Additive combinatorics from Combinatorial perspective

Huy Tuan Pham

California Institute of Technology

NZMRI - January 2026

Additive combinatorics

Setup:

- Let G be an abelian group.
- Given a finite $A \subseteq G$, define the sumset $A + A = \{a + b : a, b \in A\}$.
- Define the doubling $K = \frac{|A+A|}{|A|}$.

Additive combinatorics

Setup:

- Let G be an abelian group.
- Given a finite $A \subseteq G$, define the sumset $A + A = \{a + b : a, b \in A\}$.
- Define the doubling $K = \frac{|A+A|}{|A|}$.

Theme in additive combinatorics:

$$\text{Small doubling } K \qquad \leftrightarrow \qquad \text{Additively structured } A.$$

Additive structures and Freiman's theorem

Example:

- $G = \mathbb{Z}$.
- For any finite $A \subseteq \mathbb{Z}$:
  - $|A + A| \leq \binom{|A|+1}{2}$.
  - $|A + A| \geq 2|A| - 1$, with equality iff A is an arithmetic progression.

Additive structures and Freiman's theorem

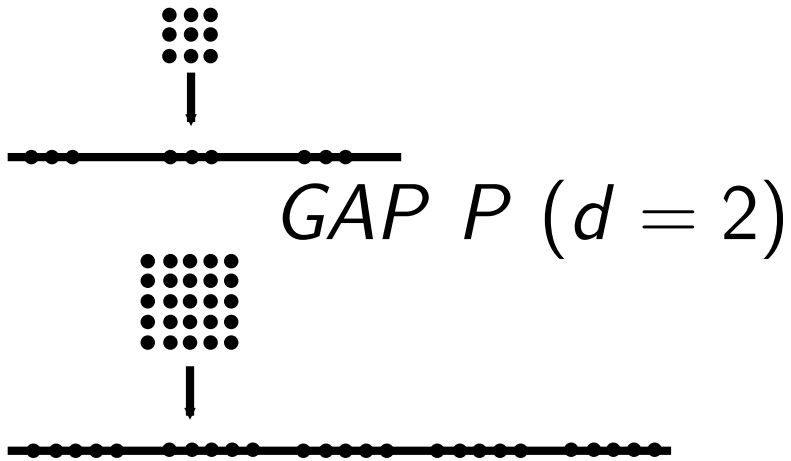
Example:

- $G = \mathbb{Z}$.
- For any finite $A \subseteq \mathbb{Z}$:
  - $|A + A| \leq \binom{|A|+1}{2}$.
  - $|A + A| \geq 2|A| - 1$, with equality iff A is an arithmetic progression.

In general, for bounded d, a generalized arithmetic progression (GAP)

$$P := x_0 + \left\{ \sum_{i=1}^{d} a_i x_i : \ell_i \leq a_i \leq u_i \right\}$$

has a small doubling.



Additive structures and Freiman-Ruzsa's theorem

For $A \subseteq \mathbb{Z}$:

- $|A+A| \geq 2|A|-1$, with equality iff A is an arithmetic progression.
- $|A+A| \leq \binom{|A|+1}{2}$.

In general, any dense subset of a generalized arithmetic progression with bounded dimension d has bounded doubling K.

Additive structures and Freiman-Ruzsa's theorem

For $A \subseteq \mathbb{Z}$:

- $|A+A| \geq 2|A|-1$, with equality iff A is an arithmetic progression.
- $|A+A| \leq \binom{|A|+1}{2}$.

In general, any dense subset of a generalized arithmetic progression with bounded dimension d has bounded doubling K.

Theorem (Freiman's theorem '64, Ruzsa '92, '94)

If $A \subseteq \mathbb{Z}$ is so that $|A+A| \leq K|A|$, then A is contained in a GAP P of dimension $d = O_K(1)$ and size $|P| = O_K(|A|)$.

Additive structures and Freiman-Ruzsa's theorem

For $A \subseteq \mathbb{Z}$:

- $|A+A| \geq 2|A|-1$, with equality iff A is an arithmetic progression.
- $|A+A| \leq \binom{|A|+1}{2}$.

In general, any dense subset of a generalized arithmetic progression with bounded dimension d has bounded doubling K.

Theorem (Freiman's theorem '64, Ruzsa '92, '94)

If $A \subseteq \mathbb{Z}$ is so that $|A+A| \leq K|A|$, then A is contained in a GAP P of dimension $d = O_K(1)$ and size $|P| = O_K(|A|)$.

Quantitative aspects of Freiman's theorem are of fundamental interest in additive combinatorics.

Perspectives on sets with small doubling

Major theme in additive combinatorics:

A has small doubling $\frac{|A+A|}{|A|} \leq K \quad \Rightarrow \quad A$ is structured/ dense in a structured object.

Perspectives on sets with small doubling

Major theme in additive combinatorics:

A has small doubling $\frac{|A+A|}{|A|} \leq K \quad \Rightarrow \quad A$ is structured/ dense in a structured object.

Applications: Random matrix theory, approximate groups and growth in groups, sum-product estimates, Szemerédi's theorem, Meyer set (quasicrystals), theoretical computer science.

Perspectives on sets with small doubling

Major theme in additive combinatorics:

A has small doubling $\frac{|A+A|}{|A|} \leq K \quad \Rightarrow \quad A$ is structured/ dense in a structured object.

Applications: Random matrix theory, approximate groups and growth in groups, sum-product estimates, Szemerédi's theorem, Meyer set (quasicrystals), theoretical computer science.

Drawback: Weak quantitative dependence on K, only applicable when K is very small compared to $|A|$.

Perspectives on sets with small doubling

Many applications require to allow for K to grow in $|A|$ and motivate different notions of structure:

- Structural: What is the structure of sets A with small doubling $K_A \leq K$?

Perspectives on sets with small doubling

Many applications require to allow for K to grow in $|A|$ and motivate different notions of structure:

- Structural: What is the structure of sets A with small doubling $K_A \leq K$?
- Statistical: Are there few sets A with small doubling $K_A \leq K$?

Perspectives on sets with small doubling

Many applications require to allow for K to grow in $|A|$ and motivate different notions of structure:

- Structural: What is the structure of sets A with small doubling $K_A \leq K$?
- Statistical: Are there few sets A with small doubling $K_A \leq K$?
- Probabilistic: Can every sumset $A + A$ for A with small doubling $K_A \leq K$ be efficiently approximated using few bits?

Perspectives on sets with small doubling

Many applications require to allow for K to grow in $|A|$ and motivate different notions of structure:

- Structural: What is the structure of sets A with small doubling $K_A \leq K$?
- Statistical: Are there few sets A with small doubling $K_A \leq K$?
- Probabilistic: Can every sumset $A + A$ for A with small doubling $K_A \leq K$ be efficiently approximated using few bits?

New approach:

- Combinatorial: "Forget" the group structure and move to general graph-theoretic representation of sets with small doubling.

Perspectives on sets with small doubling

Many applications require to allow for K to grow in $|A|$ and motivate different notions of structure:

- Structural: What is the structure of sets A with small doubling $K_A \leq K$?
- Statistical: Are there few sets A with small doubling $K_A \leq K$?
- Probabilistic: Can every sumset $A + A$ for A with small doubling $K_A \leq K$ be efficiently approximated using few bits?

New approach:

- Combinatorial: "Forget" the group structure and move to general graph-theoretic representation of sets with small doubling.
- Probabilistic: Probe and approximate the structure of sets with small doubling via randomness.

New perspectives

New perspectives and new ways to quantify the complexity of sets with small doubling:

- Resolve old questions about classical notion of structure.
- Quantitatively efficient or nearly optimal.
- Provide nontrivial information already when $K = o(|A|)$.
- Combinatorial/Probabilistic perspective: Flexible and generalize significantly beyond additive setting.

New perspectives

Complexity notion Key ingredient	Applications
Expanding structures in sets with small doubling Main combinatorial lemma	**Ruzsa's conjecture;** **Counting sets with small doubling in general groups;** **Ramsey properties of random Cayley graphs - Alon's conjecture;** Robust Freiman-Ruzsa lemma; Random sumset extractors; Dimension of sets with small doubling
Low-complexity subsets of sumsets Efficient covering lemma	**Independence number of sparse random Cayley graphs;** Large sets which are not sumsets (Green); Structured subsets of sumsets of dense sets (Lovett)
Low-complexity approximations of sumsets Approximation lemma	**Sharp counting of sets with small doubling in abelian groups (Alon-Balogh-Morris-Samotij)**

Additive structures and Freiman-Ruzsa's theorem

We say that an abelian group G has exponent r if r is the smallest integer such that the order of every group element divides r.

Example: $G = \mathbb{Z}_r^d$.

Additive structures and Freiman-Ruzsa's theorem

We say that an abelian group G has exponent r if r is the smallest integer such that the order of every group element divides r.

Example: $G = \mathbb{Z}_r^d$.

For $A \subseteq G$ for a finite abelian group G:

- $|A + A| \geq |A|$, with equality iff A is a subgroup of G.

Additive structures and Freiman-Ruzsa's theorem

We say that an abelian group G has exponent r if r is the smallest integer such that the order of every group element divides r.

Example: $G = \mathbb{Z}_r^d$.

For $A \subseteq G$ for a finite abelian group G:

- $|A + A| \geq |A|$, with equality iff A is a subgroup of G.

