Investigation of genuinely non-Abelian difference sets in groups of order 676.

Contributed paper at American Math Society central section meeting; Ohio University; Athens, OH; March 26, 2004.

Paul Becker and Jennifer Mendes Ulrich

Penn State Erie, The Behrend College
\[(v, k, \lambda)\text{ difference set}\]

A \((v, k, \lambda)\) difference set is a polynomial, \(\Delta \in \mathbb{Z}G\) satisfying:

\[
\Delta \Delta^{(-1)} = (k - \lambda)I + \lambda G.
\]

Parameters of \((v, k, \lambda)\) symmetric designs:

- \(v\) = order of group \(G\);
- \(k\) = weight of polynomial;
- \(\lambda\) = number of copies of group produced in \(\Delta \Delta^{(-1)}\).

Example: a \((11, 5, 2)\) difference set in \(\mathbb{Z} \mathbb{Z}_{11}\).

\[
\Delta = x + x^3 + x^4 + x^5 + x^9
\]

The development of \(\Delta\) in \(\mathbb{Z}_{11}\) is a symmetric design.

\(\mathbb{Z}_{11}\) is a point-regular automorphism group of that design. (See appendix (c) for definitions.)
Genuinely non-Abelian difference sets

A difference set in a group $G$ is non-Abelian if $G$ is non-Abelian.

A difference set is genuinely non-Abelian if its development (design) does not admit any Abelian point-regular automorphism group.

Only known genuinely non-Abelian difference sets are Menon-Hadamard:

$$(4u^2, 2u^2 + u, u^2 - u) \; ; \; u = \text{a multiple of 2, 3, or 5}.$$ 

Examples:

- $(100, 45, 20)$ [Smith, 1995];
- $(100, 45, 20)$ [Golemac and Vucicic, 2001].

Theorem [McFarland, 1989]:
If $p > 3$ is prime, then any $(4p^2, 2p^2 - p, p^2 - p)$ difference set is genuinely non-Abelian.

Theorem [Iiams, 1995]:
Suppose $p > 3$ is a prime and $G$ contains a $(4p^2, 2p^2 - p, p^2 - p)$ difference set. $G$ must be one of five specific non-Abelian groups (or six groups if $p \equiv 1 \mod 4$).

Our focus:
Search for Menon-Hadamard $(676, 325, 156)$ difference sets; $(p = 13)$. 
Quotient Images

\[ G \xrightarrow{\pi} G/N \]
\[ \mathbb{Z}G \xrightarrow{\Pi} \mathbb{Z}(G/N) \]

If \( \Delta \in \mathbb{Z}G \) is a difference set, \( \delta = \Pi(\Delta) \) is a quotient image.

Theorem:
If \( \Delta \in \mathbb{Z}G \) satisfies \( \Delta \Delta^{(-1)} = (\kappa - \lambda)I + \lambda G \), then \( \delta \in \mathbb{Z}(G/N) \) satisfies \( \delta\delta^{(-1)} = (\kappa - \lambda)I + \lambda|N|(G/N) \).

Complementary quotient images

If \( G \cong N \times H \) then \( \delta_H \in G/N \) and \( \delta_N \in G/H \) are complementary.

If \( G \cong N \rtimes H \) then \( \delta_H \in G/N \) and \( \delta_N' \in G/core(H) \) are complementary.

General Principle:
Cross-referencing of complementary quotient images frequently identifies difference sets (or quotient images in larger groups).
**Possible groups [Iiams]**

Groups which might admit \((4p^2, 2p^2 - p, p^2 - p)\) difference sets

\[< x, y \mid x^p = y^p = 1, x y = y x > \times < z \mid z^4 = 1 >\]

