

Authors' Notes, April 16, 2007.

This section introduces algebraic combinatorics with the study of difference sets as a motivation.

It contains Lemmas 1, 2 and Theorems 1, 2.

Expand the references.

A monograph might have additional exercises and examples. I have added a brief section on Cayley graphs. (April 2007.)

The sections are

1. Fundamental example
2. Difference sets
3. The fundamental motivation for using group theory
4. Cayley graphs

1 Motivation for group theory in combinatorics

Combinatorial designs and other combinatorial structures have many applications in today's technological and information-theoretic society. Useful combinatorial objects often have a large collection of symmetries, a finite group of symmetries. Group theory is then important in the study of combinatorial objects.

Given a finite group G , the integral group ring $\mathbb{Z}[G]$ is a natural place in which to do combinatorial computations ("counting") about the group G . To better analyze a group G of symmetries, we use the representation theory (character theory) of the group G . The representation theory of a finite group G is naturally related to idempotents in the group ring $\mathbb{Z}[G]$. These idempotents provide a basic theory for the understanding of (and computations with) the elements of the integral group ring.

In this paper we develop the basic theory necessary for applying group ring idempotents to combinatorial configurations. At the end, a series of examples will demonstrate the power of this "idempotent" approach to combinatorics.

Difference sets and symmetric designs provide the most obvious examples so we focus on these combinatorial objects. But other combinatorial objects: strongly regular graphs/partial difference sets, group divisible designs/relative difference sets, distance regular graphs, perfect ternary arrays/group-invariant weighing matrices, association schemes, finite geometries – all these families of configurations provide useful examples.

Major references are: Lander, Hall, Cameron & van Lint,...

1.1 A Fundamental Example

Combinatorics is the study of arrangements of finite objects. A fundamental example of a combinatorial structure is the Fano plane. We first view the Fano plane as a combinatorial design or a finite projective plane. Take seven objects, say the members of the set $\{0, 1, 2, 3, 4, 5, 6\}$. We require that they be collected into seven sets, each of size three, so that each pair of elements occurs exactly once in each set. One may construct this object, exhaustively, by hand. However, the simplest construction is to take the set $B_0 = \{1, 2, 4\}$ as a starter set and then consider the sets $B_i := \{1 + i, 2 + i, 4 + i\}$ where addition is done modulo seven. Thus the seven sets are

$$B_0 = \{1, 2, 4\},$$

$$B_1 = \{2, 3, 5\},$$

$$B_2 = \{3, 4, 6\},$$

$$B_3 = \{4, 5, 0\},$$

$$B_4 = \{5, 6, 1\},$$

$$B_5 = \{6, 0, 2\},$$

$$B_6 = \{0, 1, 3\}.$$

These seven sets form the blocks of a symmetric design with parameters $(7, 3, 1)$. They also give the smallest nontrivial projective geometry: these seven blocks (“lines”) each have the property that each pair of blocks meet in exactly one point; in addition, every pair of points is on exactly one block.

Although it is fairly easy to construct a $(7, 3, 1)$ design by hand, combinatorial objects become much more difficult to construct if the parameters are much larger.

There are shortcuts. The starter set, $B_0 = \{1, 2, 4\}$ above, obeys a certain property. Let’s do arithmetic modulo 7, treating 7 as 0 and equating each integer with its remainder after division by 7. Every integer is then equivalent with the set $\{0, 1, 2, 3, 4, 5, 6\}$, the set of residues modulo 7. Now take the set $D = \{1, 2, 4\}$ and consider all differences from D , modulo 7:

$$2 - 1 = 1,$$

$$4 - 2 = 2,$$

$$4 - 1 = 3,$$

$$1 - 4 = 3 = 4,$$

$$2 - 4 = -2 = 5,$$

$$1 - 2 = -1 = 6,$$

Each nonzero residue appears exactly once as a difference. The set D is a “ $(7, 3, 1)$ difference set”, that is, it consists of three members of the residues modulo 7, where every nonzero element appears once in the collection of differences.

1.2 Difference Sets

Definition. (First definition of difference set.) Let \mathbb{Z}_v be the set $\{0, 1, 2, \dots, v - 1\}$ of residues mod v . A proper, nonempty subset D of \mathbb{Z}_v is a (v, k, λ) **difference set** if D has k elements and in the list of $k(k - 1)$ differences $d_1 - d_2$ of distinct pairs d_1, d_2 of D , each nonzero element of \mathbb{Z}_v occurs exactly λ times.

Example 2. An $(11, 5, 2)$ difference set.

