Difference Set Transfers

Dylan Peifer[1]
San Diego State University

Summary

Difference sets are subsets of groups with combinatorial properties. Fundamental questions involve determining which groups do or do not contain difference sets, finding all difference sets up to a natural definition of equivalence, and developing techniques to construct and classify difference sets. The tools used to approach these questions generally come from algebra, combinatorics, representation theory, algebraic number theory, and computer programming.

In our 8-week program, we addressed the question of the existence of Hadamard difference sets in groups of order 64, discovered and defined the concept of a difference set transfer, and categorized and explained transfers in groups of order 16.

Definition (Difference Set)

A (v, k, λ)-*difference set* is a subset D of a group G such that

- $|G| = v$
- $|D| = k$
- each nonidentity element $g \in G$, can be represented as a "difference" $g = d_1 d_2^{-1}$ for exactly λ pairs $(d_1, d_2) \in D^2$.

Alternatively, we can work in the group ring $\mathbb{Z}[G]$ of formal sums

$$\sum_{i=1}^{n} c_i \cdot g_i \qquad c_1, ..., c_n \in \mathbb{Z},$$

with addition and multiplication defined naturally. Abusing notation, let

$$G := \sum_{g \in G} g \qquad D := \sum_{d \in D} d \qquad D^{(-1)} := \sum_{d \in D} d^{-1}.$$

Under this notation, the condition for a group ring element D to be a difference set is having coefficients $c_i = 0, 1$ with k coefficients equal to 1 and satisfying the equation

$$DD^{(-1)} = (k - \lambda) \cdot 1_G + \lambda \cdot G$$

for some λ.

Example (Difference Set)

Consider the group $G = C_7 = \langle x \mid x^7 = 1 \rangle$ and the subset $D = \{x, x^2, x^4\}$. Organizing all differences $d_1 d_2^{-1}$ in a table yields

d_1 \ d_2	x	x^2	x^4
x	1	x^6	x^4
x^2	x	1	x^5
x^4	x^3	x^2	1

Each nonidentity element appears once in the table, so we have that D is a (7,3,1)-difference set.

In the group ring viewpoint we have $D = x + x^2 + x^4$, and $D^{(-1)} = x^6 + x^5 + x^3$. Thus

$$\begin{aligned} DD^{(-1)} &= (x + x^2 + x^4)(x^6 + x^5 + x^3) \\ &= (1 + x^6 + x^4) + (x + 1 + x^5) + (x^3 + x^2 + 1) \\ &= 3 + x + x^2 + x^3 + x^4 + x^5 + x^6 \\ &= 2 + G \end{aligned}$$

and again D is a (7,3,1)-difference set.

Definition (Hadamard Difference Set)

A *Hadamard Difference Set* (HDS) is a (v, k, λ)-difference set such that $v = 4(k - \lambda)$. The name Hadamard refers to the fact that the incidence matrix of the associated block design given by a Hadamard difference set is a regular Hadamard matrix. Hadamard difference sets form the largest category of known examples of difference sets.

Theorem (The Hadamard Parameters)

For any (v, k, λ)-HDS, $(v, k, \lambda) = (4m^2, 2m^2 \pm m, m^2 \pm m)$ for some $m \in \mathbb{Z}_{>0}$.

Because $(4m^2, 2m^2 - m, m^2 - m)$-difference sets and $(4m^2, 2m^2 + m, m^2 + m)$-difference sets are complementary, we may consider all Hadamard difference sets as having parameters

$$(v, k, \lambda) = (4m^2, 2m^2 - m, m^2 - m).$$

Motivation - A Strange Result in Groups of Order 64

Our first task involved finding Hadamard difference sets in groups of order 64, which we accomplished using previous results and the computer algebra system GAP. GAP is specifically designed to do computational group theory, and we used it to automate algorithms for finding and constructing difference sets. GAP also has a catalog of all groups of small order. It is convenient to store difference sets in "GAP notation" by specifying the group number in GAP's catalog and the elements that form a difference set from GAP's ordered list of group elements. For example, SmallGroup(64, 12) has the difference set [1, 2, 3, 4, 5, 6, 8, 10, 11, 12, 14, 17, 18, 20, 26, 27, 31, 32, 33, 34, 35, 38, 39, 44, 50, 56, 60, 63] .

