An Algorithm for Enumerating Difference Sets

Dylan Peifer

Cornell University

14 October 2017

Difference Sets

Definition

A $\langle v, k, \lambda \rangle$-difference set is a proper subset D of a group G such that $|G| = v$, $|D| = k$, and each nonidentity element $g \in G$, can be represented as a "difference" $g = d_1 d_2^{-1}$ for exactly λ pairs $(d_1, d_2) \in D^2$.

Difference Sets

Definition

A $\langle v, k, \lambda \rangle$-difference set is a proper subset D of a group G such that $|G| = v$, $|D| = k$, and each nonidentity element $g \in G$, can be represented as a "difference" $g = d_1 d_2^{-1}$ for exactly λ pairs $(d_1, d_2) \in D^2$.

Example

$G = \langle x \mid x^7 = 1 \rangle$, $D = \{x, x^2, x^4\}$.

	x	x^2	x^4
x	1	x^6	x^4
x^2	x	1	x^5
x^4	x^3	x^2	1

D is a $\langle 7, 3, 1 \rangle$-difference set.

Difference Sets

Example

$D = \{1, x, x^3\}$ is a $\langle 7, 3, 1\rangle$-difference set in $G = \langle x \mid x^7 = 1\rangle$.

	1	x	x^3
1	1	x^6	x^4
x	x	1	x^5
x^3	x^3	x^2	1

Difference Sets

Example

$D = \{1, x, x^3\}$ *is a* $\langle 7, 3, 1 \rangle$*-difference set in* $G = \langle x \mid x^7 = 1 \rangle$.

	1	x	x^3
1	1	x^6	x^4
x	x	1	x^5
x^3	x^3	x^2	1

Example

$D = \{x, x^2, x^3\}$ *is not a difference set in* $G = \langle x \mid x^7 = 1 \rangle$.

	x	x^2	x^3
x	1	x^6	x^5
x^2	x	1	x^6
x^3	x^2	x	1

Some Quick Lemmas

Lemma

Every one element subset of any group is a difference set.

Some Quick Lemmas

Lemma

Every one element subset of any group is a difference set.

Lemma

The complement of a difference set is a difference set.

Some Quick Lemmas

Lemma

Every one element subset of any group is a difference set.

Lemma

The complement of a difference set is a difference set.

Lemma

If $D \subset G$ is a difference set then

$$gD = \{gd \mid d \in D\}$$

and

$$\phi(D) = \{\phi(d) \mid d \in D\}$$

are both difference sets for any $g \in G$ and any $\phi \in \mathrm{Aut}(G)$.

Equivalent Difference Sets

Because of the first two lemmas, we typically only consider difference sets with $2 \leq k \leq \frac{v}{2}$, which means we ignore trivial one element sets and always choose the smaller of any complementary pair. In addition, the last lemma gives a notion of equivalence.

Definition

Two difference sets D_1, D_2 in a group G are equivalent if

$$D_1 = g\phi(D_2) = \{g\phi(d) \mid d \in D_2\}$$

for some $g \in G$ and $\phi \in \mathrm{Aut}(G)$.

Example

$D_1 = \{x, x^2, x^4\}$ and $D_2 = \{1, x, x^3\}$ are equivalent difference sets in $G = \langle x \mid x^7 = 1 \rangle$, since $D_1 = xD_2$.

Natural Questions

Question

Let G be a group. Does G contain a difference set?

Question

Let G be a group. How many difference sets does G contain up to equivalence? Can we produce a collection of representatives for the equivalence classes?

Natural Questions

Question

Let G be a group. Does G contain a difference set?

Question

Let G be a group. How many difference sets does G contain up to equivalence? Can we produce a collection of representatives for the equivalence classes?

While the first question can be addressed with theorems about nonexistence or constructions that produce difference sets, fully answering the second question will require some level of exhaustive search.

Exhaustive Search

Groups of order $4m^2$ contain Hadamard difference sets, which have parameters $\langle 4m^2, 2m^2 - m, m^2 - m \rangle$. Many Hadamard difference sets exist, and they provide a useful target for computation.

