Most groups are hyperbolic, or ... most groups are trivial ?

Enric Ventura

Departament de Matemàtica Aplicada III

Universitat Politècnica de Catalunya

Seminari Grafs, Barcelona

March 18th, 2010.

Outline

Outline

Gromov's claim

Claim (Gromov '87)

Most finite presentations of groups, present an hyperbolic infinite group.

- Stated in his influential paper on hyperbolic groups: "Essays in group theory", 75-263, Springer, 1987,
- no proof, only the idea,
- the meaning of "most" is not precise,
- statement made precise and proved, later by other authors.

Gromov's claim

Claim (Gromov '87)

Most finite presentations of groups, present an hyperbolic infinite group.

- Stated in his influential paper on hyperbolic groups:
  "Essays in group theory", 75-263, Springer, 1987,
- no proof, only the idea,
- the meaning of "most" is not precise,
- statement made precise and proved, later by other authors.

Gromov's claim

Claim (Gromov '87)

Most finite presentations of groups, present an hyperbolic infinite group.

- Stated in his influential paper on hyperbolic groups: "Essays in group theory", 75-263, Springer, 1987,
- no proof, only the idea,
- the meaning of "most" is not precise,
- statement made precise and proved, later by other authors.

Gromov's claim

Claim (Gromov '87)

Most finite presentations of groups, present an hyperbolic infinite group.

- Stated in his influential paper on hyperbolic groups:
  "Essays in group theory", 75-263, Springer, 1987,
- no proof, only the idea,
- the meaning of "most" is not precise,
- statement made precise and proved, later by other authors.

Gromov's claim

Claim (Gromov '87)

Most finite presentations of groups, present an hyperbolic infinite group.

- Stated in his influential paper on hyperbolic groups: "Essays in group theory", 75-263, Springer, 1987,
- no proof, only the idea,
- the meaning of "most" is not precise,
- statement made precise and proved, later by other authors.

Presentations of groups

Notation

- $A = \{a_1, \ldots, a_k\}$ *is a finite alphabet (n letters).*
- $A^{\pm 1} = A \cup A^{-1} = \{a_1, a_1^{-1}, \ldots, a_k, a_k^{-1}\}$.
- *Usually,* $A = \{a, b, c\}$.
- $(A^{\pm 1})^*$ *the free monoid on* $A^{\pm 1}$ *(words on* $A^{\pm 1}$*).*
- $F_A = (A^{\pm 1})^* / \sim$ *is the free group on A (words on* $A^{\pm 1}$ *modulo reduction).*
- *Every* $w \in A^*$ *has a unique reduced form,*
- 1 *denotes the empty word, and* $|\cdot|$ *the (shortest) length in* F_A*:*
  $|1| = 0, \quad |aba^{-1}| = |abbb^{-1}a^{-1}| = 3, \quad |uv| \leqslant |u| + |v|$.
- *The free group* F_A *is usually denoted by:*

$$F_A = \langle a_1, \ldots, a_r \mid - \rangle.$$

Presentations of groups

Notation

- $A = \{a_1, \ldots, a_k\}$ *is a finite alphabet (n letters).*
- $A^{\pm 1} = A \cup A^{-1} = \{a_1, a_1^{-1}, \ldots, a_k, a_k^{-1}\}$.
- *Usually,* $A = \{a, b, c\}$.
- $(A^{\pm 1})^*$ *the free monoid on* $A^{\pm 1}$ *(words on* $A^{\pm 1}$*).*
- $F_A = (A^{\pm 1})^* / \sim$ *is the free group on* A *(words on* $A^{\pm 1}$ *modulo reduction).*
- *Every* $w \in A^*$ *has a unique reduced form,*
- 1 *denotes the empty word, and* $|\cdot|$ *the (shortest) length in* F_A*:*
  $|1| = 0, \quad |aba^{-1}| = |abbb^{-1}a^{-1}| = 3, \quad |uv| \leqslant |u| + |v|$.
- *The free group* F_A *is usually denoted by:*