The set $D = \{1, 3, 4, 5, 9\}$ is an $(11, 5, 2)$ difference set. We can verify that it is a difference set by creating a subtraction table: In this table, the entry in the i th row and j th column will be $a_i - b_j \pmod{11}$ where a_i is the row label for the i th row and b_j is the column label for the j th column.

-	1	3	4	5	9
1	0	9	8	7	3
3	2	0	10	9	5
4	3	1	0	10	6
5	4	2	1	0	7
9	8	6	5	4	0

Note that each element of $\mathbb{Z}_{11} - \{0\}$ appears exactly *twice* in this table.

Exercises.

1. Show that $\{0, 3, 5, 6\}$ is a $(7, 4, 2)$ difference set.
2. Show that $\{0, 1, 3, 9\}$ is a $(13, 4, 1)$ difference set.

3. Show that $\{3, 6, 7, 12, 14\}$ is a $(21, 5, 1)$ difference set.
4. Exactly one of the sets $D_1 = \{0, 1, 2, 4, 5, 8, 10\}$ and $D_2 = \{0, 3, 5, 6, 9, 10, 12\}$ is a $(15, 7, 3)$ difference set. Which one? (Is there an easy way to tell?)

Definition. (Second definition of difference set.) Let $(G, +)$ be an abelian group written additively. Set $v := |G|$. A proper, nonempty set $D \subseteq G$ is a (v, k, λ) **difference set** if D has k elements and in the list of $k(k-1)$ differences $d_1 - d_2$ of distinct pairs d_1, d_2 of D , each nonzero element of G occurs exactly λ times.

Example 3. A difference set in a noncyclic group.

Let $G = Z_4 \times Z_4$, the direct product of two cyclic groups of order four. The subgroup $H := \langle \{(0, 2)\}, \{(2, 0)\} \rangle = \{(0, 0), (0, 2), (2, 0), (2, 2)\}$ partitions G into the four cosets: $H, H + (0, 1), H + (1, 0)$, and $H + (1, 1)$. The subgroup H itself has three proper nontrivial subgroups. They are $K_1 := \langle (0, 2) \rangle = \{(0, 0), (0, 2)\}$, $K_2 := \langle (2, 0) \rangle = \{(0, 0), (2, 0)\}$, and $K_3 := \langle (2, 2) \rangle = \{(0, 0), (2, 2)\}$.

The set $D := (K_1 + (0, 1)) \cup (K_2 + (1, 0)) \cup (K_3 + (1, 1))$ is a $(16, 6, 2)$ difference set in an abelian (but not cyclic) group.

Example 4. Let $G := \langle x, y : x^8 = y^2 = 1, xy = yx \rangle$. This is the abelian group $C_8 \times C_2$, written in multiplicative notation. One can verify that the set $D := \{1, x, y, x^3y, x^5y, x^7y\}$ is a $(16, 6, 2)$ difference set, that is, the list (multi-set) of elements $\{d_1d_2^{-1} : d_1, d_2 \in D\}$ covers all the nonzero elements of G exactly twice.

For which parameters (v, k, λ) does there exist a difference set? This existence question will be a driving force throughout this paper. Simple counting gives us a fundamental result, a necessary but not sufficient condition for the existence of a (v, k, λ) difference set. There are $k(k-1)$ distinct differences from a difference set D , and since each of the $v-1$ nonzero elements of the group G must appear λ times in this list, we have that $k(k-1) = (v-1)\lambda$.

Theorem 1 *If a (v, k, λ) difference set exists then $k(k-1) = (v-1)\lambda$ and $v > k > \lambda$.*

Proof The paragraph above gives a proof that $k(k-1) = (v-1)\lambda$. D is a proper subset of a group of size v , so $v > k$. Therefore $v-1 > k-1$ and dividing both sides of the equation $k(k-1) = (v-1)\lambda$ by $k-1$, we have $k > \lambda$.

We may rewrite the basic equation $k(k-1) = (v-1)\lambda$ as

$$k - \lambda = k^2 - v\lambda.$$

The value $k - \lambda$ is called the **order** of the design; we will see why it is important later. The order of a design is often denoted by the symbol n .

Observation. If D is a difference set in G then so is $G - D$, the complement of D in G . If the parameters of D are (v, k, λ) then the parameters of the complementary difference set are $(v, v-k, v-2k+\lambda)$. In particular, the order of complementary difference sets is the same. By replacing D with its complement, we may assume $k \leq \frac{v}{2}$.

