Very Small Product Sets

Matt DeVos

Setup

- G is a group written additively,
- $A, B \subseteq G$ are finite and nonempty,
- $A + B = \{a + b \mid a \in A \text{ and } b \in B\}$.

Setup

- G is a group written additively,
- $A, B \subseteq G$ are finite and nonempty,
- $A + B = \{a + b \mid a \in A \text{ and } b \in B\}$.

Central Questions

1. **Lower Bounds:** How small can $|A + B|$ be?

Setup

- G is a group written additively,
- $A, B \subseteq G$ are finite and nonempty,
- $A + B = \{a + b \mid a \in A \text{ and } b \in B\}$.

Central Questions

1. **Lower Bounds:** How small can $|A + B|$ be?
2. **Structure:** If $|A + B|$ is small, then why?

Setup

- G is a group written additively,
- $A, B \subseteq G$ are finite and nonempty,
- $A + B = \{a + b \mid a \in A \text{ and } b \in B\}$.

Central Questions

1. **Lower Bounds:** How small can $|A + B|$ be?
2. **Structure:** If $|A + B|$ is small, then why?

Definition

(A, B) is **critical** if $|A + B| < |A| + |B|$.

Setup

- G is a group written multiplicatively,
- $A, B \subseteq G$ are finite and nonempty,
- $AB = \{ab \mid a \in A \text{ and } b \in B\}$.

Central Questions

1. **Lower Bounds:** How small can $|AB|$ be?
2. **Structure:** If $|AB|$ is small, then why?

Definition

(A, B) is **critical** if $|AB| < |A| + |B|$.

$G = \mathbb{Z}_p := \mathbb{Z}/p\mathbb{Z}$

$G = \mathbb{Z}_p$

1. Lower Bound (Cauchy-Davenport)

If p is prime and $A, B \subseteq \mathbb{Z}_p$ are nonempty, then

$$|A + B| \geq \min\{p, |A| + |B| - 1\}.$$

$G = \mathbb{Z}_p$

1. Lower Bound (Cauchy-Davenport)

If p is prime and $A, B \subseteq \mathbb{Z}_p$ are nonempty, then

$$|A + B| \geq \min\{p, |A| + |B| - 1\}.$$

Proof Ingredients

- induction on $|A|$.

1. Lower Bound (Cauchy-Davenport)

If p is prime and $A, B \subseteq \mathbb{Z}_p$ are nonempty, then

$$|A + B| \geq \min\{p, |A| + |B| - 1\}.$$

Proof Ingredients

- induction on $|A|$.
- *shifting:* $A \to A + \{g\}$, $B \to B + \{g\}$

$G = \mathbb{Z}_p$

1. Lower Bound (Cauchy-Davenport)

If p is prime and $A, B \subseteq \mathbb{Z}_p$ are nonempty, then

$$|A+B| \geq \min\{p, |A|+|B|-1\}.$$

Proof Ingredients

- induction on $|A|$.
- *shifting:* $A \to A+\{g\}$, $B \to B+\{g\}$
- *intersection-union transform:* $(A, B) \to (A \cap B, A \cup B)$

1. Lower Bound (Cauchy-Davenport)

If p is prime and $A, B \subseteq \mathbb{Z}_p$ are nonempty, then

$$|A + B| \geq \min\{p, |A| + |B| - 1\}.$$

Proof Ingredients

- induction on $|A|$.
- *shifting:* $A \to A + \{g\}$, $B \to B + \{g\}$
- *intersection-union transform:* $(A, B) \to (A \cap B, A \cup B)$
  - $(A \cap B) + (A \cup B) \subseteq A + B$
  - $|A \cap B| + |A \cup B| = |A| + |B|$

1. Lower Bound (Cauchy-Davenport)

If p is prime and $A, B \subseteq \mathbb{Z}_p$ are nonempty, then

$$|A + B| \geq \min\{p, |A| + |B| - 1\}.$$

$G = \mathbb{Z}_p$

1. Lower Bound (Cauchy-Davenport)

If p is prime and $A, B \subseteq \mathbb{Z}_p$ are nonempty, then

$$|A + B| \geq \min\{p, |A| + |B| - 1\}.$$

2. Structure (Vosper)

If (A, B) is critical one of the following holds

(I) $A + B = \mathbb{Z}_p$ (trivial)

$G = \mathbb{Z}_p$

1. Lower Bound (Cauchy-Davenport)

If p is prime and $A, B \subseteq \mathbb{Z}_p$ are nonempty, then

$$|A + B| \geq \min\{p, |A| + |B| - 1\}.$$

2. Structure (Vosper)

If (A, B) is critical one of the following holds

(I) $A + B = \mathbb{Z}_p$ (trivial)

