Difference Sets Satisfying $v = 4n$

Mitchell Riley — 42313942

June 3, 2014

Combinatorial designs are well-studied objects with applications in fields as diverse as finite geometry, tournament scheduling and mathematical biology. A common way to construct combinatorial designs is to begin with a different object known as a difference set. A central question in this field is: for which sets of parameters does a difference set exist?

Difference sets satisfying the relation $v = 4n$ form the richest source of known examples of difference sets. They were first explored by Menon[6], who constructed an infinite family of such sets.

After defining difference sets, we follow Menon's proof of the composition theorem and prove the existence of certain families of difference sets. Finally, we use the theorems in the paper to construct a Hadamard matrix of order 16.

1 Definitions

First we recall some basic definitions and results.

Definition 1.1. Given a v-element finite set of points X, a (v, k, λ) balanced incomplete block design (BIBD) is a collection of k-element subsets of X such that, for any two elements $x, y \in X$, exactly λ blocks contain both x and y.

Definition 1.2. A symmetric BIBD, (SBIBD) is a block design with an equal number of points and blocks.

One way of constructing SBIBDs is to find a difference set with the same set of parameters.

Definition 1.3. A (v, k, λ)-*difference set* is a subset D of size k of a group G of order v such that every nonzero element of G can be expressed as a difference $d_1 d_2^{-1}$ exactly λ ways.

Definition 1.4. The *order* n of a difference set is defined to be $n = k - \lambda$.

Example 1.5. In the group $\mathbb{Z}_7$, the subset $D = \{1, 2, 4\}$ forms a $(7, 3, 1)$-difference set with order $n = 2$.

We can characterise difference sets in another way. The set of differences between elements of D hits every non-identity element λ times, and the identity element k times. Therefore, using multiset notation, a subset $D \subset G$ is a (v, k, λ)-difference set if and only if

$$DD^{-1} = (k - \lambda)e + \lambda G = ne + \lambda G,$$

where e is the identity element of G.

Given a (v, k, λ)-difference set D, we can construct a SBIBD(v, k, λ) as follows. Given an element $g \in G$, the *translate* gD is the set $\{gd : d \in D\}$. The set of all translates, called the *development* of D, is a SBIBD(v, k, λ).

Example 1.6. The development of $D = \{1, 2, 4\}$ is the SBIBD$(7, 3, 1)$ with subsets

$$\{1, 2, 4\}, \{2, 3, 5\}, \{3, 4, 6\}, \{4, 5, 0\}, \{5, 6, 1\}, \{6, 0, 2\}, \{0, 1, 3\}$$

Not any set of parameters (v, k, λ) supports the existence of a difference set.

Theorem 1.7. In any difference set D, $\lambda(v - 1) = k(k - 1)$.

Proof. There are $k(k-1)$ ordered pairs of elements of D, and the differences of these must equal each of the $v-1$ nonzero elements of G exactly λ times. □

Corollary 1.8. In any difference set, the following identities hold:

$$k^2 = n + \lambda v$$
$$k = n + \lambda$$

Given a (v, k, λ) difference set D, the set complement of D inside the group G, written $\overline{D}$ is also a difference set.

Theorem 1.9. The complement of a (v, k, λ)-difference set is a $(v, v-k, v-2k + \lambda)$-difference set.

Example 1.10. The complement of $D = \{1, 2, 4\}$ in $\mathbb{Z}_7$ is $\overline{D} = \{0, 3, 5, 6\}$, a $(7, 4, 2)$-difference set.

Note that a difference set and its complement have the same order $n = (v - k) - (v - 2k + \lambda) = k - \lambda$.

2 Results

We now consider difference sets where the relation $v = 4n$ holds, as studied by Menon. Imposing this condition has some immediate consequences.

Firstly, v is even. By the famous Bruck-Ryser-Chowla theorem[1], n must be a perfect square, say

$$n = l^2.$$

After combining this with Corollary 1.8 and performing some simple algebraic manipulations, we find there are only two classes of parameters for such a difference set.

$$\begin{array}{llll} v = 4l^2, & k = l(2l-1), & \lambda = l(l-1), & n = l^2 \\ v = 4l^2, & k = l(2l+1), & \lambda = l(l+1), & n = l^2 \end{array}$$

Menon notes that if a difference set of one class exists for a particular value of l, the complement is a difference set belonging to the other class. Also, changing the sign of l reduces either class to the other, giving the following theorem.

