Difference Sets

Definition

Suppose that G = (G,+) is a finite group of order v with identity 0 written additively but not necessarily abelian.
A (v,k,λ)-difference set in G is a subset D of G of size k such that the multiset
{x-y| x,y ε D, x ≠ y} contains every element of G\{0} λ times.

Example: In $\mathbb{Z}_{13}$ the set D = {0,1,3,9} is a (13,4,1)-difference set. Consider

1 – 0 = 1	0 – 1 = -1 = 12
3 – 0 = 3	0 – 3 = -3 = 10
9 – 0 = 9	0 – 9 = -9 = 4
3 – 1 = 2	1 – 3 = -2 = 11
9 – 1 = 8	1 – 9 = -8 = 5
9 – 3 = 6	3 – 9 = -6 = 7

More Examples

Example:

D = {(0,1), (0,2), (0,3), (1,0), (2,0), (3,0)} is a (16,6,2) difference set in $(\mathbb{Z}_4 \times \mathbb{Z}_4, +)$.

Example:

D = {a, a^2, b, b^2, b^4} is a (21, 5, 1)difference set in the non-abelian group

$$G = \{a^i b^j : a^3 = b^7 = 1, ba = ab^4\}.$$

Since this group is written multiplicatively the difference set definition takes on the form:

$$\{xy^{-1} \mid x, y \in D, x \neq y\} = G \backslash \{1\}.$$

So What?

If a (v,k,λ)- difference set exists then

$$\lambda(v-1) = k(k-1).$$

This is immediate since the the LHS counts the number of non-zero elements of the set each with multiplicity λ, while the RHS counts the number of ordered pairs of distinct elements (each representing a difference).

The notation and this relation seem to imply a relationship between difference sets and symmetric BIBDs.

If D is a difference set in group (G,+), then

$$D+g = \{x + g \mid x \in D\}$$

is called a ***translate of D*** for any $g \in G$. The multiset of all v (= |G|) translates of D is denoted **Dev(D)** and called the ***development of D***.

The Connection

Theorem: Let D be a (v,k,λ)-difference set in an abelian group (G,+). Then (G, Dev(D)) is a symmetric (v,k,λ)-BIBD.

Pf. Suppose $x,y \in G$, $x \neq y$. Let $x - y = d$. There are λ pairs (x_i,y_i), with $x_i, y_i \in D$ and $x_i - y_i = d$. Define $g_i = -x_i + x$. Then we also have $g_i = -y_i + y$ and $\{x,y\} = \{x_i + g_i, y_i + g_i\} \subseteq D + g_i$. The g_i's are distinct since the x_i's are, so there are at least λ translates that contain {x,y}.

Now suppose that there are m translates $D + h_j$, $1 \leq j \leq m$ which contain {x,y}. Then $(x - h_j) + (h_j - y) = x-y = d$ for each j. $\{x-h_j, y-h_j\} \subseteq D$ and the h_j's are all distinct, so we have found m ordered pairs $\{x',y'\} \subseteq D$ such that $x' - y' = d$. Thus, $m = \lambda$ and we see that we have a symmetric BIBD.

Example

Only this proof required abelian groups, the result is valid for all groups.

Corollary: If D is a difference set then Dev(D) has distinct blocks.

Pf: If D + g = D + h with g ≠ h. The symmetric BIBD whose blocks are Dev(D) would have two blocks intersecting in k points, but two blocks intersect in λ points in a symmetric design.

Example: D = {0,1,3,9} is a (13, 4, 1) – difference set.
Dev(D) = 0139, 124A, 235B, 346C, 0457, 1568, 2679,
378A, 489B, 59AC, 06AB, 17BC, 028C
with A = 10, B = 11 and C = 12. This design is the projective plane of order 3.

Automorphisms

Theorem: Aut(G, Dev(D)) contains a subgroup (G',◦) isomorphic to (G,+).

Pf: For each g in G, define the map t_g: G → G by

$(x)t_g = x + g.$ Note change from text.

Each t_g is a bijection. Let G' = {t_g| g ε G}. It is easy to check that G' is a permutation group (called the ***permutation representation of G***).

Define α: G → G' by α(g) = t_g . α is a group isomorphism since, $(x)\,(\alpha(g)\circ\alpha(h)) = (x)t_g t_h = (x+g)\,t_h = (x+g)+h = x+(g+h)$

$= (x)t_{g+h} = (x)\,\alpha(g+h).$

Automorphisms

Theorem: Aut(G, Dev(D)) contains a subgroup (G',◦) isomorphic to (G,+).