<table>
<thead>
<tr>
<th>Group</th>
<th>(zxz^{-1})</th>
<th>(zyz^{-1})</th>
<th>Normal (N)</th>
<th>Quotient (H)</th>
<th>Comp. Quotient (G/Core(H))</th>
</tr>
</thead>
<tbody>
<tr>
<td>(G_{11})</td>
<td>(x)</td>
<td>(y^{-1})</td>
<td>(\langle y \rangle \cong \mathbb{Z}_p)</td>
<td>(\langle x, z \rangle \cong \mathbb{Z}_{4p})</td>
<td>(G_{11}/\langle x, z^2 \rangle \cong D_{2p})</td>
</tr>
<tr>
<td>(G_{13})</td>
<td>(y^{-1})</td>
<td>(x)</td>
<td>(N \cong \mathbb{Z}_p)</td>
<td>(H \cong F_{p^4})</td>
<td>(G_{13}/\text{core}(H) \cong F_{p^4})</td>
</tr>
<tr>
<td>(G_{14})</td>
<td>(x)</td>
<td>(y^f)</td>
<td>(\langle y \rangle \cong \mathbb{Z}_p)</td>
<td>(\langle x, z \rangle \cong \mathbb{Z}_{4p})</td>
<td>(G_{14}/\langle x \rangle \cong F_{p^4})</td>
</tr>
<tr>
<td>(G_{15})</td>
<td>(x^{-1})</td>
<td>(y^f)</td>
<td>(\langle x \rangle \cong \mathbb{Z}_p)</td>
<td>(\langle y, z \rangle \cong F_{p^4})</td>
<td>(G_{15}/\langle y, z^2 \rangle \cong D_{2p})</td>
</tr>
<tr>
<td>(G_{16})</td>
<td>(x^f)</td>
<td>(y^f)</td>
<td>(\langle x \rangle \cong \mathbb{Z}_p)</td>
<td>(\langle y, z \rangle \cong F_{p^4})</td>
<td>(G_{16}/\langle y \rangle \cong F_{p^4})</td>
</tr>
</tbody>
</table>

\((f^2 \equiv -1 \mod p^2)\)

Each group above can be viewed as:

\[G \cong \langle a \mid a^p = 1 \rangle \times \langle b, c \mid b^p = c^4 = 1 \rangle \]

\[\cong \mathbb{Z}_p \times F_{p^4}\]

If \(p \equiv 1 \mod 4\), we also have:

\[G_4 \cong \langle x, z \mid x^{p^2} = z^4 = 1; zxz^{-1} = x^f \rangle\]

\[G_4/\langle x^p \rangle \cong F_{p^4}\]
Results for \( p = 13 \).

Proposition [Iiams]:
The groups \( \mathbb{Z}_{2p} \) and \( D_{2p} \) admit specific (known) quotient images.

Proposition [Mendes]:
If \( p = 13 \), then \( \mathbb{Z}_{4p} \) does not admit a \((4p^2, 2p^2 - p, p^2 - p)\) quotient image. Consequently, groups \( G_{11} \) and \( G_{14} \) do not contain M-H difference sets when \( p = 13 \).

\textit{proof}:
Correlation of complementary quotient images.

Known examples:
Groups \( G_{13} \) and \( G_{15} \) are known to contain difference sets when \( p = 5 \).

<table>
<thead>
<tr>
<th>Group</th>
<th>( zxz^{-1} )</th>
<th>( zyz^{-1} )</th>
<th>Normal (N)</th>
<th>Quotient (H)</th>
<th>Comp. Quotient (G/Core(H))</th>
</tr>
</thead>
<tbody>
<tr>
<td>( G_{11} )</td>
<td>( x )</td>
<td>( y^{-1} )</td>
<td>( \langle y \rangle \cong \mathbb{Z}_p )</td>
<td>( \langle x, z \rangle \cong \mathbb{Z}_{4p} )</td>
<td>( G_{11}/\langle x, z^2 \rangle \cong D_{2p} )</td>
</tr>
<tr>
<td>( G_{13} )</td>
<td>( y^{-1} )</td>
<td>( x )</td>
<td>( \langle x^3y^2 \rangle \cong \mathbb{Z}_p )</td>
<td>( \langle x^3y^{-2}, z \rangle \cong F_{p,4} )</td>
<td>( G_{13}/\langle x^3y^{-2} \rangle \cong F_{p,4} )</td>
</tr>
<tr>
<td>( G_{14} )</td>
<td>( x )</td>
<td>( y^f )</td>
<td>( \langle y \rangle \cong \mathbb{Z}_p )</td>
<td>( \langle x, z \rangle \cong \mathbb{Z}_{4p} )</td>
<td>( G_{14}/\langle x \rangle \cong F_{p,4} )</td>
</tr>
<tr>
<td>( G_{15} )</td>
<td>( x^{-1} )</td>
<td>( y^f )</td>
<td>( \langle x \rangle \cong \mathbb{Z}_p )</td>
<td>( \langle y, z \rangle \cong F_{p,4} )</td>
<td>( G_{15}/\langle y, z^2 \rangle \cong D_{2p} )</td>
</tr>
<tr>
<td>( G_{16} )</td>
<td>( x^f )</td>
<td>( y^f )</td>
<td>( \langle x \rangle \cong \mathbb{Z}_p )</td>
<td>( \langle y, z \rangle \cong F_{p,4} )</td>
<td>( G_{16}/\langle y \rangle \cong F_{p,4} )</td>
</tr>
</tbody>
</table>

\[ G_4 \cong \langle x, z \mid x^{p^2} = z^4 = 1; zxz^{-1} = x^f \rangle \]
\[ G_4/\langle x^p \rangle \cong F_{p,4} \]
Difference sets in semidirect product groups

\[ F_{p,4} \cong \langle x, z \mid x^p = z^4 = 1; zxz^{-1} = x^f \mod p \rangle \]
\[ \cong \langle x \mid x^p = 1 \rangle \times \langle z \mid z^4 = 1 \rangle \]
\[ \cong N \rtimes \mathbb{Z}_4 \]

