Multipliers of difference sets
and how to find them

Ezra Brown
Virginia Tech

MD/DC/VA Fall Section Meeting
Bowie State University
November 8, 2014
What to expect

- Difference sets
- Multipliers
- Orbits
- Finding difference sets using multipliers
A \((v, k, \lambda)\) difference set is a \(k\)-element subset \(D\) of \(V = \mathbb{Z} \mod v\) such that every nonzero element of \(V\) can be expressed as a difference \(a - b\) of elements \(a, b \in D\) in exactly \(\lambda\) ways. Here are a couple of examples.
The $(7, 3, 1)$ difference set

Let $D = \{1, 2, 4\}$, a 3-element set ($k = 3$).

Look at the differences of elements of $D$ mod 7 ($\nu = 7$):

\[
\begin{align*}
2 - 1 &\equiv 1 & 1 - 4 &\equiv 4 \\
4 - 2 &\equiv 2 & 2 - 4 &\equiv 5 \\
4 - 1 &\equiv 3 & 1 - 2 &\equiv 6 \\
\end{align*}
\]

The numbers \{1, 2, 3, 4, 5, 6\} are each expressible as a difference of elements of $D$ in exactly 1 way ($\lambda = 1$).

Hence, $D = \{1, 2, 4\}$ is a $(\nu, k, \lambda) = (7, 3, 1)$ difference set.
The (11, 5, 2) difference set

Look at the differences of elements of $D\{1, 3, 4, 5, 9\}$ mod 11:

1 $\equiv$ 4 $-$ 3 $\equiv$ 5 $-$ 4  
2 $\equiv$ 3 $-$ 1 $\equiv$ 5 $-$ 3  
3 $\equiv$ 4 $-$ 1 $\equiv$ 1 $-$ 9  
4 $\equiv$ 5 $-$ 1 $\equiv$ 9 $-$ 5  
5 $\equiv$ 9 $-$ 4 $\equiv$ 3 $-$ 9  
6 $\equiv$ 9 $-$ 3 $\equiv$ 4 $-$ 9  
7 $\equiv$ 1 $-$ 5 $\equiv$ 5 $-$ 9  
8 $\equiv$ 9 $-$ 1 $\equiv$ 1 $-$ 4  
9 $\equiv$ 1 $-$ 3 $\equiv$ 3 $-$ 5  
10 $\equiv$ 3 $-$ 4 $\equiv$ 4 $-$ 5

The numbers $\{1, 2, \ldots, 10\}$ are each expressible as a difference of elements of $D$ in exactly 2 ways.

Hence, $D = \{1, 3, 4, 5, 9\}$ is a $(v, k, \lambda) = (11, 5, 2)$ difference set.
Let $D$ be a $(v, k, \lambda)$ difference set. Then

- $D$ contains $k$ elements, so there are $k(k - 1)$ pairs of distinct elements of $D$.
- The $k(k - 1)$ nonzero differences between pairs of elements of $D$ mod $v$ account for $\lambda$ copies of the $v - 1$ nonzero integers mod $v$.
- Hence, $k(k - 1) = \lambda(v - 1)$.

This is a necessary condition on the parameters for the existence of a $(v, k, \lambda)$ difference set. We need a sufficient condition that's easy to check.

That's where multipliers come in.
Let $D = \{x_1, \ldots, x_k\}$ be a difference set. A \textit{multiplier} of $D$ is an integer $m$ such that $\{mx_i \pmod{v} : i = 1, \ldots, k\}$ is equal to a translation $D + r \pmod{v}$ for some integer $r$.

Example: $D = \{2, 3, 5\}$ is a $(7, 3, 1)$ difference set, and

$$2D \pmod{7} = D + 1 \pmod{7} = \{3, 4, 6\}.$$

How does this help?
The Multiplier Theorem

Let $D$ be a $(v, k, \lambda)$ difference set, and let $p$ be a prime such that $(p, v) = 1$, $p > \lambda$, and $p|(k - \lambda)$. Then

- $p$ is a multiplier of $D$, and
- There exists $j$ such that $p \cdot (D + j) \equiv D + j \pmod{v}$.

More generally, if there is a $(v, k, \lambda)$-difference set $D$ with a multiplier $m$, then there is a difference set $D'$ on these parameters such that $D' \equiv mD' \pmod{v}$. 
Examples:

(1) It turns out that 2 is a multiplier for the \((7, 3, 1)\) difference set \(D = \{1, 2, 4\}\), and \(2D \equiv D \mod 7\).

(2) Similarly, multiplication by 3 fixes the \((11, 5, 2)\) difference set \(D = \{1, 3, 4, 5, 9\}\).