Pf: (cont)

We now show that G' consists of automorphisms. .

$$(D + h)\,\alpha(g) = \{(x)\alpha(g) \mid x \in D + h\}$$
$$= \{x + g \mid x \in D + h\}$$
$$= \{d + h + g \mid d \in D\}$$
$$= D + (h + g)$$

So, α(g) maps translates of D to translates of D and is an automorphism of Dev(D).

Example

Consider D = {(0,1), (0,2), (0,3), (1,0), (2,0), (3,0)} a (16,6,2) difference set in $(\mathbb{Z}_4 \times \mathbb{Z}_4, +) = G$.

We will number the elements of G as follows:

0 = (0,0)	8 = (2,0)
1 = (0,1)	9 = (2,1)
2 = (0,2)	A = (2,2)
3 = (0,3)	B = (2,3)
4 = (1,0)	C = (3,0)
5 = (1,1)	D = (3,1)
6 = (1,2)	E = (3,2)
7 = (1,3)	F = (3,3)

$(0,1) \rightarrow (0123)(4567)(89AB)(CDEF)$
$(1,0) \rightarrow (048C)(159D)(26AE)(37BF)$
$(1,2) \rightarrow (068E)(179F)(24AC)(35BD)$

$D = \{1,2,3,4,8,C\}$
$D^{(0,1)} = \{2,3,1,5,9,D\} = D+1$
$D^{(1,2)} = \{7,4,5,A,E,2\} = D+6$

A useful lemma

Lemma: In a symmetric BIBD, the number of fixed points of any automorphism equals the number of fixed blocks.

Pf: Let α be an automorphism of the BIBD (X,B) which has incidence matrix A. There exist permutation matrices corresponding to the action of α on the points (P) and on the blocks (Q) such that

$$PA = AQ,$$

since α is an automorphism and preserves the design. A is a square, non-singular matrix and so has an inverse. From which we derive $P = AQA^{-1}$, i.e., P and Q are similar matrices. The sum of the elements of P (or Q) on the diagonal (the trace of the matrix) is the number of fixed points(or blocks) of α. Similar matrices have the same trace.

Example

The (7,3,1)-difference set {0,1,3} produces the Fano plane with blocks 013, 124, 235, 346, 045, 156, 026 has the automorphism α = (25)(46). This has 3 fixed points and cycle structure $[1^3, 2^2]$. The text would write [1,1,1,2,2].

α fixes blocks 013, 235 and 346, while it interchanges blocks 124 ↔ 156 and 045 ↔ 026, so cycle structure on the blocks is also $[1^3, 2^2]$.

More Generally

Theorem: An automorphism of a symmetric BIBD has the same cycle type on the points as it does on the blocks.

We have just seen an example of this. As the proof involves the Möbius Inversion Formula we shall skip it for now.

Conversely

Theorem: If a symmetric (v,k,λ)-BIBD admits an automorphism which permutes the points in a single cycle of length v, then there is a (v,k,λ)-difference set in $(\mathbb{Z}_v,+)$.

Pf: Let $X = \{x_0, \ldots, x_{v-1}\}$ and $\alpha(x_i) = x_{i+1 \bmod v}$. Choose any block and call it A_0 and define

$$A_j = \{\alpha^j(x) \mid x \in A_0\} = \{x_{i+j \bmod v} \mid x_i \in A_0\}.$$

Each of the A_j is a block of the design since α is an automorphism. We also have $\alpha(A_j) = A_{j+1 \bmod v}$ by the way in which the A_i's are defined. Since the cycle type of α on points is $[v^1]$, it must permute the blocks in a single orbit of length v, so the A_i's are distinct and all blocks are of this type.

Conversely

Theorem: If a symmetric (v,k,λ)-BIBD admits an automorphism which permutes the points in a single cycle of length v, then there is a (v,k,λ)-difference set in $(\mathbb{Z}_v,+)$.

Pf: (cont) Now define

$$D = \{i \mid x_i \in A_0\}.$$

Let $g \in \mathbb{Z}_v \setminus \{0\}$. The pair $\{x_0, x_g\}$ occurs in λ blocks of the design, $A'_1, \ldots, A'_\lambda$. For each occurrence of a pair $\{x_0, x_g\} \subseteq A'_j$, we have a pair with difference g in the set D, namely,

$(g - j) - (-j) \equiv g \bmod v$, where $\{-j \bmod v, g-j \bmod v\} \subseteq D$.

