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. 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. How small can $|A + B|$ be?
2. 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. How small can $|A + B|$ be?
2. If $|A + B|$ is small, then why?

Definition

$|A + B|$ is *very small* 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. How small can $|AB|$ be?
2. If $|AB|$ is small, then why?

Definition

$|AB|$ is *very small* if $|AB| < |A| + |B|$.

Observation

If $A, B \subseteq \mathbb{Z}$ are finite and nonempty then $|A + B| \geq |A| + |B| - 1$.

Observation

If $A, B \subseteq \mathbb{Z}$ are finite and nonempty then $|A + B| \geq |A| + |B| - 1$.

Proof:

Let $A = \{a_1 \ldots a_m\}, B = \{b_1 \ldots b_n\}$ with $a_1 < \ldots < a_m$ and $b_1 < \ldots < b_n$.

Observation

If $A, B \subseteq \mathbb{Z}$ are finite and nonempty then $|A + B| \geq |A| + |B| - 1$.

Proof:

Let $A = \{a_1 \dots a_m\}, B = \{b_1 \dots b_n\}$ with $a_1 < \dots < a_m$ and $b_1 < \dots < b_n$. Then $A + B$ contains the distinct elements

$$a_1 + b_1 < a_2 + b_1 < \dots < a_m + b_1 < a_m + b_2 < \dots < a_m + b_n.$$

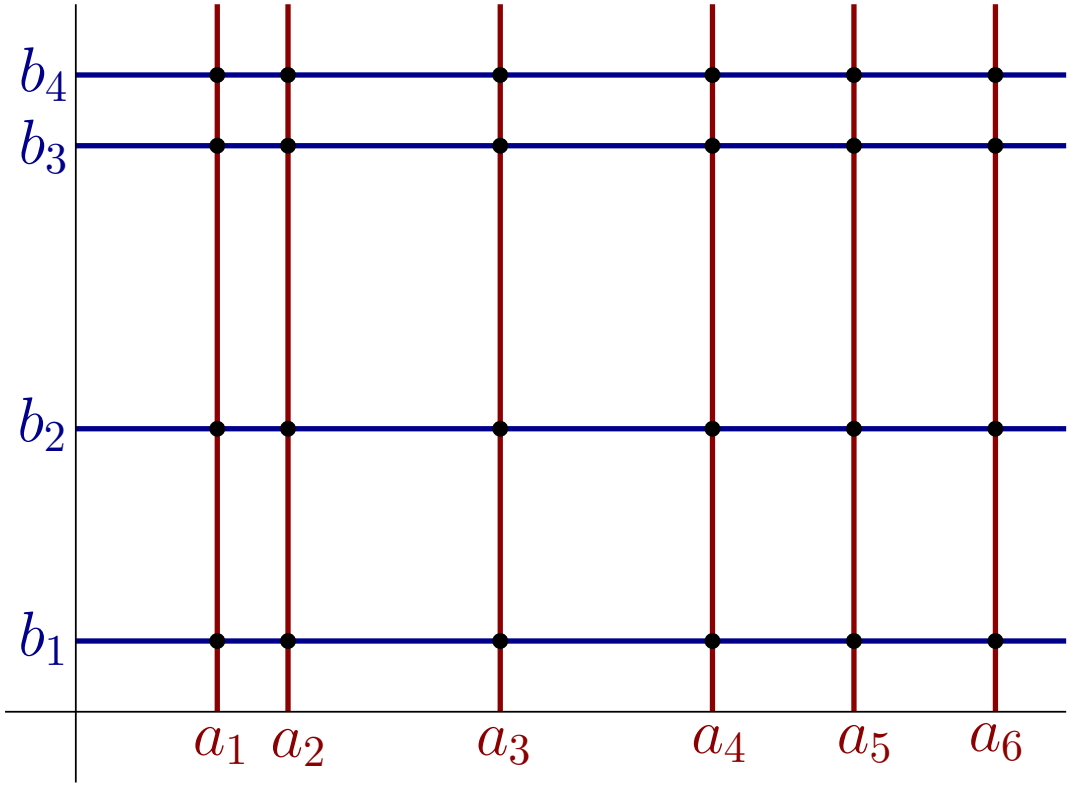
□

More generally

If we start from $a_1 + b_1$ and move to $a_m + b_n$ by incrementing one index each step, we find $m + n - 1$ distinct elements.

