Ceylon Journal of Science: Physical Sciences, 15, 17-25 (2009)

EQUIVALENCE OF SQUARE DESIGNS, DIFFERENCE SETS AND COMPLETE GRAPHS

A.A.I. PERERA
Department of Mathematics, University of Peradeniya, Peradeniya.

ABSTRACT

Difference sets can be constructed by different techniques. In this work, we construct difference sets using *quadratic residues* and *orbits*.
The equivalence between $(v,k,\lambda)-$ difference sets in a group G and a symmetric (square) $(v,k,\lambda)-$ design with a regular automorphism group G is well known. We prove the equivalence of graphs, square designs and difference sets using complete graphs and the equivalence is illustrated by an example. Generalization of this result for a regular graph is also given.

1. INTRODUCTION

A combinatorial design is a way of choosing, from a given finite set, a collection of subsets with particular properties. The study of designs were begun by Euler in 1782. Later were by Woolhouse (1844), Kirkman (1847) and Steiner (1853).

The first result on the theory of block designs was due to Fisher in 1926. Later, Yates (1936), Chowla and Riser (1950), Mann(1969) and modern contribution by Shrikhande, Seberry[1], Yamada[1], Jungnicke[2], Beth[3] and Pott[4]. Th Beth, D. Jungnickel and H. Lenz[3] have mentioned that a complete graph can be partitioned in to subgraphs. This was based on my research and proved the Theorem 3.1.

Let G be a group of order v written multiplicatively. A (v,k,λ)-difference set in G is a k-element subset D so that the multi-set $\{d_1d_2^{-1}: d_1,d_2 \in D,\ d_1 \neq d_2\}$ contains each non-identity element of G exactly λ times. The integer $n = k-\lambda$ is the order of D.
If G is an additive group, then instead of a multi-set we consider the set $\{d_1 - d_2:\ d_1,d_2 \in D, d_1 \neq d_2\}$

Note that any group has four types of trivial difference sets, namely, the empty set, G itself, any singleton subset of G, and its complement. In general, difference sets occur in set-complementary pairs. Indeed, if D is a (v,k,λ)-difference set in G, then $D' = G - D$ is a $(v, v-k, v-2k+\lambda)$- difference set in G. Thus to simplify classification and to eliminate the trivial types from consideration, we choose $1 < k < v/2$ [4,5]

A difference set is called abelian, non-abelian or cyclic according as the underlying group is abelian, non-abelian or cyclic respectively.

The study of difference sets is closely connected with coding theory because the code over a field F of the symmetric design corresponding to a (v,k,λ) difference set may be considered as the right ideal generated by D in the group algebra $F[G]$.

Abelian difference sets arise naturally in the solution of many problems of signal design in digital communication, including synchronization, radar, coded aperture imaging and optical image alignment.

Part of this work is the construction of difference sets using quadratic residues and orbits (or numerical multipliers). In the latter part, we use graph theory, specially complete graphs and regular graphs, to obtain equivalence between graphs, designs and difference sets. This equivalence can be illustrated graphically and it helps to construct codes, that may be used in digital communication.

2. METHODOLOGY

2.1 Graphs

A simple graph G is a pair $(V(G),E(G))$, where $V(G)$ is a finite nonempty set of elements called *vertices* and $E(G)$ is a finite set of unordered pairs of distinct elements of $V(G)$ called *edges.* [6]

The number of vertices of G is called the *order* of G, and denote by v. Two vertices that are incident with a common edge are said to be adjacent. [6] A set of vertices in which every distinct pair is adjacent is called a *clique.* A $k-$clique (called a complete graph of k vertices) is a clique with k vertices.

There are two types of graphs that are of particular importance in our work. They are the complete graphs and the regular graphs. A complete graph K_n is a simple graph in which each pair of distinct vertices is joined by an edge and a regular graph is a graph in which every vertex has the same degree. It can be easily seen that every complete graph is regular, but the converse is not true, in general [3,7,8]

2.2 Block Designs

A *block design* is a family of b subsets of a set S of v elements such that, for some fixed k and λ, with $k < v, \lambda > 0$,

(i). each subset has k elements,

(ii).each pair of elements of S occur together in exactly λ subsets.