These λ pairs in D are distinct, so D is a (v,k,λ)-difference set.

More Generally

Theorem: If a symmetric (v,k,λ)-BIBD admits a sharply transitive automorphism group G, then there is a (v,k,λ)-difference set in the group G.

Sharply transitive means that for every ordered pair of elements (a, b), there is a unique element g ε G, so that $b = a^g$. This generalizes the last result since the group generated by an automorphism which is a single cycle of length v is sharply transitive in its action on X.

The proof is similar to the last result and so is omitted.

Quadratic Residues

Let $\mathbf{F}=\mathbf{F}_q$ = GF(q) be a finite field of odd prime power order q.

QR(q) = {non-zero squares in **F**}

which is called the set of **quadratic residues** of **F**. The set of non-zero elements that are not in QR form the set of **quadratic non-residues** QNR(q).

In terms of a primitive element, ω of F, the quadratic residues are the even powers of ω, and the quadratic non-residues are the odd powers.

Ex: QR(7) = {1,4,2} 3 is a primitive element of $\mathbb{Z}_7$ = GF(7).

$3^0 = 1$, $3^1 = 3$, $3^2 = 2$, $3^3 = 6$, $3^4 = 4$, $3^5 = 5$, $3^6 = 1$.

Properties

Since the non-zero elements of a finite field (= $\mathbf{F}^* = \mathbf{F}\backslash\{0\}$) form a multiplicative cyclic group, it is easy to see that QR(q) is a subgroup of this cyclic group which must be of order ½(q-1). NQR(q) is the coset of this group in $\mathbf{F}^*$.

Thm: For odd q, $-1 \in QR(q)$ if and only if $q \equiv 1 \bmod 4$.

Pf: Let ω be a primitive element of $\mathbf{F}_q$. Let $\gamma = \omega^{(q-1)/2}$ then $\gamma^2 = \omega^{(q-1)} = 1$, but since $\gamma \neq 1$ we have $\gamma = -1$.

Ex: In GF(7), -1 = 6 which is in NQR(7) since $7 \equiv 3 \bmod 4$.

In GF(5), -1 = 4, clearly in QR(5) and $5 \equiv 1 \bmod 4$.

QR Difference Sets

Thm: If $q \equiv 3 \bmod 4$, then QR(q) is a $(q, \frac{1}{2}(q-1), \frac{1}{4}(q-3))$-difference set in $(\mathbf{F}_q, +)$.

Pf: Denote D = QR(q). We have $|D| = \frac{1}{2}(q-1)$, so we need only show that every non-zero element of $\mathbf{F}_q$ occurs $\frac{1}{4}(q-3)$ times as a difference of two elements in D.

For any $d \in \mathbf{F}_q \setminus \{0\}$, define

$$a_d = |\{(x,y) : x,y \in D, x - y = d\}|.$$

$gx - gy = g(x-y)$ for all g, x, y, so the number of times any given difference d occurs in D is the same as the number of times the difference gd occurs in gD, where $gD = \{gx : x \in D\}$. Suppose that $g \in D$, then $gD = D$ so $a_d = a_{gd}$ and there exists a constant λ such that $a_d = \lambda$ for all $d \in D$.

QR Difference Sets

Thm: If $q \equiv 3 \bmod 4$, then QR(q) is a $(q, \frac{1}{2}(q-1), \frac{1}{4}(q-3))$- difference set in $(\mathbf{F}_q, +)$.

Pf: (cont) Now suppose that $d \in QNR(q)$ and let $e = -d$. Since $q \equiv 3 \bmod 4$, $-1 \in QNR$ so $e \in D$. Note that $a_d = a_e$ because $x-y = d$ if and only if $y-x = e$. Therefore it follows that $a_d = \lambda$ for all $d \in \mathbf{F}_q \setminus \{0\}$, and so D is a $(q, \frac{1}{2}(q-1), \lambda)$-difference set. We can now calculate λ using

$$\lambda(v-1) = k(k-1)$$

so

$$\lambda(q-1) = \tfrac{1}{2}(q-1)(\tfrac{1}{2})(q-3)$$

$$\lambda = \tfrac{1}{4}(q-3).$$

Example

The QR difference set obtained when q = 11 is an (11,5,2)- difference set which produces a biplane with k=5.