(II) $|A| = 1$ or $|B| = 1$ (small set)

$G = \mathbb{Z}_p$

1. Lower Bound (Cauchy-Davenport)

If p is prime and $A, B \subseteq \mathbb{Z}_p$ are nonempty, then

$$|A + B| \geq \min\{p, |A| + |B| - 1\}.$$

2. Structure (Vosper)

If (A, B) is critical one of the following holds

(I) $A + B = \mathbb{Z}_p$ (trivial)

(II) $|A| = 1$ or $|B| = 1$ (small set)

(III) $|A + B| = p - 1$ (small set)

$G = \mathbb{Z}_p$

1. Lower Bound (Cauchy-Davenport)

If p is prime and $A, B \subseteq \mathbb{Z}_p$ are nonempty, then

$$|A + B| \geq \min\{p, |A| + |B| - 1\}.$$

2. Structure (Vosper)

If (A, B) is critical one of the following holds

- **(I)** $A + B = \mathbb{Z}_p$ (trivial)
- **(II)** $|A| = 1$ or $|B| = 1$ (small set)
- **(III)** $|A + B| = p - 1$ (small set)
- **(IV)** A, B arithmetic progressions with a common difference. (progression)

G abelian

1. Lower Bound (Kneser)

Let A, B be finite nonempty subsets of an additive abelian group G. Then there exists $H \leq G$ so that

(I) $|A + B| \geq |A| + |B| - |H|$, and

(II) $A + B + H = A + B$.

G abelian

1. Lower Bound (Kneser)

Let A, B be finite nonempty subsets of an additive abelian group G. Then there exists $H \leq G$ so that

(I) $|A + B| \geq |A| + |B| - |H|$, and

(II) $A + B + H = A + B$.

2. Structure (Kemperman)

The nontrivial critical pairs can be constructed using a recursive process involving small sets and progressions.

G arbitrary

Lower Bound (D.)

Let A, B be finite nonempty subsets of an arbitrary multiplicative group G. Then there exists $H \leq G$ so that

(I) $|AB| \geq |A| + |B| - |H|$,

(II) For every $x \in AB$ there exists $y \in G$ so that $x(yHy^{-1}) \subseteq AB$.

G arbitrary

Lower Bound (D.)

Let A, B be finite nonempty subsets of an arbitrary multiplicative group G. Then there exists $H \leq G$ so that

(I) $|AB| \geq |A| + |B| - |H|$,

(II) For every $x \in AB$ there exists $y \in G$ so that $x(yHy^{-1}) \subseteq AB$.

Structure (D.)

Again the nontrivial critical pairs can be constructed recursively using small sets and progressions.

G arbitrary

Lower Bound (D.)

Let A, B be finite nonempty subsets of an arbitrary multiplicative group G. Then there exists $H \leq G$ so that

(I) $|AB| \geq |A| + |B| - |H|$,

(II) For every $x \in AB$ there exists $y \in G$ so that $x(yHy^{-1}) \subseteq AB$.

Structure (D.)

Again the nontrivial critical pairs can be constructed recursively using small sets and progressions.

Proof Ingredients

- recasting the problem in an algebraic graph theory setting.

G arbitrary

Lower Bound (D.)

Let A, B be finite nonempty subsets of an arbitrary multiplicative group G. Then there exists $H \leq G$ so that

(I) $|AB| \geq |A| + |B| - |H|$,

(II) For every $x \in AB$ there exists $y \in G$ so that $x(yHy^{-1}) \subseteq AB$.

Structure (D.)

Again the nontrivial critical pairs can be constructed recursively using small sets and progressions.

Proof Ingredients

- recasting the problem in an algebraic graph theory setting.
- a transform due to Kemperman.

Kemperman's Transform

Let $A, B \subseteq G$ and let $g \in G$.
Consider the pairs $(A \cap Ag, B \cup g^{-1}B)$ and $(A \cup Ag, B \cap g^{-1}B)$

Kemperman's Transform

Let $A, B \subseteq G$ and let $g \in G$.
Consider the pairs $(A \cap Ag, B \cup g^{-1}B)$ and $(A \cup Ag, B \cap g^{-1}B)$

Properties

1. $(A \cap Ag)(B \cup g^{-1}B) \subseteq AB$

Kemperman's Transform

Let $A, B \subseteq G$ and let $g \in G$.
Consider the pairs $(A \cap Ag, B \cup g^{-1}B)$ and $(A \cup Ag, B \cap g^{-1}B)$

