Hadamard Difference Sets

Dylan Peifer

April 26, 2016

1 Definitions

A difference set is a subset of a group that has a nice combinatorial property.

Definition 1. *A $\langle v, k, \lambda \rangle$-*difference set *is a nonempty proper subset D of a finite group G such that $|G| = v$, $|D| = k$, and each nonidentity element of G can be written as $d_i d_j^{-1}$ for $d_i, d_j \in D$ in exactly λ different ways.*

Example 1. *Let $C_7 = \langle x | x^7 = 1 \rangle$ and $D = \{x, x^2, x^4\}$. Then D is a $\langle 7, 3, 1 \rangle$-difference set. We can see this most easily by organizing all the differences in a table.*

	x^{-1}	x^{-2}	x^{-4}
x	1	x^6	x^4
x^2	x	1	x^5
x^4	x^3	x^2	1

It is sometimes useful to think of D as an element of the group ring $\mathbb{Z}[G]$. 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

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

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.

Example 2. *We've already seen that $D = \{x, x^2, x^4\}$ is a $\langle 7, 3, 1 \rangle$-difference set in C_7. This can also be shown as*

$$\begin{aligned}(x + x^2 + x^4)(x + x^2 + x^4)^{(-1)} &= (x + x^2 + x^4)(x^{-1} + x^{-2} + x^{-4}) \\ &= 1 + x^6 + x^4 + x + 1 + x^5 + x^3 + x^2 + 1 \\ &= 2 + C_7.\end{aligned}$$

There are several basic examples that are always difference sets.

Example 3. *Any one element proper subset is a $\langle v, 1, 0\rangle$-difference set. These are trivial difference sets and are usually not counted as difference sets.*

Example 4. *The complement of a $\langle v, k, \lambda\rangle$-difference set is a $\langle v, v-k, \lambda+v-2k\rangle$-difference set. This is because*

$$\begin{aligned}(G-D)(G-D)^{(-1)} &= (G-D)(G-D^{(-1)})\\ &= GG - GD^{(-1)} - DG + DD^{(-1)}\\ &= (v-2k)G + (k-\lambda) + \lambda G\\ &= ((v-k) - (\lambda+v-2k)) + (\lambda+v-2k)G\end{aligned}$$

and as a result we typically only consider difference sets where $k \leq \frac{v}{2}$.

In enumerating difference sets we usually only consider up to an equivalence that allows the structure of the difference set to be translated by group multiplication and moved by automorphism.

Lemma 1. *If D is a difference set in G and we have $g \in G$ and $\phi \in \mathrm{Aut}(G)$, then $g\phi(D)$ is also a difference set.*

Definition 2. *Let D_1, D_2 be difference sets in G and let $g \in G$ and $\phi \in \mathrm{Aut}(G)$. Then D_1 and D_2 are* equivalent *difference sets if $D_1 = g\phi(D_2)$.*

Example 5. *In C_7 the difference set $\{x^2, x^3, x^5\}$ is equivalent to the difference set $\{x, x^2, x^4\}$ since $x^2 + x^3 + x^5 = x(x + x^2 + x^4)$.*

Finally, we define the Hadamard adjective that appears in the title.

Definition 3. *A* Hadamard difference set *is a difference set with parameters $\langle v, k, \lambda\rangle$ such that $v = 4(k-\lambda)$.*

Theorem 1. *Hadamard difference sets have parameters $\langle 4m^2, 2m^2 - m, m^2 - m\rangle$ for some positive integer m.*

The Hadamard parameters are interesting because they provide a large number of examples of difference sets.

Example 6. *Consider the first few values of the Hadamard parameters.*

For $m = 1$ the Hadamard parameters are $\langle 4, 1, 0\rangle$ and thus describe trivial difference sets. Each of the 2 groups of order 4 contains 1 trivial difference set up to equivalence.

For $m = 2$ the Hadamard parameters are $\langle 16, 6, 2\rangle$. There are 14 groups of order 16. Two of these groups contain no difference sets and the remaining 12 have between 1 and 4 difference sets for a total of 27 $\langle 16, 6, 2\rangle$-difference sets.

For $m = 3$ the Hadamard parameters are $\langle 36, 15, 6\rangle$. There are 14 group of order 36. Five of these groups contain no difference sets and the remaining 9 have between 1 and 6 difference sets for a total of 35 $\langle 36, 15, 6\rangle$-difference sets.

2 Existence

The fundamental question in studying difference sets is determining whether a difference set exists in a given group or with a given value of parameters.

