Sum and Difference Sets in Generalized Dihedral Groups

Ruben Ascoli
rascoli@princeton.edu

SMALL REU 2022 at Williams College
Joint work with Justin Cheigh, Guilherme Zeus Dantas e Moura, Ryan Jeong, Andrew Keisling, Astrid Lilly, Steven J. Miller, Prakod Ngamlamai, and Matthew Phang

CANT 2023

May 25, 2023

Definitions

Definition

Given a set of integers A, we define the sumset and difference set of A as follows:

$$A + A = \{a_1 + a_2 : a_1, a_2 \in A\},$$

$$A - A = \{a_1 - a_2 : a_1, a_2 \in A\}.$$

Definitions

Definition

Given a set of integers A, we define the sumset and difference set of A as follows:

$$A + A = \{a_1 + a_2 : a_1, a_2 \in A\},$$

$$A - A = \{a_1 - a_2 : a_1, a_2 \in A\}.$$

We want to compare the sizes of these two sets:

- $|A + A| > |A - A|$: A has more sums than differences (MSTD).
- $|A + A| = |A - A|$: A is sum-difference balanced.
- $|A + A| < |A - A|$: A has more differences than sums (MDTS).

Sum and difference sets in number theory

Problems in additive number theory can be written in terms of sumsets and difference sets:

Sum and difference sets in number theory

Problems in additive number theory can be written in terms of sumsets and difference sets:

Goldbach's conjecture says $\{4, 6, 8, 10, \ldots\} \subseteq P + P$.

Sum and difference sets in number theory

Problems in additive number theory can be written in terms of sumsets and difference sets:

Goldbach's conjecture says $\{4, 6, 8, 10, \ldots\} \subseteq P + P$.

The twin primes conjecture says that $P - P$ contains 2 infinitely many times.

Sum and difference sets in number theory

Problems in additive number theory can be written in terms of sumsets and difference sets:

Goldbach's conjecture says $\{4, 6, 8, 10, \ldots\} \subseteq P + P$.

The twin primes conjecture says that $P - P$ contains 2 infinitely many times.

Fermat's last theorem says that $(A_n + A_n) \cap A_n = \emptyset$, where A_n is the set of positive n^{th} powers for $n \geq 3$.

Expectation

We expect that most sets of integers are MDTS rather than MSTD.

Expectation

We expect that most sets of integers are MDTS rather than MSTD.

Addition is commutative, subtraction is not.

Expectation

We expect that most sets of integers are MDTS rather than MSTD.

Addition is commutative, subtraction is not.

Theorem (Martin-O'Bryant, 2006)

Let P be any arithmetic progression with length n. On average, the difference set of a subset of P has 4 more elements than its sumset:

$$\frac{1}{2^n}\sum_{A\subseteq P}|A-A| \sim 2n-7,$$

$$\frac{1}{2^n}\sum_{A\subseteq P}|A+A| \sim 2n-11.$$

MSTD sets of integers

Theorem (Martin-O'Bryant, 2006)

For $n \geq 15$, *the number of MSTD subsets of* $\{0, 1, 2, \ldots, n-1\}$ *is at least* $(2 \cdot 10^{-7})2^n$.

MSTD sets of integers

Theorem (Martin-O'Bryant, 2006)

For $n \geq 15$*, the number of MSTD subsets of* $\{0, 1, 2, \ldots, n-1\}$ *is at least* $(2 \cdot 10^{-7})2^n$*.*

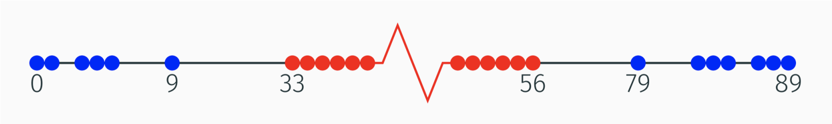
MSTD subsets can be constructed by carefully controlling the "fringes" (elements close to 0 or $n-1$).

MSTD sets of integers

Theorem (Martin-O'Bryant, 2006)

For $n \geq 15$, the number of MSTD subsets of $\{0, 1, 2, \ldots, n-1\}$ is at least $(2 \cdot 10^{-7})2^n$.