QR(11) = {1, 4, 9, 5, 3} = D

Dev(D) = {1, 4, 9, 5, 3} {2, 5, 10, 6, 4} {3, 6, 0, 7, 5}
{4, 7, 1, 8, 6} {5, 8, 2, 9, 7} {6, 9, 3, 10, 8}
{7, 10, 4, 0, 9} {8, 0, 5, 1,10} {9, 1, 6, 2, 0}
{10, 2, 7, 3, 1} {0, 3, 8, 4, 2}

Related Quartic Residues

Thm: If $p = 4t^2 + 1$ is prime and t is an odd integer, then the quartic residues in $\mathbb{Z}_p$ form a $(4t^2+1, t^2, \frac{1}{4}(t^2-1))$ – difference set in $(\mathbb{Z}_p,+)$.

With $t = 3$, $p = 37$ and Dev(quartic residues) forms a (37, 9, 2) biplane.

Thm: If $p = 4t^2 + 9$ is prime and t is an odd integer, then the quartic residues in $\mathbb{Z}_p$ together with 0, form a $(4t^2+9, t^2 + 3, \frac{1}{4}(t^2+ 3))$ – difference set in $(\mathbb{Z}_p,+)$.

Singer Difference Sets

Thm: If q is a prime power, then there exists a $(q^2+q+1, q+1, 1)$-difference set in $(\mathbb{Z}_{q^2+q+1}, +)$.

Pf: We will prove this by constructing the design and then showing that it has the right kind of automorphism to give us the difference set.

Recall that the designs with these parameters were constructed from a 3-dimensional vector space V. Points were the 1-dimensional subspaces and blocks the 2-dimensional subspaces.

Since $\mathbf{F}_{q^3}$ is a 3-dimensional vector space over $\mathbf{F}_q$ we may take $V = \mathbf{F}_{q^3}$ and construct our design. Let ω be a

Singer Difference Sets

Thm: If q is a prime power, then there exists a $(q^2+q+1, q+1, 1)$-difference set in $(\mathbb{Z}_{q2+q+1},+)$.

Pf: (cont.) primitive element of $\mathbf{F}_{q3}$ and define a map $f: V \rightarrow V$ by $f(z) = \omega z$. Now $f(z + z') = \omega(z+z') = \omega z+\omega z' = f(z)+f(z')$, and $f(cz) = \omega(cz) = (\omega c)z = (c\omega)z = c(\omega z) = cf(z)$. Thus f is a linear map of V and so preserves subspaces of V. This means that f induces an automorphism of the design.

Since $\mathbf{F}_q$ is a subfield of $\mathbf{F}_{q3}$ it is easy to see that

$$\mathbf{F}_q = \{\omega^{(q2+q+1)i} \mid 0 \le i \le q-2\} \cup \{(0,0,0)\}.$$

The map f^{q2+q+1} multiplies any vector by a scalar (an element of F_q) so fixes any 1-dim subspace, and no smaller (non-zero) power of f can do so. Thus, f permutes the points in a single cycle of length $q^2+q+1 = v$.

Example

For example consider the construction of the (13,4,1)-Singer difference set in $\mathbb{Z}_{13}$.

We start with the field $\mathbf{F}_{27}$ as a 3-dimensional vector space over $\mathbf{F}_3$. [This is the right base field since we want to construct the projective plane of order 3.]

A primitive cubic polynomial over $\mathbf{F}_3$ is given by x^3-x^2+1 [Note that $-1 \equiv 2 \bmod 3$]. If w is a primitive element of $\mathbf{F}_{27}$ then:

$w^0 = w^{26} = 1$
$w^1 = w$
$w^2 = w^2$
$w^3 = w^2 - 1$
$w^4 = w^2 - w - 1$
$w^5 = -w - 1$
$w^6 = -w^2 - w$

$w^7 = w^2 + 1$
$w^8 = w^2 + w - 1$
$w^9 = -w^2 - w - 1$
$w^{10} = w^2 - w + 1$
$w^{11} = w - 1$
$w^{12} = w^2 - w$
$w^{13} = -1$

$w^{14} = -w$
$w^{15} = -w^2$
$w^{16} = -w^2 + 1$
$w^{17} = -w^2 + w + 1$
$w^{18} = w + 1$
$w^{19} = w^2 + w$
$w^{20} = -w^2 - 1$

$w^{21} = -w^2 - w + 1$
$w^{22} = w^2 + w + 1$
$w^{23} = -w^2 + w - 1$
$w^{24} = -w + 1$
$w^{25} = -w^2 + w$