First consider the parameters. Basic counting gives the following simple lemma.

Lemma 2. *If D is a $\langle v, k, \lambda\rangle$-difference set then $\lambda(v-1) = k(k-1)$.*

Proof. There are $k(k-1)$ pairs $d_i, d_j \in D$ such that $d_i d_j^{-1} \neq 1$, and by definition these pairs must give a total of λ copies of each of the $v-1$ nonidentity elements. □

Stronger results can be stated, such as the following.

Theorem 2 (Bruck-Ryser-Chowla)**.** *Assume there exists a $\langle v, k, \lambda\rangle$-difference set. If v is even then $k-\lambda$ is a perfect square. If v is odd then the diophantine equation $x^2 = (k-\lambda)y^2 + (-1)^{(v-1)/2}\lambda z^2$ has a nonzero solution in integers x, y, z.*

Theorem 1 above follows quickly from Lemma 2 and Theorem 2.

Instead of looking at parameters, we can focus on the group. Showing that a group contains a difference set is typically done by constructing an explicit difference set or showing that a construction will work in the group. The following two constructions and their proofs are from [1].

Theorem 3 (Product Construction)**.** *Suppose that $G = H_1 H_2$ for disjoint subgroups $H_1, H_2 \subseteq G$ and that H_1 and H_2 contain Hadamard difference sets. Then G contains a Hadamard difference set.*

Proof. Consider the Hadamard transform $\hat{D}$ of a difference set defined by $\hat{D} = G - 2D$. Assuming that D is a Hadamard difference set we can compute

$$\begin{aligned}
\hat{D}\hat{D}^{(-1)} &= (G-2D)(G-2D)^{(-1)} \\
&= (G-2D)(G-2D^{(-1)}) \\
&= GG - 2GD^{(-1)} - 2DG + 4DD^{(-1)} \\
&= |G|G - 2|D|G - 2|D|G + 4((k-\lambda) + \lambda G) \\
&= (|G| - 4|D| + 4\lambda)G + 4(k-\lambda) \\
&= (4m^2 - 4(2m^2-m) + 4(m^2-m))G + 4((2m^2-m) - (m^2-m)) \\
&= 0 + 4m^2 \\
&= |G|.
\end{aligned}$$

It is straightforward to do this in the other direction to establish that $\hat{D}\hat{D}^{(-1)} = |G|$ iff D is a Hadamard difference set in G.

Now consider the situation in the theorem. Let D_1 and D_2 denote the given difference sets in H_1 and H_2. Then $\hat{D}_1\hat{D}_1^{(-1)} = |H_1|$ and $\hat{D}_2\hat{D}_2^{(-1)} = |H_2|$. Because G is a product of the trivially intersecting H_1 and H_2 we know that $\hat{D}_1\hat{D}_2$ has the form of a Hadamard transform of a set in G. Then note that

$$(\hat{D}_1\hat{D}_2)(\hat{D}_1\hat{D}_2)^{(-1)} = \hat{D}_1\hat{D}_2\hat{D}_2^{(-1)}\hat{D}_1^{(-1)} = \hat{D}_1|H_2|\hat{D}_1^{(-1)} = |H_1||H_2| = |G|$$

so that $\hat{D}_1\hat{D}_2$ is the Hadamard transform of a difference set in G. □

Example 7. *Consider* $C_4 \times C_4 = \langle x, y | x^4 = y^4 = [x, y] = 1 \rangle$. *This group is the product of the two groups* $H_1 = \langle x | x^4 = 1 \rangle$ *and* $H_2 = \langle y | y^4 = 1 \rangle$ *which have (trivial) difference sets* $\{x\}$ *and* $\{y\}$ *respectively. These give Hadamard transforms* $1 - x + x^2 + x^3$ *and* $1 - y + y^2 + y^3$ *which we multiply together to get*

$$\begin{aligned}&(1 - x + x^2 + x^3)(1 - y + y^2 + y^3)\\ &= 1 - y + y^2 + y^3 - x + xy - xy^2 - xy^3 + x^2 - x^2y + x^2y^2 + x^2y^3 + x^3 - x^3y + x^3y^2 + x^3y^3\end{aligned}$$

which is the Hadamard transform of the set $\{y, x, xy^2, xy^3, x^2y, x^3y\}$. *It can be checked that this is a difference set.*