MSTD subsets can be constructed by carefully controlling the "fringes" (elements close to 0 or $n-1$).



Example

Example

Let $A = \{0, 2, 3, 4, 7, 11, 12, 14\}$.

$$A + A = \{0, 1, \ldots, 28\} \backslash \{1, 20, 27\}, \ |A + A| = 26,$$

$$A - A = \{-14, -13, \ldots, 14\} \backslash \{-13, -6, 6, 13\}, \ |A - A| = 25.$$

Finite Groups

Miller and Vissuet considered the analogous problem with a finite group G (not necessarily abelian) in place of $\mathbb{Z}$.

Finite Groups

Miller and Vissuet considered the analogous problem with a finite group G (not necessarily abelian) in place of $\mathbb{Z}$.

Definition

Given $A \subseteq G$, we define the sumset and difference set of A as follows:

$$A + A = \{a_1 a_2 : a_1, a_2 \in A\},$$

$$A - A = \{a_1 a_2^{-1} : a_1, a_2 \in A\}.$$

Finite Groups

Miller and Vissuet considered the analogous problem with a finite group G (not necessarily abelian) in place of $\mathbb{Z}$.

Definition

Given $A \subseteq G$, we define the sumset and difference set of A as follows:

$$A + A = \{a_1 a_2 : a_1, a_2 \in A\},$$

$$A - A = \{a_1 a_2^{-1} : a_1, a_2 \in A\}.$$

The lack of fringes or commutativity significantly affect the methods and results in these cases.

Finite Groups

Miller and Vissuet considered the analogous problem with a finite group G (not necessarily abelian) in place of $\mathbb{Z}$.

Definition

Given $A \subseteq G$, we define the sumset and difference set of A as follows:

$$A + A = \{a_1 a_2 : a_1, a_2 \in A\},$$

$$A - A = \{a_1 a_2^{-1} : a_1, a_2 \in A\}.$$

The lack of fringes or commutativity significantly affect the methods and results in these cases.

Theorem (Miller-Vissuet 2014)

Let G_n be a family of finite groups such that $|G_n| \to \infty$. If $A_n \subseteq G_n$ is chosen uniformly at random, then

$$\mathbb{P}(A_n + A_n = A_n - A_n = G_n) \to 1 \text{ as } n \to \infty.$$

Dihedral groups

More MSTD than MDTS

Definition

The dihedral group D_{2n} is the group of symmetries of the regular n-gon, consisting of n "rotation" elements and n "flip" elements.

More MSTD than MDTS

Definition

The dihedral group D_{2n} is the group of symmetries of the regular n-gon, consisting of n "rotation" elements and n "flip" elements.

Conjecture (Miller-Visuet, 2014)

For all $n \geq 3$, D_{2n} has more MSTD subsets than MDTS subsets.

More MSTD than MDTS

Definition

The dihedral group D_{2n} is the group of symmetries of the regular n-gon, consisting of n "rotation" elements and n "flip" elements.

Conjecture (Miller-Visuet, 2014)

For all $n \geq 3$, D_{2n} has more MSTD subsets than MDTS subsets.

Intuition comes from splitting $A \subseteq D_{2n}$ into R (rotation elements) and F (flip elements):

Set	Rotations in set	Flips in set
A	R	F
$A+A$	$R+R, F+F$	$R+F, -R+F$
$A-A$	$R-R, F+F$	$R+F$

More MSTD than MDTS

Definition

The dihedral group D_{2n} is the group of symmetries of the regular n-gon, consisting of n "rotation" elements and n "flip" elements.

Conjecture (Miller-Visuet, 2014)

For all $n \geq 3$, D_{2n} has more MSTD subsets than MDTS subsets.

Intuition comes from splitting $A \subseteq D_{2n}$ into R (rotation elements) and F (flip elements):

Set	Rotations in set	Flips in set
A	R	F
$A+A$	$R+R, F+F$	$R+F, -R+F$
$A-A$	$R-R, F+F$	$R+F$

$R+R$ and $-R+F$ contribute to $A+A$ and not $A-A$.
Only $R-R$ contributes to $A-A$ and not $A+A$.

Partitioning by size

Haviland et al. (2020) made progress toward proving the conjecture by partitioning the subsets of D_{2n} by size.