Theorem 2.1. The parameters of a difference set satisfying $v = 4n$ are of the form

$$v = 4l^2, \qquad k = l(2l-1), \qquad \lambda = l(l-1), \qquad n = l^2$$

for some nonzero integer. Two complementary difference sets of this type have parameters that differ only by a change in the sign of l.

The following central theorem of the paper allows us to combine difference sets of this type in a natural way.

Theorem 2.2. Let S_1, S_2 be two difference sets in the groups G_1, G_2, and let $\overline{S_1}, \overline{S_2}$ be their complements. Let $G = (G_1, G_2)$ be the direct product of G_1, G_2, and S the subset of G given by the union of the subsets (S_1, S_2) and $(\overline{S_1}, \overline{S_2})$.

Then S is a difference set if and only if the parameters of both S_1 and S_2 satisfy $v = 4n$. Moreover, if S is a difference set its parameters also satisfy $v = 4n$.

Proof. For $i = 1, 2$, let S_i, $\overline{S_i}$ have the parameters

$$v_i, k_i, \lambda_i, n_i; \qquad \overline{v_i}, \overline{k_i}, \overline{\lambda_i}, \overline{n_i}$$

respectively. We have the following relations.

$$\overline{v_i} = v_i, \qquad \overline{n_i} = n_i, \qquad \lambda_i + \overline{\lambda_i} = \lambda_i + (v_i - 2k_i + \lambda_i) = v_i - 2n_i$$

Because $S_i, \overline{S_i}$ are difference sets, we know

$$\begin{aligned} S_iS_i^{-1} &= n_ie_i + \lambda_iG_i \\ \overline{S_iS_i}^{-1} &= n_ie_i + \overline{\lambda_i}G_i, \end{aligned}$$

where e_i is the identity element of G_i.

Because G_i is a group, $S_iG_i = S_iS_i^{-1} + S_i\overline{S_i}^{-1} = k_iG_i$. We therefore have

$$\begin{aligned} S_i\overline{S_i}^{-1} = \overline{S_i}S_i^{-1} &= k_iG_i - (n_ie_i + \lambda_iG_i) \\ &= n_i(G_i - e_i) \end{aligned}$$

We can now combine there results to calculate SS^{-1}.

$$\begin{aligned} SS^{-1} &= (S_1S_1^{-1}, S_2S_2^{-1}) + (\overline{S_1S_1}^{-1}, \overline{S_2S_2}^{-1}) \\ &\quad + (S_1\overline{S_1}^{-1}, S_2\overline{S_2}^{-1}) + (\overline{S_1}S_1^{-1}, \overline{S_2}S_2^{-1}) \\ &= (n_1e_1 + \lambda_1G_1, n_2e_2 + \lambda_2G_2) + (n_1e_1 + \overline{\lambda_1}G_1, n_2e_2 + \overline{\lambda_2}G_2) \\ &\quad + 2(n_1G_1 - n_1e_1, n_2G_2 - n_2e_2) \\ &= 4n_1n_2(e_1, e_2) + n_1(\lambda_2 + \overline{\lambda_2} - 2n_2)(e_1, G_2) \\ &\quad + n_2(\lambda_1 + \overline{\lambda_1} - 2n_1)(G_1, e_2) + (\lambda_1\lambda_2 + \overline{\lambda_1}\overline{\lambda_2} + 2n_1n_2)(G_1, G_2) \end{aligned}$$

This satisfies the conditions for a difference set if and only if, for $i = 1, 2$,

$$\lambda_i + \overline{\lambda_i} = 2n_i$$

or, using the identity above,

$$v_i = 4n_i.$$

Say the above holds, and let v, k, λ, n be the parameters of S. As G is the direct product of G_1, G_2, $v = v_1v_2 = 16n_1n_2$. From above $n = 4n_1n_2$ so indeed $v = 4n$. □

We can immediately use this theorem to construct infinite families of difference sets.

Theorem 2.3. If there exists a difference set corresponding to l_0, there exists a difference set with parameter $l = 2^{r-1}l_0^r$ for $r \geq 0$.