In our work, we noticed that many lists of GAP indices forming a difference set in one group would also form a difference set in another group. For example, the above difference set in SmallGroup(64,12) is a difference set in 7 groups of order 64. This is very surprising, as the chance of randomly finding a difference set in a group of order 64 is vanishingly small.

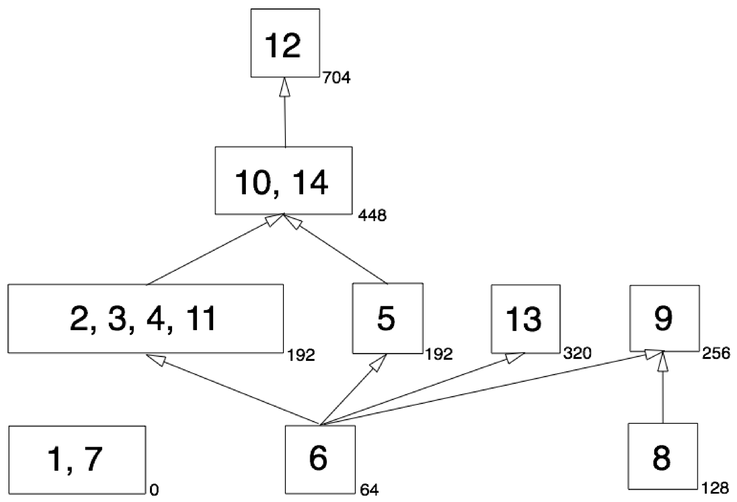
Transfers in Groups of Order 16 Using GAP

Work in order 64 is computationally difficult and complicated by the large number of groups, so we decided to study this strange result in order 16. Our goal was to categorize and explain all cases of shared GAP indices (referred to as transfers) in order 16. Hopefully this would lead to theories and generalizations that could be applied to new existence proofs and construction techniques for other orders.

The following table shows all the places transfers occur in groups of order 16. Each row and column is labeled by GAP's category number for a group of order 16. The number in each entry indicates how many difference sets in the associated row and column groups are the same when expressed as indices in GAP. For comparison, note that Hadamard difference sets in groups of order 16 are subsets of 6 elements, and there are $\binom{16}{6} = 8008$ such subsets in each group.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	192	192	192	64	64	0	64	128	192	192	192	128	192
3	0	192	192	192	64	64	0	64	128	192	192	192	128	192
4	0	192	192	192	64	64	0	64	128	192	192	192	128	192
5	0	64	64	64	192	64	0	0	64	192	64	192	64	192
6	0	64	64	64	64	64	0	0	64	64	64	64	64	64
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	64	64	64	0	0	0	128	128	64	64	64	64	64
9	0	128	128	128	64	64	0	128	256	128	128	128	128	128
10	0	192	192	192	192	64	0	64	128	448	192	448	192	448
11	0	192	192	192	64	64	0	64	128	192	192	192	128	192
12	0	192	192	192	192	64	0	64	128	448	192	704	256	448
13	0	128	128	128	64	64	0	64	128	192	128	256	320	192
14	0	192	192	192	192	64	0	64	128	448	192	448	192	448

We can focus our attention by reducing the above table to the following chart, which indicates when all difference sets in one group correspond to difference sets in another group by way of GAP indices. In the chart, groups are represented by category number in GAP. Groups are placed in the same box if all their difference sets are the same in GAP indices. At the bottom right of each box is the total number of difference sets found in the group or groups, and directed arrows indicate all difference sets in the starting group are also difference sets in the ending group when viewed as GAP indices.