\( F_{p,4} \) admits only one non-trivial quotient: \( \mathbb{Z}_4 \).
The quotient group has a trivial core.

<table>
<thead>
<tr>
<th>(&lt; x &gt;)</th>
<th>(z &lt; x &gt;)</th>
<th>(z^2 &lt; x &gt;)</th>
<th>(z^3 &lt; x &gt;)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(X_{0,0})</td>
<td>(X_{1,0})</td>
<td>(X_{2,0})</td>
<td>(X_{3,0})</td>
</tr>
<tr>
<td>(X_{0,1})</td>
<td>(X_{1,1})</td>
<td>(X_{2,1})</td>
<td>(X_{3,1})</td>
</tr>
<tr>
<td>(\vdots)</td>
<td>(\vdots)</td>
<td>(\vdots)</td>
<td>(\vdots)</td>
</tr>
<tr>
<td>(X_{0,12})</td>
<td>(X_{1,12})</td>
<td>(X_{2,12})</td>
<td>(X_{3,12})</td>
</tr>
<tr>
<td>91</td>
<td>78</td>
<td>78</td>
<td>78</td>
</tr>
<tr>
<td>87</td>
<td>84</td>
<td>82</td>
<td>72</td>
</tr>
</tbody>
</table>

If \( G = N \times H \), then quotient images provide row- and column-sums. The correlation of these quotient images allow determination of the coefficients \(X_{i,j}\). If \( G = N \rtimes H \), we may still assume column sums are known from the quotient image \( G/N \). Row sums, however, will not be known. In some cases, complementary quotient images (in \( G/core(\langle H \rangle) \)) give partial information about row sums.

When complementary quotient images are unavailable or insufficient, we use a different approach. View the columns as polynomials with known weight (sum of coefficients). We call these polynomials \textit{stripes}:

\[ X_0 = \sum_{i=0}^{3} (X_{0,i}) \cdot x^i \]
\[ X_1 = \sum_{i=0}^{3} (X_{1,i}) \cdot x^i \]
\[ X_2 = \sum_{i=0}^{3} (X_{2,i}) \cdot x^i \]
\[ X_3 = \sum_{i=0}^{3} (X_{3,i}) \cdot x^i \]
Stripe approach to semidirect difference sets

Assume that $\Delta \in \mathbb{Z} (N \rtimes \mathbb{Z}_r)$ is a $(v, k, \lambda)$ quotient image with index $s$:

$$\Delta = \sum_{i=0}^{r-1} X_i \cdot z^i$$

$$\Delta \Delta^{(-1)} = \sum_{i=0}^{r-1} \sum_{j=0}^{r-1} (X_i z^i) (X_j z^j)^{(-1)}$$

$$= \sum_{i=0}^{r-1} \sum_{j=0}^{r-1} X_i z^{i-j} X_j^{(-1)}$$

$$= \sum_{i=0}^{r-1} \sum_{j=0}^{r-1} X_i (X_j^{(-1)})^{z_{i-j}} z^{i-j}$$

$$= (k - \lambda) + \lambda(s) \sum_{i-j=0}^{r-1} N \cdot z^{i-j}$$

Definition:
For $m = 0 \ldots (r - 1)$, define $\alpha_m : N \rightarrow N$ by

$$\alpha_m(x) = z^{-m}(x^{(-1)}) z^m = (x^{(-1)})^{z^{-m}} = (x^{z^{-m}})^{(-1)}.$$

Proposition:
$\Delta$ is a quotient image with index $s$ in $N \rtimes \mathbb{Z}_r$ if and only if

$$\sum_{i=0}^{r-1} X_i \cdot \alpha_m (X_{i+m}) = \begin{cases} (k - \lambda) + \lambda s N & \text{when } m = 0 \\ \lambda s N & \text{when } m > 0 \end{cases}$$
Conclusions from striped quotient images