Proof. Take both S_1 and S_2 in the previous theorem to be this difference set. Then we get a new difference set with parameter $v = v_0^2$, corresponding to $l = 2l_0^2$. Inductively combine this new difference set with the original, giving $v = v_0^r$ for all r, corresponding to $l = 2^{r-1}l_0^r$ for $r \geq 0$. □

We kickstart the process using the following base case.

Theorem 2.4. There exist difference sets with parameters corresponding to $l = 2^r$ for any $r \geq 0$.

Proof. Let C_4 be the cyclic group of order 4, and S a subset containing exactly one element. Then S is a $(4, 1, 0)$-difference set corresponding to $l = 1$. The result follows from the previous theorem. □

Menon also gives the following difference set corresponding to the case $l = 3$. Let G be the direct product of two copies of C_6, the cyclic group of order 6. The following subset forms a $(36, 15, 6)$-difference set, corresponding to $l = 3$.

$$\begin{gathered}(0,0),(2,4),(4,2)\\(0,1),(0,3),(0,5)\\(1,0),(3,0),(5,0)\\(1,3),(3,5),(5,1)\\(3,1),(5,3),(1,5)\end{gathered}$$

It follows from the previous theorems that

Theorem 2.5. There exist difference sets corresponding to all values of l of the form 2^s3^r, $s \geq r - 1 \geq 0$.

3 Applications

Menon difference sets are closely related to Hadamard matrices[2].

Definition 3.1. A *Hadamard matrix*, H, of order n is a square $n \times n$ matrix with entries either 1 or -1, such that $HH^t = nI$, i.e., the rows are pairwise orthogonal.

A Hadamard matrix is *regular* if the row and column sums are constant.

Example 3.2. The following matrices are Hadamard matrices with orders $n = 2, 4, 8$, where an entry $-$ represents -1. The second is regular.

$$\begin{pmatrix}1 & 1\\1 & -\end{pmatrix} \qquad \begin{pmatrix}- & 1 & 1 & 1\\1 & - & 1 & 1\\1 & 1 & - & 1\\1 & 1 & 1 & -\end{pmatrix}$$

The connection between Menon designs and Hadamard matrices is given in the following theorem.

Theorem 3.3. A Menon design SBIBD$(4u^2, 2u^2 - u, u^2 - u)$ exists if and only if there exists a regular Hadamard matrix of order $4u^2$.

Proof. The proof proceeds by construction. Given a regular Hadamard matrix of order $4u^2$, replace all '-1' entries with '0' and consider the resulting matrix as the incidence matrix of a block design. Such a block design has parameters either $(4u^2, 2u^2 - u, u^2 - u)$ or $(4u^2, 2u^2 + u, u^2 + u)$. If the latter occurs, complement the design.

The process can be reversed to recover a regular Hadamard matrix from a Menon design. □

Example 3.4. Let us construct a regular Hadamard matrix of order $4 \cdot 2^2 = 16$. First we need a difference set corresponding to $l = 2$. We do this by applying the construction given in the previous section to the difference set $S_1 = S_2 = \{0\}$ in $C_4 = \{0, 1, 2, 3\}$.

$$\begin{aligned} S &= (S_1, S_2) + (\overline{S_1}, \overline{S_2}) \\ &= \{(0,0), (1,1), (1,2), (1,3), (2,1), (2,2), (2,3), (3,1), (3,2), (3,3)\} \end{aligned}$$

S is a $(16, 10, 6)$-difference set. To simplify calculations, we consider its complement, a $(16, 6, 2)$-difference set:

$$\overline{S} = \{(0,1), (0,2), (0,3), (1,0), (2,0), (3,0)\}$$

We now calculate the corresponding SBIBD$(16, 6, 2)$, given by the development of $\overline{S}$.

