Phase Transitions in Generalized Sumsets

Ginny Hogan and Kevin Vissuet
Advisor: Steven J. Miller
Young Mathematicians Conference
The Ohio State University, July 29, 2012

Outline

Introduction

Statement

A finite set of integers, $|A|$ its size. Form

- Sumset: $A + A = \{a_i + a_j : a_j, a_j \in A\}$.
- Difference set: $A - A = \{a_i - a_j : a_j, a_j \in A\}$.

Statement

A finite set of integers, $|A|$ its size. Form

- Sumset: $A + A = \{a_i + a_j : a_j, a_j \in A\}$.
- Difference set: $A - A = \{a_i - a_j : a_j, a_j \in A\}$.

Definition

We say A is difference dominated if $|A - A| > |A + A|$, balanced if $|A - A| = |A + A|$ and sum dominated (or an MSTD set) if $|A + A| > |A - A|$.

Questions

We expect a generic set to be difference dominated:

- addition is commutative, subtraction isn't.
- Generic pair (a_i, a_j) gives 1 sum, 2 differences.

Questions

We expect a generic set to be difference dominated:

- addition is commutative, subtraction isn't.
- Generic pair (a_i, a_j) gives 1 sum, 2 differences.

Questions

- What happens when we increase the number of summands?
- What happens if we let the probability of choosing elements decays with N?
- What happens if we take subsets of non-abelian groups?

Past Results

- Martin and O'Bryant, 2006: Positive percentage of sets are MSTD when sets chosen with uniform probability.

Past Results

- Martin and O'Bryant, 2006: Positive percentage of sets are MSTD when sets chosen with uniform probability.
- Iyer, Lazarev, Miller, Zhang, 2011: Generalized results above to an arbitrary number of summands.

Past Results

- Hegarty and Miller, 2008: When elements chosen with probability $p(N) \to 0$ as $N \to \infty$, then $|A - A| > |A + A|$ almost surely.

Past Results

- Hegarty and Miller, 2008: When elements chosen with probability $p(N) \to 0$ as $N \to \infty$, then $|A - A| > |A + A|$ almost surely.
- Found critical value of $\delta = \frac{1}{2}$ for probability $p(N) = cN^{-\delta}$, $\delta \in (0, 1)$. δ corresponds to the order of the number of repeated elements in the sumset.
- We call the critical value the phase transition because it is the value at which the order of the number of repeated elements is as large as the number of distinct elements.

Generalized Sumsets

Definition

For $s > d$, consider the Generalized Sumset $A_{s,d} = A + \cdots + A - A - \cdots - A$ where we have s plus signs and d minus signs. Let $h = s + d$.

Generalized Sumsets

Definition

For $s > d$, consider the Generalized Sumset $A_{s,d} = A + \cdots + A - A - \cdots - A$ where we have s plus signs and d minus signs. Let $h = s + d$.

We want to study the size of this set as a function of s,d, and δ for probability $p(N) = cN^{-\delta}$.

Our goal: Extend the results of Hegarty-Miller to the case of Generalized Sumsets and determine where the phase transition occurs for $h > 2$.

Questions

Questions

Questions

Questions

Questions

- How does d_i effect the size of A_{s_i,d_i}?

Questions

Questions

- How does d_i effect the size of A_{s_i,d_i}?
- Can we say anything about the relationship between δ and the ratio $\frac{|A_{s_1,d_1}|}{|A_{s_2,d_2}|}$ for $s_1 + d_1 = s_2 + d_2 = h$?

Questions

Questions

- How does d_i effect the size of A_{s_i,d_i}?
- Can we say anything about the relationship between δ and the ratio $\frac{|A_{s_1,d_1}|}{|A_{s_2,d_2}|}$ for $s_1 + d_1 = s_2 + d_2 = h$?
- What is the critical value as a function of δ?

Cases for δ

To answer, we must consider three different cases for δ.