Exhaustive Search

Groups of order $4m^2$ contain Hadamard difference sets, which have parameters $\langle 4m^2, 2m^2 - m, m^2 - m \rangle$. Many Hadamard difference sets exist, and they provide a useful target for computation.

The first nontrivial Hadamard difference sets occur in groups of order 16. On my computer I can do a brute force search of all groups of order 16 in 3.2 seconds. This gives very rough approximations for the next two cases of

order	subsets to check	time/group	total time
16	$\binom{16}{6} = 8.0 \times 10^3$	0.21 seconds	3.2 seconds

Exhaustive Search

Groups of order $4m^2$ contain Hadamard difference sets, which have parameters $\langle 4m^2, 2m^2 - m, m^2 - m \rangle$. Many Hadamard difference sets exist, and they provide a useful target for computation.

The first nontrivial Hadamard difference sets occur in groups of order 16. On my computer I can do a brute force search of all groups of order 16 in 3.2 seconds. This gives very rough approximations for the next two cases of

order	subsets to check	time/group	total time
16	$\binom{16}{6} = 8.0 \times 10^3$	0.21 seconds	3.2 seconds
36	$\binom{36}{15} = 5.6 \times 10^9$	1.8 days	3.7 weeks

Exhaustive Search

Groups of order $4m^2$ contain Hadamard difference sets, which have parameters $\langle 4m^2, 2m^2 - m, m^2 - m \rangle$. Many Hadamard difference sets exist, and they provide a useful target for computation.

The first nontrivial Hadamard difference sets occur in groups of order 16. On my computer I can do a brute force search of all groups of order 16 in 3.2 seconds. This gives very rough approximations for the next two cases of

order	subsets to check	time/group	total time
16	$\binom{16}{6} = 8.0 \times 10^3$	0.21 seconds	3.2 seconds
36	$\binom{36}{15} = 5.6 \times 10^9$	1.8 days	3.7 weeks
64	$\binom{64}{28} = 1.1 \times 10^{18}$	1.0 million years	270 million years.

Doing Better - Better Notation

It is sometimes useful to think of D as an element of the group ring $\mathbb{Z}[G] = \{\sum_{g\in G} c_g g \mid c_g \in \mathbb{Z}\}$. We will abuse notation to write

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

and then the statement that D is a difference set is equivalent to the equation

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

where D is a group ring element with coefficients in $\{0,1\}$. The 1_G is sometimes dropped so that isolated coefficients are assumed to be coefficients of the identity element. This notation compactly and algebraically expresses the definition of a difference set.

Doing Better - Better Notation

Example

Recall that $D = \{x, x^2, x^4\}$ *is a* $\langle 7, 3, 1\rangle$*-difference set in* $G = \langle x \mid x^7 = 1\rangle$.

	x	x^2	x^4
x	1	x^6	x^4
x^2	x	1	x^5
x^4	x^3	x^2	1

This can also be shown as

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

Doing Better - Basic Idea

Lemma

Suppose D is a difference set in G and θ is a homomorphism of G with $|\ker(\theta)| = w$. Let $S = \theta(D)$ and $H = \theta(G)$. Then

$$SS^{(-1)} = (k - \lambda) + \lambda wH.$$

Proof.

Since D is a difference set we have $DD^{(-1)} = (k - \lambda) + \lambda G$. Applying θ on the left yields

$$\theta(DD^{(-1)}) = \theta(D)\theta(D)^{(-1)} = SS^{(-1)}$$

while applying θ on the right yields

$$\theta((k - \lambda) + \lambda G) = (k - \lambda) + \lambda\theta(G) = (k - \lambda) + \lambda wH.$$

□

Difference Sums

Definition

Given a finite group G and normal subgroup N, a $\langle v, k, \lambda \rangle$-difference sum is an element S of $\mathbb{Z}[G/N]$ such that $SS^{(-1)} = (k - \lambda) + \lambda |N| G/N$ and the coefficients of S have values in $\{0, 1, \ldots, |N|\}$.

Lemma

Suppose G is a finite group with normal subgroup N. Then any difference set in $\mathbb{Z}[G]$ induces a difference sum in $\mathbb{Z}[G/N]$ by taking its image under the natural map $G \to G/N$.