Difference sets of size $k = 1$ or $k = 2$ are uninteresting. And one can show (exercise!) that $k \neq \frac{v}{2}$. Thus it is customary to assume that k falls in the interval $\frac{v}{2} > k > 2$.

Difference sets are a useful way to construct symmetric designs. We elaborate, briefly, below.

1.3 The combinatorial motivation for using group theory

A combinatorial configuration consists of a finite set \mathfrak{P} and a set \mathfrak{B} of subsets of \mathfrak{P} . The elements of \mathfrak{P} are called “points”; the elements of \mathfrak{B} are often called “blocks” or “lines.” (Note that the elements of \mathfrak{B}

are themselves sets of points; \mathfrak{P} is a set while \mathfrak{B} is a set of sets.) We usually expect some “regularity” conditions on \mathfrak{B} , some combinatorial conditions that make the structure $(\mathfrak{P}, \mathfrak{B})$ interesting. For example, we might require that each $B \in \mathfrak{B}$ have the same size and so define a block-size constant $k := |B|$. We might also require that there be constant intersection size, that is, that there be an integer λ such that every pair of distinct blocks intersect in a set of size λ . If, in addition, $|\mathfrak{P}| = |\mathfrak{B}|$, then we have a symmetric (v, k, λ) design where $v := |\mathfrak{P}|$.

In this paper we will suppose that a combinatorial configuration is simply an ordered pair $\mathfrak{D} = (\mathfrak{P}, \mathfrak{B})$ where \mathfrak{B} is a set of subsets of \mathfrak{P} .

(References for the general study of combinatorial configurations include Dembowski, Design theory, Combinatorial Theory by Hall, Cameron and VanLint.)

Suppose $\mathfrak{D} = (\mathfrak{P}, \mathfrak{B})$ is a combinatorial configuration. Any permutation of \mathfrak{P} extends naturally to a permutation of the set of subsets of \mathfrak{P} . A natural question to ask is, “Which permutations of \mathfrak{P} are also permutations of \mathfrak{B} ?” (In the late 1800’s, Felix Klein made this question – asked about infinite geometries – the center of his Erlangen program. Finite geometries and combinatorial configurations have greatly benefited from the same question.) A permutation of \mathfrak{P} which is also a permutation of \mathfrak{B} is an **automorphism** of \mathfrak{D} . Explicitly, an automorphism of \mathfrak{D} is a permutation $f : \mathfrak{P} \rightarrow \mathfrak{P}$ such that $B \in \mathfrak{B} \implies f(B) \in \mathfrak{B}$.

The set of all automorphisms of a combinatorial configuration \mathfrak{D} forms a group, the **full automorphism group** of \mathfrak{D} . More generally, an automorphism group of a design is any subgroup of the full automorphism group.

The full automorphism group of a combinatorial configuration carries a great deal of information about the configuration. In many cases, one can go as far as to construct an unknown combinatorial configuration by assuming that the configuration has a certain automorphism group.

Definition. A group G is said to “act” on a set X if there is a homomorphism ϕ defined from G into S_X , the symmetric group of permutations of X . Given $x \in X, g \in G$, we write $g(x)$ for $\phi(g)(x)$ and suppress the homomorphism ϕ . The group G acts **transitively** on X if for any $x, y \in X$, there exists $g \in G$ such that $g(x) = y$. If G acts transitively on X and for a fixed $x \in X$, $g(x) = x$ implies $g = 1_G$ then we say G is **sharply transitive** (or **regular**) on X .

sharplytransitive

Lemma 1 *Suppose G acts transitively on X . Then the following are equivalent.*

1. G is sharply-transitive on X ,
2. for any $x \in X$, $g(x) = x$ implies g is the identity,
3. $|G| = |X|$.

difset

Theorem 2 *A symmetric design (P, B) with parameters (v, k, λ) which has an automorphism group G acting regularly (“sharply transitively”) on the point set P is equivalent to the existence of a difference set D in G .*

Proof We wish to prove, first, that given a (v, k, λ) difference set D in a group G we may construct a symmetric (v, k, λ) design on which G acts regularly and second, that given a (v, k, λ) design with regular automorphism group G , we may construct a (v, k, λ) difference set D in G .