Cases for δ

To answer, we must consider three different cases for δ.

- Fast Decay: $\delta > \frac{h-1}{h}$.
- Critical Decay: $\delta = \frac{h-1}{h}$.
- Slow Decay: $\delta < \frac{h-1}{h}$.

Cases for δ

To answer, we must consider three different cases for δ.

- Fast Decay: $\delta > \frac{h-1}{h}$.
- Critical Decay: $\delta = \frac{h-1}{h}$.
- Slow Decay: $\delta < \frac{h-1}{h}$.

These three cases correspond to the speed at which the probability of choosing elements decays to 0.

Fast Decay

- For $\delta > \frac{h-1}{h}$, the set with more differences is larger 100% of the time.
- Ratio is a function of $\binom{h}{d}$.
- Results rely on the scarcity of elements chosen to be in A.

Proof I

- Compute the number of distinct h-tuples.

Proof I

- Compute the number of distinct h-tuples.

- For h-tuples $a = (a_1, \cdots, a_h)$,$b = (b_1, \cdots, b_h)$, define indicator variable $Y_{a,b}$ to be 1 when a and b generate the same element.

Proof I

- Compute the number of distinct h-tuples.
- For h-tuples $a = (a_1, \cdots, a_h)$,$b = (b_1, \cdots, b_h)$, define indicator variable $Y_{a,b}$ to be 1 when a and b generate the same element.
- Define $Y = \sum_{a,b} Y_{a,b}$

Proof I

- Compute the number of distinct h-tuples.
- For h-tuples $a = (a_1, \cdots, a_h)$,$b = (b_1, \cdots, b_h)$, define indicator variable $Y_{a,b}$ to be 1 when a and b generate the same element.
- Define $Y = \sum_{a,b} Y_{a,b}$
- Bound the expected value and variance of Y.

Proof II

- Use Chebyshev's Inequality:

$$\Pr\left(|X-\mu| \geq k\sigma\right) \leq \frac{1}{k^2}$$

- Show that Y is close to $E(Y)$.

Proof II

- Use Chebyshev's Inequality:

$$\Pr\left(|X-\mu| \geq k\sigma\right) \leq \frac{1}{k^2}$$

- Show that Y is close to $E(Y)$.

- Conclude that almost all h-tuples generate a distinct number as $N \to \infty$.

Proof II

- Use Chebyshev's Inequality:

$$\Pr\left(|X-\mu| \geq k\sigma\right) \leq \frac{1}{k^2}$$

- Show that Y is close to $E(Y)$.

- Conclude that almost all h-tuples generate a distinct number as $N \to \infty$.

- Using combinatorics, conclude that ratio is:
$\frac{|A_{s_1,d_1}|}{|A_{s_2,d_2}|} = \frac{\binom{h}{d_1}}{\binom{h}{d_2}} = \frac{s_2!d_2!}{s_1!d_1!}$.

Critical Decay

- Set with more minus signs is larger 100% of time.

Critical Decay

- Set with more minus signs is larger 100% of time.
- In the two-case, for $g(x) = 2\sum \frac{(-1)^{k-1}x^k}{(k+1)!}$, $S \sim g\left(\frac{c^2}{2}\right) N$ and $D \sim g\left(c^2\right) N$.

Critical Decay

- Set with more minus signs is larger 100% of time.

- In the two-case, for $g(x) = 2\sum \frac{(-1)^{k-1}x^k}{(k+1)!}$, $S \sim g\left(\frac{c^2}{2}\right) N$ and $D \sim g\left(c^2\right) N$.

- For $A + A + A$, $g(x) = \sum (-1)^{k-1}\left(\frac{1}{k12^k} + \frac{c_k}{(-8)^k}\right) x^k$ with $c_k = \int_{-\frac{1}{\sqrt{3}}}^{\frac{1}{\sqrt{3}}} (x^2 - 1)^k dx$.