Question

What can we say about sets $A \subseteq G$ with $|A + A| \leq K|A|$?

Additive structures and Freiman-Ruzsa's theorem

We say that an abelian group G has exponent r if r is the smallest integer such that the order of every group element divides r.

For $A \subseteq G$ for a finite abelian group G:

- $|A+A| \geq |A|$, with equality iff A is a subgroup of G.

Theorem (Ruzsa's theorem, '99)

If G is an abelian group with exponent r and $A \subseteq G$ is so that $|A+A| \leq K|A|$, then A is contained in subgroup H of size $|H| = O_{r,K}(|A|)$.

Additive structures and Freiman-Ruzsa's theorem

We say that an abelian group G has exponent r if r is the smallest integer such that the order of every group element divides r.

For $A \subseteq G$ for a finite abelian group G:

- $|A+A| \geq |A|$, with equality iff A is a subgroup of G.

Theorem (Ruzsa's theorem, '99)

If G is an abelian group with exponent r and $A \subseteq G$ is so that $|A+A| \leq K|A|$, then A is contained in subgroup H of size $|H| = O_{r,K}(|A|)$.

Conjecture (Ruzsa's conjecture, '99)

There is a constant $C > 0$ such that the following holds. If G is an abelian group with exponent r and $A \subseteq G$ is so that $|A+A| \leq K|A|$, then A is contained in subgroup H of size $|H| \leq r^{CK}|A|$.

Additive structures and Freiman-Ruzsa's theorem

We say that an abelian group G has exponent r if r is the smallest integer such that the order of every group element divides r.

For $A \subseteq G$ for a finite abelian group G:

- $|A+A| \geq |A|$, with equality iff A is a subgroup of G.

Theorem (Ruzsa's theorem, '99)

If G is an abelian group with exponent r and $A \subseteq G$ is so that $|A+A| \leq K|A|$, then A is contained in subgroup H of size $|H| = O_{r,K}(|A|)$.

Conjecture (Ruzsa's conjecture, '99)

There is a constant $C > 0$ such that the following holds. If G is an abelian group with exponent r and $A \subseteq G$ is so that $|A+A| \leq K|A|$, then A is contained in subgroup H of size $|H| \leq r^{CK}|A|$.

In general, we may need $|H| \geq r^{(2-o(1))K}|A|$.

Additive structures and Freiman-Ruzsa's theorem

Theorem (Ruzsa's theorem, '99)

If G is an abelian group with exponent r and $A \subseteq G$ is so that $|A+A| \leq K|A|$, then A is contained in subgroup H of size $|H| = O_{r,K}(|A|)$.

Conjecture (Ruzsa's conjecture, '99)

There is a constant $C > 0$ such that the following holds. If G is an abelian group with exponent r and $A \subseteq G$ is so that $|A+A| \leq K|A|$, then A is contained in subgroup H of size $|H| \leq r^{CK}|A|$.

Additive structures and Freiman-Ruzsa's theorem

Theorem (Ruzsa's theorem, '99)

If G is an abelian group with exponent r and $A \subseteq G$ is so that $|A+A| \leq K|A|$, then A is contained in subgroup H of size $|H| = O_{r,K}(|A|)$.

Conjecture (Ruzsa's conjecture, '99)

There is a constant $C > 0$ such that the following holds. If G is an abelian group with exponent r and $A \subseteq G$ is so that $|A+A| \leq K|A|$, then A is contained in subgroup H of size $|H| \leq r^{CK}|A|$.

In general, we may need $|H| \geq r^{(2-o(1))K}|A|$.

Additive structures and Freiman-Ruzsa's theorem

Theorem (Ruzsa's theorem, '99)

If G is an abelian group with exponent r and $A \subseteq G$ is so that $|A+A| \leq K|A|$, then A is contained in subgroup H of size $|H| = O_{r,K}(|A|)$.

Conjecture (Ruzsa's conjecture, '99)

There is a constant $C > 0$ such that the following holds. If G is an abelian group with exponent r and $A \subseteq G$ is so that $|A+A| \leq K|A|$, then A is contained in subgroup H of size $|H| \leq r^{CK}|A|$.

In general, we may need $|H| \geq r^{(2-o(1))K}|A|$.

Example:

- $G = \mathbb{Z}_r^d$, $A = \{0, e_1, \ldots, e_d\}$.
- $|A+A| = \frac{(d+1)(d+2)}{2} = \frac{d+2}{2}|A|$.
- $|\langle A \rangle| = |G| = r^d$.

Additive structures and Freiman-Ruzsa's theorem

Theorem (Ruzsa's theorem '99)

If G is an abelian group with exponent r and $A \subseteq G$ is so that $|A+A| \leq K|A|$, then A is contained in subgroup H of size $|H| = O_{r,K}(|A|)$.

Conjecture (Ruzsa's conjecture, '99)

There is a constant $C > 0$ such that the following holds. If G is an abelian group with exponent r and $A \subseteq G$ is so that $|A+A| \leq K|A|$, then A is contained in subgroup H of size $|H| \leq r^{CK}|A|$.

Additive structures and Freiman-Ruzsa's theorem

Theorem (Ruzsa's theorem '99)

If G is an abelian group with exponent r and $A \subseteq G$ is so that $|A+A| \leq K|A|$, then A is contained in subgroup H of size $|H| = O_{r,K}(|A|)$.

Conjecture (Ruzsa's conjecture, '99)

There is a constant $C > 0$ such that the following holds. If G is an abelian group with exponent r and $A \subseteq G$ is so that $|A+A| \leq K|A|$, then A is contained in subgroup H of size $|H| \leq r^{CK}|A|$.

Theorem (Gowers-Green-Manners-Tao, '24)

If G is an abelian group with exponent r and $A \subseteq G$ is so that $|A+A| \leq K|A|$, then there is a subgroup H with $|H| \leq K^C|A|$ for which A is covered by K^C translates of H.

Previous results

Ruzsa's conjecture '99

There is a constant $C > 0$ such that the following holds. If G is an abelian group with exponent r and $A \subseteq G$ is so that $|A + A| \leq K|A|$, then A is contained in subgroup H of size $|H| \leq r^{CK}|A|$.

Previous results

Ruzsa's conjecture '99

There is a constant $C > 0$ such that the following holds. If G is an abelian group with exponent r and $A \subseteq G$ is so that $|A + A| \leq K|A|$, then A is contained in subgroup H of size $|H| \leq r^{CK}|A|$.

Theorem (Ruzsa '99)

We can find $H \supseteq A$ with $|H| \leq K^2 r^{K^4}|A|$.

Previous results

Ruzsa's conjecture '99

There is a constant $C > 0$ such that the following holds. If G is an abelian group with exponent r and $A \subseteq G$ is so that $|A + A| \leq K|A|$, then A is contained in subgroup H of size $|H| \leq r^{CK}|A|$.

Theorem (Ruzsa '99)

We can find $H \supseteq A$ with $|H| \leq K^2 r^{K^4}|A|$.

Theorem (Green-Ruzsa '06)

We can find $H \supseteq A$ with $|H| \leq K^2 r^{2K^2-2}|A|$.

Previous results

Ruzsa's conjecture '99

There is a constant $C > 0$ such that the following holds. If G is an abelian group with exponent r and $A \subseteq G$ is so that $|A + A| \leq K|A|$, then A is contained in subgroup H of size $|H| \leq r^{CK}|A|$.

Theorem (Ruzsa '99)

We can find $H \supseteq A$ with $|H| \leq K^2 r^{K^4}|A|$.

Theorem (Green-Ruzsa '06)

We can find $H \supseteq A$ with $|H| \leq K^2 r^{2K^2-2}|A|$.

Theorem (Sanders '12)

We can find $H \supseteq A$ with $|H| \leq r^{K(\log K)^{O(1)}}|A|$.

Previous results - The case of prime torsion

Ruzsa's conjecture '99

There is a constant $C > 0$ such that the following holds. If G is an abelian group with exponent r and $A \subseteq G$ is so that $|A + A| \leq K|A|$, then A is contained in subgroup H of size $|H| \leq r^{CK}|A|$.

Previous results - The case of prime torsion

Ruzsa's conjecture '99

There is a constant $C > 0$ such that the following holds. If G is an abelian group with exponent r and $A \subseteq G$ is so that $|A + A| \leq K|A|$, then A is contained in subgroup H of size $|H| \leq r^{CK}|A|$.

Theorem (Green-Tao '09)

For $G = \mathbb{F}_2^d$, we can find $H \supseteq A$ with $|H| \leq 2^{2K+O(\sqrt{K}\log K)}|A|$.

Previous results - The case of prime torsion

Ruzsa's conjecture '99

There is a constant $C > 0$ such that the following holds. If G is an abelian group with exponent r and $A \subseteq G$ is so that $|A + A| \leq K|A|$, then A is contained in subgroup H of size $|H| \leq r^{CK}|A|$.

Theorem (Green-Tao '09)

For $G = \mathbb{F}_2^d$, we can find $H \supseteq A$ with $|H| \leq 2^{2K+O(\sqrt{K}\log K)}|A|$.

Theorem (Even-Zohar '12)

For $G = \mathbb{F}_2^d$, we can find $H \supseteq A$ with $|H| \leq \frac{2^{2K}}{2K}|A|$.