Difference Sums

Definition

Given a finite group G and normal subgroup N, a $\langle v, k, \lambda\rangle$-difference sum is an element S of $\mathbb{Z}[G/N]$ such that $SS^{(-1)} = (k - \lambda) + \lambda|N|G/N$ and the coefficients of S have values in $\{0, 1, \ldots, |N|\}$.

Lemma

Suppose G is a finite group with normal subgroup N. Then any difference set in $\mathbb{Z}[G]$ induces a difference sum in $\mathbb{Z}[G/N]$ by taking its image under the natural map $G \to G/N$.

Difference sums (or similar types of objects) are sometimes referred to as intersection numbers, signatures, or difference lists.

Difference Sets Induce Difference Sums

Let G be group with $\langle 16, 6, 2\rangle$-difference set D and normal subgroup N of order 2. D induces a difference sum in $\mathbb{Z}[G/N]$.

<table>
<tr><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>1</td><td>1</td><td>0</td><td>1</td><td>0</td><td>1</td><td>0</td><td>G</td></tr>
<tr><td colspan="2">2</td><td colspan="2">0</td><td colspan="2">0</td><td colspan="2">0</td><td colspan="2">1</td><td colspan="2">1</td><td colspan="2">1</td><td colspan="2">1</td><td>G/N</td></tr>
</table>

Every difference set induces a difference sum, so the only place to look for difference sets is preimages of difference sums. Note that this difference sum has 16 possible preimages in $\mathbb{Z}[G]$. If there are few elements of $\mathbb{Z}[G/N]$ that pass the test for being a difference sum then searching only their preimages could be much easier than searching all subsets of G.

More Difference Sums

Lemma

Suppose G is a finite group with normal subgroups N_1, N_2 such that $N_2 \subseteq N_1$. Then any difference sum in G/N_2 induces a difference sum in G/N_1.

More Difference Sums

Lemma

Suppose G is a finite group with normal subgroups N_1, N_2 such that $N_2 \subseteq N_1$. Then any difference sum in G/N_2 induces a difference sum in G/N_1.

This means that if we have a series of normal subgroups

$$G = N_1 \triangleright N_2 \triangleright \cdots \triangleright N_n = \{1\}$$

where each N_i is normal in G then a difference set induces difference sums in each of the $\mathbb{Z}[G/N_i]$, and these further induced difference sums can also be viewed as induced by the previous difference sums.

Difference Sums Induce Difference Sums

Let G be group with $\langle 16, 6, 2 \rangle$-difference set D and normal series

$$G = N_1 \rhd N_2 \rhd N_3 \rhd N_4 \rhd N_5 = \{1\}$$

D induces difference sums in the $\mathbb{Z}[G/N_i]$.

<table>
<tr><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>1</td><td>1</td><td>0</td><td>1</td><td>0</td><td>1</td><td>0</td><td>G/N_5</td></tr>
<tr><td colspan="2">2</td><td colspan="2">0</td><td colspan="2">0</td><td colspan="2">0</td><td colspan="2">1</td><td colspan="2">1</td><td colspan="2">1</td><td colspan="2">1</td><td>G/N_4</td></tr>
<tr><td colspan="4">2</td><td colspan="4">0</td><td colspan="4">2</td><td colspan="4">2</td><td>G/N_3</td></tr>
<tr><td colspan="8">2</td><td colspan="8">4</td><td>G/N_2</td></tr>
<tr><td colspan="16">6</td><td>G/N_1</td></tr>
</table>

The difference sum in $\mathbb{Z}[G/N_1]$ will always be 6 for any $\langle 16, 6, 2 \rangle$-difference set in G, since the size of the set is 6. The idea is to reverse this process, starting with 6 and refining upwards.

Equivalent Difference Sums

We only care about difference sets up to equivalence. We can define a corresponding equivalence of difference sums.

Definition

Let S_1 and S_2 be difference sums in $\mathbb{Z}[G/N]$. Then S_1 is equivalent to S_2 if $S_1 = g\phi(S_2)$ where $g \in G/N$ and ϕ is an automorphism of G/N induced by an automorphism of G.