$$F_A = \langle a_1, \ldots, a_r \mid - \rangle.$$

Presentations of groups

Notation

- $A = \{a_1, \ldots, a_k\}$ *is a finite alphabet (n letters).*
- $A^{\pm 1} = A \cup A^{-1} = \{a_1, a_1^{-1}, \ldots, a_k, a_k^{-1}\}$.
- *Usually,* $A = \{a, b, c\}$.
- $(A^{\pm 1})^*$ *the free monoid on* $A^{\pm 1}$ *(words on* $A^{\pm 1}$*).*
- $F_A = (A^{\pm 1})^* / \sim$ *is the free group on A (words on* $A^{\pm 1}$ *modulo reduction).*
- *Every* $w \in A^*$ *has a unique reduced form,*
- 1 *denotes the empty word, and* $|\cdot|$ *the (shortest) length in* F_A*:*
  $|1| = 0, \quad |aba^{-1}| = |abbb^{-1}a^{-1}| = 3, \quad |uv| \leqslant |u| + |v|.$
- *The free group* F_A *is usually denoted by:*

$$F_A = \langle a_1, \ldots, a_r \mid - \rangle.$$

Presentations of groups

Notation

- $A = \{a_1, \ldots, a_k\}$ *is a finite alphabet (n letters).*
- $A^{\pm 1} = A \cup A^{-1} = \{a_1, a_1^{-1}, \ldots, a_k, a_k^{-1}\}$.
- *Usually,* $A = \{a, b, c\}$.
- $(A^{\pm 1})^*$ *the free monoid on* $A^{\pm 1}$ *(words on* $A^{\pm 1}$*).*
- $F_A = (A^{\pm 1})^* / \sim$ *is the free group on A (words on* $A^{\pm 1}$ *modulo reduction).*
- *Every* $w \in A^*$ *has a unique reduced form,*
- 1 *denotes the empty word, and* $|\cdot|$ *the (shortest) length in* F_A*:* $|1| = 0, \quad |aba^{-1}| = |abbb^{-1}a^{-1}| = 3, \quad |uv| \leqslant |u| + |v|$.
- *The free group* F_A *is usually denoted by:*

$$F_A = \langle a_1, \ldots, a_r \mid - \rangle.$$

Presentations of groups

Notation

- $A = \{a_1, \ldots, a_k\}$ *is a finite alphabet (n letters).*
- $A^{\pm 1} = A \cup A^{-1} = \{a_1, a_1^{-1}, \ldots, a_k, a_k^{-1}\}$.
- *Usually,* $A = \{a, b, c\}$.
- $(A^{\pm 1})^*$ *the free monoid on* $A^{\pm 1}$ *(words on* $A^{\pm 1}$*).*
- $F_A = (A^{\pm 1})^* / \sim$ *is the free group on* A *(words on* $A^{\pm 1}$ *modulo reduction).*
- *Every* $w \in A^*$ *has a unique reduced form,*
- 1 *denotes the empty word, and* $|\cdot|$ *the (shortest) length in* F_A*:*
  $|1| = 0, \quad |aba^{-1}| = |abbb^{-1}a^{-1}| = 3, \quad |uv| \leqslant |u| + |v|$.
- *The free group* F_A *is usually denoted by:*

$$F_A = \langle a_1, \ldots, a_r \mid - \rangle.$$

Presentations of groups

Notation

- $A = \{a_1, \ldots, a_k\}$ *is a finite alphabet (n letters).*
- $A^{\pm 1} = A \cup A^{-1} = \{a_1, a_1^{-1}, \ldots, a_k, a_k^{-1}\}$.
- *Usually,* $A = \{a, b, c\}$.
- $(A^{\pm 1})^*$ *the free monoid on* $A^{\pm 1}$ *(words on* $A^{\pm 1}$*).*
- $F_A = (A^{\pm 1})^* / \sim$ *is the free group on A (words on* $A^{\pm 1}$ *modulo reduction).*
- *Every* $w \in A^*$ *has a unique reduced form,*
- 1 *denotes the empty word, and* $|\cdot|$ *the (shortest) length in* F_A*:*
  $|1| = 0, \quad |aba^{-1}| = |abbb^{-1}a^{-1}| = 3, \quad |uv| \leqslant |u| + |v|$.
- *The free group* F_A *is usually denoted by:*