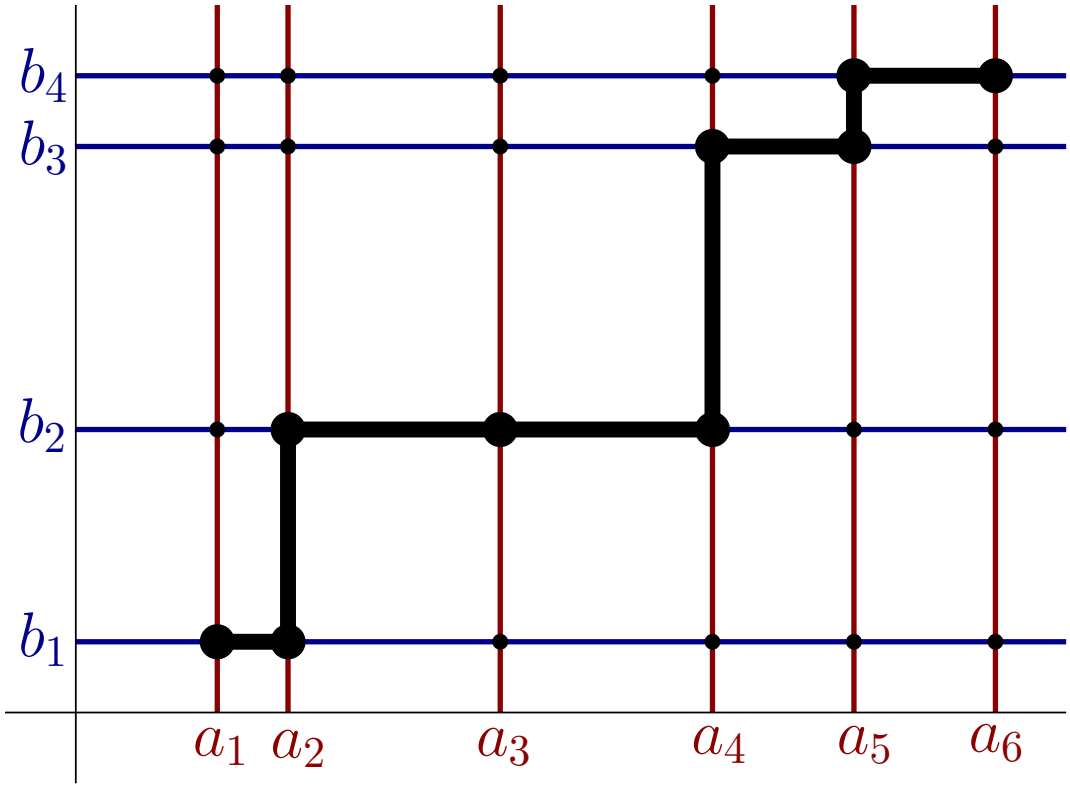
More generally

If we start from $a_1 + b_1$ and move to $a_m + b_n$ by incrementing one index each step, we find $m + n - 1$ distinct elements.



More generally

However we start from $a_1 + b_1$ and move to $a_m + b_n$ by increasing one index by one each step, we find $m + n - 1$ distinct elements.



this leads to...

Observation

If $A, B \subseteq \mathbb{Z}$ are finite and nonempty and $|A + B|$ is very small, then one of the following holds:

1. $|A| = 1$ or $|B| = 1$,
2. A and B are arithmetic progressions with a common difference.

Theorem (Cauchy-Davenport)

If p is prime and $A, B \subseteq \mathbb{Z}/p\mathbb{Z}$ are nonempty, then either $A + B = \mathbb{Z}/p\mathbb{Z}$, or $|A + B| \geq |A| + |B| - 1$.

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

Theorem (Cauchy-Davenport)

If p is prime and $A, B \subseteq \mathbb{Z}/p\mathbb{Z}$ are nonempty, then either $A + B = \mathbb{Z}/p\mathbb{Z}$, or $|A + B| \geq |A| + |B| - 1$.

Very Small Sumsets (Vosper)

1. $|A| = 1$ or $|B| = 1$
2. A, B arithmetic progressions with a common difference.

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

Theorem (Cauchy-Davenport)

If p is prime and $A, B \subseteq \mathbb{Z}/p\mathbb{Z}$ are nonempty, then either $A + B = \mathbb{Z}/p\mathbb{Z}$, or $|A + B| \geq |A| + |B| - 1$.

Very Small Sumsets (Vosper)

1. $|A| = 1$ or $|B| = 1$
2. A, B arithmetic progressions with a common difference.
3. $|A + B| \geq p - 1$

G abelian

Theorem (Kneser)

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

1. $|A + B| \geq |A| + |B| - |H|$, and
2. $A + B + H = A + B$.

G abelian

Theorem (Kneser)

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

1. $|A + B| \geq |A| + |B| - |H|$, and
2. $A + B + H = A + B$.

Very Small Sumsets (Kemperman)

G arbitrary

Theorem (D.)

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

1. $|AB| \geq |A| + |B| - |H|$,
2. For every $x \in AB$ there exists $y \in G$ so that $x(yHy^{-1}) \subseteq AB$.