$$\begin{gathered}
\{(0,1),(0,2),(0,3),(1,0),(2,0),(3,0)\}, \\
\{(1,1),(1,2),(1,3),(2,0),(3,0),(0,0)\}, \\
\{(2,1),(2,2),(2,3),(3,0),(0,0),(1,0)\}, \\
\{(3,1),(3,2),(3,3),(0,0),(1,0),(2,0)\}, \\
\{(0,2),(0,3),(0,0),(1,1),(2,1),(3,1)\}, \\
\{(1,2),(1,3),(1,0),(2,1),(3,1),(0,1)\}, \\
\{(2,2),(2,3),(2,0),(3,1),(0,1),(1,1)\}, \\
\{(3,2),(3,3),(3,0),(0,1),(1,1),(2,1)\}, \\
\{(0,3),(0,0),(0,1),(1,2),(2,2),(3,2)\}, \\
\{(1,3),(1,0),(1,1),(2,2),(3,2),(0,2)\}, \\
\{(2,3),(2,0),(2,1),(3,2),(0,2),(1,2)\}, \\
\{(3,3),(3,0),(3,1),(0,2),(1,2),(2,2)\}, \\
\{(0,0),(0,1),(0,2),(1,3),(2,3),(3,3)\}, \\
\{(1,0),(1,1),(1,2),(2,3),(3,3),(0,3)\}, \\
\{(2,0),(2,1),(2,2),(3,3),(0,3),(1,3)\}, \\
\{(3,0),(3,1),(3,2),(0,3),(1,3),(2,3)\},
\end{gathered}$$

Finally, we calculate the incidence matrix of this block design and replace '0' with '-1' to get our Hadamard matrix of order 16:

$$\begin{pmatrix}
- & 1 & 1 & 1 & 1 & - & - & - & 1 & - & - & - & 1 & - & - & - \\
1 & - & - & - & - & 1 & 1 & 1 & 1 & - & - & - & 1 & - & - & - \\
1 & - & - & - & 1 & - & - & - & - & 1 & 1 & 1 & 1 & - & - & - \\
1 & - & - & - & 1 & - & - & - & 1 & - & - & - & - & 1 & 1 & 1 \\
1 & - & 1 & 1 & - & 1 & - & - & - & 1 & - & - & - & 1 & - & - \\
- & 1 & - & - & 1 & - & 1 & 1 & - & 1 & - & - & - & 1 & - & - \\
- & 1 & - & - & - & 1 & - & - & 1 & - & 1 & 1 & - & 1 & - & - \\
- & 1 & - & - & - & 1 & - & - & - & 1 & - & - & 1 & - & 1 & 1 \\
1 & 1 & - & 1 & - & - & 1 & - & - & - & 1 & - & - & - & 1 & - \\
- & - & 1 & - & 1 & 1 & - & 1 & - & - & 1 & - & - & - & 1 & - \\
- & - & 1 & - & - & - & 1 & - & 1 & 1 & - & 1 & - & - & 1 & - \\
- & - & 1 & - & - & - & 1 & - & - & - & 1 & - & 1 & 1 & - & 1 \\
1 & 1 & 1 & - & - & - & - & 1 & - & - & - & 1 & - & - & - & 1 \\
- & - & - & 1 & 1 & 1 & 1 & - & - & - & - & 1 & - & - & - & 1 \\
- & - & - & 1 & - & - & - & 1 & 1 & 1 & 1 & - & - & - & - & 1 \\
- & - & - & 1 & - & - & - & 1 & - & - & - & 1 & 1 & 1 & 1 & -
\end{pmatrix}$$

Hadamard matrices can be used to create error correcting codes. “Olivia MFSK” is a digital amateur radio protocol that uses a Hadamard matrix of order 64 to encode characters before transmission.

These matrices also find use in statistics and experimental design, where the orthogonality of the columns is used to isolate the effects of different factors.

References

[1] Richard H Bruck and Herbert J Ryser. “The nonexistence of certain finite projective planes”. In: *Canad. J. Math* 1.191 (1949), p. 9.

[2] Charles J Colbourn. *CRC handbook of combinatorial designs.* CRC press, 1996.

[3] James A Davis and Jonathan Jedwab. “A survey of Hadamard difference sets”. In: (1996).

[4] Marshall Hall. “A survey of difference sets”. In: *Proceedings of the American Mathematical Society* 7.6 (1956), pp. 975–986.

[5] P. Kesava Menon. “Difference Sets in Abelian Groups”. In: *Proceedings of the American Mathematical Society* 11.3 (1960), pp. 368–376.

[6] P Kesava Menon. “On difference sets whose parameters satisfy a certain relation”. In: *Proceedings of the American Mathematical Society* 13.5 (1962), pp. 739–745.