Critical Decay

- Set with more minus signs is larger 100% of time.

- In the two-case, for $g(x) = 2\sum \frac{(-1)^{k-1}x^k}{(k+1)!}$, $S \sim g\left(\frac{c^2}{2}\right) N$ and $D \sim g\left(c^2\right) N$.

- For $A+A+A$, $g(x) = \sum (-1)^{k-1}\left(\frac{1}{k12^k} + \frac{c_k}{(-8)^k}\right) x^k$ with $c_k = \int_{-\frac{1}{\sqrt{3}}}^{\frac{1}{\sqrt{3}}} (x^2-1)^k dx$.

- For $A+A-A$, $g(x) = \sum_{k=1}^{m} (-1)^{k-1} \frac{1}{k!}((-\frac{3}{8})^k c_k + \frac{1}{k})x^k$.

Critical Decay

- Set with more minus signs is larger 100% of time.

- In the two-case, for $g(x) = 2\sum \frac{(-1)^{k-1}x^k}{(k+1)!}$, $S \sim g\left(\frac{c^2}{2}\right) N$ and $D \sim g\left(c^2\right) N$.

- For $A + A + A$, $g(x) = \sum (-1)^{k-1} \left(\frac{1}{k12^k} + \frac{c_k}{(-8)^k}\right) x^k$ with $c_k = \int_{-\frac{1}{\sqrt{3}}}^{\frac{1}{\sqrt{3}}} (x^2 - 1)^k dx$.

- For $A + A - A$, $g(x) = \sum_{k=1}^{m} (-1)^{k-1} \frac{1}{k!}((-\frac{3}{8})^k c_k + \frac{1}{k})x^k$.

Slow Decay

- If $\delta < \frac{h-1}{h}$, an even more delicate argument is needed.
- Now the number of repeated elements are of a higher order.
- Martingale Machinery of Kim and Vu.

Non-Abelian Finite Groups

Some new Definitions

- Since we are now looking at groups we need an analogous definition.

Some new Definitions

- Since we are now looking at groups we need an analogous definition.
- So the sumset becomes $S \cdot S = \{xy : x, y \in S\}$.
- While the sum-difference becomes $S \cdot S^{-1} = \{xy^{-1} : x, y \in S\}$.

Dihedral Group

- The non-abelian group we will look at for this presentation: the Dihedral Group with $2n$ elements (D_{2n}).

Dihedral Group

- The non-abelian group we will look at for this presentation: the Dihedral Group with $2n$ elements (D_{2n}).

	I	R_{90}	R_{180}	R_{270}	L_1	L_2	L_3	L_4
I	I	R_{90}	R_{180}	R_{270}	L_1	L_2	L_3	L_4
R_{90}	R_{90}	R_{180}	R_{270}	I	L_4	L_1	L_2	L_3
R_{180}	R_{180}	R_{270}	I	R_{90}	L_3	L_4	L_1	L_2
R_{270}	R_{270}	I	R_{90}	R_{180}	L_2	L_3	L_4	L_1
L_1	L_1	L_2	L_3	L_4	I	R_{90}	R_{180}	R_{270}
L_2	L_2	L_3	L_4	L_1	R_{270}	I	R_{90}	R_{180}
L_3	L_3	L_4	L_1	L_2	R_{180}	R_{270}	I	R_{90}
L_4	L_4	L_1	L_2	L_3	R_{90}	R_{180}	R_{270}	I

Dihedral Group

- The non-abelian group we will look at for this presentation: the Dihedral Group with $2n$ elements (D_{2n}).