Partitioning by size

Haviland et al. (2020) made progress toward proving the conjecture by partitioning the subsets of D_{2n} by size.

Notation: Let $\mathcal{S}_m$ denote the set of subsets of D_{2n} of size m.

Partitioning by size

Haviland et al. (2020) made progress toward proving the conjecture by partitioning the subsets of D_{2n} by size.

Notation: Let $\mathcal{S}_m$ denote the set of subsets of D_{2n} of size m.

Lemma (Haviland et al. 2020)

$\mathcal{S}_2$ has strictly more MSTD subsets than MDTS subsets.

Partitioning by size

Haviland et al. (2020) made progress toward proving the conjecture by partitioning the subsets of D_{2n} by size.

Notation: Let $\mathcal{S}_m$ denote the set of subsets of D_{2n} of size m.

Lemma (Haviland et al. 2020)

$\mathcal{S}_2$ has strictly more MSTD subsets than MDTS subsets.

We further extended this piecemeal approach:

Lemma (A. et al. 2022+)

$\mathcal{S}_3$ has strictly more MSTD subsets than MDTS subsets.

Large subsets

Haviland et al. (2020) also showed that sufficiently large subsets must be sum-difference balanced:

Lemma (Haviland et al. 2020)

Given $A \subseteq D_{2n}$*, if* $|A| > n$*, then* $A + A = A - A = D_{2n}$*.*

Large subsets

Haviland et al. (2020) also showed that sufficiently large subsets must be sum-difference balanced:

Lemma (Haviland et al. 2020)

Given $A \subseteq D_{2n}$, if $|A| > n$, then $A + A = A - A = D_{2n}$.

It remains to show that $\mathcal{S}_m$ does not have more MDTS sets than MSTD sets for $4 \leq m \leq n$.

Composition of A

Our main new idea: further partition $\mathcal{S}_m$ by the number of rotation elements versus flip elements.

Writing each $A \subseteq D_{2n}$ as $R \cup F$ (rotations and flips), we have:

Lemma (A. et al. 2022+)

If $|R| > \frac{n}{2}$ or $|F| > \frac{n}{2}$, then A cannot be MDTS.

Composition of A

Our main new idea: further partition $\mathcal{S}_m$ by the number of rotation elements versus flip elements.

Writing each $A \subseteq D_{2n}$ as $R \cup F$ (rotations and flips), we have:

Lemma (A. et al. 2022+)

If $|R| > \frac{n}{2}$ or $|F| > \frac{n}{2}$, then A cannot be MDTS.

Proof. Recall this table:

Set	Rotations in set	Flips in set
$A + A$	$R + R, F + F$	$R + F, -R + F$
$A - A$	$R - R, F + F$	$R + F$

We can only have $|A - A| > |A + A|$ if $R - R$ contains rotation elements that $A + A$ does not have.

Composition of A

Our main new idea: further partition $\mathcal{S}_m$ by the number of rotation elements versus flip elements.

Writing each $A \subseteq D_{2n}$ as $R \cup F$ (rotations and flips), we have:

Lemma (A. et al. 2022+)

If $|R| > \frac{n}{2}$ or $|F| > \frac{n}{2}$, then A cannot be MDTS.

Proof. Recall this table:

Set	Rotations in set	Flips in set
$A+A$	$R+R, F+F$	$R+F, -R+F$
$A-A$	$R-R, F+F$	$R+F$

We can only have $|A-A| > |A+A|$ if $R-R$ contains rotation elements that $A+A$ does not have. But if $|R| > \frac{n}{2}$ (resp. $|F| > \frac{n}{2}$), then $R+R$ (resp. $F+F$) contributes all of the possible rotations in D_{2n}.

Counting collisions

Results

For large n, we extended to certain values in $4 \leq m \leq n$ by probabilistic methods.

Results

For large n, we extended to certain values in $4 \leq m \leq n$ by probabilistic methods.

Theorem (A. et al. 2022+)

For any n, more of the subsets in $\mathcal{S}_m$ are MSTD than MDTS for $6 \leq m \leq c \cdot \sqrt{n}$ where c is a global constant.

This holds for any n with $c = 0.12$, but if n is very large, we can improve c to 0.53.

