All (96, 20, 4) Difference Sets

Dylan Peifer

Cornell University

11 January 2018

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.

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 $D_1 = xD_2$.

Enumeration

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?

Enumeration

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?

Answering this question will require some level of exhaustive search.

Exhaustive Search

By a simple counting argument, we can show that difference sets in groups of order 16 must have 6 elements. My computer can search through all such subsets in all fourteen groups in roughly 3.2 seconds. Similarly, groups of order 36, 64, and 96 only have one possible size for difference sets. At this rate we have

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

By a simple counting argument, we can show that difference sets in groups of order 16 must have 6 elements. My computer can search through all such subsets in all fourteen groups in roughly 3.2 seconds. Similarly, groups of order 36, 64, and 96 only have one possible size for difference sets. At this rate we have

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

By a simple counting argument, we can show that difference sets in groups of order 16 must have 6 elements. My computer can search through all such subsets in all fourteen groups in roughly 3.2 seconds. Similarly, groups of order 36, 64, and 96 only have one possible size for difference sets. At this rate we have

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

Exhaustive Search

By a simple counting argument, we can show that difference sets in groups of order 16 must have 6 elements. My computer can search through all such subsets in all fourteen groups in roughly 3.2 seconds. Similarly, groups of order 36, 64, and 96 only have one possible size for difference sets. At this rate we have

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
96	$\binom{96}{20} = 2.2 \times 10^{20}$	200 million years	45 billion years.

Exhaustive Search

By a simple counting argument, we can show that difference sets in groups of order 16 must have 6 elements. My computer can search through all such subsets in all fourteen groups in roughly 3.2 seconds. Similarly, groups of order 36, 64, and 96 only have one possible size for difference sets. At this rate we have

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
96	$\binom{96}{20} = 2.2 \times 10^{20}$	200 million years	45 billion years.

In 1978, Robert Kibler completed searches in order 36. In 2016, Ken W. Smith and Omar A. AbuGhneim almost completed searches in order 64 and 96.

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 G/N.

1	1	0	0	0	0	0	0	0	1	1	0	1	0	1	0	G
2		0		0		0		1		1		1		1		G/N

Every difference set induces a difference sum, so the only place to look for difference sets is preimages of difference sums.

Note that difference sums (or similar objects) are sometimes referred to as intersection numbers, signatures, or difference lists.

Difference Sums Induce Difference Sums

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

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

D induces difference sums in the G/N_i.

1	1	0	0	0	0	0	0	0	1	1	0	1	0	1	0	G/N_5
2		0		0		0		1		1		1		1		G/N_4
2				0				2				2				G/N_3
2								4								G/N_2
6																G/N_1

The difference sum in 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.

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.

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 1008 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	6.4 hours	61 days

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

Results

The algorithm does well when:

1. There are many (small) normal subgroups and a long chief series.
   (For example, the five groups of order 96 taking the longest computation time are five of the six groups with fewest normal subgroups in this order.)
2. The possible sizes of k are small. (For example, order 96 is much easier than other groups of similar order.)
3. The final list of difference sets is small. (For example, the eight groups of order 64 with no difference sets were computed the fastest, beating the next fastest groups of order 64 by an order of magnitude.)
4. The automorphism group is small. (For example, four of the five groups of order 64 taking the largest amount of time are the four groups with the largest automorphism groups in this order.)

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 outside 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!

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