Previous results - The case of prime torsion

Ruzsa's conjecture '99

There is a constant $C > 0$ such that the following holds. If G is an abelian group with exponent r and $A \subseteq G$ is so that $|A + A| \leq K|A|$, then A is contained in subgroup H of size $|H| \leq r^{CK}|A|$.

Theorem (Green-Tao '09)

For $G = \mathbb{F}_2^d$, we can find $H \supseteq A$ with $|H| \leq 2^{2K+O(\sqrt{K}\log K)}|A|$.

Theorem (Even-Zohar '12)

For $G = \mathbb{F}_2^d$, we can find $H \supseteq A$ with $|H| \leq \frac{2^{2K}}{2K}|A|$.

Theorem (Even-Zohar – Lovett '14)

For $G = \mathbb{F}_p^d$, we can find $H \supseteq A$ with $|H| \leq \frac{p^{2K-2}}{2K-1}|A|$.

Previous results

The techniques in previous work roughly come in two directions.

Previous results

The techniques in previous work roughly come in two directions.

Analytic technique:

- Fourier analysis (Bogolyubov-Ruzsa lemma), Covering lemma, Modelling lemma, Plünnecke-Ruzsa inequality
- Works in general abelian groups.

Previous results

The techniques in previous work roughly come in two directions.

Analytic technique:

- Fourier analysis (Bogolyubov-Ruzsa lemma), Covering lemma, Modelling lemma, Plünnecke-Ruzsa inequality
- Works in general abelian groups.

Compression technique over finite field vector spaces:

- Perform local modifications (compressions) to reduce to explicit structured examples.
- Rely strongly on the vector space structure.

Previous results

The techniques in previous work roughly come in two directions.

Analytic technique:

- Fourier analysis (Bogolyubov-Ruzsa lemma), Covering lemma, Modelling lemma, Plünnecke-Ruzsa inequality
- Works in general abelian groups.

Compression technique over finite field vector spaces:

- Perform local modifications (compressions) to reduce to explicit structured examples.
- Rely strongly on the vector space structure.

There are cases in which groups with exponent divisible by more than one prime behave significantly different from those with prime power torsion!

Main resuilts

Theorem (Fox-P. '25+)

If G is an abelian group with exponent r and $A \subseteq G$ is so that $|A+A| \leq K|A|$, then A is contained in subgroup H of size $|H| \leq r^{(2+o(1))K}|A|$.

In particular, Ruzsa's conjecture holds.

Main resuilts

Theorem (Fox-P. '25+)

If G is an abelian group with exponent r and $A \subseteq G$ is so that $|A+A| \leq K|A|$, then A is contained in subgroup H of size $|H| \leq r^{(2+o(1))K}|A|$.

In particular, Ruzsa's conjecture holds.

Our key ingredient is the main combinatorial lemma producing *expanding structures* inside sets with small doubling.

The combinatorial setup & The key combinatorial lemma

Combinatorial view on sets with small doubling

Additive input:

- Abelian group G
- Subset $A \subseteq G$ with $|A + A| \leq K|A|$.

Combinatorial view on sets with small doubling

Additive input:

- Abelian group G
- Subset $A \subseteq G$ with $|A + A| \leq K|A|$.

Combinatorial picture:

- Complete graph on G, with proper edge coloring $c(\{x, y\}) = x + y$.

Combinatorial view on sets with small doubling

Additive input:

- Abelian group G
- Subset $A \subseteq G$ with $|A + A| \leq K|A|$.

Combinatorial picture:

- Complete graph on G, with proper edge coloring $c(\{x, y\}) = x + y$.
- A set A with doubling K corresponds to a vertex subset whose induced subgraph receives few colors under edge coloring c.

Combinatorial view on sets with small doubling

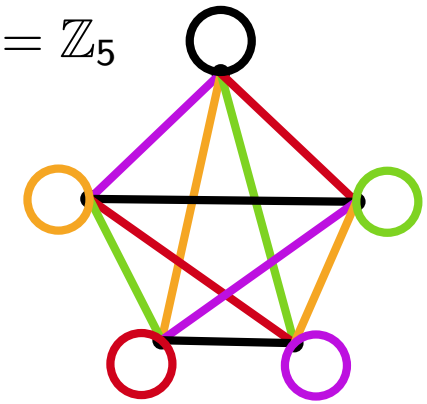
Additive input:

- Abelian group G
- Subset $A \subseteq G$ with $|A + A| \leq K|A|$.

Combinatorial picture:

- Complete graph on G, with proper edge coloring $c(\{x, y\}) = x + y$.
- A set A with doubling K corresponds to a vertex subset whose induced subgraph receives few colors under edge coloring c.

$G = \mathbb{Z}_5$



Combinatorial view on sets with small doubling

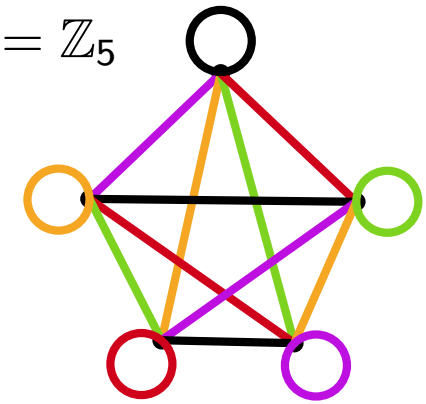
Additive input:

- Abelian group G
- Subset $A \subseteq G$ with $|A + A| \leq K|A|$.

Combinatorial picture:

- Complete graph on G, with proper edge coloring $c(\{x, y\}) = x + y$.
- A set A with doubling K corresponds to a vertex subset whose induced subgraph receives few colors under edge coloring c.

$G = \mathbb{Z}_5$



Surprise: Suffice to work in general combinatorial setup.

- Complete graph (on A) with a proper edge coloring using at most $K|A|$ many colors.

The key combinatorial lemma

Given an edge coloring of the complete graph, let $N(A, B)$ denote the set of colors between vertex sets A, B.

The key combinatorial lemma

Given an edge coloring of the complete graph, let $N(A, B)$ denote the set of colors between vertex sets A, B.

The key combinatorial lemma

Consider a proper edge coloring on A of size n using at most Kn colors, each appearing $O(n/K)$ times. There exists a set of $O(K)$ colors S such that the edges with colors in S partition A into sets B_i satisfying:

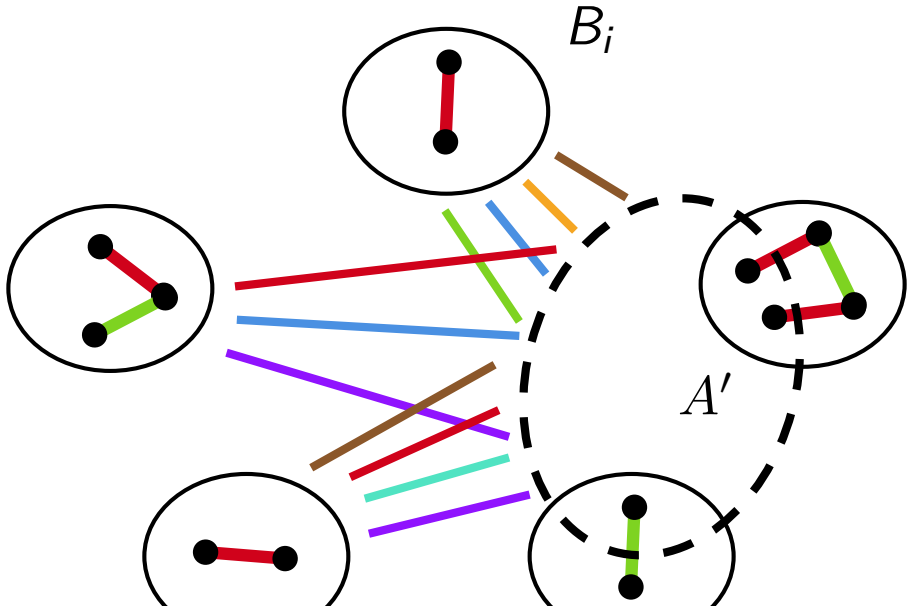
- At least $|A|/2$ vertices of A are contained in the sets B_i.
- Each B_i is connected using only edges with colors in S.
- For any set B_i and any $A' \subseteq A$ with $|A'| = \Omega(n)$, $N(B_i, A') = \Omega(Kn)$.