Results

For large n, we extended to certain values in $4 \leq m \leq n$ by probabilistic methods.

Theorem (A. et al. 2022+)

For any n, more of the subsets in $\mathcal{S}_m$ are MSTD than MDTS for $6 \leq m \leq c \cdot \sqrt{n}$ where c is a global constant.

This holds for any n with $c = 0.12$, but if n is very large, we can improve c to 0.53.

Even more can be said if we further restrict m:

Theorem (A. et al. 2022+)

For any $\epsilon > 0$, there exist m_ϵ and c_ϵ such that for all $n \gg 0$, if $m_\epsilon \leq m \leq c_\epsilon \sqrt{n}$, the proportion of MSTD sets in $\mathcal{S}_m$ is at least $1 - \epsilon$.

MSTD with no overlaps

The proof relies on limiting the number of overlapping sums in $A + A$.

MSTD with no overlaps

The proof relies on limiting the number of overlapping sums in $A + A$. Recall this table again:

Set	Rotations in set	Flips in set
$A + A$	$R + R, F + F$	$R + F, -R + F$
$A - A$	$R - R, F + F$	$R + F$

MSTD with no overlaps

The proof relies on limiting the number of overlapping sums in $A + A$. Recall this table again:

Set	Rotations in set	Flips in set
$A + A$	$R + R, F + F$	$R + F, -R + F$
$A - A$	$R - R, F + F$	$R + F$

Let $|A| = m$, $|F| = k$, and $|R| = m - k$. Assuming no overlaps, and not counting $F + F$:

Type	A+A	A-A
Rotations	$\binom{m-k}{2} + (m - k)$	$2\binom{m-k}{2}$
Flips	$2(m - k)k$	$(m - k)k$

MSTD with no overlaps

The proof relies on limiting the number of overlapping sums in $A+A$. Recall this table again:

Set	Rotations in set	Flips in set
$A+A$	$R+R, F+F$	$R+F, -R+F$
$A-A$	$R-R, F+F$	$R+F$

Let $|A| = m$, $|F| = k$, and $|R| = m-k$. Assuming no overlaps, and not counting $F+F$:

Type	A+A	A-A
Rotations	$\binom{m-k}{2} + (m-k)$	$2\binom{m-k}{2}$
Flips	$2(m-k)k$	$(m-k)k$

This implies that, with no overlaps, A is MSTD if

$$\binom{m-k}{2} + (m-k) + 2(m-k)k \ > \ 2\binom{m-k}{2} + (m-k)k.$$

Collisions

Definition

Let $A \in \mathcal{S}_m$, and let $i = (a, b, c, d) \in A^4$. We call the event that $ab = cd$ (or equivalently, $d = c^{-1}ab$) a *collision*.

Collisions

Definition

Let $A \in \mathcal{S}_m$, and let $i = (a, b, c, d) \in A^4$. We call the event that $ab = cd$ (or equivalently, $d = c^{-1}ab$) a *collision*.

For our purposes, we will disregard three types of collisions:

$$(a, b, a, b),$$
$$(a, b, b, a) : a, b \in R,$$
$$(a, b, c, d) : a, b, c, d \in F.$$

Collisions

Definition

Let $A \in \mathcal{S}_m$, and let $i = (a, b, c, d) \in A^4$. We call the event that $ab = cd$ (or equivalently, $d = c^{-1}ab$) a *collision*.

For our purposes, we will disregard three types of collisions:

$$(a, b, a, b),$$
$$(a, b, b, a) : a, b \in R,$$
$$(a, b, c, d) : a, b, c, d \in F.$$

These *redundant collisions* have already been accounted for in the previous analysis.