$$F_A = \langle a_1, \ldots, a_r \mid - \rangle.$$

Presentations of groups

Notation

- $A = \{a_1, \ldots, a_k\}$ *is a finite alphabet (n letters).*
- $A^{\pm 1} = A \cup A^{-1} = \{a_1, a_1^{-1}, \ldots, a_k, a_k^{-1}\}$.
- *Usually,* $A = \{a, b, c\}$.
- $(A^{\pm 1})^*$ *the free monoid on* $A^{\pm 1}$ *(words on* $A^{\pm 1}$*).*
- $F_A = (A^{\pm 1})^* / \sim$ *is the free group on A (words on* $A^{\pm 1}$ *modulo reduction).*
- *Every* $w \in A^*$ *has a unique reduced form,*
- 1 *denotes the empty word, and* $|\cdot|$ *the (shortest) length in* F_A*:*
  $|1| = 0, \quad |aba^{-1}| = |abbb^{-1}a^{-1}| = 3, \quad |uv| \leqslant |u| + |v|$.
- *The free group* F_A *is usually denoted by:*

$$F_A = \langle a_1, \ldots, a_r \mid - \rangle.$$

Presentations of groups

Notation

- $A = \{a_1, \ldots, a_k\}$ *is a finite alphabet (n letters).*
- $A^{\pm 1} = A \cup A^{-1} = \{a_1, a_1^{-1}, \ldots, a_k, a_k^{-1}\}$.
- *Usually,* $A = \{a, b, c\}$.
- $(A^{\pm 1})^*$ *the free monoid on* $A^{\pm 1}$ *(words on* $A^{\pm 1}$*).*
- $F_A = (A^{\pm 1})^* / \sim$ *is the free group on A (words on* $A^{\pm 1}$ *modulo reduction).*
- *Every* $w \in A^*$ *has a unique reduced form,*
- 1 *denotes the empty word, and* $|\cdot|$ *the (shortest) length in* F_A*:*
  $|1| = 0, \quad |aba^{-1}| = |abbb^{-1}a^{-1}| = 3, \quad |uv| \leqslant |u| + |v|$.
- *The free group* F_A *is usually denoted by:*

$$F_A = \langle a_1, \ldots, a_r \mid - \rangle.$$

Presentations of groups

Theorem

Every finitely generated group G is a quotient of F_A (for some r), i.e.

$$G \simeq F_A/N = \langle a_1, \ldots, a_r \mid w_1, w_2, \ldots \rangle,$$

where N is the normal closure of $w_1, w_2, \ldots \in F_A$ in F_A.

- If G admits a presentation with finitely many w_i's (*relations*) we say it is *finitely presented*.
- Very different presentations can give isomorphic groups:

$$\langle a \mid a \rangle = 1 = \langle a, b \mid a^{-1}ba = b^2,\ b^{-1}ab = a^2 \rangle$$

- Deciding whether a finite presentation presents the trivial group is algorithmically unsolvable.

Presentations of groups

Theorem

Every finitely generated group G is a quotient of F_A (for some r), i.e.

$$G \simeq F_A/N = \langle a_1, \ldots, a_r \mid w_1, w_2, \ldots \rangle,$$

where N is the normal closure of $w_1, w_2, \ldots \in F_A$ in F_A.

- If G admits a presentation with finitely many w_i's (*relations*) we say it is *finitely presented*.
- Very different presentations can give isomorphic groups:

$$\langle a \mid a \rangle = 1 = \langle a, b \mid a^{-1}ba = b^2, \ b^{-1}ab = a^2 \rangle$$

- Deciding whether a finite presentation presents the trivial group is algorithmically unsolvable.