G arbitrary

Theorem (D.)

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

1. $|AB| \geq |A| + |B| - |H|$,
2. For every $x \in AB$ there exists $y \in G$ so that $x(yHy^{-1}) \subseteq AB$.

Note

We prove this by classifying the very small product sets.

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

Theorem (Cauchy-Davenport)

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

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

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

Theorem (Cauchy-Davenport)

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

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

Shifting

For an element $g \in G$ and a set $C \subseteq G$ we define $g + C = \{g\} + C$ and $C + g = C + \{g\}$, and we call sets of this form *shifts* of C.

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

Theorem (Cauchy-Davenport)

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

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

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

Theorem (Cauchy-Davenport)

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

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

Key Property

$$(A \cap (A + g)) + (B \cup (-g + B)) \subseteq A + B$$

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

Theorem (Cauchy-Davenport)

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

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

Key Property

$$(A \cap (A + g)) + (B \cup (-g + B)) \subseteq A + B$$

x y

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

Theorem (Cauchy-Davenport)

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

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

Key Property

$$(A \cap (A + g)) + (B \cup (-g + B)) \subseteq A + B$$

x y

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

Theorem (Cauchy-Davenport)

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

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

Key Property

$$(A \cap (A + g)) + (B \cup (-g + B)) \subseteq A + B$$

$$x \qquad\qquad y \qquad\qquad x + y$$

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

Theorem (Cauchy-Davenport)

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

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

Key Property

$$(A \cap (A + g)) + (B \cup (-g + B)) \subseteq A + B$$

x y

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

Theorem (Cauchy-Davenport)

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

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

Key Property

$$\underset{x}{(A \cap (A + g))} + \underset{y}{(B \cup (-g + B))} \subseteq \underset{x+y}{A + B}$$

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

Theorem (Cauchy-Davenport)

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

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

Key Property

$$(A \cap (A + g)) + (B \cup (-g + B)) \subseteq A + B$$

$$(A \cup (A + g)) + (B \cap (-g + B)) \subseteq A + B$$

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

Theorem (Cauchy-Davenport)

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

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

Proof:

Consider a counterexample A, B for which

1. $|A| + |B| - |A + B|$ is maximum.
2. $|A|$ is minimum (subj. to 1.).

Theorem (Cauchy-Davenport)

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

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

Proof:

Consider a counterexample A, B for which

1. $|A| + |B| - |A + B|$ is maximum.
2. $|A|$ is minimum (subj. to 1.).

Since we have a counterexample, $1 < |A| < p$.

Theorem (Cauchy-Davenport)

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

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

Proof:

Consider a counterexample A, B for which

1. $|A| + |B| - |A + B|$ is maximum.
2. $|A|$ is minimum (subj. to 1.).

Since we have a counterexample, $1 < |A| < p$.
Choose $g \neq 0$ so that $A \cap (A + g) \neq \emptyset$.

Theorem (Cauchy-Davenport)

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

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

Proof:

Consider a counterexample A, B for which

1. $|A| + |B| - |A + B|$ is maximum.
2. $|A|$ is minimum (subj. to 1.).

Since we have a counterexample, $1 < |A| < p$.
Choose $g \neq 0$ so that $A \cap (A + g) \neq \emptyset$.
Note that $A \cap (A + g) \neq A$.

Theorem (Cauchy-Davenport)

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

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

Proof:

Consider a counterexample A, B for which

1. $|A| + |B| - |A + B|$ is maximum.
2. $|A|$ is minimum (subj. to 1.).

Since we have a counterexample, $1 < |A| < p$.
Choose $g \neq 0$ so that $A \cap (A + g) \neq \emptyset$.
Note that $A \cap (A + g) \neq A$.
Consider $(A \cap (A + g)) + (B \cup (-g + B)) \subseteq A + B$ and
$(A \cup (A + g)) + (B \cap (-g + B)) \subseteq A + B$.

Theorem (Cauchy-Davenport)

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

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

Proof:

Consider a counterexample A, B for which

1. $|A| + |B| - |A + B|$ is maximum.
2. $|A|$ is minimum (subj. to 1.).

Since we have a counterexample, $1 < |A| < p$.
Choose $g \neq 0$ so that $A \cap (A + g) \neq \emptyset$.
Note that $A \cap (A + g) \neq A$.
Consider $(A \cap (A + g)) + (B \cup (-g + B)) \subseteq A + B$ and
$(A \cup (A + g)) + (B \cap (-g + B)) \subseteq A + B$.
One of these pairs contradicts our choice of A, B. $\square$

G arbitrary

General Technique

In an arbitrary (multiplicative) group we still have the identities
$(A \cap (Ag)) \cdot (B \cup (g^{-1}B)) \subseteq AB$ and
$(A \cup (Ag)) \cdot (B \cap (g^{-1}B)) \subseteq AB$.