Theorem 4 (Dihedral Trick)**.** *Let* H *be any abelian group and* $G = \langle H, q | qhq^{-1} = h^{-1} \forall h \in H \rangle$ *the generalized dihedral group of* H. *If* G *contains a difference set then so does every abelian group which contains* H *as a subgroup of index 2.*

Proof. By construction we have $G = H + qH$, so we can write the difference set D in G as $D = X + qY$ for X, Y subsets of H. Then since D is a difference set we have

$$\begin{aligned}(k - \lambda) + \lambda G &= DD^{(-1)}\\ &= (X + qY)(X + qY)^{(-1)}\\ &= (X + qY)(X^{(-1)} + Y^{(-1)}q)\\ &= XX^{(-1)} + XY^{(-1)}q + qYX^{(-1)} + qYY^{(-1)}q\\ &= XX^{(-1)} + YY^{(-1)} + 2qYX^{(-1)}\end{aligned}$$

so that since $X, Y \subseteq H$ we must have $XX^{(-1)} + YY^{(-1)} = (k - \lambda) + \lambda H$ and $YX^{(-1)} = \frac{1}{2}\lambda H$.

Now suppose K is abelian and contains H with index 2. Then $K = H + rH$ and we can then define $C = X + rY$. Since

$$\begin{aligned}CC^{(-1)} &= (X + rY)(X + rY)^{(-1)}\\ &= (X + rY)(X^{(-1)} + Y^{(-1)}r^{-1})\\ &= XX^{(-1)} + XY^{(-1)}r^{-1} + rYX^{(-1)} + rYY^{(-1)}r^{-1}\\ &= XX^{(-1)} + YY^{(-1)} + (YX^{(-1)})^{(-1)}r^{-1} + rYX^{(-1)}\\ &= (k - \lambda) + \lambda H + \left(\frac{1}{2}\lambda H\right)^{(-1)} r^{-1} + r\left(\frac{1}{2}\lambda H\right)\\ &= (k - \lambda) + \lambda H + r\lambda H\\ &= (k - \lambda) + \lambda K\end{aligned}$$

we have that C is a difference set in K. □

While the Dihedral Trick seems to provide a way to construct difference sets, it is typically used in its contrapositive form with the following theorem to show the nonexistence of difference sets.

Theorem 5 (Turyn's Bound)**.** *If* G *is an abelian group of order* 2^{2s+2} *containing a difference set then* G *has exponent at most* 2^{s+2}.

Example 8. *Consider groups of order* $16 = 2^{2(1)+2}$*. Turyn's Bound gives that groups containing a difference set can have exponent at most* $2^{1+2} = 8$*. Thus* C_{16} *does not contain a difference set. The Dihedral Trick then gives the* D_8 *cannot contain a difference set either.*

For abelian 2-groups Turyn's Bound is necessary and sufficient. For non-abelian 2-groups it is conjectured that Turyn's Bound and the Dihedral Trick combined are necessary and sufficient. There are many, many more constructions and theorems along these lines.

3 Enumeration

Another natural question to ask is if we can find all difference sets in a group or set of groups. This is a more computational than theoretical question, and I'm not sure what is currently known. In [3], Kibler finds all Hadamard difference sets in order 16 and order 36 groups. Order 64, the next place to find Hadamard difference sets, will be our benchmark. Past Lemma 3 these results are my own, with influence from Jason Steinberg during our time at the SDSU REU, where he worked on a similar method for Hadamard difference sets in the order 64 groups.

This is a hard problem. On my computer I can do a completely unoptimized brute force search of order 16 in 85 seconds. At this rate we have roughly

order	subsets to check	time/group
16	$\binom{16}{6} = 8008$	6 seconds
36	$\binom{36}{15} = 5567902560$	48 days
64	$\binom{64}{28} = 1118770292985239888$	27 million years

so brute force will clearly not work.

The foundation of a good approach is this key lemma.

Lemma 3. *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*

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

Proof. Since D is a difference set we have

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

Applying θ to both sides and using that θ is a homomorphism with kernel of size w and image H yields

$$\theta(D)\theta(D)^{(-1)} = SS^{(-1)} = (k - \lambda) + \lambda\theta(G) = (k - \lambda) + \lambda w H.$$

□

The idea is that we can search for these S objects in an image of G and then pullback to G. This motivates the following definition.

Definition 4. *Given a finite group G and normal subgroup N, a* (v, k, λ)-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 4. *Suppose G is a finite group with normal subgroup N. Then any difference set in G induces a difference sum in G/N.*

Proof. This follows directly from Definition 4 and Lemma 3. Counting elements in each coset of N ensures that the coefficients of S have appropriate values. □

But we don't need to pullback from the quotient group to the group. We can pullback from quotient group to quotient group so that the full pullback to difference sets in the group can be done in multiple stages.