Presentations of groups

Theorem

Every finitely generated group G is a quotient of F_A (for some r), i.e.

$$G \simeq F_A/N = \langle a_1, \ldots, a_r \mid w_1, w_2, \ldots \rangle,$$

where N is the normal closure of $w_1, w_2, \ldots \in F_A$ in F_A.

- If G admits a presentation with finitely many w_i's (*relations*) we say it is *finitely presented*.
- Very different presentations can give isomorphic groups:

$$\langle a \mid a \rangle = 1 = \langle a, b \mid a^{-1}ba = b^2, \ b^{-1}ab = a^2 \rangle$$

- Deciding whether a finite presentation presents the trivial group is algorithmically unsolvable.

Presentations of groups

Theorem

Every finitely generated group G is a quotient of F_A (for some r), i.e.

$$G \simeq F_A/N = \langle a_1, \ldots, a_r \mid w_1, w_2, \ldots \rangle,$$

where N is the normal closure of $w_1, w_2, \ldots \in F_A$ in F_A.

- If G admits a presentation with finitely many w_i's (*relations*) we say it is *finitely presented*.
- Very different presentations can give isomorphic groups:

$$\langle a \mid a \rangle = 1 = \langle a, b \mid a^{-1}ba = b^2,\ b^{-1}ab = a^2 \rangle$$

- Deciding whether a finite presentation presents the trivial group is algorithmically unsolvable.

Presentations of groups

Theorem

Every finitely generated group G is a quotient of F_A (for some r), i.e.

$$G \simeq F_A/N = \langle a_1, \ldots, a_r \mid w_1, w_2, \ldots \rangle,$$

where N is the normal closure of $w_1, w_2, \ldots \in F_A$ in F_A.

- If G admits a presentation with finitely many w_i's (*relations*) we say it is *finitely presented*.
- Very different presentations can give isomorphic groups:

$$\langle a \mid a \rangle = 1 = \langle a, b \mid a^{-1}ba = b^2,\ b^{-1}ab = a^2 \rangle$$

- Deciding whether a finite presentation presents the trivial group is algorithmically unsolvable.

Hyperbolicity

Let G be a group, $S \subseteq G$, and $\chi(G,S)$ the Cayley graph of G w.r.t. S.

- $\chi(G,S)$ is connected if and only if S generates G.
- $\chi(G,S)$ has non-trivial closed paths if and only if S satisfy non-trivial relations.
- $\chi(G,S)$ is a tree if and only if G is free with basis S.

Definition

A group G is δ-hyperbolic if every geodesic triangle in $\chi(G,S)$ is δ-thin. (Free groups are 0-thin with respect to bases).

So, intuitively, hyperbolic groups are "close" to free groups (in a geometric sense).

Let G be a group, $S \subseteq G$, and $\chi(G, S)$ the Cayley graph of G w.r.t. S.

- $\chi(G, S)$ is connected if and only if S generates G.
- $\chi(G, S)$ has non-trivial closed paths if and only if S satisfy non-trivial relations.
- $\chi(G, S)$ is a tree if and only if G is free with basis S.

Definition

A group G is δ-hyperbolic if every geodesic triangle in $\chi(G, S)$ is δ-thin. (Free groups are 0-thin with respect to bases).

So, intuitively, hyperbolic groups are "close" to free groups (in a geometric sense).

Hyperbolicity

Let G be a group, $S \subseteq G$, and $\chi(G, S)$ the Cayley graph of G w.r.t. S.

- $\chi(G, S)$ is connected if and only if S generates G.
- $\chi(G, S)$ has non-trivial closed paths if and only if S satisfy non-trivial relations.
- $\chi(G, S)$ is a tree if and only if G is free with basis S.

Definition

A group G is δ-hyperbolic if every geodesic triangle in $\chi(G, S)$ is δ-thin. (Free groups are 0-thin with respect to bases).

So, intuitively, hyperbolic groups are “close” to free groups (in a geometric sense).