Example

We now need a 2-dimensional subspace. We can pick any two vectors (elements of $\mathbf{F}_{27}$) as a basis for the subspace as long as they aren't scalar multiples of each other. For instance 1 and w will work. We now form <1,w> = {a + bw} where a, b range through $\mathbf{F}_3 = \{0,1,-1 = w^{13}\}$. This gives us

$0 + 0w = 0$	$1 + 0w = 1$	$-1 + 0w = w^{13}$
$0 + w = w$	$1 + w = w^{18}$	$-1 + w = w^{11}$
$0 - w = w^{14}$	$1 - w = w^{24}$	$-1 - w = w^{5}$

Now, taking only the non-zero elements and reducing the exponents mod 13 (to get only one vector in each 1-dim subspace) we get: $\{1, w, w^5, w^{11}\} = \langle 1,w \rangle$. The difference set in $\mathbb{Z}_{13}$ is thus {0,1,5,11}.

Multipliers

From now on we will be working with abelian groups.

Let D be a (v,k,λ)-difference set in an abelian group $(G,+)$ of order v. For an integer m, define

$$mD = \{mx \mid x \in D\},$$

where mx is the sum of m copies of x (computed in G). m is called a ***multiplier of D*** if $mD = D+g$ for some $g \in G$. If $mD = D$, we say that D is ***fixed*** by the multiplier m.

Ex: $D = \{0,3,4,9,11\}$ is a (21,5,1)-difference set in $\mathbb{Z}_{21}$.

Consider $2D = \{0,6,8,18,1\} = D + 18$ so 2 is a multiplier.

$\{3,6,7,12,14\}$ is also a (21,5,1)-difference set in $\mathbb{Z}_{21}$ and it is fixed by the multiplier 2.

Properties of Multipliers

Lemma: If m is a multiplier of a (v,k,λ)-difference set in an abelian group G of order v, then $\gcd(v,m) = 1$.

Pf. Suppose that $\gcd(v,m) = s > 1$. Let p be a prime divisor of s. Since G is abelian, there will be an element of order p in G; select one and call it d. There must exist elements x,y in the difference set D so that $x - y = d$. Then, $mx - my = md = 0$ since p divides m. So the set mD contains repeated elements and therefore $mD \neq D + g$ for any g in G. m is thus not a multiplier, a contradiction.

Properties of Multipliers - 2

Lemma: If m is a multiplier of a (v,k,λ)-difference set D in an abelian group G then the map α: G → G given by α(x) = mx is an automorphism of (G, Dev(D)).

Pf: Since m is a multiplier, mD = D + g for some g ε G. Consider

α(D + h) = m(D + h) = mD + mh = D + g + mh ε Dev(D).

So α maps blocks to blocks. If α is a bijection then it will be an automorphism of (G, Dev(D)). Since G is finite, we need only show that a is an injection to prove that it is a bijection. Suppose α(x) = α(y). Then mx = my, or m(x-y)=0. If x -y ≠ 0, then the order of x – y must divide m and v, but this contracts the last lemma, so x = y.

The Multiplier Theorem

Theorem: Let D be a (v,k,λ)-difference set in an abelian group G. If

1. p is a prime,
2. gcd(v,p) = 1,
3. $k - \lambda \equiv 0 \bmod p$, and $k - \lambda$ is the order of the design
4. $p > \lambda$,

then p is a multiplier of D.

Example: A (21,5,1)-difference set in $\mathbb{Z}_{21}$ would have 2 as a multiplier and we shall construct one shortly.

A (31, 10, 3) -difference set in $\mathbb{Z}_{31}$ would have 7 as a multiplier, but we will see that no such difference set exists.

Using the Multiplier Theorem

There are some properties of multipliers which make using the theorem easier.

Theorem: If m is a multiplier of a difference set D in an abelian group G, then there is a translate of D which is fixed by m.

Pf: Recall that the map $\alpha(x)= mx$ is an automorphism of the design (G, Dev(D)). Since $\alpha(0) = 0$, α has at least one fixed point and so it must fix at least one block of Dev(D).

Examples

If there is a (21,5,1)-difference set in $\mathbb{Z}_{21}$, then 2 is a multiplier by the multiplier theorem, but how do we find the difference set?