The elements of S are called the *varieties*, and the subsets of S are called the *blocks.* [9]

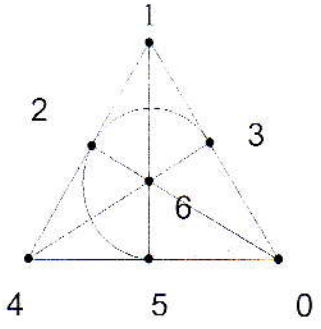
Example 1

Take $S = \{0,1,2,3,4,5,6\}$, and consider the following seven subsets of S:

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

Here $b = 7, \quad v = 7, \quad k = 3, \quad \lambda = 1$

A simple geometrical representation of this design is as follows. The elements $0, 1, 2, \cdots, 6$ are represented by points, and the blocks are represented by lines.



There is another useful way of representing the design given in the example. The string of seven bits of 0s and 1s can be used to represent the first set {0,1,3} as

1 1 0 1 0 0 0

Similarly, writing all the block corresponding to the sets, we can obtain the following (0,1)-matrix which is the *incidence matrix* of the design.

$$\begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

The advantage of using an incidence matrix to describe a block design instead of listing the sets element by element is that the structure of the design could be seen more clearly without any irrelevant information.

Theorem 1

In a block design each element lies in exactly r blocks, where

$$r(k-1) = \lambda(v-1) \quad \text{and} \quad bk = vr$$

Proof: - Given in [9]

When $b = v$, the incidence matrix is a square matrix, and such a design is called a *square* or *symmetric design*.

Example 2

A *finite projective plane of order n* is defined to be a (v,k,λ) - configuration in which $v = n^2 + n + 1$, $k = n + 1$ and $\lambda = 1$, for some positive integer $n \geq 2$. The seven – point plane corresponds to $n = 2$. (Example 1)

2.3. Difference sets

There are several types of difference sets such as *Planar, Hadamard, Singer, Menon-Hadamard, McFarland, Spence*, etc. In this section we discuss constructions of specific families of difference sets by using quadratic residues and numerical multiplier (orbits)[5,8]

Definition 1

The development of a difference set D is the incidence structure $devD$ whose points are the elements of G and whose blocks are the *translates* $D + g = \{d + g : d \in D\}$.[8]

$$devD = \{D + g : g \in G\}$$

Definition 2

Let D be a difference set in G. A *multiplier* for G is an automorphism α of G such that $D^{\alpha} = D + g$ for some $g \in G$. If α is the automorphism which maps h to $t.h$, then t is called a *numerical* multiplier.[5]

Definition 3

$a \in Z$ is said to be a *quadratic residue* modulo n if $(a,n) = 1$ and $x^2 \equiv a (\mathrm{mod}\, n)$ has a solution. If not it is said to be *quadratic non-residue modulo n.*

Example 3

Construction of (19,9,4) – difference set using quadratic residues.

Consider $x^2 \equiv a \,(\mathrm{mod}\, 19)$ ---------- (1)

Since (1) has solutions when $a = 1, 4, 5, 6, 7, 9, 11, 16, 17$, The set of residues modulo 19 is $\{1, 4, 5, 6, 7, 9, 11, 16, 17\}$. Further, difference of these elements modulo 19 gives each non zero element of Z_{19} exactly 4 times.

$\therefore$ {1,4,5,6,7,9,11,16,17} is a (19, 9,4)- difference set.

Example 4

Construction of (21,5,1)- difference set using multipliers.

Here $n = k - \lambda = 5 - 1 = 4$, and 2 is a multiplier

We may assume that D consists of orbits under $M = \{1, 2, 4, 8, 16, 11\}$. Since $k = 5$, the only candidates are the "small" orbits, namely, {0}, {7, 14}, {3, 6, 12} and {9, 18, 15}. Thus, D has to be the union of {7, 14} with one of the 3-element orbits.

In fact, both possible choices D_1 and D_2 work.

i.e. $D_1 = \{3, 6, 7, 12, 14\}$ and $D_2 = \{7, 9, 14, 15, 18\}$ are (21,5,1)- difference sets.

3. RESULTS

The equivalence of square designs, difference sets and graphs are given by Theorem 3.1. Complete graphs of order v, where $v = n^2 + n + 1$; $n \geq 2$ have been used, and illustrate this result by using an example. Moreover, the generalisation of this result is given by Theorem 3.2.

Theorem 3.1

Let G be a finite cyclic group of order v, where $v = n^2 + n + 1$; $n \geq 2$ and let D be a subset of G with $(n+1)$ elements. Then the following are equivalent:

(i). There is a complete graph of order $(n^2 + n + 1)$.

(ii). There is a $(n^2 + n + 1, n + 1, 1)$ – square design such that G acts regularly as an automorphism group

(iii). D is a difference set with parameters $(n^2 + n + 1, n + 1, 1)$ in G.