Lemma 5. *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.*

Proof. Let S_2 be the difference sum in G/N_2. Then by definition

$$S_2 S_2^{(-1)} = (k - \lambda) + \lambda|N_2|G/N_2.$$

Using the third isomorphism theorem, let $\phi : G/N_2 \to G/N_1$ be the homomorphism obtained by composing the quotient map $\phi_1 : G/N_2 \to (G/N_2)/(N_1/N_2)$ with the isomorphism $\phi_2 : (G/N_2)/(N_1/N_2) \to G/N_1$. Then applying ϕ to both sides of the above equality yields

$$\begin{aligned}
\phi(S_2)\phi(S_2)^{(-1)} &= (k - \lambda) + \lambda|N_2|\phi(G/N_2) \\
&= (k - \lambda) + \lambda|N_2||\ker(\phi)|G/N_1 \\
&= (k - \lambda) + \lambda|N_2||N_1/N_2|G/N_1 \\
&= (k - \lambda) + \lambda|N_1|G/N_1
\end{aligned}$$

so that $\phi(S_2)$ is a difference sum in G/N_1. □

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

Definition 5. *Let S_1 and S_2 be difference sums in 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 6. *Suppose S_1, S_2 are equivalent difference sums in 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.*

Proof. Let $\theta : G \to G/N$. We have $S_1 = g\phi(S_2)$ for some $g \in G/N$ and ϕ an induced automorphism from some $\rho \in \mathrm{Aut}(G)$. Then $g = \theta(h)$ for some $h \in G$, $S_1 = \theta(D_1)$, and $\phi \circ \theta = \theta \circ \rho$. Thus

$$S_2 = \phi^{-1}(g^{-1}\theta(D_1)) = \theta \circ \rho^{-1} \circ \theta^{-1}(\theta(h^{-1}D_1)) = \theta(\rho^{-1}(h^{-1}D_1))$$

so that $\rho^{-1}(h^{-1}D_1)$ is an equivalent difference set to D_1 that induces S_2. □

These ideas lead to a simple algorithm. The algorithm starts at $G/G = \{1\}$, where the only difference sum is k, the size of the desired difference set. Then we proceed up a sequence of larger and larger quotient groups G/N_i. Since we need $N_{i+1} \subseteq N_i$ and both to be normal in G so that both give quotient groups, the maximum number of stages we can use is given by a chief series of G. At each stage we (1) enumerate pre-images of our current difference sums, (2) filter out non-difference sums, and (3) filter out equivalent difference sums. At the final stage we pullback to difference sets and filter as before.

Implemented in GAP, the search for all Hadamard difference sets in a group of order 36 takes on the order of minutes, while the search for all Hadamard difference sets in a group of order 64 takes on the order of hours. My code has successfully searched 264 of the 267 groups of order 64. The remaining three groups have exceptionally large automorphism groups and the search in each was cut off after 12 hours.

Questions for the future:

- Given a specific $g \in G$, any difference set is equivalent to a difference set containing 1 and g. Can this force picking of elements be used in the algorithm?
- There are multiple chief series of a group. Is it possible to determine which is best to use or use the information from multiple chief series together?
- The algorithm depends on the automorphism group of the group we are searching in, which can be much larger and more complicated than the group. Is there any way to handle large automorphism groups better, perhaps by force picking or ignoring some of the automorphisms?
- Irreducible representations and characters can also be used to check that group ring elements are equal. Could using representations give a faster implementation?
- Other ideas?

References

[1] J. F. Dillon. Variations on a scheme of McFarland for noncyclic difference sets. *Journal of Combinatorial Theory, Series A*, 40(1):9 – 21, 1985.

[2] Jonathan Jedwab and James Davis. A survey of Hadamard difference sets. *Hewlett Packard Laboratories*, 1994.

[3] Robert E. Kibler. A summary of noncyclic difference sets, $k < 20$. *Journal of Combinatorial Theory, Series A*, 25(1):62 – 67, 1978.

[4] Emily H. Moore and Harriet S. Pollatsek. *Difference Sets: Connecting Algebra, Combinatorics, and Geometry*. American Mathematical Society, 2013.

[5] Ken W. Smith. Non-abelian Hadamard difference sets. *Journal of Combinatorial Theory, Series A*, 70(1):144–156, 1995.