The key combinatorial lemma

The key combinatorial lemma

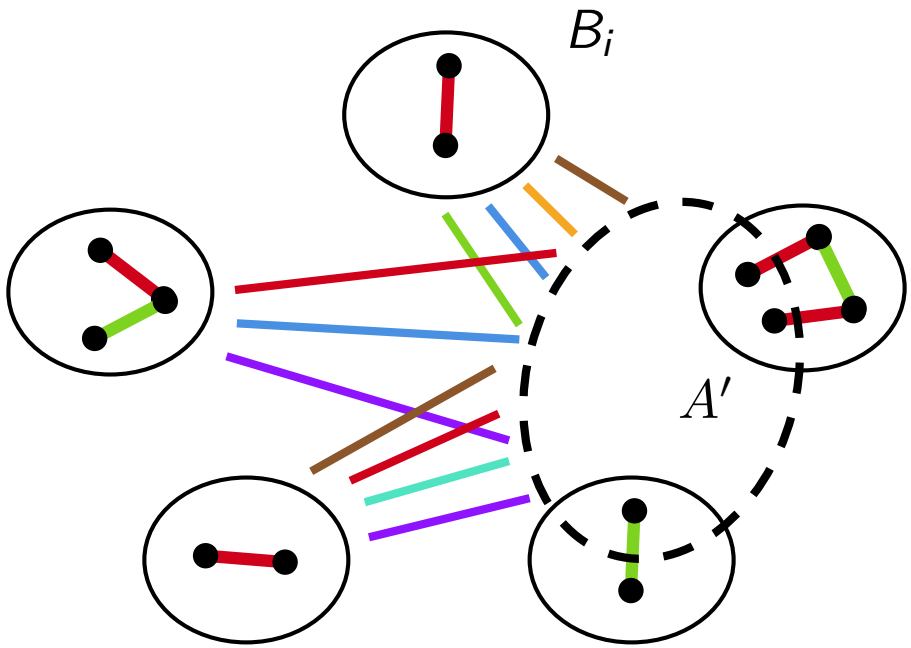
Consider a proper edge coloring on A of size n using at most Kn colors, each appearing $O(n/K)$ times. There exists a set of $O(K)$ colors S such that the edges with colors in S partition A into sets B_i satisfying:

- At least $|A|/2$ vertices of A are contained in the sets B_i.
- Each B_i is connected using only edges with colors in S.
- For any set B_i and any $A' \subseteq A$ with $|A'| = \Omega(n)$, $N(B_i, A') = \Omega(Kn)$.



Approach to Ruzsa's conjecture

Step 1. Apply the key combinatorial lemma.



Approach to Ruzsa's conjecture

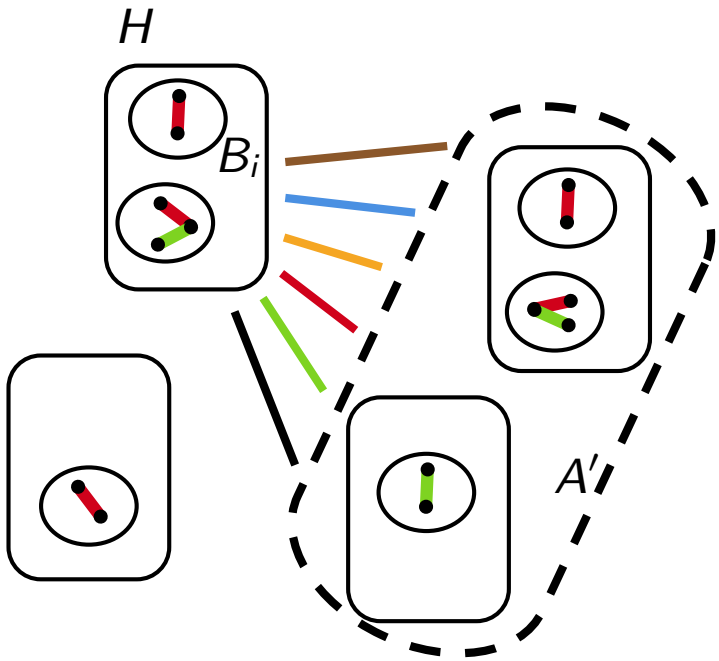
Step 1. Apply the key combinatorial lemma.

Approach to Ruzsa's conjecture

Step 1. Apply the key combinatorial lemma.

Step 2. Let H denote the subgroup spanned by the colors in S. Deduce that

$$|A \mod H + A \mod H| \leq \tilde{O}(1)|A \mod H|.$$

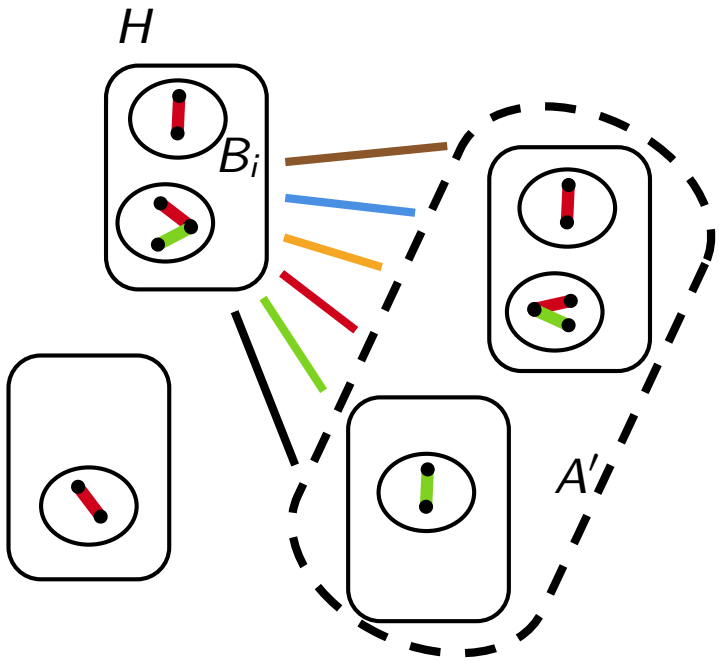


Approach to Ruzsa's conjecture

Step 1. Apply the key combinatorial lemma.

Step 2. Let H denote the subgroup spanned by the colors in S. Deduce that

$$|A \mod H + A \mod H| \leq \tilde{O}(1)|A \mod H|.$$



Step 3. Via qualitative version of Ruzsa's theorem, deduce that A is contained in a subgroup H with $|H| \leq |A| \exp(O(K))$.

Ramsey Cayley graphs, Dense Random Cayley graphs & Sets with small doubling in general groups

Ramsey graphs

Definition (Ramsey graphs)

A graph on N vertices is *C-Ramsey* if it has no clique or independent set of size $C \log_2 N$.

Ramsey graphs

Definition (Ramsey graphs)

A graph on N vertices is *C-Ramsey* if it has no clique or independent set of size $C \log_2 N$.

Theorem (Erdős-Szekeres '35)

There is no $\frac{1}{2}$-Ramsey graph.

Ramsey graphs

Definition (Ramsey graphs)

A graph on N vertices is *C-Ramsey* if it has no clique or independent set of size $C \log_2 N$.

Theorem (Erdős-Szekeres '35)

There is no $\frac{1}{2}$-Ramsey graph.

Theorem (Campos-Griffiths-Morris-Sahasrabudhe '23)

There is no $(\frac{1}{2} + c)$-Ramsey graph.

Ramsey graphs

Definition (Ramsey graphs)

A graph on N vertices is *C-Ramsey* if it has no clique or independent set of size $C \log_2 N$.

Theorem (Erdős-Szekeres '35)

There is no $\frac{1}{2}$-Ramsey graph.

Theorem (Campos-Griffiths-Morris-Sahasrabudhe '23)

There is no $(\frac{1}{2} + c)$-Ramsey graph.

Theorem (Erdős '47)

Almost all graphs on N vertices are 2-Ramsey.

Erdős' remarkable proof

Theorem (Erdős '47)

Almost all graphs on N vertices are 2-Ramsey.

- One of the first applications of the probabilistic method.
- Erdős shows that $G(N, 1/2)$ does not have a clique or independent set of size $n = 2\log_2 N$ by considering the first moment (expectation) obstruction: The expected number of such cliques or independent sets is $\binom{N}{n}2^{-\binom{n}{2}} = o_N(1)$.

Erdős' remarkable proof

Theorem (Erdős '47)

Almost all graphs on N vertices are 2-Ramsey.

- One of the first applications of the probabilistic method.
- Erdős shows that $G(N, 1/2)$ does not have a clique or independent set of size $n = 2\log_2 N$ by considering the first moment (expectation) obstruction: The expected number of such cliques or independent sets is $\binom{N}{n}2^{-\binom{n}{2}} = o_N(1)$.

Problem (Erdős '47)

Explicitly construct C-Ramsey graphs for some constant C.

Ramsey Cayley graphs

Definition (Cayley graph)

For a group G and symmetric subset $S \subset G$, the *Cayley graph* G_S has vertex set G and distinct x, y are adjacent if $xy^{-1} \in S$.

Ramsey Cayley graphs

Definition (Cayley graph)

For a group G and symmetric subset $S \subset G$, the *Cayley graph* G_S has vertex set G and distinct x, y are adjacent if $xy^{-1} \in S$.

Given $p \in (0,1)$, the random Cayley graphs $G(p)$ is the Cayley graph G_S where each $\{g, g^{-1}\}$ is included independently in S with probability p.

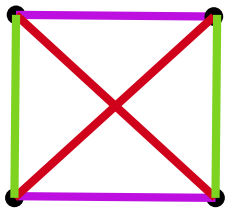
Ramsey Cayley graphs

Definition (Cayley graph)

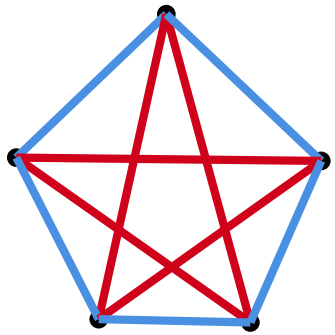
For a group G and symmetric subset $S \subset G$, the *Cayley graph* G_S has vertex set G and distinct x, y are adjacent if $xy^{-1} \in S$.