Proof :

(i) $\Rightarrow$ (ii)

There is a complete graph of order $(n^2 + n + 1)$.

It is known that K_{n^2+n+1} has $\frac{(n^2 + n + 1)(n^2 + n)}{2}$ edges, $(n^2 + n + 1)$ vertices, and any pair of distinct vertices are joined by an edge.

Let us partition K_{n^2+n+1} into $(n^2 + n + 1)$ subgraphs, each is having $\frac{n(n+1)}{2}$ edges.

Since the degree of each vertex of K_{n^2+n+1} is $n(n+1)$, without loss of generality one can consider that each vertex of K_{n^2+n+1} is in $(n+1)$ subgraphs and each subgraph contributes n to the degree of each vertex of K_{n^2+n+1}.

If each subgraph has v_0 vertices, then

$$\frac{nv_0}{2} = \frac{n(n+1)}{2} \Rightarrow v_0 = n + 1.$$

That is, each subgraph has $n+1$ vertices and is regular of degree n.

$\therefore$ each subgraph is a complete graph with $n+1$ vertices or a $(n+1)$ – clique.

Hence K_{n^2+n+1} can be decomposed into $(n^2 + n + 1)$ such cliques.

Claim: Each edge is in exactly one clique.

Suppose that there exists an edge $x_i x_j$ which is common to both cliques Q_1 and Q_2 where x_i and x_j are two distinct vertices in both Q_1 and Q_2.

$\because x_i \in Q_1$ and $x_j \in Q_2$ which are complete graph of $n+1$ vertices, and each of Q_1 and Q_2 contributes n to the degree of x_i. But $x_i x_j$ is an edge common both Q_1 and Q_2.

$\therefore$ degree of x_i due to Q_1 and Q_2 is $2n - 1$.

$\because$ vertex x_i is in the other $n-1$ cliques, total contribution to the degree of x_i is,

$$n(n-1)+(2n-1)=n^2+n-1\ ,$$

which is a contradiction, since the degree of each vertex is n^2+n. Hence, each edge is in exactly one clique.

If we denote each vertex of a clique by 1 and other vertices of the graph by 0, we can obtain a block of 0's and 1's. By doing this for all the cliques, one can obtain all the blocks, which gives a $(n^2+n+1)\times(n^2+n+1)$ square matrix with the following properties:

(i) Each block has $(n+1)$ points

(ii) Each pair of elements of G occurs together in exactly one block.

If we take one block and shift it by one place we can get next block of the design. Therefore this is the incidence structure of $(n^2+n+1, n+1, 1)$ - square design such that G acts regularly as an automorphism group.

(ii) $\Rightarrow$ (iii)

Suppose there is a square $(v,k,\lambda)-$ design with a regular automorphism group G. One may then select a "base point" p_0 and identify the point set of the design with the group G as follows: If g is the unique element of G mapping p_0 to p, then we identify p with g; in particular, p_0 is identified with $0 \in G$. (We write G additively for the time being, even if G is non-abelian.) Now, choose a "base block" B_0, and let D be the corresponding k-set of elements of G (so all blocks now take the form $D+h$ for some $h \in G$). Then D is a (v,k,λ) -difference set in G. To see this, one just notes that the two distinct points g and 0 are on a block $D+x$ if and only if one has the equations $g=d+x$ and $0=d'+x$ for some $d,d' \in D$. But these equations are equivalent to $g=d-d'$ and $g=d+x$, and the fact that g and 0 are on exactly λ common blocks now given us exactly λ different representatives $g=d-d'$ for g.

(iii) $\Rightarrow$ (i)

Suppose D is a difference set with parameters $(n^2+n+1, n+1, 1)$. Then $dev\ D=\{D+g; g \in G\}$ gives the collection of difference sets of G. Let us construct a graph of (n^2+n+1) vertices in the following way. Label all the vertices of the graph by $1,2,\ldots,n^2+n+1$. Take the difference set D and join each possible distinct pair of elements by an edge. This corresponds to a complete graph of $n+1$ vertices (or $n+1-$clique). Now construct $n+1-$cliques for each difference set $D+g; g \in G$. Then, the resulting graph is the complete graph of n^2+n+1 vertices.

Example to illustrate the theorem

Consider the complete graph (K_{13}) of 13 vertices. $13=3^2+3+1$, gives $n=3$. Labeling vertices from $0, 1, 2, \cdots, 12$ which are the elements of $(Z_{13}, +)$, and decompose the graph into 13 cliques with 4 vertices each and each pair of distinct vertices are joined by an edge.

