSs and PDSs are studied within the context of the group ring $\mathbf{Z}[G]$. For a subset D in G we can write $D = \sum_{d \in D} d$ and $D^{(-1)} = \sum_{d \in D} d^{-1}$. This is abuse of notation which is widely accepted; so that depending on the context D will represent the difference set D or the element $\sum_{d \in D} d$ in the group ring $\mathbf{Z}[G]$. If D is a PDS we have the following group ring equations as immediate consequences of the definition of PDSs. These equations will be useful when considering the relationship between PDSs and character theory:

$$\begin{aligned} DD^{(-1)} &= (k - \mu)1 + \mu G + (\lambda - \mu)D \text{ where } 1 \notin D \\ DD^{(-1)} &= (k - \lambda)1 + \mu G + (\lambda - \mu)D \text{ where } 1 \in D. \end{aligned}$$

The following propositions are useful when considering partial difference sets. These propositions do not apply to difference sets and relative difference sets. They can be found, for example, in the survey article of Ma as Theorem 2.2 and Proposition 3.1 [10]. We will spend a little more time with PDSs, but could alternatively have developed results on DSs and RDSs. Instead we will state the major results on these types of set without the details.

Proposition 1 *If D is a (v, k, λ, μ) -PDS in a group G with $\lambda \neq \mu$ then $D = D^{(-1)}$; in other words, $d \in D$ if and only if $d^{-1} \in D$.*

Proof: $d_1 d_2^{-1} = d$ if and only if $d_2 d_1^{-1} = d^{-1}$. Corresponding to the pair (d_1, d_2) in $D \times D$ with $d_1 d_2^{-1} = d$ there is the pair (d_2, d_1) with $d_2 d_1^{-1} = d^{-1}$. So there exist exactly λ pairs (d_1, d_2) in $D \times D$ so that $d_1 d_2^{-1} = d$ if and only if there exist exactly λ pairs (d_2, d_1) in $D \times D$ so that $d_2 d_1^{-1} = d^{-1}$. Since $\lambda \neq \mu$ it follows that $d \in D$ if and only if $d^{-1} \in D$.

□

Proposition 2 *If D is a (v, k, λ, μ) -PDS with $1 \in D$ then $D - \{1\}$ is a $(v, k - 1, \lambda - 2, \mu)$ -PDS.*

Proof: From the list of differences of D we remove the differences $1d^{-1}$ and $d1$ to obtain the list of differences of $D - \{1\}$. Thus each element in D appears exactly two fewer times in the list of differences of $D - \{1\}$, while the elements in $G - D$ appear the same number of times.

□

Now we are ready to consider the relationship between PDSs and character theory. Character theory is frequently used to simplify calculations with difference sets and partial difference sets in abelian groups. In [14] Turyn and separately Yamamoto [19] first used character theory to study abelian difference sets. A *character* on an abelian group G is a homomorphism from the group to the complex numbers with modulus 1 under multiplication. The set of all characters on a finite abelian group forms a group, G^* , under multiplication, the dual group of G , and $|G^*| = |G|$. The *principal character*, which is 1 on all the elements of G , is the identity for G^* ; any other character in G^* is called *nonprincipal*. One can naturally extend a character on G to a homomorphism of the group ring $\mathbf{Z}[G]$ as follows: if χ is a character on G , then for an element $A = \sum_{g \in G} a_g g$ let $\chi(A) = \sum a_g \chi(g)$ so that if S is a subset of G , then $\chi(S) = \sum_{s \in S} \chi(s)$.

We will need the following well-known lemmas:

Lemma 1 (1) For any group G and any nonprincipal character χ on G , $\chi(G) = 0$. For χ principal, $\chi(G) = |G|$. (2) Similarly, for every $g \in G$ with $g \neq 1$, $\sum_{\chi \in G^*} \chi(g) = 0$; $\sum_{\chi \in G^*} \chi(1) = |G|$.

Proof: (1)(found in van Lint[15]) Suppose χ is a nonprincipal character, so there exists an $h \in G$ with $\chi(h) \neq 1$. Then consider the following equation:

$$\chi(h)\chi(G) = \chi(h) \sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(hg) = \sum_{g \in G} \chi(g) = \chi(G).$$

Since $\chi(h) \neq 1$ it follows that $\chi(G) = 0$. If χ is principal, then $\chi(g) = 1$ for all $g \in G$, so clearly $\chi(G) = |G|$. The proof of (2) is analogous to (1).