Given $p \in (0,1)$, the random Cayley graphs $G(p)$ is the Cayley graph G_S where each $\{g, g^{-1}\}$ is included independently in S with probability p.

$G = \mathbb{Z}_2 \times \mathbb{Z}_2$



$G = \mathbb{Z}_5$



Ramsey Cayley graphs

Definition (Cayley graph)

For a group G and symmetric subset $S \subset G$, the *Cayley graph* G_S has vertex set G and distinct x, y are adjacent if $xy^{-1} \in S$.

Given $p \in (0,1)$, the random Cayley graphs $G(p)$ is the Cayley graph G_S where each $\{g, g^{-1}\}$ is included independently in S with probability p.

Ramsey Cayley graphs

Definition (Cayley graph)

For a group G and symmetric subset $S \subset G$, the *Cayley graph* G_S has vertex set G and distinct x, y are adjacent if $xy^{-1} \in S$.

Given $p \in (0,1)$, the random Cayley graphs $G(p)$ is the Cayley graph G_S where each $\{g, g^{-1}\}$ is included independently in S with probability p.

Motivations:

- Small Ramsey graphs are Cayley; random analog of Paley graphs.
- Extensively studied in applications in theoretical computer science, combinatorics, number theory, group theory.
- Strong connections to coding theory, spectral graph theory, etc.

Ramsey Cayley graphs

Ramsey Cayley graphs

Definition (Cayley graph)

For a group G and symmetric subset $S \subset G$, the *Cayley graph* G_S has vertex set G and distinct x, y are adjacent if $xy^{-1} \in S$.

Given $p \in (0,1)$, the random Cayley graphs $G(p)$ is the Cayley graph G_S where each $\{g, g^{-1}\}$ is included independently in S with probability p.

Ramsey Cayley graphs

Definition (Cayley graph)

For a group G and symmetric subset $S \subset G$, the *Cayley graph* G_S has vertex set G and distinct x, y are adjacent if $xy^{-1} \in S$.

Given $p \in (0,1)$, the random Cayley graphs $G(p)$ is the Cayley graph G_S where each $\{g, g^{-1}\}$ is included independently in S with probability p.

Question

What is the size of the largest clique or independent set in uniform random Cayley graphs $G(1/2)$? Are uniform random Cayley graphs Ramsey?

Ramsey Cayley graphs

Definition (Cayley graph)

For a group G and symmetric subset $S \subset G$, the *Cayley graph* G_S has vertex set G and distinct x, y are adjacent if $xy^{-1} \in S$.

Given $p \in (0,1)$, the random Cayley graphs $G(p)$ is the Cayley graph G_S where each $\{g, g^{-1}\}$ is included independently in S with probability p.

Question

What is the size of the largest clique or independent set in uniform random Cayley graphs $G(1/2)$? Are uniform random Cayley graphs Ramsey?

Conjecture (Alon '89)

There is a constant C such that every finite group has a Cayley graph which is C-Ramsey.

Random graphs meet additive combinatorics

Connection to additive combinatorics and group theory:

- For $A \subseteq G$, define the product set

$$AA^{-1} := \{ab^{-1} : a, b \in A\}.$$

In an abelian group, this is the difference set $A - A$.

Random graphs meet additive combinatorics

Connection to additive combinatorics and group theory:

- For $A \subseteq G$, define the product set

$$AA^{-1} := \{ab^{-1} : a, b \in A\}.$$

In an abelian group, this is the difference set $A - A$.

- A is an independent set in G_S if and only if $AA^{-1} \setminus \{1_G\} \subset S^c$.

Random graphs meet additive combinatorics

Connection to additive combinatorics and group theory:

- For $A \subseteq G$, define the product set

$$AA^{-1} := \{ab^{-1} : a, b \in A\}.$$

  In an abelian group, this is the difference set $A - A$.

- A is an independent set in G_S if and only if $AA^{-1} \setminus \{1_G\} \subset S^c$.

The first moment of the number of independent sets in a random Cayley graph is intimately related to the number of sets with small product sets:

$$\mathbb{E}[\#\text{independent sets of size } t \text{ in } G(p)] = \sum_{|A|=t} (1-p)^{\Theta(|AA^{-1}|)}.$$

Random graphs meet additive combinatorics

Connection to additive combinatorics and group theory:

- For $A \subseteq G$, define the product set

$$AA^{-1} := \{ab^{-1} : a, b \in A\}.$$

  In an abelian group, this is the difference set $A - A$.

- A is an independent set in G_S if and only if $AA^{-1} \setminus \{1_G\} \subset S^c$.

The first moment of the number of independent sets in a random Cayley graph is intimately related to the number of sets with small product sets:

$$\mathbb{E}[\#\text{independent sets of size } t \text{ in } G(p)] = \sum_{|A|=t} (1-p)^{\Theta(|AA^{-1}|)}.$$

Controlling the first moment of the number of independent sets in a random Cayley graph reduces to bounding the number of sets with small product sets.

Independence number of random Cayley graphs

Independence number of random Cayley graphs

Theorem (Alon '95)

The independence number of a uniform random Cayley graph on any group G of order N is $O(\log^2 N)$ with high probability.

Independence number of random Cayley graphs

Theorem (Alon '95)

The independence number of a uniform random Cayley graph on any group G of order N is $O(\log^2 N)$ with high probability.

Theorem (Green '05, Green-Morris '16)

For N prime, the independence number of a uniform random Cayley graph on $\mathbb{Z}_N$ is $(2 + o(1)) \log_2 N$ with high probability.

Independence number of random Cayley graphs

Theorem (Alon '95)

The independence number of a uniform random Cayley graph on any group G of order N is $O(\log^2 N)$ with high probability.

Theorem (Green '05, Green-Morris '16)

For N prime, the independence number of a uniform random Cayley graph on $\mathbb{Z}_N$ is $(2 + o(1)) \log_2 N$ with high probability.

Theorem (Green '05, Mrazović '17)

The independence number of a uniform random Cayley graph on $\mathbb{F}_p^d$ with $N = p^d$ is $\Theta_p(\log N \log\log N)$ with high probability.

Random graphs meet additive combinatorics

Theorem (Conlon-Fox-P.-Yepremyan '24)

With high probability, the independence number of a uniform random Cayley graph on any group G of order N is $O(\log N \log\log N)$.

Random graphs meet additive combinatorics

Theorem (Conlon-Fox-P.-Yepremyan '24)

With high probability, the independence number of a uniform random Cayley graph on any group G of order N is $O(\log N \log\log N)$.

Theorem (Conlon-Fox-P.-Yepremyan '24)

In any group G of order N, the number of subsets $A \subset G$ with $|A| = n$ and $|AA^{-1}| \leq Kn$ is at most $N^{C(K+\log n)}(CK)^n$.

- In general, the above bound is sharp (up to the constant C).

Random graphs meet additive combinatorics

Theorem (Conlon-Fox-P.-Yepremyan '24)

With high probability, the independence number of a uniform random Cayley graph on any group G of order N is $O(\log N \log\log N)$.

Theorem (Conlon-Fox-P.-Yepremyan '24)

In any group G of order N, the number of subsets $A \subset G$ with $|A| = n$ and $|AA^{-1}| \leq Kn$ is at most $N^{C(K+\log n)}(CK)^n$.

- In general, the above bound is sharp (up to the constant C).

Sets A with small product sets AA^{-1} are structured in the statistical sense.

Random graphs meet additive combinatorics

Theorem (Conlon-Fox-P.-Yepremyan '24)

With high probability, the independence number of a uniform random Cayley graph on any group G of order N is $O(\log N \log\log N)$.

Theorem (Conlon-Fox-P.-Yepremyan '24)

In any group G of order N, the number of subsets $A \subset G$ with $|A| = n$ and $|AA^{-1}| \leq Kn$ is at most $N^{C(K+\log n)}(CK)^n$.

- In general, the above bound is sharp (up to the constant C).

Sets A with small product sets AA^{-1} are structured in the statistical sense.

Our proof of the theorem is entirely combinatorial!

Combinatorial view on Cayley graphs

Combinatorial view of the group structure:

- Complete graph on G with an edge coloring $c(\{x, y\}) = \{xy^{-1}, yx^{-1}\}$.
  - In this edge-coloring each color class is 1 or 2-regular.

Combinatorial view on Cayley graphs

Combinatorial view of the group structure:

- Complete graph on G with an edge coloring $c(\{x, y\}) = \{xy^{-1}, yx^{-1}\}$.
  - In this edge-coloring each color class is 1 or 2-regular.
- A set A of size n with $|AA^{-1}| \leq m$ corresponds to a vertex subset of size n inducing at most m colors.

Combinatorial view on Cayley graphs

Combinatorial view of the group structure:

- Complete graph on G with an edge coloring $c(\{x, y\}) = \{xy^{-1}, yx^{-1}\}$.
  - In this edge-coloring each color class is 1 or 2-regular.
- A set A of size n with $|AA^{-1}| \leq m$ corresponds to a vertex subset of size n inducing at most m colors.
- A Cayley graph on G is the edge-union of some color classes.