Hyperbolicity

Let G be a group, $S \subseteq G$, and $\chi(G, S)$ the Cayley graph of G w.r.t. S.

- $\chi(G, S)$ is connected if and only if S generates G.
- $\chi(G, S)$ has non-trivial closed paths if and only if S satisfy non-trivial relations.
- $\chi(G, S)$ is a tree if and only if G is free with basis S.

Definition

A group G is δ-hyperbolic if every geodesic triangle in $\chi(G, S)$ is δ-thin. (Free groups are 0-thin with respect to bases).

So, intuitively, hyperbolic groups are "close" to free groups (in a geometric sense).

Hyperbolicity

Let G be a group, $S \subseteq G$, and $\chi(G, S)$ the Cayley graph of G w.r.t. S.

- $\chi(G, S)$ is connected if and only if S generates G.
- $\chi(G, S)$ has non-trivial closed paths if and only if S satisfy non-trivial relations.
- $\chi(G, S)$ is a tree if and only if G is free with basis S.

Definition

A group G is δ-hyperbolic if every geodesic triangle in $\chi(G, S)$ is δ-thin. (Free groups are 0-thin with respect to bases).

So, intuitively, hyperbolic groups are "close" to free groups (in a geometric sense).

Hyperbolicity

Let G be a group, $S \subseteq G$, and $\chi(G, S)$ the Cayley graph of G w.r.t. S.

- $\chi(G, S)$ is connected if and only if S generates G.
- $\chi(G, S)$ has non-trivial closed paths if and only if S satisfy non-trivial relations.
- $\chi(G, S)$ is a tree if and only if G is free with basis S.

Definition

A group G is δ-hyperbolic if every geodesic triangle in $\chi(G, S)$ is δ-thin. (Free groups are 0-thin with respect to bases).

So, intuitively, hyperbolic groups are “close” to free groups (in a geometric sense).

The meaning of "most"

Let X be an infinite set. What is the meaning of sentences like "most elements in X have property $\mathcal{P}$" ?

- Define a notion of size, $|\cdot| \colon X \to \mathbb{N}$, with finite preimages.
- Define the balls: $B(n) = \{x \in X \mid |x| \leqslant n\}$ (which are finite).
- Count the proportion $\rho_n = \frac{|\{x \in X | x \text{ satisfies } \mathcal{P}\}|}{|B(n)|} = \frac{|\mathcal{P} \cap B(n)|}{|B(n)|}$.
- Define the density of X as $\rho = \lim_{n\to\infty} \rho_n$ ($\in [0, 1]$ if it exists).
- $\mathcal{P}$ is generic (or generically many elements satisfy $\mathcal{P}$) if $\rho = 1$.
- $\mathcal{P}$ is negligible if $\rho = 0$.

Of course, everything depends on the chosen size function, i.e. on the direction to infinity inside X.

The meaning of "most"

Let X be an infinite set. What is the meaning of sentences like "most elements in X have property $\mathcal{P}$" ?

- Define a notion of size, $|\cdot|: X \to \mathbb{N}$, with finite preimages.
- Define the balls: $B(n) = \{x \in X \mid |x| \leqslant n\}$ (which are finite).
- Count the proportion $\rho_n = \frac{|\{x \in X | x \text{ satisfies } \mathcal{P}\}|}{|B(n)|} = \frac{|\mathcal{P} \cap B(n)|}{|B(n)|}$.
- Define the density of X as $\rho = \lim_{n\to\infty} \rho_n$ ($\in [0, 1]$ if it exists).
- $\mathcal{P}$ is generic (or generically many elements satisfy $\mathcal{P}$) if $\rho = 1$.
- $\mathcal{P}$ is negligible if $\rho = 0$.

Of course, everything depends on the chosen size function, i.e. on the direction to infinity inside X.

The meaning of “most”

Let X be an infinite set. What is the meaning of sentences like “most elements in X have property $\mathcal{P}$” ?