□

Lemma 2 (Fourier Inversion Formula) Let G be a finite group with dual G^* . Then if $A = \sum_{g \in G} a_g g$, then

$$a_h = (1/|G|) \sum_{\chi \in G^*} \chi(A) \overline{\chi(h)}.$$

Note that $\overline{\chi(h)}$ is the usual complex conjugate.

Proof:

$$\begin{aligned} \sum_{\chi \in G^*} \chi(A) \overline{\chi(h)} &= \sum_{\chi \in G^*} \left(\sum_{g \in G} a_g \chi(g) \right) \overline{\chi(h)} = \sum_{g \in G} \sum_{\chi \in G^*} a_g \chi(gh^{-1}) = \\ &= \sum_{g \in G, g \neq h} 0 + a_h \sum_{\chi \in G^*} \chi(hh^{-1}) = a_h |G|. \end{aligned}$$

Dividing through by $|G|$ gives the result. □

At last we can consider the main theorems relating character theory to abelian partial difference sets, difference sets, and relative difference sets. A proof of the partial difference set result is included, and the proofs of the other results are very similar.

Theorem 1 *The subset D (with $1 \notin D$) of the abelian group G is a (v, k, λ, μ) -PDS with $\lambda \neq \mu$ iff $\chi(D) = \frac{\lambda - \mu \pm \sqrt{(\lambda - \mu)^2 + 4\gamma}}{2}$ for every nonprincipal character χ of G and $k^2 = k + \lambda k + \mu(v - k - 1)$. Recall that $\gamma = k - \mu$.*

Proof: Suppose D is a (v, k, λ, μ) -PDS in the group G . Consider the group ring equation above (we can assume $1 \notin D$ because of Proposition 2 above):

$$DD^{(-1)} = (k - \mu)1 + \mu G + (\lambda - \mu)D.$$

By Proposition 1, $D = D^{(-1)}$ for $\lambda \neq \mu$ so we replace the equation with:

$$DD = (k - \mu)1 + \mu G + (\lambda - \mu)D.$$

Then we have for χ a nonprincipal character on G

$$\begin{aligned} \chi(DD) &= (k - \mu)\chi(1) + \mu\chi(G) + \chi((\lambda - \mu)D) \\ &= (k - \mu) + (\lambda - \mu)\chi(D). \end{aligned}$$

Thus we have the expression:

$$(\chi(D))^2 = (k - \mu) + (\lambda - \mu)\chi(D).$$

Solving for $\chi(D)$ gives $\chi(D) = \frac{\lambda - \mu \pm \sqrt{(\lambda - \mu)^2 + 4\gamma}}{2}$. The condition that $k^2 = k + \lambda k + \mu(v - k - 1)$ follows from counting the nonidentity elements in $DD^{(-1)}$ in two ways: there are $k(k - 1)$ such elements clearly, but for D to be a PDS it must be that each element in D has λ representations in $DD^{(-1)}$ while each nonidentity element of $G - D$ has μ representations. Therefore $k(k - 1) = \lambda k + \mu(v - k - 1)$. The equation also follows from evaluating the principal character on the equation for DD .

Now suppose $\chi(D) = \frac{\lambda - \mu \pm \sqrt{(\lambda - \mu)^2 + 4\gamma}}{2}$ for every nonprincipal character χ on G and that $k^2 = k + \lambda(k) + \mu(v - k - 1)$ (χ_0 will denote the principal character). This implies that if χ is nonprincipal on G then $\chi(DD) = (\lambda - \mu)\chi(D) + (k - \mu)$. Now we apply the Fourier Inversion Formula on the set $DD = \sum_{g \in G} a_g g$, and have:

$$\begin{aligned} a_1 &= 1/v \sum_{\chi \in G^*} \chi(DD) \overline{\chi(1)} = 1/v \sum_{\chi \in G^*} \chi(DD) = 1/v \left[\sum_{\chi \neq \chi_0} (\lambda - \mu)\chi(D) + (k - \mu) \right] + k^2/v \\ &= \frac{(k - \mu)(v - 1) + k^2}{v} + \frac{\lambda - \mu}{v} \sum_{\chi \neq \chi_0} \chi(D) = \frac{(k - \mu)(v - 1) + k^2}{v} + \frac{\lambda - \mu}{v} \sum_{\chi \neq \chi_0} \sum_{d \in D} \chi(d) \\ &= \frac{(k - \mu)(v - 1) + k^2}{v} + \frac{\lambda - \mu}{v} \sum_{d \in D} \sum_{\chi \neq \chi_0} \chi(d) = \frac{(k - \mu)(v - 1) + k^2}{v} + \frac{\lambda - \mu}{v} (-k). \end{aligned}$$