Properties

1. $(A \cap Ag)(B \cup g^{-1}B) \subseteq AB$
2. $(A \cup Ag)(B \cap g^{-1}B) \subseteq AB$

Kemperman's Transform

Let $A, B \subseteq G$ and let $g \in G$.
Consider the pairs $(A \cap Ag, B \cup g^{-1}B)$ and $(A \cup Ag, B \cap g^{-1}B)$

Properties

1. $(A \cap Ag)(B \cup g^{-1}B) \subseteq AB$
2. $(A \cup Ag)(B \cap g^{-1}B) \subseteq AB$
3. $|A \cap Ag| + |A \cup Ag| + |B \cap g^{-1}B| + |B \cup g^{-1}B| = 2|A| + 2|B|$

A Third Set

Suppose G is an finite multiplicative group and (A, B) is critical. Define $C = G \setminus (AB)^{-1}$.

A Third Set

Suppose G is an finite multiplicative group and (A, B) is critical. Define $C = G \setminus (AB)^{-1}$.

Observe

1. $1 \notin ABC$,

A Third Set

Suppose G is an finite multiplicative group and (A, B) is critical. Define $C = G \setminus (AB)^{-1}$.

Observe

1. $1 \notin ABC$,
2. $|A| + |B| + |C| = |A| + |B| + |G| - |AB| > |G|$.

A Third Set

Suppose G is an finite multiplicative group and (A, B) is critical. Define $C = G \setminus (AB)^{-1}$.

Observe

1. $1 \notin ABC$,
2. $|A| + |B| + |C| = |A| + |B| + |G| - |AB| > |G|$.
3. (B, C) is critical. (since BC is disjoint from A^{-1})
4. (C, A) is critical. (since CA is disjoint from B^{-1})

Trios

Definition

A **Trio** is a triple (A, B, C) of subsets of G with $1 \notin ABC$.

Trios

Definition

A **Trio** is a triple (A, B, C) of subsets of G with $1 \notin ABC$.
The trio (A, B, C) is

- **Critical** if $|A| + |B| + |C| > |G|$
- **Trivial** if one of A, B, C is empty

Trios

Definition

A **Trio** is a triple (A, B, C) of subsets of G with $1 \notin ABC$.
The trio (A, B, C) is

- **Critical** if $|A| + |B| + |C| > |G|$
- **Trivial** if one of A, B, C is empty

Note

To classify the critical pairs, it suffices to classify all nontrivial critical trios.

Trios

Definition

A **Trio** is a triple (A, B, C) of subsets of G with $1 \notin ABC$.
The trio (A, B, C) is

- **Critical** if $|A| + |B| + |C| > |G|$
- **Trivial** if one of A, B, C is empty

Note

To classify the critical pairs, it suffices to classify all nontrivial critical trios.

Theorem (Vosper)

If p is prime and (A, B, C) is a nontrivial trio in $\mathbb{Z}_p$ then one of the following holds:

(I) $\min\{|A|, |B|, |C|\} = 1$

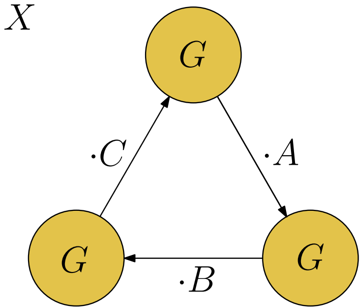
(II) A, B, C are all arithmetic progressions with a common difference.

Graphs

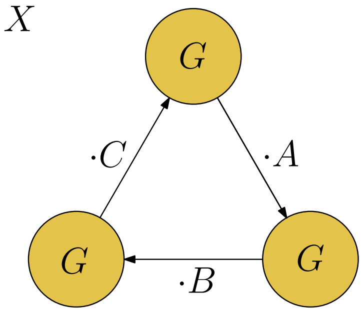
Let (A, B, C) be a critical trio and define a **trio** graph X by:

Graphs

Let (A, B, C) be a critical trio and define a **trio** graph X by:



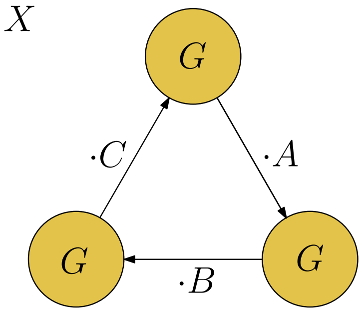
Graphs



Observe

1. X has no triangle

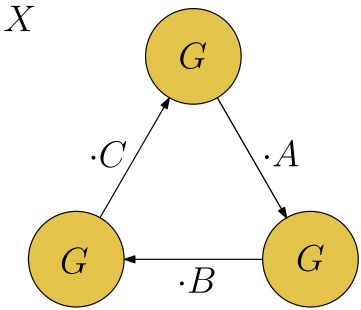
Graphs



Observe

1. X has no triangle
2. The sum of the densities of the three bipartite subgraphs between blocks is $\frac{|A|}{|G|} + \frac{|B|}{|G|} + \frac{|C|}{|G|} > 1$.