Lemma

Suppose S_1, S_2 are equivalent difference sums in $\mathbb{Z}[G/N]$. Then if D_1 is any difference set in G that induces S_1, there exists a difference set D_2 that induces S_2 such that D_1 and D_2 are equivalent.

The Algorithm

1. Starting with a given group G, we first compute a list of possible k values and a chief series (maximal length normal series) $\{N_i\}$ of G. Each value of k will be handled separately.
2. The algorithm starts at $G/G = \{1\}$, where the only difference sum is k, the size of the desired difference set.
3. Then we proceed up a sequence of larger and larger quotient groups G/N_i. For each i we
   (a) enumerate preimages of our current difference sums and filter out non-difference sums,
   (b) remove all but one representative of each equivalence class.
4. At the final stage we enumerate difference sets and filter and remove as before.

The Algorithm - Example

Let $G = \texttt{SmallGroup(16, 5)}$. The only possible size of a difference set is 6 and G has a chief series

$$G = N_1 \triangleright N_2 \triangleright N_3 \triangleright N_4 \triangleright N_5 = \{1\}$$

with $|N_i| = 2^{5-i}$.

The Algorithm - Example

Let $G =$ `SmallGroup(16, 5)`. The only possible size of a difference set is 6 and G has a chief series

$$G = N_1 \triangleright N_2 \triangleright N_3 \triangleright N_4 \triangleright N_5 = \{1\}$$

with $|N_i| = 2^{5-i}$.

Difference Sums:

[6]

The Algorithm - Example

Let $G =$ `SmallGroup(16, 5)`. The only possible size of a difference set is 6 and G has a chief series

$$G = N_1 \rhd N_2 \rhd N_3 \rhd N_4 \rhd N_5 = \{1\}$$

with $|N_i| = 2^{5-i}$.

Difference Sums:

[0, 6], [1, 5], [2, 4], [3, 3], [4, 2], [5, 1], [6, 0]

The Algorithm - Example

Let $G = \texttt{SmallGroup(16, 5)}$. The only possible size of a difference set is 6 and G has a chief series

$$G = N_1 \triangleright N_2 \triangleright N_3 \triangleright N_4 \triangleright N_5 = \{1\}$$

with $|N_i| = 2^{5-i}$.

Difference Sums:

[0, 6], [1, 5], [2, 4], [3, 3], [4, 2], [5, 1], [6, 0]

The Algorithm - Example

Let $G = \texttt{SmallGroup(16, 5)}$. The only possible size of a difference set is 6 and G has a chief series

$$G = N_1 \triangleright N_2 \triangleright N_3 \triangleright N_4 \triangleright N_5 = \{1\}$$

with $|N_i| = 2^{5-i}$.

Difference Sums:

[2, 4], [4, 2]

The Algorithm - Example

Let $G =$ `SmallGroup(16, 5)`. The only possible size of a difference set is 6 and G has a chief series

$$G = N_1 \triangleright N_2 \triangleright N_3 \triangleright N_4 \triangleright N_5 = \{1\}$$

with $|N_i| = 2^{5-i}$.

Difference Sums:

[4, 2]

The Algorithm - Example

Let $G = \texttt{SmallGroup(16, 5)}$. The only possible size of a difference set is 6 and G has a chief series

$$G = N_1 \triangleright N_2 \triangleright N_3 \triangleright N_4 \triangleright N_5 = \{1\}$$

with $|N_i| = 2^{5-i}$.

Difference Sums:

[0, 4, 0, 2], [1, 3, 0, 2], [2, 2, 0, 2], [3, 1, 0, 2], [4, 0, 0, 2], [0, 4, 1, 1], [1, 3, 1, 1], [2, 2, 1, 1], [3, 1, 1, 1], [4, 0, 1, 1], [0, 4, 2, 0], [1, 3, 2, 0], [2, 2, 2, 0], [3, 1, 2, 0], [4, 0, 2, 0]

The Algorithm - Example

Let $G =$ `SmallGroup(16, 5)`. The only possible size of a difference set is 6 and G has a chief series

$$G = N_1 \triangleright N_2 \triangleright N_3 \triangleright N_4 \triangleright N_5 = \{1\}$$

with $|N_i| = 2^{5-i}$.