MSTD, counting overlaps

Let $|A| = m$, $|F| = k$, and $|R| = m - k$. Let X_A denote the number of nonredundant collisions in A. Then, A is MSTD if

$$\binom{m-k}{2} + (m-k) + 2(m-k)k - X_A \; > \; 2\binom{m-k}{2} + (m-k)k,$$

or, solving for k,

$$\frac{2m - \sqrt{m^2 - 6X_A}}{3} \; \leq \; k \; \leq \; \frac{2m + \sqrt{m^2 - 6X_A}}{3}$$

MSTD, counting overlaps

Let $|A| = m$, $|F| = k$, and $|R| = m - k$. Let X_A denote the number of nonredundant collisions in A. Then, A is MSTD if

$$\binom{m-k}{2} + (m-k) + 2(m-k)k - X_A \ > \ 2\binom{m-k}{2} + (m-k)k,$$

or, solving for k,

$$\frac{2m - \sqrt{m^2 - 6X_A}}{3} \ \leq \ k \ \leq \ \frac{2m + \sqrt{m^2 - 6X_A}}{3}$$

Takeaway: If X_A is at most a small constant times m^2, then for most values of k, A is MSTD.

Expected value of X_A

When A is chosen randomly from $\mathcal{S}_m$, X_A is a random variable.

Expected value of X_A

When A is chosen randomly from $\mathcal{S}_m$, X_A is a random variable.

Lemma (A. et al. 2022+)

Suppose A is chosen from $\mathcal{S}_m$ uniformly at random. Then,

$$\mathbb{E}[X_A] \leq 0.42\frac{m^4}{n}.$$

Expected value of X_A

When A is chosen randomly from $\mathcal{S}_m$, X_A is a random variable.

Lemma (A. et al. 2022+)

Suppose A is chosen from $\mathcal{S}_m$ uniformly at random. Then,

$$\mathbb{E}[X_A] \leq 0.42\frac{m^4}{n}.$$

By Markov's inequality, the probability that X_A exceeds c times its expectation is at most $1/c$.

Expected value of X_A

When A is chosen randomly from $\mathcal{S}_m$, X_A is a random variable.

Lemma (A. et al. 2022+)

Suppose A is chosen from $\mathcal{S}_m$ uniformly at random. Then,

$$\mathbb{E}[X_A] \leq 0.42\frac{m^4}{n}.$$

By Markov's inequality, the probability that X_A exceeds c times its expectation is at most $1/c$.

When $m \leq 0.12\sqrt{n}$, this bound suffices to show that most subsets in $\mathcal{S}_m$ are MSTD.

Expected value of X_A

When A is chosen randomly from $\mathcal{S}_m$, X_A is a random variable.

Lemma (A. et al. 2022+)

Suppose A is chosen from $\mathcal{S}_m$ uniformly at random. Then,

$$\mathbb{E}[X_A] \leq 0.42\frac{m^4}{n}.$$

By Markov's inequality, the probability that X_A exceeds c times its expectation is at most $1/c$.

When $m \leq 0.12\sqrt{n}$, this bound suffices to show that most subsets in $\mathcal{S}_m$ are MSTD. And, if we further restrict m, we can prove that a very high proportion of subsets in $\mathcal{S}_m$ are MSTD!

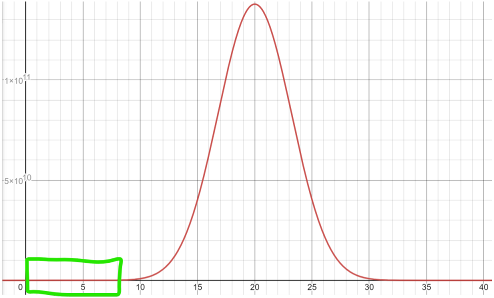
Where are the non-balanced sets?

We showed that when $6 < m < c\sqrt{n}$, there are more MSTD subsets of D_{2n} of size m than MDTS subsets.

Where are the non-balanced sets?

We showed that when $6 < m < c\sqrt{n}$, there are more MSTD subsets of D_{2n} of size m than MDTS subsets.

But most subsets of D_{2n} have size around n, not $\sqrt{n}$. We are focusing on a very small collection of subsets of D_{2n}!



Where are the non-balanced sets?

We showed that when $6 < m < c\sqrt{n}$, there are more MSTD subsets of D_{2n} of size m than MDTS subsets.

But most subsets of D_{2n} have size around n, not $\sqrt{n}$. We are focusing on a very small collection of subsets of D_{2n}!

However, recall that almost all subsets of D_{2n} are balanced. Computer-assisted methods suggest that a phase transition occurs around $m = O(\sqrt{n})$ where $\mathcal{S}_m$ goes from having mostly MSTD subsets to having mostly balanced subsets.