Graphs



Observe

1. X has no triangle
2. The sum of the densities of the three bipartite subgraphs between blocks is $\frac{|A|}{|G|} + \frac{|B|}{|G|} + \frac{|C|}{|G|} > 1$.
3. G has a natural action on X which is transitive on each block.

New problem

Classify all tripartite graphs X which satisfy

1. X has no triangle
2. The sum of the densities of the three bipartite subgraphs between blocks is > 1.
3. The subgroup of $Aut(X)$ which fixes each block setwise still acts transitively on each block.

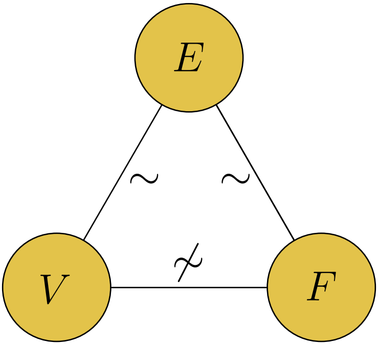
We call these **special** graphs.

Example

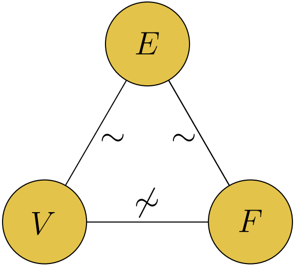
Consider a graph embedded in a surface with vertices V, edges E, and faces F for which the automorphism group acts transitively on V, E, and F.

Example

Consider a graph embedded in a surface with vertices V, edges E, and faces F for which the automorphism group acts transitively on V, E, and F. Define a graph X as follows



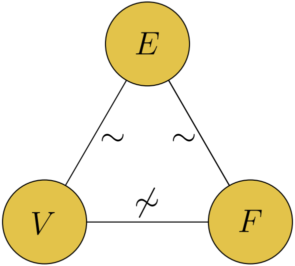
Example



Observe:

- X has no triangle.

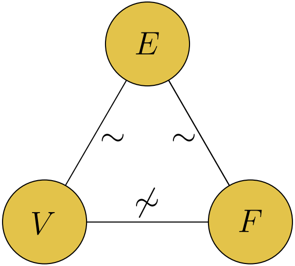
Example



Observe:

- X has no triangle.
- The automorphism group is transitive on V, E, and F.

Example

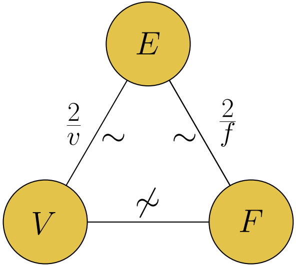


Observe:

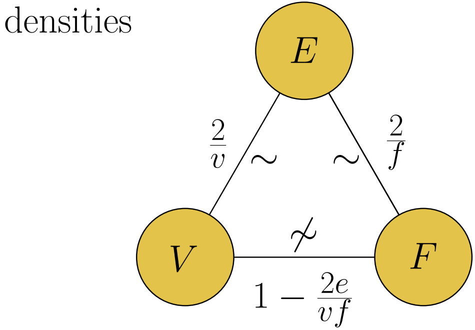
- X has no triangle.
- The automorphism group is transitive on V, E, and F.
- next we compute compute densities..

Example

densities

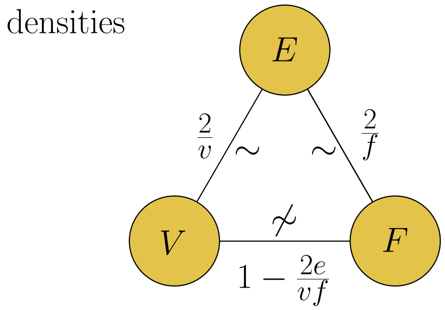


Example



- The number of vertex-face incidences is $2e$
- The density of the vertex-face incidence bipartite graph is $\frac{2e}{vf}$
- The density of the vertex-face nonincidence bipartite graph is $1 - \frac{2e}{vf}$

Example



So the sum of the densities of the three bipartite graphs is

$$\frac{2}{f} + \left(1 - \frac{2e}{vf}\right) + \frac{2}{v} = 1 + \frac{2}{vf}\,(v - e + f)$$

so X is special precisely when $v - e + f > 0$

Back to Subsets

Although V, E and F generally have different sizes, these graphs do come from subset trios..

