Difference Set Transfers
Dylan Peifer
San Diego State University

Summary
Difference sets are subsets of groups with combinatorial properties. Fundamental questions involve identifying 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 \((v,k,l)\)-difference set is a subset \(D\) of a group \(G\) such that
\[
\begin{align*}
|D| &= v, \\
|D^2| &= k, \\
|D^3| &= l.
\end{align*}
\]
Each nonidentity element \(g \in G\) can be represented as a “difference” \(g = d_{ij}^{-1}\) for exactly \(\lambda\) pairs \((d_i, d_j) \in D^2\).

Alternatively, we can work in the group ring \(Z[G]\) of formal sums
\[
\sum_{g \in G} c_g \cdot g, \quad c_g \in Z
\]
with addition and multiplication defined naturally. Abusing notation, let
\[
G = \sum_{g \in G} g, \quad D = \sum_{d \in D} d, \quad D^{-1} = \sum_{d \in D^{-1}} d.
\]
Under this notation, the condition for a group ring element \(D\) to be a difference set is having coefficients \(c_d = 0\) with \(k\) nonidentity elements and satisfying the equation
\[
DD^{-1} - (k - \lambda)I_g = \lambda G
\]
for some \(\lambda\).

Example (Difference Set)
Consider the group \(G = C_7 = \langle x \rangle\) and the subset \(D = \langle x, x^2, x^3\rangle\). Organizing all differences \(d_{ij}^{-1}\) in a table yields
\[
\begin{array}{c|ccc}
\hline
\pm x & x^2 & x^3 \\
\hline
x^2 & x^4 & x^6 \\
x^3 & x^5 & x^7 \\
\pm x & x^2 & x^3 \\
\hline
\end{array}
\]
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 the difference set.

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 (Hadamard Difference Set)
A Hadamard Difference Set (HDS) is a \((v,k,l)\)-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 (Hadamard Parameters)
For any \((v,k,l)\)-HDS, \((v,k,l) = (4m^2, 2m^2, 2m^2 m)\) for some \(m \in \mathbb{Z}^+\).
Because \((4m^2, 2m^2, 2m^2 m)\)-difference sets and \((4m^2, 2m^2, 2m^2 m)\)-difference sets are complementary, we may consider all Hadamard difference sets as having parameters
\[
(v,k,l) = (4m^2, 2m^2 m, 2m^2 m).
\]

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 order 64. 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, SmalGroup(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 SmalGroup(64,12) is a difference set in 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.

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

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 \(E = C_2 \times C_2\) using the spread construction. If this \(E\) is in \(Z(G)\), the center of \(G\), these are all difference sets.

Theorem 2
Given \(\{G = 16\}\) for \(E = G, E \neq G, C_2 \times C_2, B \neq G \in Z(G)\) then a spread construction over \(G\) 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