Let {0, 1, 3, 9} be a vertex set of such a clique. Adding 1 to each entry can construct all the cliques and can color with 13 different colors.

$$\begin{bmatrix}
1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\
1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\
1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1
\end{bmatrix}$$

Finally, it can be seen that each block corresponds to a $(13, 4, 1)$ – difference set.
This result can be generalized for $\lambda > 1$. Then, instead of looking at a complete graph K_v, we look at a $\lambda(v-1)$ regular multi-graph of order v, when each distinct pair of vertices are joined by λ edges.

Theorem 3.2

Let G be a finite cyclic group of order v and let D be a subset of G with k elements. Then the following statements are equivalent:

(i) There is a $\lambda(v-1)$-regular graph of order v (λ is the number of edges joined by any distinct pair of vertices).

(ii) There is a (v, k, λ)-square design such that G acts regularly as an automorphism group.

(iii) D is a difference set with parameters (v, k, λ) in G.

Difference sets constructed by using quadratic residues and multipliers.

n	v	k	λ	Difference Set	Comment
2	7	3	1	{1, 2, 4}	Singer / Planar / Hadamard
3	13	4	1	{0, 1, 3, 9}; {0, 2, 5, 6}; {0, 4, 10, 12}	Singer / Planar
3	11	5	2	{1, 3, 4, 5, 9}; {2, 6, 7, 8, 10}	Hadamard
4	15	7	3	{0, 1, 2, 4, 5, 8, 10}; {0, 5, 7, 10, 11, 13, 14}	Singer / Hadamard
4	21	5	1	{3, 6, 7, 12, 14}; {7, 9, 14, 15, 18}	Planar
5	19	9	4	{1, 4, 5, 6, 7, 9, 11, 16, 17} {2, 3, 8, 10, 12, 13, 14, 15, 18}	Hadamard
5	31	6	1	{1, 5, 11, 24, 25, 27}; {2, 3, 10, 13, 15, 19} {8, 9, 12, 14, 21, 29}; {4, 6, 7, 20, 26, 30}	Singer / Planar
6	23	11	5	{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18} {5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22}	Hadamard
7	57	8	1	{1, 6, 7, 9, 19, 38, 42, 49}	Singer / Planar
8	31	15	7	{1, 2, 4, 5, 7, 8, 9, 10, 14, 16, 18, 19, 20, 25, 28} {1, 2, 3, 4, 6, 8, 12, 15, 16, 17, 23, 24, 27, 29, 30}	Singer / Hadamard
8	73	9	1	{3, 6, 12, 19, 23, 24, 38, 46, 48} {1, 2, 4, 8, 16, 32, 37, 55, 64}	Singer / Planar
9	35	17	8	{0, 1, 3, 4, 7, 9, 11, 12, 13, 14, 16, 17, 21, 27, 28, 29, 33}	Hadamard
	91	10	1	{0, 1, 3, 9, 27, 49, 56, 61, 77, 81}	Planar

4. CONCLUSION

Theorem on equivalence of Graphs, Designs and Difference sets have been proved considering complete graphs, and illustrated by an example. Further this theorem has been generalized for a regular graph and is given as Theorem 3.2.

A Difference set of higher order has been constructed using *Quadratic Residues and Multipliers*. For some values of the parameters, this design corresponds to a Hadamard design and the corresponding Hadamard matrix can be obtained.

REFERENCES

1. Seberry J. and Yamada M., Hadamard, Matrices, Sequences, and Block designs, *Contemporary Design Theory*, A collection of Surveys, Wiley, New York (1992.
2. Jungnickel D., *Canad. J. of Maths.*, 32, 257 (1982).
3. Beth T., Jungnickel D. and Lenz H., *Design Theory*, Cambridge University Press, Cambridge, (1993).
4. Jungnickel D. and Pott A., *Difference sets: Abelian*, The CRC Handbook of Combinatorial Designs, eds. C.J. Colbourn and J.H. Dinitz, The Chemical Rubber Company, Cleveland (1996).
5. Davis J.A. and Jedwab J., *A survey of Hadamard difference sets*, Group Difference Sets and the Monster, Walter de Gruyter, Berlin, (1996).
6. Wilson R.J., Introduction to Graph Theory, Longman, New York (1972).
7. Dinitz J.H. and Stinson D.R., Contemporary Design Theory: A collection of Surveys, John Wiley & Sons, Inc., New York (1992).
8 Iiams J.E., *Journal of Combinatorial Theory*, Series A 72, 256(1995).
9. Anderson I., A First course in Combinatorial Mathematics, Clarendon Press, Oxford, (1974).