By the last result we know that 2 would fix a translate of the difference set (which is itself a difference set), so we should try to find it. If 2 fixes this block, then the points in the block must form orbits of the action given by multiplying by 2 (mod 21). The orbits of this action are: [0], [1 2 4 8 16 11], [3 6 12], [5 10 20 19 17 3], [7 14], and [9 18 15]. A block of size 5 can only be made up of orbits of sizes 2 and 3 (from this list with no repeated elements). So, we check {3,6,7,12,14} and {7,9,14,15,18} both of which happen to work – that is, give difference sets.

Examples

Similar to the last example, a (31, 10, 3)-difference set in $\mathbb{Z}_{31}$ would have 7 as a multiplier.

As before we would look for a block fixed by multiplication by 7 (i.e., made up of orbits of this action), but these orbits are:

[0],
[1 7 18 2 14 5 4 28 10 8 25 20 16 19 9]
[3 21 23 6 11 15 12 22 30 24 13 29 17 26 27]

as it is impossible to obtain a block of size 10 from these orbits of size 15, there can be no such difference set.

Using the Multiplier Theorem - 2

Theorem: If there exists a (v,k,λ)-difference set D in an abelian group G of order v where gcd(v,k) = 1, then there is a translate of D which is fixed by every multiplier.

Pf: Let $$s = \sum_{x \in D} x .$$

It follows that $$\sum_{x \in D+g} x = s + kg .$$

Now suppose that s + kg = s + kh, with g ≠ h. Then k(g-h) = 0, so the order of g-h divides k. But the order of any element of a group divides the order of the group (v in this case). Since gcd(k,v) = 1, we have g – h = 0 →←

Using the Multiplier Theorem - 2a

Theorem: If there exists a (v,k,λ)-difference set D in an abelian group G of order v where gcd(v,k) = 1, then there is a translate of D which is fixed by every multiplier.

Pf:(cont) This shows that g → s + kg is one-to-one. Since G is finite, this map is a bijection, and so a surjection and there must be a unique g for which s + kg = 0. For this g,

$$\sum_{x \in D+g} x = 0 .$$

Now let m be any multiplier of D. m is also a multiplier of any translate of D, so

$$\sum_{x \in m(D+g)} x = m \sum_{x \in D+g} x = 0 .$$

But since there is a unique translate which adds up to 0, we have m(D+g) = D+g, so D+g is fixed by all multipliers.

Example

Consider a projective plane of order n with $n \equiv 0 \bmod 6$, that is a symmetric $(n^2+n+1, n+1, 1)$-design. Both 2 and 3 satisfy the conditions of the multiplier theorem. Since $n^2+n+1 = n(n+1) + 1$, $\gcd(v,k) = 1$ so there would be a difference set which is fixed by both multipliers by the last result. If $x \neq 0$ is an element of such a D, then 2x and 3x must also be elements. None of the elements x, 2x or 3x can be equal and the differences 2x – x and 3x – 2x are both equal to x, contradicting the fact that $\lambda = 1$. So no such difference set can exist.

Notice that this does not rule out the existence of a projective plane of order 12, only one that comes from a difference set (these are called cyclic projective planes.)

The Group Ring

Let G be an abelian group. The group ring $\mathbb{Z}[G]$ consists of all formal sums of the form

$$\sum_{g \in G} a_g x^g$$

where $a_g \varepsilon \mathbb{Z}$ and x is an indeterminate. The elements of the group ring look like polynomials in x with integer coefficients. We exploit that resemblance and define:

$$(a+b)(x) = \sum_{g \in G} (a_g + b_g) x^g$$

and

$$(a \cdot b)(x) = \sum_{g \in G} \sum_{h \in G} (a_g b_h) x^{g+h}$$

where $a(x) = \sum_{g \in G} a_g x^g$ and $b(x) = \sum_{g \in G} b_g x^g$

The Group Ring - 2

With those definitions it is straight forward to show that $\mathbb{Z}[G]$ is in fact a ring.

Sometimes we replace $\mathbb{Z}$ by $\mathbb{Z}_p$ and will write

$a(x) \equiv b(x) \bmod p \leftrightarrow a_g \equiv b_g \pmod p$ for all $g \in G$.