Combinatorial view on Cayley graphs

Combinatorial view of the group structure:

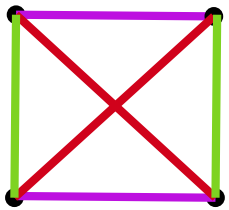
- Complete graph on G with an edge coloring $c(\{x, y\}) = \{xy^{-1}, yx^{-1}\}$.
  - In this edge-coloring each color class is 1 or 2-regular.
- A set A of size n with $|AA^{-1}| \leq m$ corresponds to a vertex subset of size n inducing at most m colors.
- A Cayley graph on G is the edge-union of some color classes.

Combinatorial view on Cayley graphs

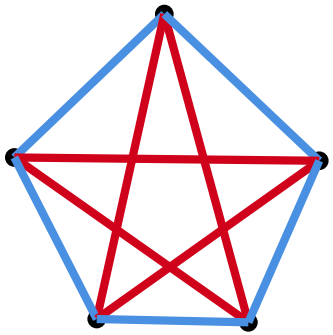
Combinatorial view of the group structure:

- Complete graph on G with an edge coloring $c(\{x, y\}) = \{xy^{-1}, yx^{-1}\}$.
  - In this edge-coloring each color class is 1 or 2-regular.
- A set A of size n with $|AA^{-1}| \leq m$ corresponds to a vertex subset of size n inducing at most m colors.
- A Cayley graph on G is the edge-union of some color classes.

$G = \mathbb{Z}_2 \times \mathbb{Z}_2$



$G = \mathbb{Z}_5$

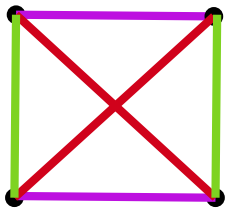


Combinatorial view on Cayley graphs

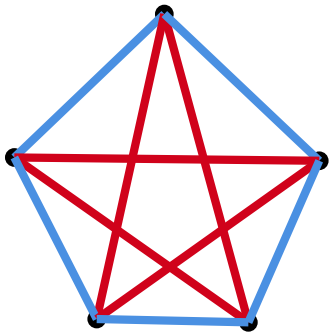
Combinatorial view of the group structure:

- Complete graph on G with an edge coloring $c(\{x, y\}) = \{xy^{-1}, yx^{-1}\}$.
  - In this edge-coloring each color class is 1 or 2-regular.
- A set A of size n with $|AA^{-1}| \leq m$ corresponds to a vertex subset of size n inducing at most m colors.
- A Cayley graph on G is the edge-union of some color classes.

$G = \mathbb{Z}_2 \times \mathbb{Z}_2$



$G = \mathbb{Z}_5$



Surprise: The combinatorial constraint on the degree of color classes is sufficient!

Counting sets with small product set

Theorem 1 (Conlon-Fox-P.-Yepremyan '24)

In a Δ-bounded edge-coloring of the complete graph on N vertices, the number of n-vertex subsets with at most Kn colors is at most

$$N^{C\Delta(K+\log n)}(C\Delta K)^n.$$

Counting sets with small product set

Theorem 1 (Conlon-Fox-P.-Yepremyan '24)

In a Δ-bounded edge-coloring of the complete graph on N vertices, the number of n-vertex subsets with at most Kn colors is at most

$$N^{C\Delta(K+\log n)}(C\Delta K)^n.$$

Lemma

For any vertex set of size n with a proper edge coloring using Kn colors, we can find a tree with $O(K+\log n)$ colors on $.99n$ vertices.

Counting sets with small product set

Theorem 1 (Conlon-Fox-P.-Yepremyan '24)

In a Δ-bounded edge-coloring of the complete graph on N vertices, the number of n-vertex subsets with at most Kn colors is at most

$$N^{C\Delta(K+\log n)}(C\Delta K)^n.$$

Lemma

For any vertex set of size n with a proper edge coloring using Kn colors, we can find a tree with $O(K+\log n)$ colors on $.99n$ vertices.

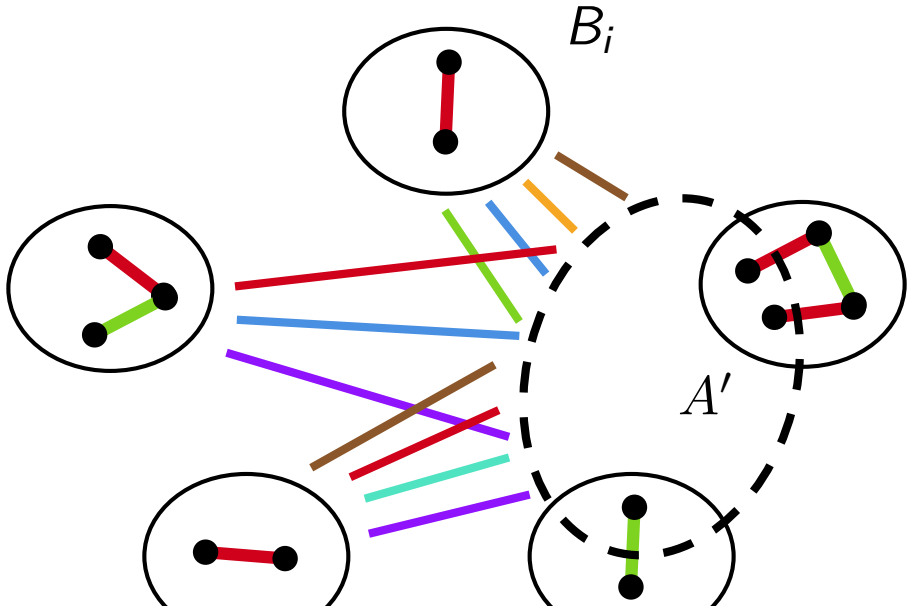
The lemma follows from the key combinatorial lemma.

The key combinatorial lemma

The key combinatorial lemma

Consider a proper edge coloring on A of size n using at most Kn colors, each appearing $O(n/K)$ times. There exists a set of $O(K)$ colors S such that the edges with colors in S partition A into sets B_i satisfying:

- At least $|A|/2$ vertices of A are contained in the sets B_i.
- Each B_i is connected using only edges with colors in S.
- For any set B_i and any $A' \subseteq A$ with $|A'| = \Omega(n)$, $N(B_i, A') = \Omega(Kn)$.



Alon's conjecture - Going beyond uniform random

Alon's conjecture

Conjecture (Alon '89)

There is a constant C such that every finite group has a Cayley graph which is C-Ramsey.

Alon's conjecture - Going beyond uniform random

Over $\mathbb{F}_p^d$, a uniformly random Cayley graph is not Ramsey w.h.p.

Alon's conjecture - Going beyond uniform random

Over $\mathbb{F}_p^d$, a uniformly random Cayley graph is not Ramsey w.h.p.

We define an alternative distribution of random Cayley graphs to "remove" the problematic cliques.

Theorem (Conlon-Fox-P.-Yepremyan '24)

For $p \geq 5$, there exists Cayley graphs over $\mathbb{F}_p^d$ with clique and independence number $(2 + o(1)) \log_2 N$ where $N = p^d$.
For $p = 1 \pmod 4$, these Cayley graphs are self-complementary.

Answer a question of Alon and Orlitsky ('95) motivated by zero-error capacity and dual-source coding.

Alon's conjecture - Going beyond uniform random

Over $\mathbb{F}_p^d$, a uniformly random Cayley graph is not Ramsey w.h.p.

We define an alternative distribution of random Cayley graphs to "remove" the problematic cliques.

Theorem (Conlon-Fox-P.-Yepremyan '24)

For $p \geq 5$, there exists Cayley graphs over $\mathbb{F}_p^d$ with clique and independence number $(2 + o(1)) \log_2 N$ where $N = p^d$.
For $p = 1 \pmod 4$, these Cayley graphs are self-complementary.

Answer a question of Alon and Orlitsky ('95) motivated by zero-error capacity and dual-source coding.

Theorem (Conlon-Fox-P.-Yepremyan '24)

For almost all N, all abelian groups G of order N have a Cayley graph which is C-Ramsey.

Alon's conjecture - Going beyond uniform random

Over $\mathbb{F}_p^d$, a uniformly random Cayley graph is not Ramsey w.h.p.

We define an alternative distribution of random Cayley graphs to "remove" the problematic cliques.

Theorem (Conlon-Fox-P.-Yepremyan '24)

For $p \geq 5$, there exists Cayley graphs over $\mathbb{F}_p^d$ with clique and independence number $(2 + o(1)) \log_2 N$ where $N = p^d$.
For $p = 1 \pmod 4$, these Cayley graphs are self-complementary.

Answer a question of Alon and Orlitsky ('95) motivated by zero-error capacity and dual-source coding.

Theorem (Conlon-Fox-P.-Yepremyan '24)

For almost all N, all abelian groups G of order N have a Cayley graph which is C-Ramsey.

Recent generalization to all groups of order coprime to 6 by Schildkraut.

Alon's conjecture - Going beyond uniform random

Theorem (Conlon-Fox-P.-Yepremyan '24)

There is a C-Ramsey self-complementary Cayley graph on $\mathbb{F}_5^d$.

Model. For each nonzero $x \in \mathbb{F}_5^d$, randomly pick exactly one of $\{x, 4x\}$ or $\{2x, 3x\}$ to be a subset of the generating set S:

Alon's conjecture - Going beyond uniform random

Theorem (Conlon-Fox-P.-Yepremyan '24)

There is a C-Ramsey self-complementary Cayley graph on $\mathbb{F}_5^d$.