	I	R_{90}	R_{180}	R_{270}	L_1	L_2	L_3	L_4
I	I	R_{90}	R_{180}	R_{270}	L_1	L_2	L_3	L_4
R_{90}	R_{90}	R_{180}	R_{270}	I	L_4	L_1	L_2	L_3
R_{180}	R_{180}	R_{270}	I	R_{90}	L_3	L_4	L_1	L_2
R_{270}	R_{270}	I	R_{90}	R_{180}	L_2	L_3	L_4	L_1
L_1	L_1	L_2	L_3	L_4	I	R_{90}	R_{180}	R_{270}
L_2	L_2	L_3	L_4	L_1	R_{270}	I	R_{90}	R_{180}
L_3	L_3	L_4	L_1	L_2	R_{180}	R_{270}	I	R_{90}
L_4	L_4	L_1	L_2	L_3	R_{90}	R_{180}	R_{270}	I

- Recall that a presentation for the dihedral group is D_{2n} is $\langle a, b | a^n = abab = b^2 = e \rangle$.

Dihedral Group

- The non-abelian group we will look at for this presentation: the Dihedral Group with $2n$ elements (D_{2n}).

	I	R_{90}	R_{180}	R_{270}	L_1	L_2	L_3	L_4
I	I	R_{90}	R_{180}	R_{270}	L_1	L_2	L_3	L_4
R_{90}	R_{90}	R_{180}	R_{270}	I	L_4	L_1	L_2	L_3
R_{180}	R_{180}	R_{270}	I	R_{90}	L_3	L_4	L_1	L_2
R_{270}	R_{270}	I	R_{90}	R_{180}	L_2	L_3	L_4	L_1
L_1	L_1	L_2	L_3	L_4	I	R_{90}	R_{180}	R_{270}
L_2	L_2	L_3	L_4	L_1	R_{270}	I	R_{90}	R_{180}
L_3	L_3	L_4	L_1	L_2	R_{180}	R_{270}	I	R_{90}
L_4	L_4	L_1	L_2	L_3	R_{90}	R_{180}	R_{270}	I

- Recall that a presentation for the dihedral group is D_{2n} is $\langle a, b | a^n = abab = b^2 = e \rangle$.
- Note: at least half the elements in D_{2n} are of order 2.

Theorem

Theorem

If we let S be a random subset of D_{2n} (if $\alpha \in D_{2n}$ then $\mathbb{P}(\alpha \in S) = 1/2$) then

$$\lim_{n\to\infty} \mathbb{P}(|S \cdot S| = |S \cdot S^{-1}|) = 1.$$

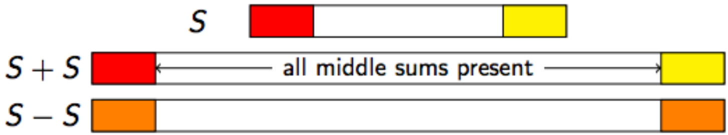
It is also true that

$$\lim_{n\to\infty} \mathbb{P}(|S \cdot S| = |S \cdot S^{-1}| = 2n) = 1.$$

We compute this instead, as it serve as a sufficient lower bound.

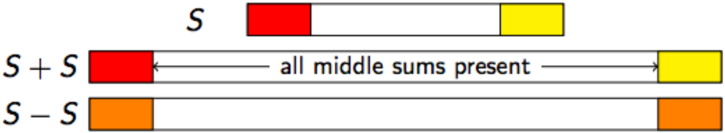
Intuition

- Key Idea: In the $\mathbb{Z}$ case, fringe matters most, middle sums and differences are present with high probability



Intuition

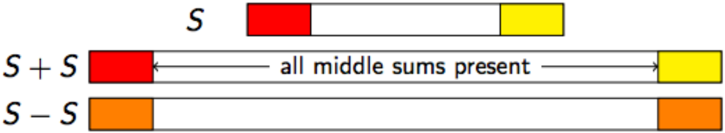
- Key Idea: In the $\mathbb{Z}$ case, fringe matters most, middle sums and differences are present with high probability



- *If we choose the "fringe" of S cleverly, the middle of S will become largely irrelevant. - Martin O'Bryant 2007*

Intuition

- Key Idea: In the $\mathbb{Z}$ case, fringe matters most, middle sums and differences are present with high probability



- *If we choose the "fringe" of S cleverly, the middle of S will become largely irrelevant. - Martin O'Bryant 2007*

- In $\mathbb{Z}/n\mathbb{Z}$ there is no fringe. So the "largely irrelevant" is the only thing that can be relevant.