Trios

Def:
Suppose G is an finite multiplicative group and AB is a very small product set. Define $C = G \setminus (AB)^{-1}$.

Trios

Def:
Suppose G is an finite multiplicative group and AB is a very small product set. Define $C = G \setminus (AB)^{-1}$.

Observe

1. $1 \notin ABC$,

Trios

Def:
Suppose G is an finite multiplicative group and AB is a very small product set. Define $C = G \setminus (AB)^{-1}$.

Observe

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

Trios

Def:
Suppose G is an finite multiplicative group and AB is a very small product set. Define $C = G \setminus (AB)^{-1}$.

Observe

1. $1 \notin ABC$,
2. $|A| + |B| + |C| = |A| + |B| + |G| - |AB| > |G|$.
3. BC is very small.

(this follows from the fact that BC is disjoint from $G \setminus A^{-1}$, so $|BC| \leq |G| - |A^{-1}| < |B| + |C|$)

Trios

Def:
Suppose G is an finite multiplicative group and AB is very small. Define $C = G \setminus (AB)^{-1}$.

Observe

1. $1 \notin ABC$,
2. $|A| + |B| + |C| = |A| + |B| + |G| - |AB| > |G|$.
3. BC is very small.
4. CA is very small.

Trios

Def:
Suppose G is an finite multiplicative group and AB is very small. Define $C = G \setminus (AB)^{-1}$.

Observe

1. $1 \notin ABC$,
2. $|A| + |B| + |C| = |A| + |B| + |G| - |AB| > |G|$.
3. BC is very small.
4. CA is very small.

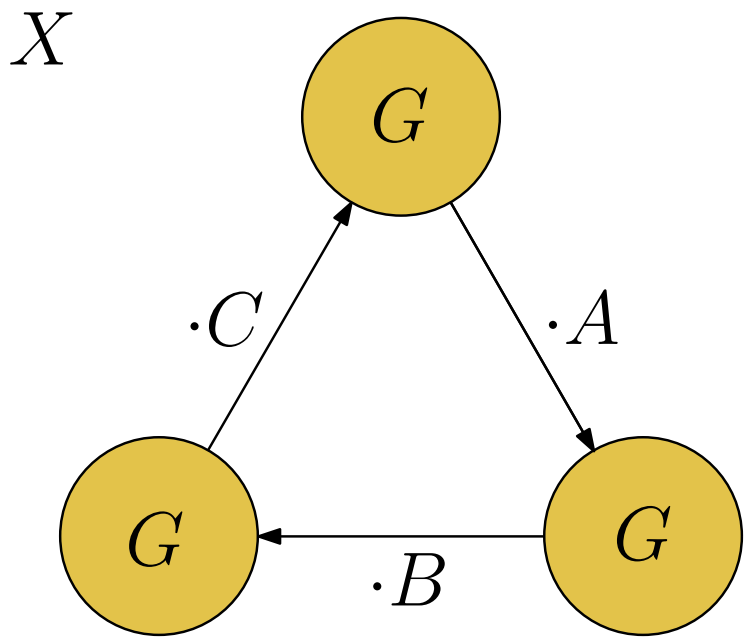
Def:
A *Trio* is a triple (A, B, C) of subsets of G with $1 \notin ABC$. We call it *very small* if $|A| + |B| + |C| > |G|$.

Graphs

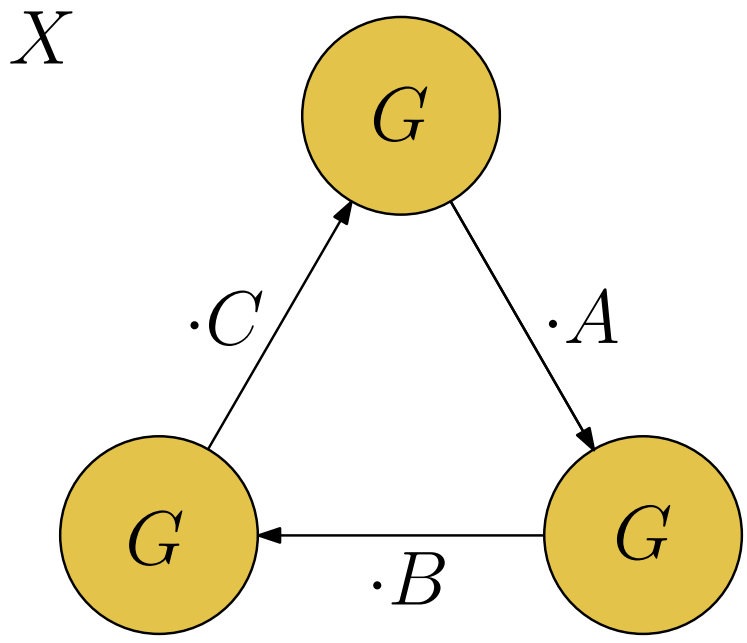
Let (A, B, C) be a very small trio and define a graph X as follows