Using the equation $k^2 = k + \lambda k + \mu(v - k - 1)$ to simplify gives $a_1 = k$. Now suppose that $d_0 \in D$, then:

$$\begin{aligned} a_{d_0} &= 1/v \sum_{\chi \in G^*} \chi(DD) \overline{\chi(d_0)} = 1/v \sum_{\chi \in G^*} \chi(DD) \chi(d_0^{-1}) \\ &= 1/v \sum_{\chi \neq \chi_0} [(\lambda - \mu)\chi(D)\chi(d_0^{-1}) + (k - \mu)\chi(d_0^{-1})] + k^2/v \\ &= 1/v [(\lambda - \mu) \sum_{\chi \neq \chi_0} \sum_{d \in D} \chi(d)\chi(d_0^{-1}) + (k - \mu) \sum_{\chi \neq \chi_0} \chi(d_0^{-1}) + k^2] \\ &= 1/v [(\lambda - \mu) \sum_{d \in D, d \neq d_0} \sum_{\chi \neq \chi_0} \chi(dd_0^{-1}) + (v - 1)(\lambda - \mu) + (\mu - k) + k^2] \\ &= 1/v [(\lambda - \mu)(-k + 1) + (v - 1)(\lambda - \mu) + (\mu - k) + k^2]. \end{aligned}$$

Using the equation $k^2 = k + \lambda k + \mu(v - k - 1)$ to simplify gives $a_{d_0} = \lambda$. A similar calculation gives $a_g = \mu$ for $g \in G - D$ and $g \neq 1$.

Hence we have that $DD = (k - \mu)1 + (\lambda - \mu)D + (\mu)G$ so D is a (v, k, λ, μ) -PDS in G .

□

Notice that the preceding result does not involve an absolute value. The result reveals that for D a partial difference set in an abelian group G with $\lambda \neq \mu$, the character sum, $\chi(D)$, must be a real number for all characters on G . The equivalent theorem for difference sets requires the modulus; this implies that the character sums for difference sets need not be real. For a more detailed description of the relationship between DSs and character theory see Turyn [14]. We conclude with Theorem 3, which is the analogous result for RDSs.

Theorem 2 *The k -element subset D of the abelian group G is a (v, k, λ) -DS iff $|\chi(D)| = \sqrt{n}$ for every nonprincipal character χ , where $n = k - \lambda$ is the order of the difference set.*

A (v, k, λ, μ) -partial difference set is isomorphic to a strongly regular Cayley graph with a regular automorphism group. To construct a Cayley graph, $X(G, S)$ (this notation comes from Dicks and Dunwoody [7]), from a subset S of a group G , let the vertices of the graph be the elements of the group. Two vertices g_1 and g_2 are connected by a directed edge if $g_2 = sg_1$ for $s \in S$. If the subset is a partial difference set, D , with $\lambda \neq \mu$ then we know from Proposition 1 that $d \in D$ implies $d^{-1} \in D$. Thus if $g_2 = dg_1$ then $g_1 = d^{-1}g_2$, so we can consider the Cayley graph, $X(G, D)$, associated with D to be undirected.

A (v, k, λ, μ) -strongly regular graph is a graph with v vertices so that each vertex is connected to k other vertices, and with the additional property that distinct vertices x and y share edges with either λ or μ common vertices as x and y are either adjacent or non-adjacent.

Lemma 3 *If D is a (v, k, λ, μ) -PDS with $\lambda \neq \mu$ in a group G then the associated Cayley graph, $X(G, D)$, is a (v, k, λ, μ) -strongly regular graph.*