Back to Subsets

Although V, E and F generally have different sizes, these graphs do come from subset trios..

Say that two vertices are **clones** if they have exactly the same neighbours.

Back to Subsets

Although V, E and F generally have different sizes, these graphs do come from subset trios..

Say that two vertices are **clones** if they have exactly the same neighbours.

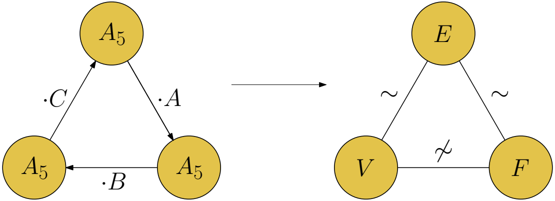
Note: If X is a special graph, identifying clones brings us to a new special graph.

Back to Subsets

Although V, E and F generally have different sizes, these graphs do come from subset trios..

Say that two vertices are **clones** if they have exactly the same neighbours.

Note: If X is a special graph, identifying clones brings us to a new special graph.



Dodecahedron

Sabidussi's Theorem

Theorem (Sabidussi)

Every special graph can be obtained from a trio graph by identifying clones.

Sabidussi's Theorem

Theorem (Sabidussi)

Every special graph can be obtained from a trio graph by identifying clones.

More precisely: If X is a special graph and H is a subgroup of the automorphism group of X which acts transitively on each block, then we may obtain X from a trio graph using any group G which has a quotient isomorphic to H.

Sabidussi's Theorem

Theorem (Sabidussi)

Every special graph can be obtained from a trio graph by identifying clones.

More precisely: If X is a special graph and H is a subgroup of the automorphism group of X which acts transitively on each block, then we may obtain X from a trio graph using any group G which has a quotient isomorphic to H.

Example

The special graph based on Dodecahedron comes from critical trios in $A_5 \times \mathbb{Z}_2$ and A_5 (and more generally any group with a quotient isomorphic to one of these).

Sabidussi's Theorem

Theorem (Sabidussi)

Every special graph can be obtained from a trio graph by identifying clones.

More precisely: If X is a special graph and H is a subgroup of the automorphism group of X which acts transitively on each block, then we may obtain X from a trio graph using any group G which has a quotient isomorphic to H.

Example

The special graph based on Dodecahedron comes from critical trios in $A_5 \times \mathbb{Z}_2$ and A_5 (and more generally any group with a quotient isomorphic to one of these).

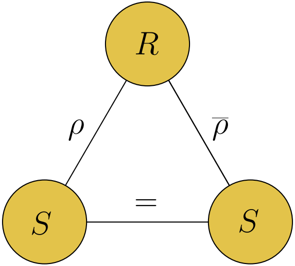
Note

To classify critical trios, we will first classify special graphs, then determine their automorphism groups

Describing the Classification

Every maximal special graph may be obtained by a sequential construction involving three recursive structures, terminating in one of three types of elementary structure.

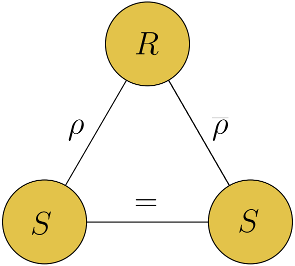
Elementary Structure 1



Associated critical trios (A, B, C)

Trios with $|B| = 1$

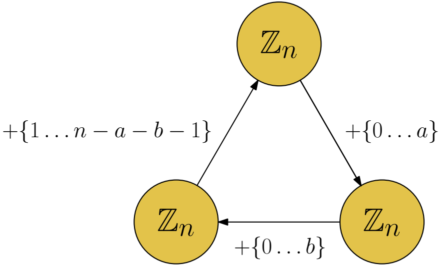
Elementary Structure 1



Associated critical trios (A, B, C)

Trios with $|B| = 1$ and more generally to those for which $AH = A$ and $B = Hx$ for some $H < G$.

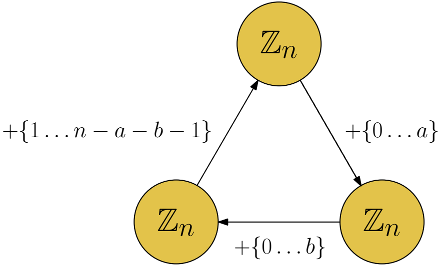
Elementary Structure 2



Associated critical trios (A, B, C)

Those in cyclic groups where A, B, C are all progressions with a common difference.