- Define a notion of size, $|\cdot|\colon X \to \mathbb{N}$, with finite preimages.
- Define the balls: $B(n) = \{x \in X \mid |x| \leqslant n\}$ (which are finite).
- Count the proportion $\rho_n = \frac{|\{x \in X \mid x \text{ satisfies } \mathcal{P}\}|}{|B(n)|} = \frac{|\mathcal{P} \cap B(n)|}{|B(n)|}$.
- Define the density of X as $\rho = \lim_{n\to\infty} \rho_n$ ($\in [0, 1]$ if it exists).
- $\mathcal{P}$ is generic (or generically many elements satisfy $\mathcal{P}$) if $\rho = 1$.
- $\mathcal{P}$ is negligible if $\rho = 0$.

Of course, everything depends on the chosen size function, i.e. on the direction to infinity inside X.

The meaning of "most"

Let X be an infinite set. What is the meaning of sentences like "most elements in X have property $\mathcal{P}$" ?

- Define a notion of size, $|\cdot|\colon X \to \mathbb{N}$, with finite preimages.
- Define the balls: $B(n) = \{x \in X \mid |x| \leqslant n\}$ (which are finite).
- Count the proportion $\rho_n = \frac{|\{x \in X \mid x \text{ satisfies } \mathcal{P}\}|}{|B(n)|} = \frac{|\mathcal{P} \cap B(n)|}{|B(n)|}$.
- Define the density of X as $\rho = \lim_{n\to\infty} \rho_n$ ($\in [0,1]$ if it exists).
- $\mathcal{P}$ is generic (or generically many elements satisfy $\mathcal{P}$) if $\rho = 1$.
- $\mathcal{P}$ is negligible if $\rho = 0$.

Of course, everything depends on the chosen size function, i.e. on the direction to infinity inside X.

The meaning of “most”

Let X be an infinite set. What is the meaning of sentences like “most elements in X have property $\mathcal{P}$” ?

- Define a notion of size, $|\cdot|\colon X \to \mathbb{N}$, with finite preimages.
- Define the balls: $B(n) = \{x \in X \mid |x| \leqslant n\}$ (which are finite).
- Count the proportion $\rho_n = \frac{|\{x \in X | x \text{ satisfies } \mathcal{P}\}|}{|B(n)|} = \frac{|\mathcal{P} \cap B(n)|}{|B(n)|}$.
- Define the density of X as $\rho = \lim_{n\to\infty} \rho_n$ ($\in [0,1]$ if it exists).
- $\mathcal{P}$ is generic (or generically many elements satisfy $\mathcal{P}$) if $\rho = 1$.
- $\mathcal{P}$ is negligible if $\rho = 0$.

Of course, everything depends on the chosen size function, i.e. on the direction to infinity inside X.

The meaning of “most”

Let X be an infinite set. What is the meaning of sentences like “most elements in X have property $\mathcal{P}$” ?

- Define a notion of size, $|\cdot|\colon X \to \mathbb{N}$, with finite preimages.
- Define the balls: $B(n) = \{x \in X \mid |x| \leqslant n\}$ (which are finite).
- Count the proportion $\rho_n = \frac{|\{x \in X \mid x \text{ satisfies } \mathcal{P}\}|}{|B(n)|} = \frac{|\mathcal{P} \cap B(n)|}{|B(n)|}$.
- Define the density of X as $\rho = \lim_{n\to\infty} \rho_n$ ($\in [0, 1]$ if it exists).
- $\mathcal{P}$ is generic (or generically many elements satisfy $\mathcal{P}$) if $\rho = 1$.
- $\mathcal{P}$ is negligible if $\rho = 0$.

Of course, everything depends on the chosen size function, i.e. on the direction to infinity inside X.

The meaning of "most"

Let X be an infinite set. What is the meaning of sentences like "most elements in X have property $\mathcal{P}$" ?