Proof: Suppose D is a (v, k, λ, μ) -PDS in a group G . Clearly the graph $X(G, D)$ has v vertices (one for each element of G). Since there are k elements in D , from every vertex g there are k vertices dg which share an edge with g . Consider the number of vertices x which share an edge with the two distinct vertices g_1 and g_2 . Then $x = d_1g_1 = d_2g_2$ for $d_1, d_2 \in D$. The number of solutions x is the number of ordered pairs (d_1, d_2) that satisfy $d_1g_1 = d_2g_2$, or $g_1g_2^{-1} = d_2d_1^{-1}$. If $g_1g_2^{-1} \in D$ then there are λ solutions, while if $g_1g_2^{-1} \in G - D$ then there are μ solutions. But $g_1g_2^{-1} \in D$ implies g_1 and g_2 are adjacent, while $g_1g_2^{-1} \in G - D$ implies g_1 and g_2 are not adjacent. So $X(G, D)$ is a (v, k, λ, μ) -strongly regular graph. □

Informally we show that the other direction also holds. Suppose $X(G, D)$ is a (v, k, λ, μ) -strongly regular graph with a regular automorphism group. Then clearly $|G| = v$ and $|D| = k$ (assuming an edge implies both directions). Take a vertex x and consider an adjacent vertex xd . They share λ neighbors z with $z = xd_1 = xdd_2$, so there are λ solutions to the equation $d = d_1d_2^{-1}$. This holds for all $d \in D$. A similar argument holds for x and xg where $g \notin D$. So a strongly regular Cayley graph with a regular automorphism group yields a partial difference set also.

4 Some Interesting Examples

In Section 2, we saw that characters could be used to examine difference sets, partial difference sets, and relative difference sets. In this section we will informally see how this theory can be used.

Throughout this section let $G = \mathbf{Z}_3 \times \mathbf{Z}_3$. We can split G into 4 subgroups that intersect only at the identity. Namely, we have the subgroups $H_1 = \langle (0, 1) \rangle = \{(0, 0), (0, 1), (0, 2)\}$, $H_2 = \langle (1, 0) \rangle = \{(0, 0), (1, 0), (2, 0)\}$, $H_3 = \langle (1, 1) \rangle =$

$\{(0,0), (1,1), (2,2)\}$, and $H_4 = \langle (1,2) \rangle = \{(0,0), (2,1), (1,2)\}$. Lemma 1 gives us that for any of these subgroups H and for any character χ on G , $\chi(H) = 0$ or $\chi(H) = 3$. In fact, it is also true that if χ is nonprincipal on G , then of the 4 subgroups listed above there will be exactly one subgroup H' such that $\chi(H') = 3$ and for all others $\chi(H) = 0$.

Partial Difference Set Example

Let $D = \langle (0,1) \rangle \cup \langle (1,0) \rangle - \{(0,0)\} = \{(0,1), (0,2), (1,0), (2,0)\}$. We use Theorem 1 to see that this is a $(9,4,1,2)$ -PDS in G (for this small example you admittedly could just list all the differences and check the result by definition of PDS). It is easy to check that $k^2 = k + \lambda k + \mu(v - k - 1)$. Suppose that χ is some nonprincipal character on G . We want the character sums on D to be -2 or 1 . By the above discussion, we know that χ will be principal on exactly one of the 4 subgroups we listed, so we have one of 2 possibilities:

Case 1: χ is principal on neither of the subgroups involved in forming D , whence $\chi(\langle (0,1) \rangle) = \chi(\langle (1,0) \rangle) = 0$ so $\chi(D) = (\chi(\langle (0,1) \rangle) - \chi(0,0)) + (\chi(\langle (1,0) \rangle) - \chi(0,0)) = (0 - 1) + (0 - 1) = -2$.

Case 2: χ is principal on one of the two subgroups involved, suppose that it be $\langle (0,1) \rangle$ without loss of generality. We either have $\chi(0,1) + \chi(0,2) = 2$ while $\chi(1,0) + \chi(2,0) = -1$, so $\chi(D) = 1$. The same character sum results when χ is principal on $\langle (1,0) \rangle$.

This type of example has many generalizations, for example in [3, 5, 6, 11].

Difference Set Example

Let the overall group be $G' = \mathbf{Z}_4 \times G$. Then let $D = (0, G - H_1) \cup (1, H_2) \cup (2, H_3) \cup (3, H_4)$. We will show that D is a $(36,15,6)$ -DS in G' . Let χ be an arbitrary nonprincipal character on G' . We will show that $|\chi(D)| = 3$, thereby showing that D is a difference set by Theorem 2.