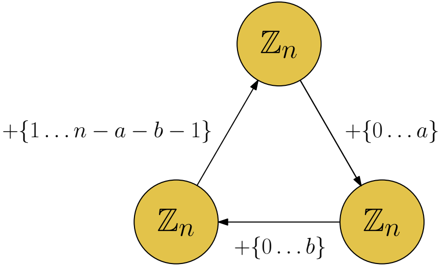
Elementary Structure 2



Associated critical trios (A, B, C)

Those in cyclic groups where A, B, C are all progressions with a common difference. Trios in dihedral groups where A, B, C are all "dihedral progressions" with a common difference.

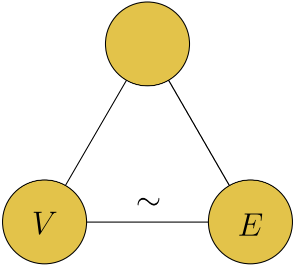
Elementary Structure 2



Associated critical trios (A, B, C)

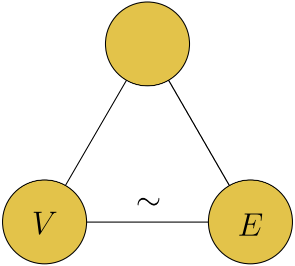
Those in cyclic groups where A, B, C are all progressions with a common difference. Trios in dihedral groups where A, B, C are all "dihedral progressions" with a common difference. More generally, this yields critical trios in groups G which cyclic or dihedral quotients.

Elementary Structure 3



Here (V, E) is a vertex and edge transitive graph.

Elementary Structure 3

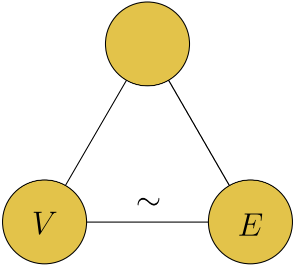


Here (V, E) is a vertex and edge transitive graph.

Associated critical trios (A, B, C)

Those for which $B = Hx \cup Hy$ for some $H < G$.

Elementary Structure 3



Here (V, E) is a vertex and edge transitive graph.

Associated critical trios (A, B, C)

Those for which $B = Hx \cup Hy$ for some $H < G$.

Example

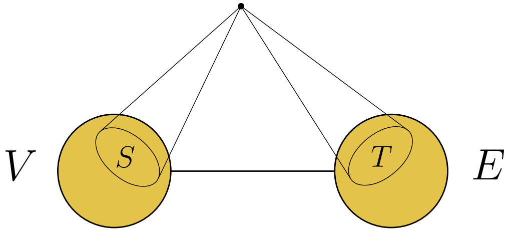
Let $A = H \cup xH$ and $B = H \cup Hx$. Then
$AB = H \cup xH \cup Hx \cup xHx$ has size $< 4|H| = |A| + |B|$

Graphs

Suppose (V, E) is a d-regular vertex and edge transitive graph, when can we use it to construct a very small product set?

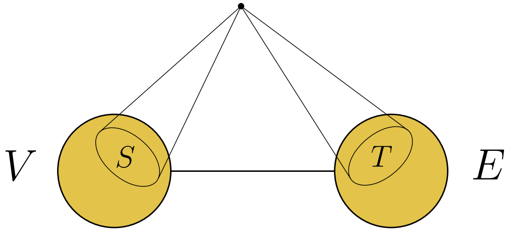
Graphs

Suppose (V, E) is a d-regular vertex and edge transitive graph, when can we use it to construct a very small product set?



Graphs

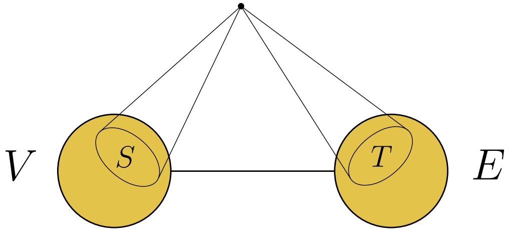
Suppose (V, E) is a d-regular vertex and edge transitive graph, when can we use it to construct a very small product set?



The density condition translates to the property that the edge cut separating S from the rest of the graph has size $< 2d$.

Graphs

Suppose (V, E) is a d-regular vertex and edge transitive graph, when can we use it to construct a very small product set?

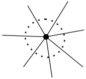


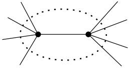
The density condition translates to the property that the edge cut separating S from the rest of the graph has size $< 2d$.