- Define a notion of size, $|\cdot|\colon X \to \mathbb{N}$, with finite preimages.
- Define the balls: $B(n) = \{x \in X \mid |x| \leqslant n\}$ (which are finite).
- Count the proportion $\rho_n = \frac{|\{x \in X \mid x \text{ satisfies } \mathcal{P}\}|}{|B(n)|} = \frac{|\mathcal{P} \cap B(n)|}{|B(n)|}$.
- Define the density of X as $\rho = \lim_{n\to\infty} \rho_n$ ($\in [0,1]$ if it exists).
- $\mathcal{P}$ is generic (or generically many elements satisfy $\mathcal{P}$) if $\rho = 1$.
- $\mathcal{P}$ is negligible if $\rho = 0$.

Of course, everything depends on the chosen size function, i.e. on the direction to infinity inside X.

The meaning of "most"

Let X be an infinite set. What is the meaning of sentences like "most elements in X have property $\mathcal{P}$" ?

- Define a notion of size, $|\cdot|\colon X \to \mathbb{N}$, with finite preimages.
- Define the balls: $B(n) = \{x \in X \mid |x| \leqslant n\}$ (which are finite).
- Count the proportion $\rho_n = \frac{|\{x \in X | x \text{ satisfies } \mathcal{P}\}|}{|B(n)|} = \frac{|\mathcal{P} \cap B(n)|}{|B(n)|}$.
- Define the density of X as $\rho = \lim_{n\to\infty} \rho_n$ ($\in [0, 1]$ if it exists).
- $\mathcal{P}$ is generic (or generically many elements satisfy $\mathcal{P}$) if $\rho = 1$.
- $\mathcal{P}$ is negligible if $\rho = 0$.

Of course, everything depends on the chosen size function, i.e. on the direction to infinity inside X.

Classical example: visible points

Definition

A point $(x_1, \ldots, x_k) \in \mathbb{Z}^k$ *is visible if* $\gcd(x_1, \ldots, x_k) = 1$.

Theorem (Mertens, 1874 (case $k = 2$))

The density of visible points in $\mathbb{Z}^k$ *is* $1/\zeta(k)$, *where* $\zeta(k) = \sum_{n=1}^{\infty} \frac{1}{n^k}$ *is the Riemann zeta-function (with respect to* $||\cdot||_1$*).*

In particular, visible points in the plane have density $\frac{6}{\pi^2}$.

With artificial definitions of size, one can force it to be any $\alpha \in [0, 1]$.

Classical example: visible points

Definition

A point $(x_1, \ldots, x_k) \in \mathbb{Z}^k$ *is visible if* $\gcd(x_1, \ldots, x_k) = 1$.

Theorem (Mertens, 1874 (case $k = 2$))

The density of visible points in $\mathbb{Z}^k$ *is* $1/\zeta(k)$, *where* $\zeta(k) = \sum_{n=1}^{\infty} \frac{1}{n^k}$ *is the Riemann zeta-function (with respect to* $||\cdot||_1$*).*

In particular, visible points in the plane have density $\frac{6}{\pi^2}$.

With artificial definitions of size, one can force it to be any $\alpha \in [0, 1]$.

Classical example: visible points

Definition

A point $(x_1, \ldots, x_k) \in \mathbb{Z}^k$ *is visible if* $\gcd(x_1, \ldots, x_k) = 1$.

Theorem (Mertens, 1874 (case $k = 2$))

The density of visible points in $\mathbb{Z}^k$ *is* $1/\zeta(k)$, *where* $\zeta(k) = \sum_{n=1}^{\infty} \frac{1}{n^k}$ *is the Riemann zeta-function (with respect to* $||\cdot||_1$*).*

In particular, visible points in the plane have density $\frac{6}{\pi^2}$.

With artificial definitions of size, one can force it to be any $\alpha \in [0, 1]$.

Classical example: visible points

Definition

A point $(x_1, \ldots, x_k) \in \mathbb{Z}^k$ *is visible if* $\gcd(x_1, \ldots, x_k) = 1$.

Theorem (Mertens, 1874 (case $k = 2$))

The density of visible points in $\mathbb{Z}^k$ *is* $1/\zeta(k)$, *where* $\zeta(k) = \sum_{n=1}^{\infty} \frac{1}{n^k}$ *is the Riemann zeta-function (with respect to* $||\cdot||_1$*).*

In particular, visible points in the plane have density $\frac{6}{\pi^2}$.