Sketch of Proof

- Let $S \subseteq D_{2n}$

Sketch of Proof

- Let $S \subseteq D_{2n}$
- Let $S = R \cup F$ where R is the set of rotations in S and F is the set of flips in S.

Sketch of Proof

- Let $S \subseteq D_{2n}$
- Let $S = R \cup F$ where R is the set of rotations in S and F is the set of flips in S.

Set	Rotations in Set	Flips in Set
S	R	F
S+S	R+R, F+F	R+F, -R+F
S-S	R-R, F+F	R+F

Sketch of Proof

- Let $S \subseteq D_{2n}$
- Let $S = R \cup F$ where R is the set of rotations in S and F is the set of flips in S.

Set	Rotations in Set	Flips in Set
S	R	F
S+S	R+R, F+F	R+F, -R+F
S-S	R-R, F+F	R+F

- For now we can ignore $R - R, -R + F$.

Sketch of Proof

- Let $S \subseteq D_{2n}$
- Let $S = R \cup F$ where R is the set of rotations in S and F is the set of flips in S.

Set	Rotations in Set	Flips in Set
S	R	F
S+S	R+R, F+F	R+F, -R+F
S-S	R-R, F+F	R+F

- For now we can ignore $R - R, -R + F$.
- We use that both $F + F$ and $R + F$ are in $S \cdot S$ and $S \cdot S^{-1}$ to compute lower bounds.

Reduction to Cyclic Groups

- Note that elements in R have the form a^i, and elements in F have the form $a^i b$,

Reduction to Cyclic Groups

- Note that elements in R have the form a^i, and elements in F have the form $a^i b$,
- so elements in $R + R$ look like a^{x+y}, while elements in $F + F$ look like $a^{x-y} b$.

Reduction to Cyclic Groups

- Note that elements in R have the form a^i, and elements in F have the form $a^i b$,
- so elements in $R + R$ look like a^{x+y}, while elements in $F + F$ look like $a^{x-y} b$.
- This observation allows us to look at powers of the elements as an cyclic group instead.

Flips and Rotations

- If we let R^* and F^* be random subsets of $\mathbb{Z}/n\mathbb{Z}$ then we have the following:

$$\begin{aligned}\mathbb{P}(|S\cdot S^{-1}| = |S\cdot S|) &\geq \mathbb{P}(|S\cdot S^{-1}| = 2n \text{ and } |S\cdot S| = 2n)\\ &\geq \mathbb{P}(|S\cdot S^{-1}| = 2n)\mathbb{P}(S\cdot S = 2n)\\ &\geq \mathbb{P}(|S\cdot S^{-1}| = 2n)^2\\ &= \mathbb{P}(|F^* - F^*| = n \;\&\; |F^* + R^*| = n)^2\end{aligned}$$

Probability of Missing Elements

- We now proceed by computing the probability that an element is *not* in the desired set.

Lemma (Number of Missing Flips)

$\mathbb{P}(k \notin F^* + R^*) = O((3/4)^n)$

- This follows immediately from the number of ways one can add numbers in $\mathbb{Z}/n\mathbb{Z}$ to equal k.