Now, by the Multiplier Theorem, if there is a \((21, 5, 1)\) difference set \(D\), then 2 is a multiplier of \(D\). How do we find \(D\)?
A *permutation* on a set $S$ is a 1-1 mapping of the set onto itself.

For example, let $S = \{1, 2, 3, 4, 5\}$, and define $\pi$ by $\pi(1) = 3$, $\pi(2) = 5$, $\pi(3) = 4$, $\pi(4) = 1$, $\pi(5) = 2$.

If $f$ is a permutation on $S$, and $x \in S$, then the *orbit of $f$ containing $x$* is the set of iterated images $\{x, f(x), f(f(x)), \ldots\}$

Thus, the orbits of $\pi$ are $\{1, 3, 4\}$ and $\{2, 5\}$.
The orbits of $x \mapsto 2x \mod 7$ on $\mathbb{Z}_7$ are $\{0\}$, $\{1, 2, 4\}$, and $\{3, 6, 5\}$.

$\{1, 2, 4\}$ is a $(7, 3, 1)$ difference set fixed by this map.

Isn’t that interesting?

The orbits of $x \mapsto 3x \mod 11$ on $\mathbb{Z}_{11}$ are $\{0\}$, $\{1, 3, 9, 5, 4\}$, and $\{2, 6, 7, 10, 8\}$ — and $\{1, 3, 9, 5, 4\}$ is an $(11, 5, 2)$ difference set fixed by the given mapping.

Isn’t that interesting?
FACT 1: If \((m, v) = 1\), then the mapping \(m \mapsto 2m \mod v\) is a permutation on \(\mathbb{Z}_v\).

FACT 2: If \(m\) is a multiplier of a \((v, k, \lambda)\) difference set \(D\), then some translation of \(D\) is fixed by \(m \mapsto 2m \mod v\). Therefore:

FACT 3: If a \((v, k, \lambda)\) difference set \(D\) is fixed by a multiplier \(m\), then \(D\) is a union of orbits of the map \(m \mapsto 2m \mod v\). So:
WILD IDEA: If \( \nu \), \( k \), and \( \lambda \) satisfy the relation \( k(k-1) = \lambda(\nu-1) \), and \( p \) satisfies the conditions in the Multiplier Theorem, then the set of orbits of \( x \mapsto px \mod \nu \) just might contain a \((\nu, k, \lambda)\) difference set.

ACTION PLAN: Look through such orbits and find some of them whose union (a) contains \( k \) elements and (b) produces a \((\nu, k, \lambda)\) difference set.
The Multiplier Theorem tells us that if $D$ is a $(21, 5, 1)$ difference set, then 2 is a multiplier of $D$ — and so it fixes a translate of $D$.

The orbits of $x \mapsto 2x \mod 21$ are \{0\}, \{1, 2, 4, 8, 16, 11\}, \{3, 6, 12\}, \{5, 10, 20, 19, 17, 13\}, \{7, 14\}, and \{9, 18, 15\}. We find that

\{3, 6, 7, 12, 14\} = \{3, 6, 12\} \cup \{7, 14\} is indeed a $(21, 5, 1)$ difference set.

The orbits of $x \mapsto 2x \mod 15$ are \{0\}, \{1, 2, 4, 8\}, \{3, 6, 12, 9\}, \{5, 10\}, and \{7, 14, 13, 11\}; — and \{0, 1, 2, 4, 8, 5, 10\} is a $(15, 7, 3)$ difference set.
Using this method led to the discovery of these difference sets:

\{1, 5, 25, 17, 22, 23\} is a \((31, 6, 1)\) difference set with multiplier 5.

\{1, 7, 9, 10, 12, 16, 26, 33, 34\} is a \((37, 9, 2)\) difference set with multiplier 7.

\{0, 1, 3, 5, 9, 15, 22, 25, 26, 27, 34, 35, 38\} is a \((40, 13, 4)\) difference set with multiplier 3.

But we can also use this method to disprove the existence of certain difference sets.
If a \((31,10,3)\) difference set were to exist, then 7 would be a multiplier.

But the map \(x \mapsto 7x \mod{31}\) has one orbit of size 1 and two of size 15. No union of these can be of size 10.

Hence, a \((31,10,3)\) difference set does not exist.

A \((56,11,2)\) difference set does not exist. The map \(x \mapsto 3 \mod{56}\) does contain orbits with unions of size 11, but none of them give rise to such a difference set.

As for a \((43,7,1)\) difference set, there are three orbits for \(m=2\) of size 14 and one of size 1, and there is one orbit for \(m=3\) of size 42 and one of size 1. Thus, there is no \((43,7,1)\) difference set.
I hope this talk has made a difference.
THANK YOU!