Difference Sums:

[0, 4, 0, 2], [1, 3, 0, 2], [2, 2, 0, 2], [3, 1, 0, 2], [4, 0, 0, 2], [0, 4, 1, 1], [1, 3, 1, 1], [2, 2, 1, 1], [3, 1, 1, 1], [4, 0, 1, 1], [0, 4, 2, 0], [1, 3, 2, 0], [2, 2, 2, 0], [3, 1, 2, 0], [4, 0, 2, 0]

The Algorithm - Example

Let $G = \texttt{SmallGroup(16, 5)}$. The only possible size of a difference set is 6 and G has a chief series

$$G = N_1 \triangleright N_2 \triangleright N_3 \triangleright N_4 \triangleright N_5 = \{1\}$$

with $|N_i| = 2^{5-i}$.

Difference Sums:

[2, 2, 0, 2], [1, 3, 1, 1], [3, 1, 1, 1], [2, 2, 2, 0]

The Algorithm - Example

Let $G = \texttt{SmallGroup(16, 5)}$. The only possible size of a difference set is 6 and G has a chief series

$$G = N_1 \triangleright N_2 \triangleright N_3 \triangleright N_4 \triangleright N_5 = \{1\}$$

with $|N_i| = 2^{5-i}$.

Difference Sums:

[3, 1, 1, 1], [2, 2, 2, 0]

The Algorithm - Example

Let $G = \texttt{SmallGroup(16, 5)}$. The only possible size of a difference set is 6 and G has a chief series

$$G = N_1 \rhd N_2 \rhd N_3 \rhd N_4 \rhd N_5 = \{1\}$$

with $|N_i| = 2^{5-i}$.

Difference Sums:

[0, 3, 1, 0, 1, 0, 1, 0], [1, 2, 1, 0, 1, 0, 1, 0], [2, 1, 1, 0, 1, 0, 1, 0], [3, 0, 1, 0, 1, 0, 1, 0], [0, 3, 0, 1, 1, 0, 1, 0], [1, 2, 0, 1, 1, 0, 1, 0], [2, 1, 0, 1, 1, 0, 1, 0], [3, 0, 0, 1, 1, 0, 1, 0], [0, 3, 1, 0, 0, 1, 1, 0], [1, 2, 1, 0, 0, 1, 1, 0], [2, 1, 1, 0, 0, 1, 1, 0], [3, 0, 1, 0, 0, 1, 1, 0], [0, 3, 1, 0, 1, 0, 0, 1], [1, 2, 1, 0, 1, 0, 0, 1], [2, 1, 1, 0, 1, 0, 0, 1], [3, 0, 1, 0, 1, 0, 0, 1], [0, 3, 0, 1, 0, 1, 1, 0], [1, 2, 0, 1, 0, 1, 1, 0], [2, 1, 0, 1, 0, 1, 1, 0], [3, 0, 0, 1, 0, 1, 1, 0], [0, 3, 1, 0, 0, 1, 0, 1], [1, 2, 1, 0, 0, 1, 0, 1], [2, 1, 1, 0, 0, 1, 0, 1], [3, 0, 1, 0, 0, 1, 0, 1], . . . (59 total preimages)

The Algorithm - Example

Let $G =$ `SmallGroup(16, 5)`. The only possible size of a difference set is 6 and G has a chief series

$$G = N_1 \triangleright N_2 \triangleright N_3 \triangleright N_4 \triangleright N_5 = \{1\}$$

with $|N_i| = 2^{5-i}$.

Difference Sums:

[0, 3, 1, 0, 1, 0, 1, 0], [1, 2, 1, 0, 1, 0, 1, 0], [2, 1, 1, 0, 1, 0, 1, 0],
[3, 0, 1, 0, 1, 0, 1, 0], [0, 3, 0, 1, 1, 0, 1, 0], [1, 2, 0, 1, 1, 0, 1, 0],
[2, 1, 0, 1, 1, 0, 1, 0], [3, 0, 0, 1, 1, 0, 1, 0], [0, 3, 1, 0, 0, 1, 1, 0],
[1, 2, 1, 0, 0, 1, 1, 0], [2, 1, 1, 0, 0, 1, 1, 0], [3, 0, 1, 0, 0, 1, 1, 0],
[0, 3, 1, 0, 1, 0, 0, 1], [1, 2, 1, 0, 1, 0, 0, 1], [2, 1, 1, 0, 1, 0, 0, 1],
[3, 0, 1, 0, 1, 0, 0, 1], [0, 3, 0, 1, 0, 1, 1, 0], [1, 2, 0, 1, 0, 1, 1, 0],
[2, 1, 0, 1, 0, 1, 1, 0], [3, 0, 0, 1, 0, 1, 1, 0], [0, 3, 1, 0, 0, 1, 0, 1],
[1, 2, 1, 0, 0, 1, 0, 1], [2, 1, 1, 0, 0, 1, 0, 1], [3, 0, 1, 0, 0, 1, 0, 1],
. . . (59 total preimages)

The Algorithm - Example

Let $G = \texttt{SmallGroup(16, 5)}$. The only possible size of a difference set is 6 and G has a chief series

$$G = N_1 \triangleright N_2 \triangleright N_3 \triangleright N_4 \triangleright N_5 = \{1\}$$

with $|N_i| = 2^{5-i}$.

Difference Sums:

[1, 1, 2, 0, 1, 1, 0, 0], [2, 0, 1, 1, 1, 1, 0, 0], [1, 1, 1, 1, 0, 2, 0, 0], [1, 2, 1, 0, 1, 0, 1, 0], [2, 1, 1, 0, 0, 1, 1, 0], [2, 1, 1, 0, 1, 0, 1, 0]

The Algorithm - Example

Let $G = \texttt{SmallGroup(16, 5)}$. The only possible size of a difference set is 6 and G has a chief series

$$G = N_1 \triangleright N_2 \triangleright N_3 \triangleright N_4 \triangleright N_5 = \{1\}$$

with $|N_i| = 2^{5-i}$.

Difference Sums:

[2, 0, 1, 1, 1, 1, 0, 0], [1, 2, 1, 0, 1, 0, 1, 0]

The Algorithm - Example

Let $G =$ `SmallGroup(16, 5)`. The only possible size of a difference set is 6 and G has a chief series

$$G = N_1 \triangleright N_2 \triangleright N_3 \triangleright N_4 \triangleright N_5 = \{1\}$$

with $|N_i| = 2^{5-i}$.

Difference Sets:

[1, 3, 2, 4, 8, 11], [1, 3, 2, 4, 8, 15], [1, 3, 2, 4, 13, 11], [1, 3, 2, 4, 13, 15], [1, 3, 2, 9, 8, 11], [1, 3, 2, 9, 8, 15], [1, 3, 2, 9, 13, 11], [1, 3, 2, 9, 13, 15], [1, 3, 6, 4, 8, 11], [1, 3, 6, 4, 8, 15], [1, 3, 6, 4, 13, 11], [1, 3, 6, 4, 13, 15], [1, 3, 6, 9, 8, 11], [1, 3, 6, 9, 8, 15], [1, 3, 6, 9, 13, 11], [1, 3, 6, 9, 13, 15], [1, 2, 6, 4, 5, 11], [1, 2, 6, 4, 5, 15], [1, 2, 6, 4, 10, 11],[1, 2, 6, 4, 10, 15], [1, 2, 6, 9, 5, 11], [1, 2, 6, 9, 5, 15], [1, 2, 6, 9, 10, 11], [1, 2, 6, 9, 10, 15], [3, 2, 6, 4, 5, 11], [3, 2, 6, 4, 5, 15], [3, 2, 6, 4, 10, 11], [3, 2, 6, 4, 10, 15], [3, 2, 6, 9, 5, 11], [3, 2, 6, 9, 5, 15], [3, 2, 6, 9, 10, 11], [3, 2, 6, 9, 10, 15]

The Algorithm - Example

Let $G =$ `SmallGroup(16, 5)`. The only possible size of a difference set is 6 and G has a chief series

$$G = N_1 \triangleright N_2 \triangleright N_3 \triangleright N_4 \triangleright N_5 = \{1\}$$

with $|N_i| = 2^{5-i}$.