Suppose $\alpha_m(X_j) = X_j^{(-1)}$ for each $j, m$:

$$\Delta \Delta^{(-1)} = \sum_m \sum_i X_i \cdot \alpha_m (X_{i+m}) z^m$$

$$\Delta \Delta^{(-1)} = \sum_m \sum_i X_i \cdot (X_{i+m})^{(-1)} z^m$$

$$\Delta \Delta^{(-1)} = (k - \lambda) + \lambda(s) (N \times \mathbb{Z}_r).$$

Now define $D \in \mathbb{Z}(N \times \mathbb{Z}_r)$ by

$$D = \sum_{i=0}^{r-1} X_i \cdot w^i.$$

$$DD^{(-1)} = \sum_m \sum_i X_i \cdot (X_{i+m})^{(-1)} w^m$$

$$DD^{(-1)} = (k - \lambda) + \lambda(s) (N \times \mathbb{Z}_r)$$

Conclusions:

1. The combination of stripes and complementary quotients is effective.

2. Extraneous multipliers of abelian difference sets may indicate semidirect difference sets.

3. If a quotient image exists in a semidirect product, and the stripes of the difference set are fixed by $\alpha_1$, then an analogous quotient image exists in a direct product.

References

Overheads available: http://vortex.bd.psu.edu/~peb8/

A. Golemac and Tanja Vucicic,
New Difference Sets in Nonabelian Groups of Order 100,
Journal of Combinatorial Designs, 9, no. 6, pp. 424 - 434.

E. Moore and H. Pollatsek,
Looking for Difference Sets in Groups with Dihedral Images,

K. Smith,
Nonabelian Hadamard difference sets,

Xiao Hong Wu,
Difference Sets: Extraneous Multipliers and Abelianization
(AMS, 3/26/04 : b)

(v, k, λ) symmetric design

<table>
<thead>
<tr>
<th></th>
<th>e</th>
<th>x</th>
<th>x^2</th>
<th>x^3</th>
<th>x^4</th>
<th>x^5</th>
<th>x^6</th>
<th>x^7</th>
<th>x^8</th>
<th>x^9</th>
<th>x^{10}</th>
</tr>
</thead>
<tbody>
<tr>
<td>e</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>x</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>x^2</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>x^3</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>x^4</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>x^5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>x^6</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>x^7</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>x^8</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>x^9</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>x^{10}</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Parameters of (v, k, λ) symmetric designs:

v = number of rows/columns;

k = weight of each row;

λ = intersections between each pair of rows.

Matrix equation: \( MM^T = (k - \lambda)I + \lambda J \)
Automorphism groups of symmetric design

<table>
<thead>
<tr>
<th></th>
<th>$e$</th>
<th>$x$</th>
<th>$x^2$</th>
<th>$x^3$</th>
<th>$x^4$</th>
<th>$x^5$</th>
<th>$x^6$</th>
<th>$x^7$</th>
<th>$x^8$</th>
<th>$x^9$</th>
<th>$x^{10}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$e\delta$</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$x\delta$</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>$x^2\delta$</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$x^3\delta$</td>
<td>0</td>
<td>1</td>
<td>0</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>
</tr>
<tr>
<td>$x^4\delta$</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$x^5\delta$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>$x^6\delta$</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$x^7\delta$</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>$x^8\delta$</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>$x^9\delta$</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>$x^{10}\delta$</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Definition:
An automorphism of a design is a permutation of the point set (column set) which preserves the block set (row set).

Definition:
An automorphism group, $G$, of a design is point-regular if, for every pair $(p, q)$ of points, there is a unique $g \in G$ which maps $p$ to $q$.

Example:
The group $\{f_m : m = 0..10\} \cong \mathbb{Z}_{11}$, where $f_m : x \to x^{1+m}$ is a point-regular automorphism group of this design.
Proposition [Dillon]:
If a difference set exists in $D_{2p}$ then an analogous difference set exists in $\mathbb{Z}_{2p}$.

Note that, in a dihedral group, there are only two stripes.

Moreover, $\sum_i X_i \cdot \alpha_1(X_{i+1}) = \sum_i X_i \cdot (X_{i+1})^{-1}$.

Definition:
A weak multiplier of a difference set $\Delta$ is an integer $m$ such that $\Delta^m = \Delta$.

Corollary to conclusion in slide 9:
Assume $f^2 \equiv -1 \mod p^2$. A $(v, k, \lambda)$ difference set (quotient image) admitting weak multiplier $f$ exists in $F_{p,4}$ if and only if a difference set admitting multiplier $f$ exists in $\mathbb{Z}_{4p}$.