Generalizations

Generalized dihedral groups

Recall that for an abelian group G, the *generalized dihedral group* of G is

$$\mathrm{Dih}(G) = \mathbb{Z}/2 \ltimes G$$

with the non-identity element of $\mathbb{Z}/2$ acting on G by inversion.

Generalized dihedral groups

Recall that for an abelian group G, the *generalized dihedral group* of G is

$$\mathrm{Dih}(G) = \mathbb{Z}/2 \ltimes G$$

with the non-identity element of $\mathbb{Z}/2$ acting on G by inversion.

Conjecture (GenDihMMSTDTMDTS)

$\mathrm{Dih}(G)$ has more MSTD subsets than MDTS subsets for all finite abelian groups G that contain an element of order at least 3.

Generalized dihedral groups

Recall that for an abelian group G, the *generalized dihedral group* of G is

$$\mathrm{Dih}(G) = \mathbb{Z}/2 \ltimes G$$

with the non-identity element of $\mathbb{Z}/2$ acting on G by inversion.

Conjecture (GenDihMMSTDTMDTS)

$\mathrm{Dih}(G)$ has more MSTD subsets than MDTS subsets for all finite abelian groups G that contain an element of order at least 3.

Our main theorems and methods for D_{2n} translate directly to $\mathrm{Dih}(G)$, as long as G doesn't have too many elements of order 2.

Infinite dihedral groups

We can also take $G = \mathbb{Z}^r$ if we restrict the $\mathbb{Z}^r$-components in $\mathrm{Dih}(\mathbb{Z}^r)$ to $[0, n-1]^r$:

Infinite dihedral groups

We can also take $G = \mathbb{Z}^r$ if we restrict the $\mathbb{Z}^r$-components in $\mathrm{Dih}(\mathbb{Z}^r)$ to $[0, n-1]^r$:

Theorem (A. et al. 2022+)

For all $n \gg 0$, more of the sets $A \subseteq \mathbb{Z}/2 \ltimes [0, n-1]^r \subseteq \mathrm{Dih}(\mathbb{Z}^r)$ of size m are MSTD than MDTS for $6 \leq m \leq c \cdot \sqrt{n}$ where c is a global constant.

Theorem (A. et al. 2022+)

For any $\epsilon > 0$, there exist m_ϵ and c_ϵ such that for all $n \gg 0$, if $m_\epsilon \leq m \leq c_\epsilon \sqrt{n}$, a proportion of at least $1 - \epsilon$ of the subsets are MSTD among $A \subseteq \mathbb{Z}/2 \ltimes [0, n-1]^r \subseteq \mathrm{Dih}(\mathbb{Z}^r)$ of size m.

Infinite dihedral groups

We can also take $G = \mathbb{Z}^r$ if we restrict the $\mathbb{Z}^r$-components in $\mathrm{Dih}(\mathbb{Z}^r)$ to $[0, n-1]^r$:

Theorem (A. et al. 2022+)

For all $n \gg 0$, more of the sets $A \subseteq \mathbb{Z}/2 \ltimes [0, n-1]^r \subseteq \mathrm{Dih}(\mathbb{Z}^r)$ of size m are MSTD than MDTS for $6 \leq m \leq c \cdot \sqrt{n}$ where c is a global constant.

Theorem (A. et al. 2022+)

For any $\epsilon > 0$, there exist m_ϵ and c_ϵ such that for all $n \gg 0$, if $m_\epsilon \leq m \leq c_\epsilon \sqrt{n}$, a proportion of at least $1 - \epsilon$ of the subsets are MSTD among $A \subseteq \mathbb{Z}/2 \ltimes [0, n-1]^r \subseteq \mathrm{Dih}(\mathbb{Z}^r)$ of size m.

Proof idea: Construct a bijection $\mathbb{Z}/2 \ltimes [0, n-1]^r \to D_{2n^r}$ that preserves collisions.

Future work

We would like to extend the bounds on m to show that for all n, D_{2n} has more MSTD sets than MDTS sets:

Future work

We would like to extend the bounds on m to show that for all n, D_{2n} has more MSTD sets than MDTS sets:

- $c\sqrt{n} < m \leq n$.
- Carefully count collisions.
- Analyze missed elements for m close to n.
- Construct injections from MDTS sets to MSTD sets in $\mathcal{S}_m$.