Some other definitions:

$$a(x^m) = \sum_{g \in G} a_g x^{mg},$$

$$a(x^{-1}) = \sum_{g \in G} a_g x^{-g},$$

$$a(1) = \sum_{g \in G} a_g,$$

$$G(x) = \sum_{g \in G} x^g, \text{ and for any set D of G}$$

$$D(x) = \sum_{g \in D} x^g.$$

Properties of the Group Ring

Lemma A: If D is a (v,k,λ)-difference set in an abelian group, then

$$D(x)D(x^{-1}) = \lambda G(x) + (k-\lambda)x^0.$$

Pf: We have

$$D(x)D(X^{-1}) = \sum_{g,h\in D} x^{g-h}$$

$$= \sum_{d\in G} \alpha_d x^d,$$

where

$$\alpha_d = |\{(g,h)\in D\times D : g-h=d\}|.$$

Clearly

$$\alpha_d = k \text{ if } d=0 \text{ and } \lambda \text{ if } d\neq 0$$

since D is a difference set.

Note similarity with incidence matrix equation.

Properties of the Group Ring -2

Lemma B: If a(x) in $\mathbb{Z}[G]$, then
a(x)G(x) = a(1)G(x).

$$a(x)G(x) = \sum_{g,h \in G} a_g x^{g+h}$$

$$= \sum_{i \in G} \left(\sum_{g \in G} a_g \right) x^i, \text{ where } g+h=i$$

$$= \sum_{i \in G} a(1) x^i$$

$$= a(1)G(x).$$

Properties of Group Rings - 3

Lemma C: If p is a prime and a(x) in $\mathbb{Z}[G]$, then
$(a(x))^p \equiv a(x^p) \pmod p$.

Pf: By induction on the number of non-zero coefficients in a(x). If a(x) ≡ 0 the statement is trivially true. If a(x) has only one non-zero coefficient then $a(x) = a_g x^g$ for some g.

$$(a(x))^p = (a_g x^g)^p = a_g{}^p x^{pg} = a_g (x^p)^g = a(x^p) \text{ in } \mathbb{Z}_p[x]$$

Now assume the result if there are j or fewer non-zero coefficients in a(x) and assume that we have an a(x) with j+1 non-zero coefficients. We can write $a(x) = a_j(x) + a_g x^g$, where $a_j(x)$ has exactly j non-zero coefficients and $a_g \neq 0$.

Properties of Group Rings - 3

Lemma C: If p is a prime and a(x) in $\mathbb{Z}[G]$, then $(a(x))^p \equiv a(x^p) \pmod p$.

Pf:(cont) We now have:

$$
\begin{aligned}
(a(x))^p &= (a_j(x) + a_g x^g)^p \\
&= (a_j(x))^p + \sum_{i=1}^{p-1} \binom{p}{i} (a_j(x))^i (a_g{}^i x^g)^{p-i} + (a_g x^g)^p \\
&\equiv (a_j(x))^p + (a_g x^g)^p \\
&\equiv a_j(x^p) + a_g x^{pg} = a(x^p).
\end{aligned}
$$

Properties of Group Rings - 4

Lemma D: If D is a (v,k,λ)-difference set in an abelian group G, and m is a positive integer with gcd(m,v) = 1, then

$$D(x^m)D(x^{-m}) = \lambda G(x) + (k-\lambda)x^0.$$

The proof is similar to that of Lemma A and is left as an exercise.

Proof of the Multiplier Theorem

Theorem: Let D be a (v,k,λ)-difference set in an abelian group G. If p is prime, gcd(v,p) = 1, p divides k – λ and p > λ, then p is a multiplier of D.

Pf: In $\mathbb{Z}_p[G]$:

$$
\begin{aligned}
D(x^p)\,D(x^{-1}) &= (D(x))^p\,D(x^{-1}) && \text{Lemma C}\\
&= (D(x))^{p-1}\,D(x)\,D(x^{-1})\\
&= (D(x))^{p-1}(\lambda G(x) + (k-\lambda)x^0) && \text{Lemma A}\\
&= \lambda k^{p-1} G(x) + (k-\lambda)(D(x))^{p-1} && \text{Lemma B \& D(1)=k}\\
&= \lambda k^{p-1} G(x)\\
&= \lambda G(x).
\end{aligned}
$$

Let $S(x) = D(x^p)D(x^{-1}) - \lambda G(x)$. We have shown $S(x) \equiv 0 \bmod p$, so all coefficients of S(x) are divisible by p. All the coefficients of $D(x^p)D(x^{-1})$ are non-negative, so the coefficients of S(x) are greater than or equal to -λ. Thus,

Proof of the Multiplier Theorem -2

Theorem: Let D be a (v,k,λ)-difference set in an abelian group G. If p is prime, gcd(v,p) = 1, p divides k – λ and p > λ, then p is a multiplier of D.