Graphs

Let (A, B, C) be a very small trio and define a graph X as follows



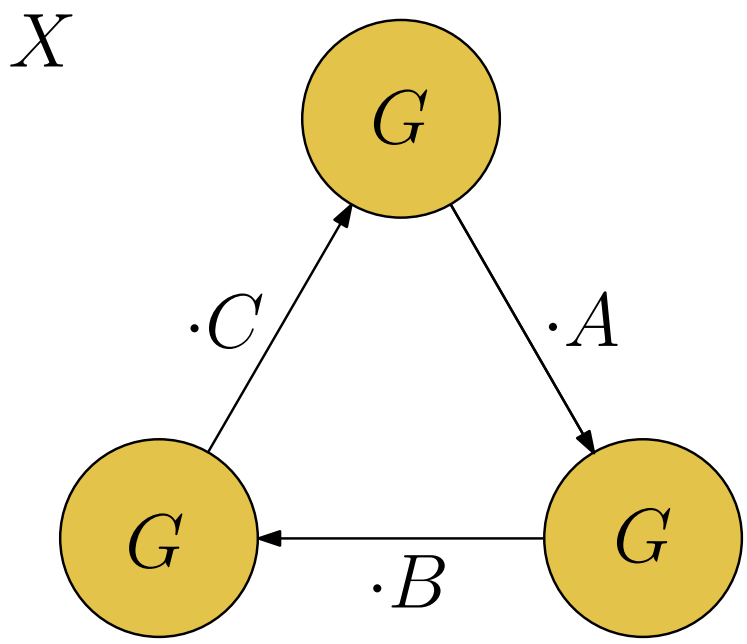
Graphs



Observe

1. X has no triangle

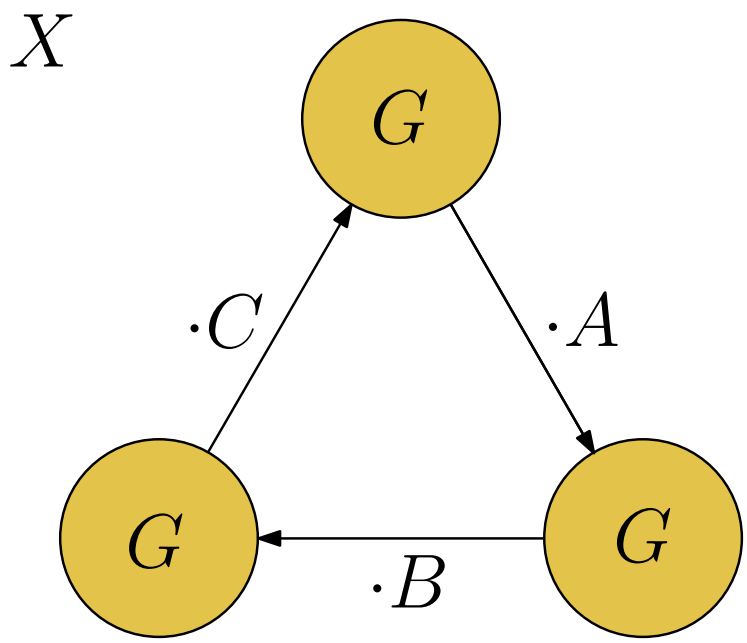
Graphs



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.