Definition (Power-Commutator Presentation)

Given a group G of order p^n, a *power-commutator presentation* of G consists of a set of generators $\{f_1, f_2, \ldots, f_n\}$ with defining relations $f_i^p = \prod_{k=i+1}^{n} f_k^{\beta(i,k)}$ and $[f_j, f_i] = \prod_{k=j+1}^{n} f_k^{\beta(i,j,k)}$, where the value of β is in $\{1, \ldots, p-1\}$ and $1 \leqslant i < j \leqslant n$.

GAP expresses p-groups in power-commutator presentations for efficient computation purposes, and lists their elements in lexicographical order as words in standard form on the generators. This means that the transfers we noticed are just equivalent sets of words.

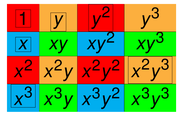
Definition (Difference Set Transfer)

Given two groups G, H of order 2^n and their power commutator presentations on generators $\{g_1, \ldots g_n\}$, $\{h_1, \ldots, h_n\}$, we say a *difference set transfer* exists between G and H when a difference set in G can be mapped to a difference set in H by mapping words on the generators of G to words on the corresponding (same index) generators of H.

Proving Transfers in Order 16 Using the Spread Construction

The spread construction is a standard technique used to build difference sets. It works on groups of order 2^{2s+2} with a normal elementary abelian subgroup of order 2^{s+1}. The construction spreads subgroups of the normal subgroup into cosets of the normal subgroup to form a difference set.

$$G = C_4 \times C_4 = \langle x, y \mid x^4 = y^4 = [x, y] = 1 \rangle$$
$$E = C_2 \times C_2 = \langle x^2, y^2 \rangle = \{1, y^2, x^2, x^2y^2\}$$
$$D = \{1, y^2, x, x^3, y, x^2y^3\}$$



With some supporting lemmas and observations, the following three theorems prove the results we see in the chart for GAP's groups 2, 3, 4, 5, 6, 11, and their attached arrows.

Theorem 1

If $|G| = 16$, we can build 192 difference sets over a normal subgroup $E \cong C_2 \times C_2$ using the spread construction. If this E is in $Z(G)$, the center of G, these are all difference sets.

Theorem 2

Given $|G| = 16$, if for $E \triangleleft G$, $E \cong C_2 \times C_2$, but $E \not\subset Z(G)$ then a spread construction over E generates at least 64 difference sets.

Theorem 3

Let G be a group of order 16 that does not contain a subgroup isomorphic to the quaternion group. If the socle of G has order 4, then every difference set in G can be generated via a spread construction over $soc(G)$.

Other Results

The chart results for GAP's groups 10 and 14 follow from basic algebra and casework. Groups 8 and 9 can be seen to have a quaternion subgroup on the same labeled generators, and their transfers can be proven by examining the interaction of difference sets with this subgroup.

While most of our theorems do not generalize to higher orders, there are still relations to prove and discover. We are convinced by the pervasiveness of difference set transfers in 2-groups that general results exist and can shed light on the study of difference sets.

References

- Chirashree Bhattacharya and Ken W. Smith. "Factoring (16,6,2) Hadamard difference sets". In: *Electron. J. Combin.* 15 (2008).
- James A. Davis and Jonathan Jedwab. "A survey of Hadamard difference sets". In: *Groups, difference sets, and the Monster (Columbus, OH, 1993)*. Vol. 4. Ohio State Univ. Math. Res. Inst. Publ. Berlin: de Gruyter, 1996, pp. 145–156.
- J. F. Dillon. "Variations on a scheme of McFarland for noncyclic difference sets". In: *J. Combin. Theory Ser. A* 40 (1985), pp. 9–21.
- Robert E. Kibler. "A summary of noncyclic difference sets, $k < 20$". In: *J. Combinatorial Theory Ser. A* 25 (1978), pp. 62–67.
- E. A. O'Brien. "The p-group generation algorithm". In: *J. Symbolic Comput.* 9 (1990), pp. 677–698.

[1]Carleton College

Funded by NSF Grant 1061366