Lemma

Lemma (Number of Missing Rotations)

$\mathbb{P}(k \notin F^* - F^*) = \frac{f(n/d)^d}{2^n} \leq (\varphi/2)^n$ where $gcd(k, n) = d$ and $f(n) = F(n+1) + F(n-1)$ where $F(n)$ is the nth Fibonacci number

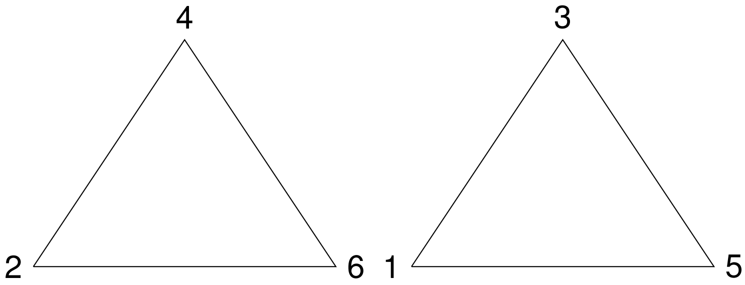
The proof does not follow as immediately as it requires some combinatorics.

Why do we care about the gcd

- Here's an example what the polygons would look like when $F^* = \mathbb{Z}/6\mathbb{Z}$ and $k \equiv 2 \pmod 6$

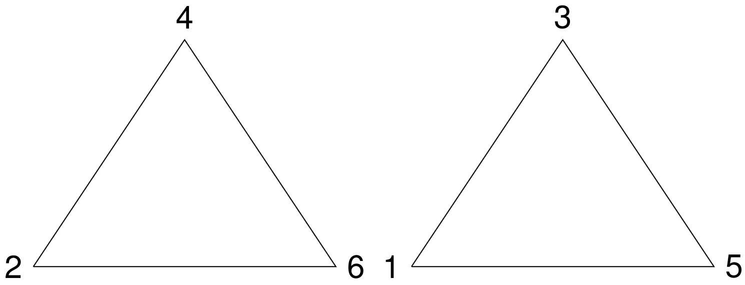
Why do we care about the gcd

- Here's an example what the polygons would look like when $F^* = \mathbb{Z}/6\mathbb{Z}$ and $k \equiv 2 \pmod 6$



Why do we care about the gcd

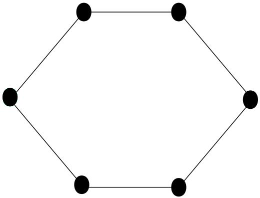
- Here's an example what the polygons would look like when $F^* = \mathbb{Z}/6\mathbb{Z}$ and $k \equiv 2 \pmod 6$



- Note that we get $\gcd(2,6) = 2$ number of polygons and they each have $6/\gcd(2,6) = 3$ vertices.

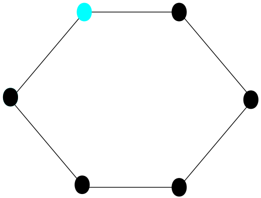
So where does Fibonacci come from?

- So the problem is thus reduced to counting the number of ways how the vertices of a n polygon can be colored either red or blue such that there are no 2 red vertices next to each other.



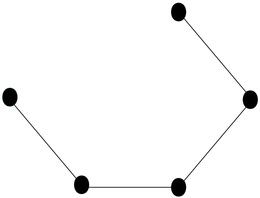
So where does Fibonacci come from?

- So the problem is thus reduced to counting the number of ways how the vertices of a n polygon can be colored either red or blue such that there are no 2 red vertices next to each other.



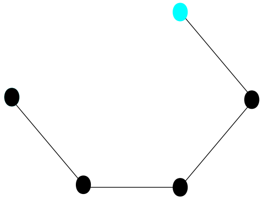
So where does Fibonacci come from?

- So the problem is thus reduced to counting the number of ways how the vertices of a n polygon can be colored either red or blue such that there are no 2 red vertices next to each other.



So where does Fibonacci come from?

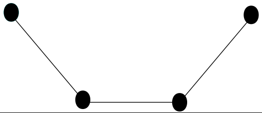
- So the problem is thus reduced to counting the number of ways how the vertices of a n polygon can be colored either red or blue such that there are no 2 red vertices next to each other.



So where does Fibonacci come from?