Case 1: If we have that χ is principal on G but not G' , then it must be that χ is nonprincipal on \mathbf{Z}_4 . So $\chi(D) = \chi(0, G - H_1) + \chi(1, H_2) + \chi(2, H_3) + \chi(3, H_4) = |G - H_1|\chi(0) + |H_2|\chi(1) + |H_3|\chi(2) + |H_4|\chi(3) = 6\chi(0) + 3\chi(1) + 3\chi(2) + 3\chi(3) = 3\chi(0) + 3\chi(\mathbf{Z}_4)$. But χ is nonprincipal on \mathbf{Z}_4 , so $\chi(\mathbf{Z}_4) = 0$ and we get $\chi(D) = 3\chi(0) = 3$.

Case 2: If χ is nonprincipal on G , then we know $\chi(H_{i'}) = 3$ for one i' and $\chi(H_i) = 0$ for all other i . If $i = 1$ we get $\chi(D) = -3\chi(0)$, while if $i \neq 1$ we get $\chi(D) = 3\chi(i)$.

For more involved examples of this type of difference set calculation, see [1, 4, 6, 16, 17, 18]. There are many others.

We will not consider any examples of relative difference set calculations, but they are fairly similar. If you want to see examples of relative difference sets with character theory, consult any of the following: [3, 6, 9, 12].

FOOTNOTES

If you are interested in learning more about difference sets, please feel free to contact the author.

Affiliation of Author: Department of Mathematics, Computer Science, and Statistics, Bloomsburg University of Pennsylvania, Bloomsburg, PA 17815
jpolhill@bloomu.edu

Funding was provided by the 2002-2003 Bloomsburg University Research and Disciplinary competition. This paper was last revised in October of 2007, but most was written following the PASSHEMA conference in 2003.

5 References

1. K.T. Arasu, J.A. Davis, J. Jedwab, and S.K. Sehgal. New constructions of Menon Difference Sets. *J. Comb. Th. (A)*, 64(2): 329-336, 1993.
2. E.F. Assmus and J.D. Key. *Designs and their Codes*. Cambridge: Cambridge University Press, 1992.
3. Y.Q. Chen, D.K. Ray-Chaudhuri, and Q. Xiang. Constructions of Partial Difference Sets and Relative Difference Sets Using Galois Rings II. *J. Comb. Th. (A)*, 76(2): 179-196, 1996.
4. Y.Q. Chen. On the existence of abelian Hadamard difference sets and a new family of difference sets. *Finite Fields and their Applications*, 3: 234-256, 1997.
5. J.A. Davis. Partial difference sets in p -groups. *Arch. Math.*, 63: 103-110, 1994.
6. J.A. Davis and J. Jedwab. A unifying construction for difference sets. *J. Comb. Th. (A)*, 80(1): 13-78, 1997.
7. W. Dicks and M.J. Dunwoody. *Groups Acting on Graphs*. Cambridge: Cambridge University Press, 1989.
8. D. Jungnickel. Difference Sets. *Contemporary Design Theory*, Wiley-Intersci. Ser. Discrete Math Optim., New York: Wiley, 1992. 241-324.
9. K. H. Leung and S.L. Ma. Constructions of partial difference sets and relative difference sets on p -groups. *Bull. London Math. Soc.*, 22: 533-539, 1990.
10. S.L. Ma. A survey of partial difference sets. *Designs, Codes and Cryptography*, 4: 221-261, 1994.
11. J. Polhill. Constructions of nested partial difference sets with Galois rings. *Designs, Codes and Cryptography*, 25: 299-309, 2002.
12. J. Polhill. A construction of layered relative difference sets with Galois rings. In preparation.
13. A. Pott, *Finite Geometry and Character Theory*, Springer-Verlag, Berlin (1995).
14. R.J. Turyn. Character sums and difference sets. *Pacific J. Math.*, 15: 319-346, 1965.

15. J.H. van Lint. *Introduction to Coding Theory*, 2nd edition. Berlin: Springer-Verlag, 1991.
16. R.M.Wilson and Q.Xiang. Constructions of Hadamard difference sets. *J. Comb. Th. (A)*, 77: 148-160, 1997.
17. M.-Y Xia. Some infinite classes of special Williamson matrices and difference sets. *J. Comb. Th. (A)*, 61: 230-242, 1992.
18. Q. Xiang and Y.Q. Chen. On Xia's construction of Hadamard difference sets. *Finite Fields and Their Applications*, 2: 87-95, 1996.
19. K. Yamamoto. Decomposition fields of difference sets. *Pacific J. Math.*, 13: 337-352, 1963.