Given a (v, k, λ) difference set D , let $(G, \{gD : g \in G\})$ be the combinatorial configuration with point set G and block set $\{gD\}$ of all left translates of D . This combinatorial configuration has exactly $v := |G|$ points and blocks. Each block has $k := |D|$ elements. Fix a point g ; that point is in the k blocks $(gd^{-1})D, d \in D$. Finally, let xD and yD be two blocks of the combinatorial configuration $(G, \{gD : g \in G\})$. Then an element g in $xD \cap yD$ provides elements $d_1, d_2 \in D$ such that $g = xd_1 = yd_2$. Therefore $x^{-1}y = d_1d_2^{-1}$. Since D is a difference set, there are exactly λ ordered pairs (d_1, d_2) whose quotient $d_1d_2^{-1}$ is $x^{-1}y$. So the cardinality of $xD \cap yD$ is λ . This proves that $(G, \{gD : g \in G\})$ is a symmetric design. Obviously G acts regularly on $(G, \{gD : g \in G\})$ by premultiplication.

Conversely, suppose we are given a symmetric (v, k, λ) design $\mathfrak{D} = (\mathfrak{P}, \mathfrak{B})$ with point set \mathfrak{P} , block set \mathfrak{B} and an automorphism group G acting regularly on points. Choose a base point $p_0 \in \mathfrak{P}$ and identify each element p of \mathfrak{P} with the group element $g \in G$ such that $g(p_0) = p$. (We will agree that group action of G on this new set of points will be premultiplication, that is, multiplication on the left. Thus a “point” $h \in G$ will be mapped to the “point” gh by the group element h .)

Choose a particular block $B_0 \in \mathfrak{B}$, called the “base block” and let $D := \{g \in G : g(p_0) \in B_0\}$. (Since G acts regularly on the blocks of \mathfrak{B} by premultiplication, then the set of blocks is equivalent to the set $\{gD : g \in G\}$.) Thus the symmetric design $(G, \{gD : g \in G\})$ is isomorphic to $(\mathfrak{P}, \mathfrak{B})$. We claim that D is a (v, k, λ) difference set.

Given any nonidentity element $g \in G$, we wish to show that there are exactly λ ordered pairs (d_1, d_2) such that $g = d_1 d_2^{-1}$. By the definition of symmetric design, the intersection of the block D and the block gD is of size λ . Any element d_1 in this intersection provides elements $d_1, d_2 \in D$ such that $d_1 = g d_2$. Conversely, if $d_1 d_2^{-1} = g$ and $d_1, d_2 \in D$ then $d_1 \in D \cap gD$.

See Lander, [35], chapter 4, pages 120-2, or Hall, [?], chapter 11 for a discussion of difference sets and regular automorphisms of symmetric designs. (Also, van Lint & Wilson?)

Equivalence

Lemma 2 *Suppose D is a (v, k, λ) difference set in a group G . Then given any element $g \in G$, the left translate gD is a (v, k, λ) difference set in G . Similarly, given any automorphism ϕ of G , the set $\phi(D)$ is a (v, k, λ) difference set in G .*

We say that the sets D and gD are **translation equivalent**. The sets D and $\phi(D)$ are **automorphism equivalent**. More generally, two sets D_1 and D_2 are said to be **equivalent** if there is a group element g and automorphism ϕ such that $D_1 = g\phi(D_2)$.

Each of the concepts of “equivalence” in the previous paragraph define an equivalence relation on subsets of a group G ; by Lemma 2, any set equivalent to a difference set is a difference set.

Two (v, k, λ) difference sets in a group G need not be equivalent; the smallest example of this occurs in the family of difference sets with parameters $(16, 6, 2)$.

Other combinatorial configurations give analogous versions of Theorem 2, above.

1.4 Cayley Graphs

Let G be a finite group and $S \subseteq G$. We may define a directed graph on the elements of G by agreeing that $g \sim h \iff gh^{-1} \in S$. This is the **Cayley graph**, $C(G, S)$, on G induced by S . This graph is connected if and only if S is a generating set for G . The graph is undirected if and only if S is closed under inverses. (See chapter 30 of [21] for a nice introduction to Cayley graphs.)

How do Cayley graphs of nonabelian groups differ from Cayley graphs of abelian groups? For example, let $G = A_4$, the alternating group on four elements, and let $S = \{(123), (132), (12)(34)\}$. The Cayley graph created this way is a cubic graph on twelve vertices; it is not a Cayley graph of an abelian group.

Research question: Can we look at the structure of this graph and recognize its inherent nonabelian-ness?

A graph with a regular automorphism group G acting on vertices is equivalent to a Cayley graph (G, S) where S is some subset of G and two “vertices” g, h are adjacent if and only if $gh^{-1} \in S$. Many of the combinatorial configurations which have a regular automorphism group may be expressed in terms of Cayley graphs. We will say more about that in the next section.

1.5 Summary

The moral here is that groups can be used to construct combinatorial objects. In the next section we look at a better way to do “combinatorial” computations in a finite group.