Difference Sets:

[1, 3, 2, 4, 8, 11], [1, 3, 2, 4, 8, 15], [1, 3, 2, 4, 13, 11], [1, 3, 2, 4, 13, 15], [1, 3, 2, 9, 8, 11], [1, 3, 2, 9, 8, 15], [1, 3, 2, 9, 13, 11], [1, 3, 2, 9, 13, 15], [1, 3, 6, 4, 8, 11], [1, 3, 6, 4, 8, 15], [1, 3, 6, 4, 13, 11], [1, 3, 6, 4, 13, 15], [1, 3, 6, 9, 8, 11], [1, 3, 6, 9, 8, 15], [1, 3, 6, 9, 13, 11], [1, 3, 6, 9, 13, 15], [1, 2, 6, 4, 5, 11], [1, 2, 6, 4, 5, 15], [1, 2, 6, 4, 10, 11], [1, 2, 6, 4, 10, 15], [1, 2, 6, 9, 5, 11], [1, 2, 6, 9, 5, 15], [1, 2, 6, 9, 10, 11], [1, 2, 6, 9, 10, 15], [3, 2, 6, 4, 5, 11], [3, 2, 6, 4, 5, 15], [3, 2, 6, 4, 10, 11], [3, 2, 6, 4, 10, 15], [3, 2, 6, 9, 5, 11], [3, 2, 6, 9, 5, 15], [3, 2, 6, 9, 10, 11], [3, 2, 6, 9, 10, 15

The Algorithm - Example

Let $G =$ `SmallGroup(16, 5)`. The only possible size of a difference set is 6 and G has a chief series

$$G = N_1 \triangleright N_2 \triangleright N_3 \triangleright N_4 \triangleright N_5 = \{1\}$$

with $|N_i| = 2^{5-i}$.

Difference Sets:

[1, 3, 2, 4, 8, 15], [1, 3, 2, 4, 13, 11], [1, 3, 2, 9, 8, 11], [1, 3, 2, 9, 13, 15], [1, 3, 6, 4, 8, 11], [1, 3, 6, 4, 13, 15], [1, 3, 6, 9, 8, 15], [1, 3, 6, 9, 13, 11], [1, 2, 6, 4, 5, 15], [1, 2, 6, 4, 10, 11], [1, 2, 6, 9, 5, 11], [1, 2, 6, 9, 10, 15], [3, 2, 6, 4, 5, 11], [3, 2, 6, 4, 10, 15], [3, 2, 6, 9, 5, 15], [3, 2, 6, 9, 10, 11]

The Algorithm - Example

Let $G =$ `SmallGroup(16, 5)`. The only possible size of a difference set is 6 and G has a chief series

$$G = N_1 \triangleright N_2 \triangleright N_3 \triangleright N_4 \triangleright N_5 = \{1\}$$

with $|N_i| = 2^{5-i}$.

Difference Sets:

[2, 3, 6, 9, 10, 11], [1, 3, 6, 9, 11, 13]

Results

The algorithm is implemented in the DifSets Package for the computer algebra system GAP. Source code, documentation, and full results can be found at

`https://github.com/dylanpeifer/difsets`

Results

The algorithm is implemented in the DifSets Package for the computer algebra system GAP. Source code, documentation, and full results can be found at

`https://github.com/dylanpeifer/difsets`

The algorithm has successfully computed results for 989 of the 1032 groups of order less than 100. Some highlights include

order	number of groups	median time	mean time	total time
36	14	0.44 seconds	43 seconds	5 minutes
64	267	21 minutes	43 minutes	8 days
96	231	3 hours	6.5 hours	62 days

(results for order 64 do not include `SmallGroup(64, 267)`).

Future Projects

1. Improve the implementation of the refining step, which currently recomputes previous information as it iterates through the preimages and tests them.
2. Implement parts of the algorithm in C and integrate with GAP.
3. Try to expand the algorithm to use all normal subgroups of the group, rather than just a single chief series.
4. Add more theoretical results to the package, such as methods to construct difference sets, more tests that guarantee nonexistence of difference sets, or additional libraries of known difference sets.

If you are interested in any of these projects, please let me know!