Model. For each nonzero $x \in \mathbb{F}_5^d$, randomly pick exactly one of $\{x, 4x\}$ or $\{2x, 3x\}$ to be a subset of the generating set S:

- S is symmetric.
- If $x \in S$, then $2x \notin S$.

Alon's conjecture - Going beyond uniform random

Theorem (Conlon-Fox-P.-Yepremyan '24)

There is a C-Ramsey self-complementary Cayley graph on $\mathbb{F}_5^d$.

Model. For each nonzero $x \in \mathbb{F}_5^d$, randomly pick exactly one of $\{x, 4x\}$ or $\{2x, 3x\}$ to be a subset of the generating set S:

- S is symmetric.
- If $x \in S$, then $2x \notin S$.

The second condition together with Plünnecke-Ruzsa inequality force any potential clique A to have $|A - A| \geq |A|^{4/3}$.

Alon's conjecture - Going beyond uniform random

Theorem (Conlon-Fox-P.-Yepremyan '24)

There is a C-Ramsey self-complementary Cayley graph on $\mathbb{F}_5^d$.

Model. For each nonzero $x \in \mathbb{F}_5^d$, randomly pick exactly one of $\{x, 4x\}$ or $\{2x, 3x\}$ to be a subset of the generating set S:

- S is symmetric.
- If $x \in S$, then $2x \notin S$.

The second condition together with Plünnecke-Ruzsa inequality force any potential clique A to have $|A - A| \geq |A|^{4/3}$.

The first moment over those A, together with the previous counting result, imply the Ramsey property.

Perspective

Cliques in dense random Cayley graphs $\leftrightarrow$ Counting sets with small doubling.

Combinatorial perspective: Main combinatorial lemma identifies novel combinatorial structures underlying sets with small doubling.

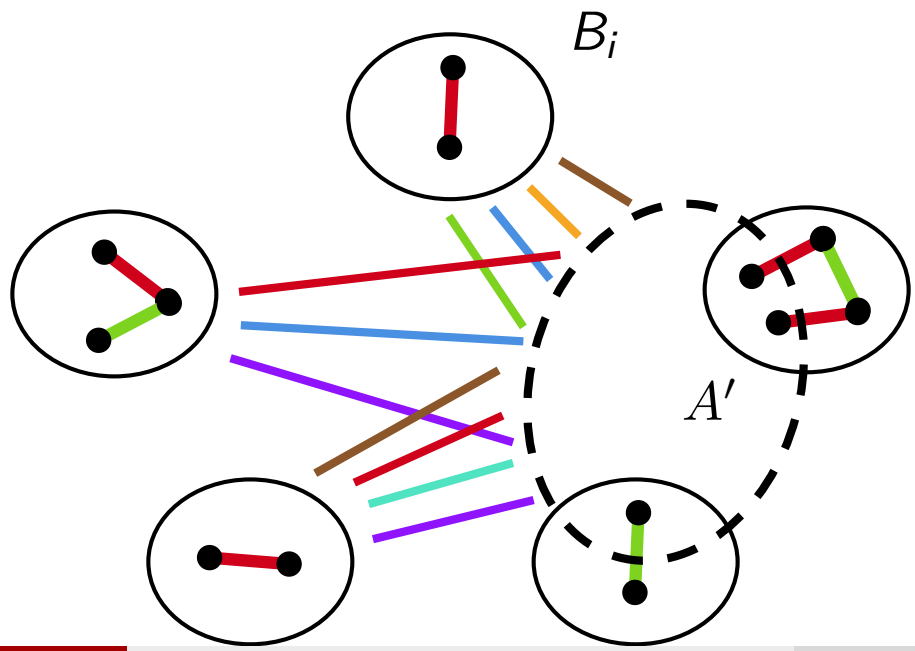
Perspective

Cliques in dense random Cayley graphs $\leftrightarrow$ Counting sets with small doubling.

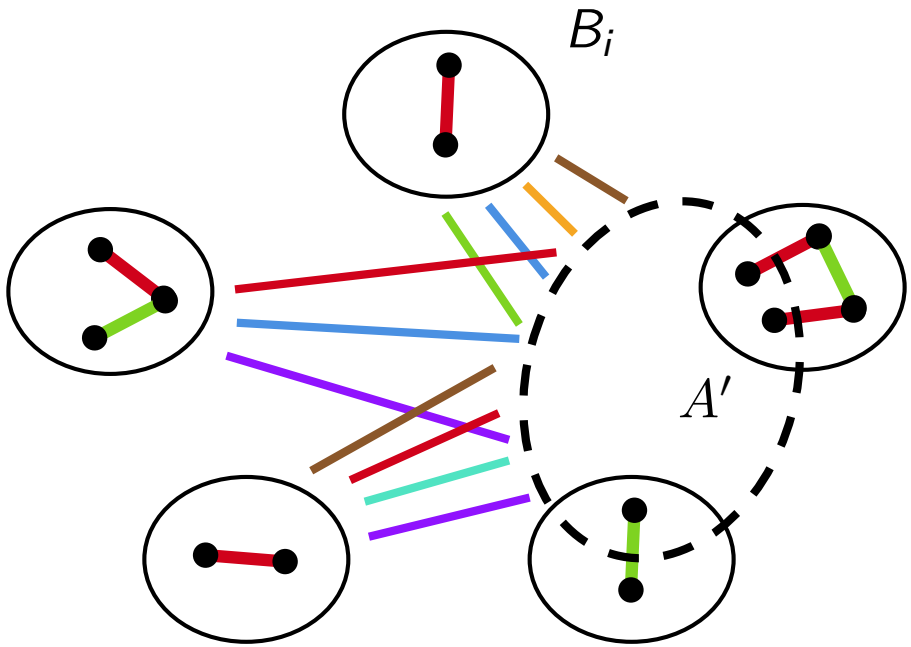
Combinatorial perspective: Main combinatorial lemma identifies novel combinatorial structures underlying sets with small doubling.

New combinatorial approach to additive combinatorics:

- Main combinatorial lemma: expanding structures in sets with small doubling.
- Refinement: Use expanding structures to probe information about the entire set.

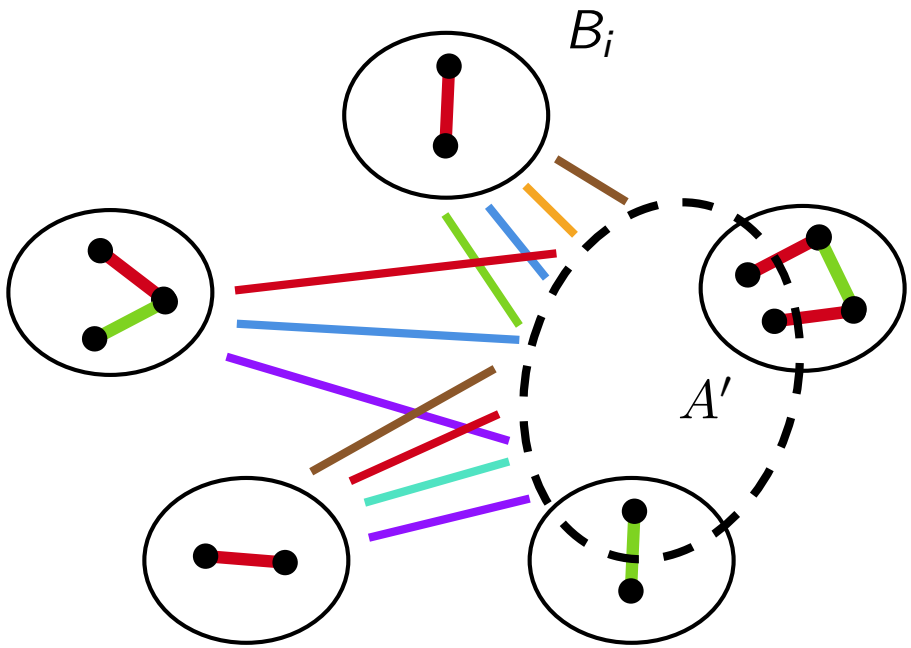


Perspective



Perspective: Instead of zooming in on explicit structures inside the set, the combinatorial lemma provides first a template that is "as random-like as possible".

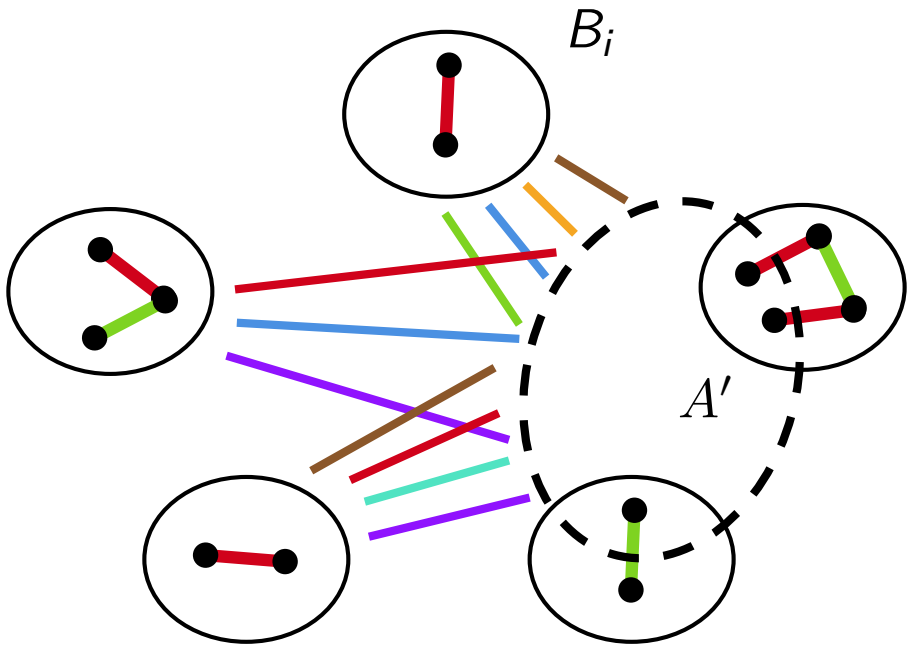
Perspective



Perspective: Instead of zooming in on explicit structures inside the set, the combinatorial lemma provides first a template that is "as random-like as possible".