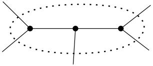
To find these very small product sets, we classify all edge-cuts of size $< 2d$ in d-regular vertex and edge transitive graphs.

Small Edge-Cuts

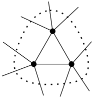
Edge cuts of size $< 2d$ in d-regular vertex and edge transitive graphs (Assume connected and $d \geq 3$)

1.  size d

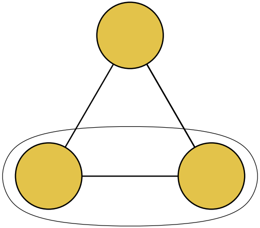
2.  size $2d - 1$

3. $d = 3$  size 5

4. G is one of Cube, Octahedron, Dodecahedron, Icosahedron, K_6, or Petersen and one side is a shortest cycle

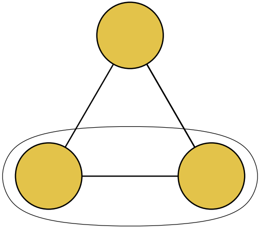
   ex. 

Recursive Structure 1

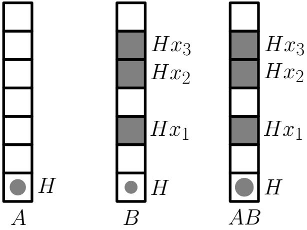


disconnected bipartite graph

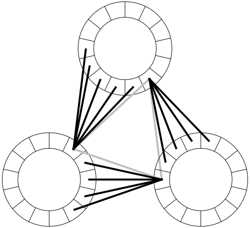
Recursive Structure 1



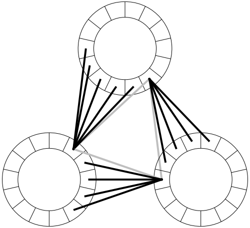
disconnected bipartite graph



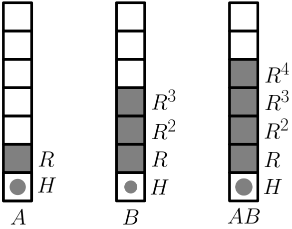
Recursive Structure 2



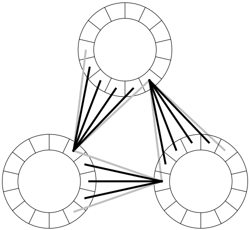
Recursive Structure 2



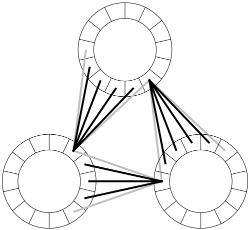
Below $N \lhd G$, and G/N is cyclic and generated by $R \in G/N$.



Recursive Structure 3

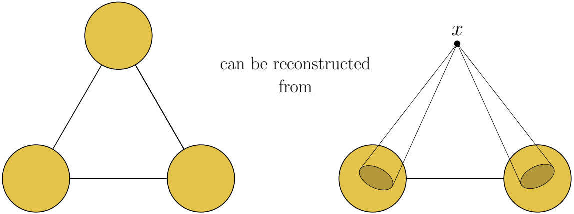


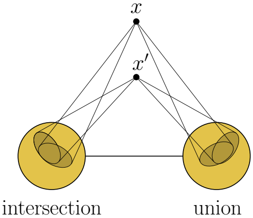
Recursive Structure 3



This double-fringed structure gives rise to critical trios in dihedral groups (and more generally groups with dihedral quotients).

Ideas in the Proof





Proving Vosper's Theorem

Theorem (Vosper)

If p is prime and (A, B, C) is a nontrivial trio in $\mathbb{Z}_p$ then one of the following holds:

(I) $\min\{|A|, |B|, |C|\} = 1$

(II) A, B, C are all arithmetic progressions with a common difference.

Proving Vosper's Theorem

Theorem (Vosper)

If p is prime and (A, B, C) is a nontrivial trio in $\mathbb{Z}_p$ then one of the following holds:

(I) $\min\{|A|, |B|, |C|\} = 1$

(II) A, B, C are all arithmetic progressions with a common difference.

Stability Lemma

The result holds when C is a nontrivial arithmetic progression.

Proving Vosper's Theorem

Theorem (Vosper)

If p is prime and (A, B, C) is a nontrivial trio in $\mathbb{Z}_p$ then one of the following holds:

(I) $\min\{|A|, |B|, |C|\} = 1$

(II) A, B, C are all arithmetic progressions with a common difference.

Stability Lemma

The result holds when C is a nontrivial arithmetic progression.