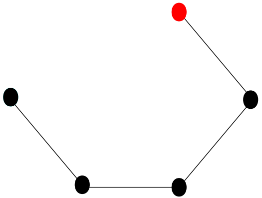
- So the problem is thus reduced to counting the number of ways how the vertices of a n polygon can be colored either red or blue such that there are no 2 red vertices next to each other.

$$f(4) =$$



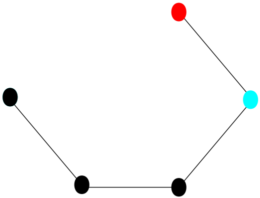
So where does Fibonacci come from?

- So the problem is thus reduced to counting the number of ways how the vertices of a n polygon can be colored either red or blue such that there are no 2 red vertices next to each other.



So where does Fibonacci come from?

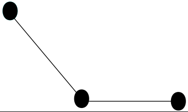
- So the problem is thus reduced to counting the number of ways how the vertices of a n polygon can be colored either red or blue such that there are no 2 red vertices next to each other.



So where does Fibonacci come from?

- So the problem is thus reduced to counting the number of ways how the vertices of a n polygon can be colored either red or blue such that there are no 2 red vertices next to each other.

$$f(3) =$$



Proof II

- Although there are dependency issues, for the sake of this theorem we can be crude enough to say if any element is missing, then all elements are missing.

Proof II

- Although there are dependency issues, for the sake of this theorem we can be crude enough to say if any element is missing, then all elements are missing.
- So by our two lemmas we have that as n goes to infinity,

$$\mathbb{P}(|F^* - F^*| = n \text{ and } |F^* + R^*| = n)^2 = 1.$$

Proof II

- Although there are dependency issues, for the sake of this theorem we can be crude enough to say if any element is missing, then all elements are missing.
- So by our two lemmas we have that as n goes to infinity,

$$\mathbb{P}(|F^* - F^*| = n \text{ and } |F^* + R^*| = n)^2 = 1.$$

- Since this is the lower bound, we are done.

Additional Results

Additional Results

Theorem (Semi-Direct Products)

For the group $\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/m\mathbb{Z}$, if either n or m go to infinity then, $\mathbb{P}(|S \cdot S| = |S \cdot S^{-1}|) = 1$.

Additional Results

Theorem (Semi-Direct Products)

For the group $\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/m\mathbb{Z}$, if either n or m go to infinity then, $\mathbb{P}(|S \cdot S| = |S \cdot S^{-1}|) = 1$.

Theorem ([Abelian Groups)

As the size of an abelian group approaches infinity, then $\mathbb{P}(|S \cdot S| = |S \cdot S^{-1}|) = 1$.

Ping Pong

Theorem (Free Group)

If we let $\langle a, b \rangle_l$ be all words up to length l and $S \subseteq \langle a, b \rangle_l$ then as l goes to infinity we have that:

$$\mathbb{P}(|S \cdot S| \geq |S \cdot S^{-1}|) = 1$$


TAKE THAT
SUM DIFFERENCE!
Stanford
ATHLETICS
JOOLA
FRANCE
138

Acknowledgements

We would like to thank the National Science Foundation for supporting our research through NSF Grant DMS0850577 and NSF Grant DMS0970067, as well as Williams College and The Ohio State University.

Bibliography

Bibliography

- G. Iyer, O. Lazarev, S.J. Miller, L. Zhang. *Generalized More Sums Than Differences Sets*. Journal of Number Theory. (132(2012),no 5, 1054–1073).
- O. Lazarev, S.J. Miller, K. O'Bryant. *Distribution of Missing Sums in Sumsets*. 2012.
- P. V. Hegarty and S. J. Miller, *When almost all sets are difference dominated*, Random Structures and Algorithms. **35** (2009), no. 1, 118–136.
- G. Martin, K. O'Bryant. *Many Sets Have More Sums Than Differences*, Additive Combinatorics, 287–305, 2007.