- The proof follows from an intricate random exploration process.

Perspective



Perspective: Instead of zooming in on explicit structures inside the set, the combinatorial lemma provides first a template that is "as random-like as possible".

- The proof follows from an intricate random exploration process.

Robust and applicable in wide generality.

New direction: Dependent random graphs

The combinatorial approach to clique number of dense random Cayley graphs suggests intriguing universal behaviors in general random graph models with significant dependencies.

New direction: Dependent random graphs

The combinatorial approach to clique number of dense random Cayley graphs suggests intriguing universal behaviors in general random graph models with significant dependencies.

Consider an edge-coloring c of a complete graph, where each color class has degree at most Δ.

New direction: Dependent random graphs

The combinatorial approach to clique number of dense random Cayley graphs suggests intriguing universal behaviors in general random graph models with significant dependencies.

Consider an edge-coloring c of a complete graph, where each color class has degree at most Δ.

Definition (Random entangled graph)

An *entangled graph* is the edge-union of some of the color classes.

New direction: Dependent random graphs

The combinatorial approach to clique number of dense random Cayley graphs suggests intriguing universal behaviors in general random graph models with significant dependencies.

Consider an edge-coloring c of a complete graph, where each color class has degree at most Δ.

Definition (Random entangled graph)

An *entangled graph* is the edge-union of some of the color classes.

The *random entangled graph* $G_c(p)$ is formed by including each color class with probability p independently.

New direction: Dependent random graphs

The combinatorial approach to clique number of dense random Cayley graphs suggests intriguing universal behaviors in general random graph models with significant dependencies.

Consider an edge-coloring c of a complete graph, where each color class has degree at most Δ.

Definition (Random entangled graph)

An *entangled graph* is the edge-union of some of the color classes.

The *random entangled graph* $G_c(p)$ is formed by including each color class with probability p independently.

Examples:

- Erdős-Rényi random graphs.
- Random Cayley graphs.
- Random Latin square graphs: Color class $C_k = \{\{i,j\} : L_{ij} = k\}$ for a Latin square L.

New direction: Random entangled graphs

Theorem 1 (Conlon-Fox-P.-Yepremyan '24)

In a Δ-bounded edge-coloring of the complete graph on N vertices, the number of n-vertex subsets with at most Kn colors is at most

$$N^{C\Delta(K+\log n)}(C\Delta K)^n.$$

New direction: Random entangled graphs

Theorem 1 (Conlon-Fox-P.-Yepremyan '24)

In a Δ-bounded edge-coloring of the complete graph on N vertices, the number of n-vertex subsets with at most Kn colors is at most

$$N^{C\Delta(K+\log n)}(C\Delta K)^n.$$

Theorem 2 (Conlon-Fox-P.-Yepremyan '24)

If an edge-coloring c of K_N is Δ-bounded, then with high probability,

$$\alpha(G_c(p)) = O_{p,\Delta}(\log N \log\log N).$$

New direction: Random entangled graphs

Theorem 1 (Conlon-Fox-P.-Yepremyan '24)

In a Δ-bounded edge-coloring of the complete graph on N vertices, the number of n-vertex subsets with at most Kn colors is at most

$$N^{C\Delta(K+\log n)}(C\Delta K)^n.$$

Theorem 2 (Conlon-Fox-P.-Yepremyan '24)

If an edge-coloring c of K_N is Δ-bounded, then with high probability,

$$\alpha(G_c(p)) = O_{p,\Delta}(\log N \log\log N).$$

- From Theorem 1, a careful union bound yields Theorem 2.
- Theorem 2 solves a conjecture of Christofides and Markström ('11) on the independence number of random Latin square graphs.

New direction: Δ-independent random graphs

New direction: Δ-independent random graphs

How much independence is needed?

New direction: Δ-independent random graphs

How much independence is needed?

The phenomena extend to a significantly broader class of random graphs.

Definition (Δ-independent graph)

An ensemble of random graphs is said to be Δ-independent if for each edge e, there is a graph G_e of maximum degree Δ such that the appearance of e is independent of all edges outside G_e.

New direction: Δ-independent random graphs

How much independence is needed?

The phenomena extend to a significantly broader class of random graphs.

Definition (Δ-independent graph)

An ensemble of random graphs is said to be Δ-independent if for each edge e, there is a graph G_e of maximum degree Δ such that the appearance of e is independent of all edges outside G_e.

Significant weakening of usual condition in the Lovász Local Lemma!

New direction: Δ-independent random graphs

How much independence is needed?

The phenomena extend to a significantly broader class of random graphs.

Definition (Δ-independent graph)

An ensemble of random graphs is said to be Δ-independent if for each edge e, there is a graph G_e of maximum degree Δ such that the appearance of e is independent of all edges outside G_e.

Significant weakening of usual condition in the Lovász Local Lemma!

All random entangled graphs defined by a Δ-bounded edge coloring are Δ-independent random graphs.

New direction: Δ-independent random graphs

How much independence is needed?

The phenomena extend to a significantly broader class of random graphs.

Definition (Δ-independent graph)

An ensemble of random graphs is said to be Δ-independent if for each edge e, there is a graph G_e of maximum degree Δ such that the appearance of e is independent of all edges outside G_e.

Significant weakening of usual condition in the Lovász Local Lemma!

All random entangled graphs defined by a Δ-bounded edge coloring are Δ-independent random graphs.

Theorem (Conlon-Fox-P.-Yepremyan '26+)

Consider a Δ-independent random graph G where the probability of appearance of each edge is $\Theta(p)$. Then, with high probability,

$$\alpha(G) = O_{p,\Delta}(\log N \log\log N).$$

New direction: Δ-independent random graphs

Definition (Δ-independent graph)

An ensemble of random graphs is said to be Δ-independent if for each edge e, there is a graph G_e of maximum degree Δ such that the appearance of e is independent of all edges outside G_e.

New direction: Δ-independent random graphs

Definition (Δ-independent graph)

An ensemble of random graphs is said to be Δ-independent if for each edge e, there is a graph G_e of maximum degree Δ such that the appearance of e is independent of all edges outside G_e.

Theorem (Conlon-Fox-P.-Yepremyan '26+)

Consider a symmetric Δ-independent random graph G where the probability of appearance of each edge is p. Then, with high probability, all nontrivial eigenvalues of G are bounded by $O(\sqrt{pN \log N})$.

New direction: Δ-independent random graphs

Definition (Δ-independent graph)

An ensemble of random graphs is said to be Δ-independent if for each edge e, there is a graph G_e of maximum degree Δ such that the appearance of e is independent of all edges outside G_e.

Theorem (Conlon-Fox-P.-Yepremyan '26+)

Consider a symmetric Δ-independent random graph G where the probability of appearance of each edge is p. Then, with high probability, all nontrivial eigenvalues of G are bounded by $O(\sqrt{pN \log N})$.

As a corollary, we obtain that G is Hamiltonian with high probability for $p \gg \log N$.

New direction: Δ-independent random graphs

Definition (Δ-independent graph)

An ensemble of random graphs is said to be Δ-independent if for each edge e, there is a graph G_e of maximum degree Δ such that the appearance of e is independent of all edges outside G_e.

Theorem (Conlon-Fox-P.-Yepremyan '26+)

Consider a symmetric Δ-independent random graph G where the probability of appearance of each edge is p. Then, with high probability, all nontrivial eigenvalues of G are bounded by $O(\sqrt{pN \log N})$.

As a corollary, we obtain that G is Hamiltonian with high probability for $p \gg \log N$.

Open direction

Study interesting properties of Δ-independent graphs (random entangled graphs, random Cayley graphs).

The next part

Probabilistic approach to sets with small doubling:

- Study independent sets in sparse random Cayley graphs.

The next part

Probabilistic approach to sets with small doubling:

- Study independent sets in sparse random Cayley graphs.
- Via the connection between threshold phenomena and first moment obstructions, probabilistic predictions **suggest** existence of significant low-complexity structures among sets with small doubling.

The next part

Probabilistic approach to sets with small doubling:

- Study independent sets in sparse random Cayley graphs.
- Via the connection between threshold phenomena and first moment obstructions, probabilistic predictions **suggest** existence of significant low-complexity structures among sets with small doubling.
- New approach to probe low-complexity structures:
  - Progress on understanding sparse random Cayley graphs.
  - Much finer understanding of sets with small doubling, Optimal enumeration results.

Thank you!