Proof of Vosper: Suppose (for a contradiction) that the result is false and choose a counterexample (A, B, C) so that

(i) $|C|$ is minimum.

(ii) $|B|$ is minimum (subject to (i))

Proving Vosper's Theorem (continued)

Note: by the Cauchy-Davenport theorem $|A| + |B| + |C| = p + 1$.

Proving Vosper's Theorem (continued)

Note: by the Cauchy-Davenport theorem $|A|+|B|+|C| = p+1$.
Our assumptions and the lemma imply $3 \leq |A| \leq |B| \leq |C|$.

Proving Vosper's Theorem (continued)

Note: by the Cauchy-Davenport theorem $|A| + |B| + |C| = p + 1$. Our assumptions and the lemma imply $3 \leq |A| \leq |B| \leq |C|$.

First suppose B is a Sidon set, so $|B \cap (B + g)| \leq 1$ for every $g \neq 0$. Then we may choose $c_1, c_2, c_3 \in C$ distinct and we have the contradiction:

$$|B+C| \geq |(B+c_1) \cup (B+c_2) \cup (B+c_3)| \geq 3|B| - 3 \geq 2|B| \geq |B| + |C|$$

Proving Vosper's Theorem (continued)

Note: by the Cauchy-Davenport theorem $|A| + |B| + |C| = p + 1$.
Our assumptions and the lemma imply $3 \leq |A| \leq |B| \leq |C|$.

We may choose $g \neq 0$ so that $|B \cap (B - g)| \geq 2$.

Proving Vosper's Theorem (continued)

Note: by the Cauchy-Davenport theorem $|A| + |B| + |C| = p + 1$.
Our assumptions and the lemma imply $3 \le |A| \le |B| \le |C|$.

We may choose $g \neq 0$ so that $|B \cap (B - g)| \ge 2$. Consider

$$(A \cap (A + g), B \cup (B - g), C)$$
$$(A \cup (A + g), B \cap (B - g), C).$$

Proving Vosper's Theorem (continued)

Note: by the Cauchy-Davenport theorem $|A| + |B| + |C| = p + 1$.
Our assumptions and the lemma imply $3 \leq |A| \leq |B| \leq |C|$.

We may choose $g \neq 0$ so that $|B \cap (B - g)| \geq 2$. Consider

$$(A \cap (A + g), B \cup (B - g), C)$$
$$(A \cup (A + g), B \cap (B - g), C).$$

If $A \cap (A + g) = \emptyset$ then we have the contradiction:

$$|A + B| \geq |(A \cup (A + g) + (B \cap (B - g))| \geq 2|A| + 1 > |A| + |B|$$

Proving Vosper's Theorem (continued)

Note: by the Cauchy-Davenport theorem $|A| + |B| + |C| = p + 1$. Our assumptions and the lemma imply $3 \leq |A| \leq |B| \leq |C|$.

We may choose $g \neq 0$ so that $|B \cap (B - g)| \geq 2$. Consider

$$(A \cap (A + g), B \cup (B - g), C)$$
$$(A \cup (A + g), B \cap (B - g), C).$$

If $A \cap (A + g) = \emptyset$ then we have the contradiction:

$$|A + B| \geq |(A \cup (A + g) + (B \cap (B - g))| \geq 2|A| + 1 > |A| + |B|$$

So $A \cap (A + g) \neq \emptyset$ and both of our new trios are nontrivial. It now follows from Cauchy-Davenport that the sum of the sizes of the three sets in both of these new trios is $p + 1$.

Proving Vosper's Theorem (continued)

Note: by the Cauchy-Davenport theorem $|A| + |B| + |C| = p + 1$. Our assumptions and the lemma imply $3 \leq |A| \leq |B| \leq |C|$.

We may choose $g \neq 0$ so that $|B \cap (B - g)| \geq 2$. Consider

$$(A \cap (A + g), B \cup (B - g), C)$$
$$(A \cup (A + g), B \cap (B - g), C).$$

If $A \cap (A + g) = \emptyset$ then we have the contradiction:

$$|A + B| \geq |(A \cup (A + g) + (B \cap (B - g))| \geq 2|A| + 1 > |A| + |B|$$

So $A \cap (A + g) \neq \emptyset$ and both of our new trios are nontrivial. It now follows from Cauchy-Davenport that the sum of the sizes of the three sets in both of these new trios is $p + 1$. By our choice of counterexample, the theorem holds true for the trio $(A \cup (A + g), B \cap (B - g), C)$. It follows that C is an arithmetic progression, and now the result follows from our lemma. $\square$

The End

Thanks for your attention!