Future work

We would like to extend the bounds on m to show that for all n, D_{2n} has more MSTD sets than MDTS sets:

- $c\sqrt{n} < m \leq n$.
- Carefully count collisions.
- Analyze missed elements for m close to n.
- Construct injections from MDTS sets to MSTD sets in $\mathcal{S}_m$.

Any results we prove for D_{2n} will hopefully translate to generalized dihedral groups.

Expected size

Calculate expected sizes of $|A+A|$ and $|A-A|$.

Expected size

Calculate expected sizes of $|A+A|$ and $|A-A|$.

Theorem (A. et al. 2022+)

For prime n and a random set $A \subseteq D_{2n}$ with $|A| = m$, we have that

$$\mathbb{E}(|A-A|) = 2n - n\frac{\binom{n}{m}}{\binom{2n}{m}}2^m - n^2(n-1)\sum_{k=1}^{m-1}\frac{\binom{n+k-m-1}{m-k-1}\binom{n-k-1}{k-1}}{\binom{2n}{m}k(m-k)} - \frac{(n-1)(2n)\binom{n-m-1}{m-1}}{(m)\binom{2n}{m}}.$$

Expected size

Calculate expected sizes of $|A+A|$ and $|A-A|$.

Theorem (A. et al. 2022+)

For prime n and a random set $A \subseteq D_{2n}$ with $|A| = m$, we have that

$$\mathbb{E}(|A-A|) = 2n - n\frac{\binom{n}{m}}{\binom{2n}{m}}2^m - n^2(n-1)\sum_{k=1}^{m-1}\frac{\binom{n+k-m-1}{m-k-1}\binom{n-k-1}{k-1}}{\binom{2n}{m}k(m-k)} - \frac{(n-1)(2n)\binom{n-m-1}{m-1}}{(m)\binom{2n}{m}}.$$

Would also require understanding of variance.

Expected size for difference sets

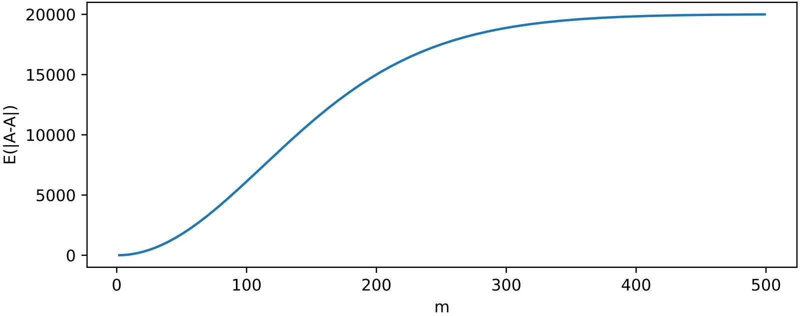


Figure: $\mathbb{E}(|A-A|)$ versus m for $n = 10007$.

Acknowledgments

Thank you!

This research was conducted as part of the **2022 SMALL REU program** at Williams College, and was supported by **NSF Grant DMS1947438**, **Harvey Mudd College**, and **Williams College** funds. We thank Steven J. Miller and our colleagues from the 2022 SMALL REU program for many helpful conversations.

References

[1] Peter V. Hegarty and Steven J. Miller. "When almost all sets are difference dominated". In: *Random Structures Algorithms* 35.1 (2009), pp. 118–136. ISSN: 1042-9832. DOI: 10.1002/rsa.20268. arXiv: 0707.3417 [math.NT]. URL: https://doi.org/10.1002/rsa.20268.

[2] Virginia Hogan and Steven J. Miller. *When Generalized Sumsets are Difference Dominated*. 2013. arXiv: 1301.5703 [math.NT].

[3] Greg Martin and Kevin O'Bryant. "Many sets have more sums than differences". In: CRM Proc. Lecture Notes 43 (2007), pp. 287–305. DOI: 10.1090/crmp/043/16. arXiv: math/0608131 [math.NT]. URL: https://doi.org/10.1090/crmp/043/16.