Pf:(cont) since p > λ, all coefficients of S(x) are ≥ 0.

$$\begin{aligned} S(x)S(x^{-1}) &= (D(x^p)D(x^{-1}) - \lambda G(x))(D(x^{-p})D(x) - \lambda G(x^{-1})) \\ &= (D(x^p)D(x^{-1}) - \lambda G(x))(D(x^{-p})D(x) - \lambda G(x)) \\ &= D(x^p)D(x^{-p})D(x)D(x^{-1}) + \lambda^2 (G(x))^2 \\ &\quad - \lambda G(x)(D(x^p)D(x^{-1}) + D(x^{-p})D(x)). \end{aligned}$$

Using Lemmas A, B and D and G(1) = v we have:

$$\begin{aligned} D(x^p)D(x^{-p})D(x)D(x^{-1}) &= (\lambda G(x) + (k-\lambda)x^0)^2 \\ &= \lambda^2 (G(x))^2 + 2(k-\lambda)\lambda G(x) + (k-\lambda)^2 x^0 \\ &= \lambda^2 v G(x) + 2(k-\lambda)\lambda G(x) + (k-\lambda)^2 x^0. \end{aligned}$$

Proof of the Multiplier Theorem -3

Theorem: Let D be a (v,k,λ)-difference set in an abelian group G. If p is prime, gcd(v,p) = 1, p divides k – λ and p > λ, then p is a multiplier of D.

Pf:(cont) In a similar vein we compute:

$$\lambda^2(G(x))^2-\lambda G(x)(D(x^p)D(x^{-1})+D(x^{-p})D(x))$$
$$=-2\lambda k^2 G(x)+\lambda^2 v G(x).$$

Combining these results we get:

$$S(x)S(x^{-1})=(\lambda^2 v+2(k-\lambda)\lambda-2\lambda k^2+\lambda^2 v)G(x)+(k-\lambda)^2 x^0$$
$$=(k-\lambda)^2 x^0.$$

Let $$S(x)=\sum_{g\in G} s_g x^g.$$

We have already shown that $s_g \geq 0$ for all g.

Proof of the Multiplier Theorem -4

Theorem: Let D be a (v,k,λ)-difference set in an abelian group G. If p is prime, gcd(v,p) = 1, p divides k – λ and p > λ, then p is a multiplier of D.

Pf:(cont) Suppose that s_g and s_h are positive for $g \neq h$. Then in $S(x)S(x^{-1})$ the coefficient of x^{g-h} would have a positive coefficient, a contradiction. Thus S(x) can only have one non-zero coefficient, say $S(x) = s_g x^g$, and we have

$$S(x)S(x^{-1}) = (s_g x^g)(s_g x^{-g}) = (s_g)^2 x^0.$$

Thus we have $S(x) = (k-\lambda)x^g$ for some g since $s_g \geq 0$.

Hence,

$$D(x^p)D(x^{-1}) = (k - \lambda)x^g + \lambda G(x).$$

So,

$$D(x^p)D(x)D(x^{-1}) = D(x)((k - \lambda)x^g + \lambda G(x)),$$

and using Lemmas A and B, we obtain:

Proof of the Multiplier Theorem -5

Theorem: Let D be a (v,k,λ)-difference set in an abelian group G. If p is prime, gcd(v,p) = 1, p divides $k - \lambda$ and $p > \lambda$, then p is a multiplier of D.

Pf:(cont)

$$D(x^p)(\lambda G(x) + (k-\lambda)x^0) = D(x)(k-\lambda)x^g + \lambda k G(x)$$

$$\lambda k G(x) + (k- \lambda)D(x^p) = D(x)(k-\lambda)x^g + \lambda k G(x)$$

$$(k- \lambda)D(x^p) = D(x)(k-\lambda)x^g$$

$$D(x^p) = x^g D(x).$$

Now, by comparing exponents we see that pD = D + g and so p is a multiplier.

Conjecture

While the condition $p > \lambda$ is used in the proof we have just seen (in an essential way), there is no known example of a prime which satisfies only the other conditions which is not a multiplier.

This has led to the conjecture first enunciated by Marshall Hall, Jr. (1947)

Conj: Given a (v,k,λ) difference set, a prime p, with $(v,p) = 1$ and which divides the order of the difference set is a multiplier of the difference set.

Proved for $n = 2p^r$ (Muzychuk 1998), $n = 3p^r$ (Qiu 2002), and $n = 5p^r$ but with some exceptions (Feng 2008).