Graphs

New problem

We intend to classify all tripartite graphs X which satisfy

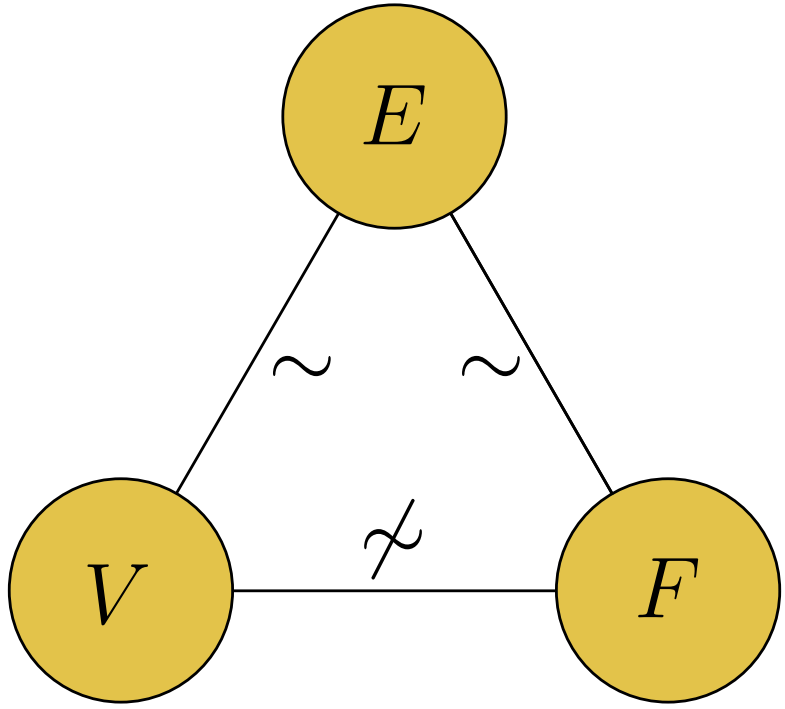
1. X has no triangle
2. The sum of the densities of the three bipartite subgraphs between blocks is > 1.
3. The subgroup of $Aut(X)$ which fixes each block setwise still acts transitively on each block.

Example

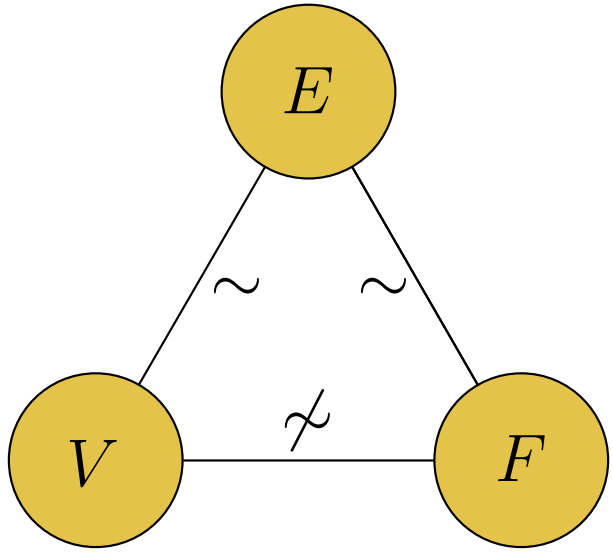
Consider a finite map on a surface with vertices V, edges E, and faces F for which the automorphism group acts transitively on V, E, and F.

Example

Consider a finite map on 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



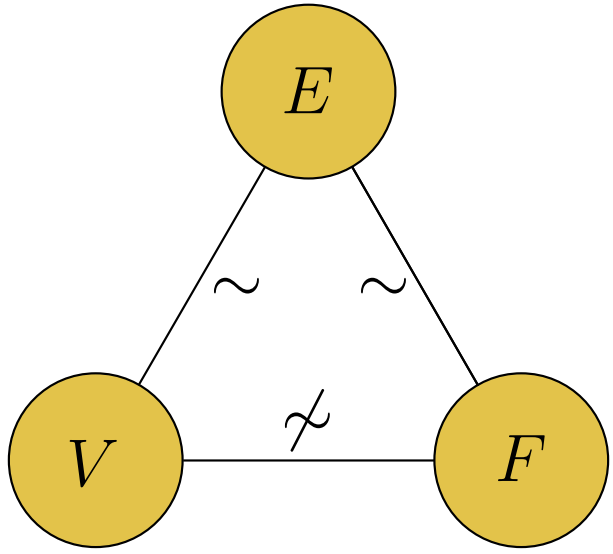
Example



Observe:

- X has no triangle.

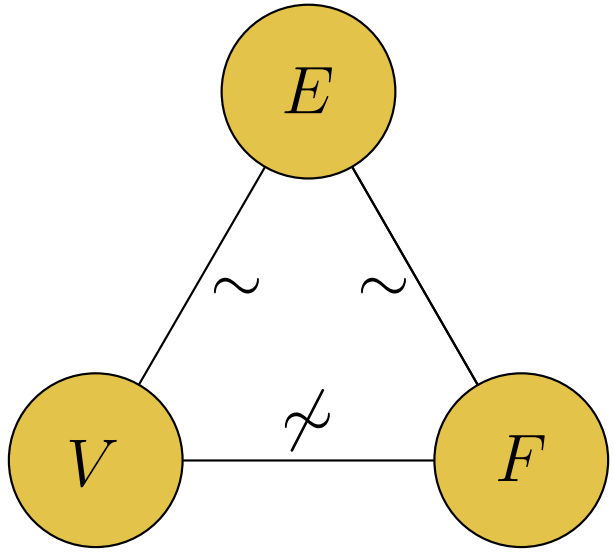
Example



Observe:

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

Example

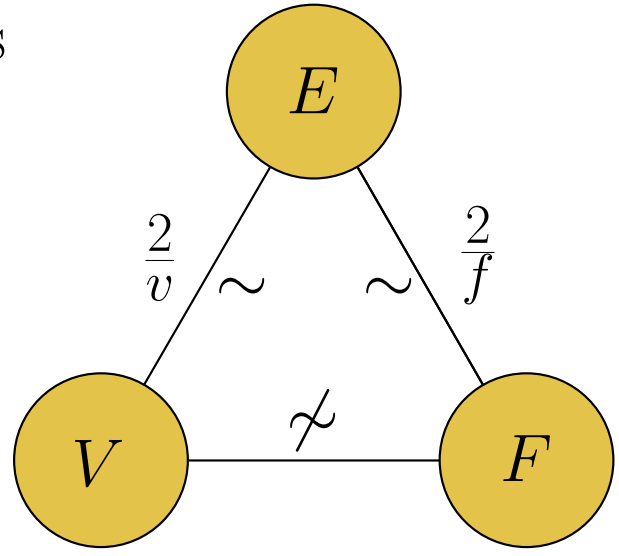


Observe:

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

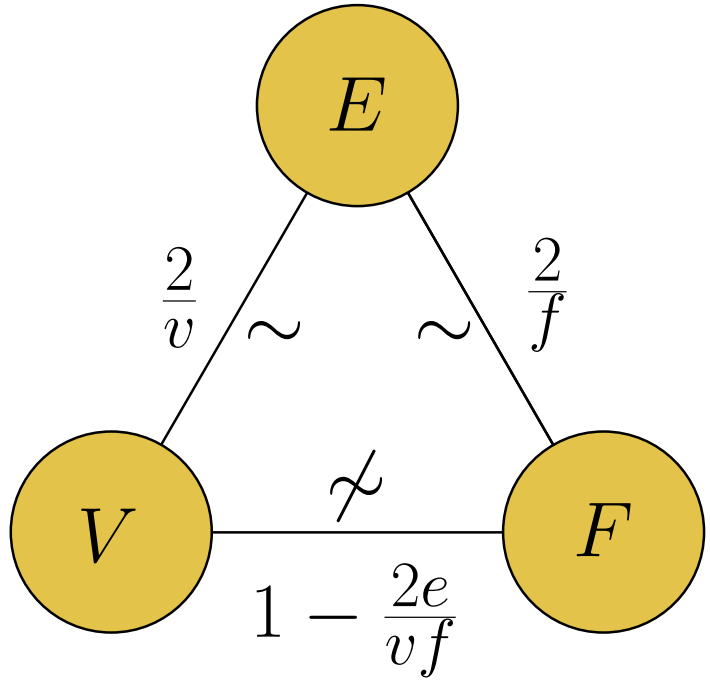
Example

densities



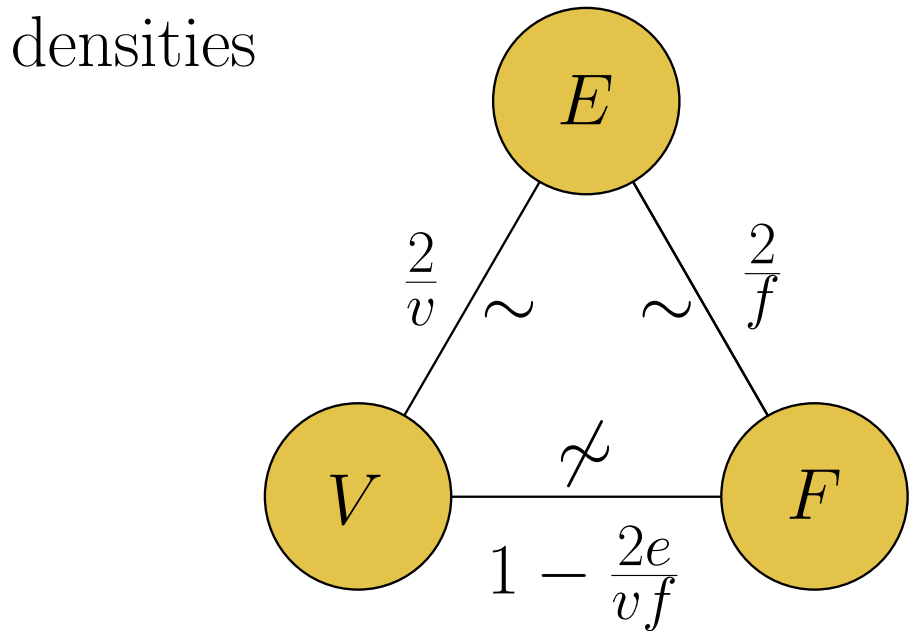
Example

densities



- 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

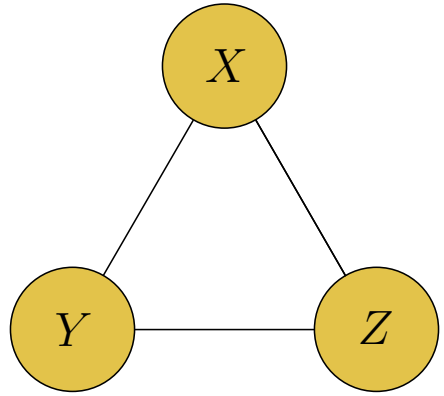


So the sum of the densities of the three bipartite graphs is

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

and X satisfies our conditions precisely when $v - e + f > 0$

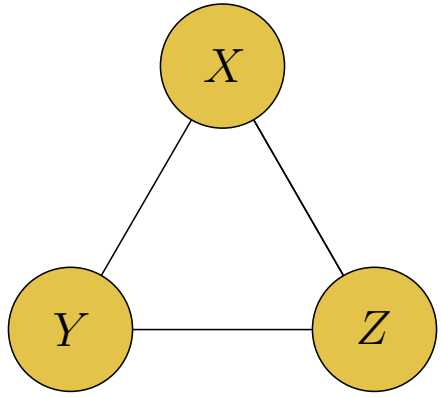
Back to Groups



Consider one of our tripartite graphs Γ

- If $G \leq Aut(\Gamma)$ acts regularly on each block, then Γ may be constructed from a very small product set in G.

Back to Groups



Consider one of our tripartite graphs Γ

- If $G \leq Aut(\Gamma)$ acts regularly on each block, then Γ may be constructed from a very small product set in G.
- (Sabidussi) In general we can construct Γ using a very small product set in G and then identifying clones.

Theorem and Proof

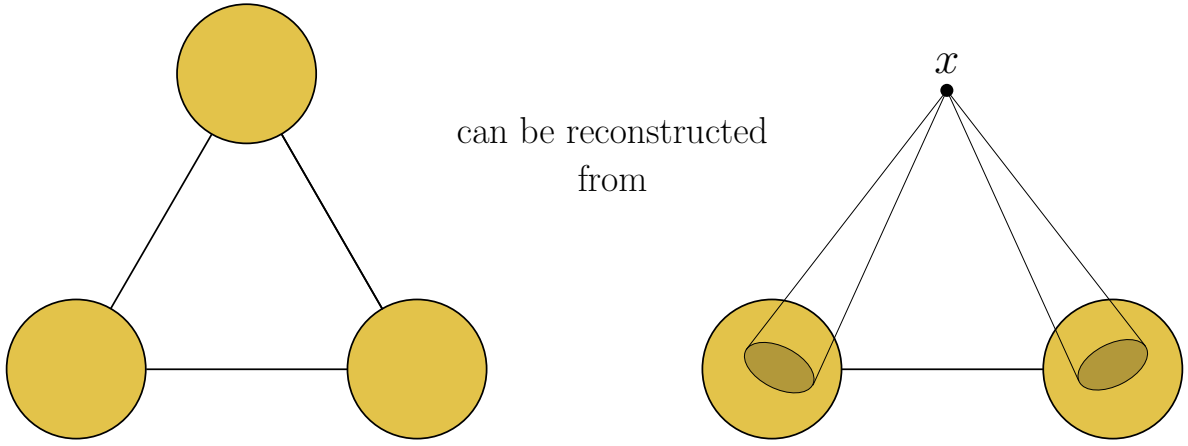
Theorem

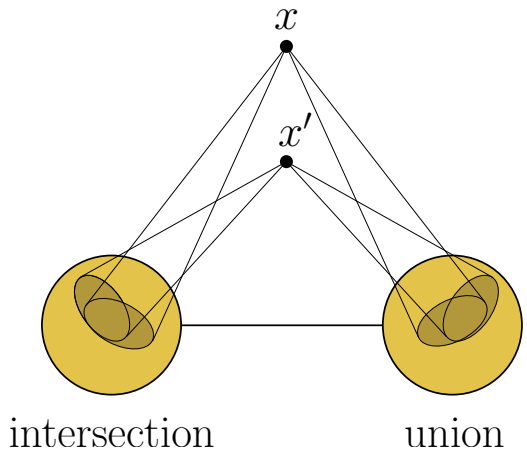
The structure theorem is extremely complex with several types of recursive structures, a few families of terminal structures, and a handful of sporadic structures based on the Platonic Solids and the regular maps on the projective plane.

Proof

The proof is very long (the paper is 147 pages!), but it relies on a delicate induction, some technical stability lemmas, and the following idea...

Theorem and Proof





The End

Thanks for your attention!