With artificial definitions of size, one can force it to be any $\alpha \in [0, 1]$.

Outline

Arzhantseva-Ol'shanskii's proof

- Fix $r \geqslant 2$ and $k \geqslant 1$.
- Consider the free group $F_A = \langle a_1, \ldots, a_r \mid - \rangle$.
- In F_A we have the natural notion of size and balls.
- For $w_1, \ldots, w_k \in F_A$, let $G_{w_1,\ldots,w_k} = \langle a_1, \ldots, a_r \mid w_1, \ldots, w_k \rangle$.

Theorem (Arzhantseva-Ol'shanskii, '96)

$$\exists \quad \lim_{n\to\infty} \frac{|\{(w_1, \ldots, w_k) \in B(n)^k \mid G_{w_1,\ldots,w_k} \textit{ is infinite hyperbolic }\}|}{|B(n)|^k} = 1.$$

- Hence, generically many presentations present an infinite hyperbolic group.
- The proof is a detailed counting, using the notion of small cancelation.

Arzhantseva-Ol'shanskii's proof

- Fix $r \geqslant 2$ and $k \geqslant 1$.
- Consider the free group $F_A = \langle a_1, \ldots, a_r \mid - \rangle$.
- In F_A we have the natural notion of size and balls.
- For $w_1, \ldots, w_k \in F_A$, let $G_{w_1,\ldots,w_k} = \langle a_1, \ldots, a_r \mid w_1, \ldots, w_k \rangle$.

Theorem (Arzhantseva-Ol'shanskii, '96)

$$\exists \quad \lim_{n\to\infty} \frac{|\{(w_1, \ldots, w_k) \in B(n)^k \mid G_{w_1,\ldots,w_k} \text{ is infinite hyperbolic } \}|}{|B(n)|^k} = 1.$$

- Hence, generically many presentations present an infinite hyperbolic group.
- The proof is a detailed counting, using the notion of small cancelation.

Arzhantseva-Ol'shanskii's proof

- Fix $r \geqslant 2$ and $k \geqslant 1$.
- Consider the free group $F_A = \langle a_1, \ldots, a_r \mid - \rangle$.
- In F_A we have the natural notion of size and balls.
- For $w_1, \ldots, w_k \in F_A$, let $G_{w_1,\ldots,w_k} = \langle a_1, \ldots, a_r \mid w_1, \ldots, w_k \rangle$.

Theorem (Arzhantseva-Ol'shanskii, '96)

$$\exists \quad \lim_{n \to \infty} \frac{|\{(w_1, \ldots, w_k) \in B(n)^k \mid G_{w_1,\ldots,w_k} \text{ is infinite hyperbolic }\}|}{|B(n)|^k} = 1.$$

- Hence, generically many presentations present an infinite hyperbolic group.
- The proof is a detailed counting, using the notion of small cancelation.

Arzhantseva-Ol'shanskii's proof

- Fix $r \geqslant 2$ and $k \geqslant 1$.
- Consider the free group $F_A = \langle a_1, \ldots, a_r \mid - \rangle$.
- In F_A we have the natural notion of size and balls.
- For $w_1, \ldots, w_k \in F_A$, let $G_{w_1,\ldots,w_k} = \langle a_1, \ldots, a_r \mid w_1, \ldots, w_k \rangle$.

Theorem (Arzhantseva-Ol'shanskii, '96)

$$\exists \lim_{n\to\infty} \frac{|\{(w_1, \ldots, w_k) \in B(n)^k \mid G_{w_1,\ldots,w_k} \textit{ is infinite hyperbolic } \}|}{|B(n)|^k} = 1.$$

- Hence, generically many presentations present an infinite hyperbolic group.
- The proof is a detailed counting, using the notion of small cancelation.

Arzhantseva-Ol'shanskii's proof

- Fix $r \geqslant 2$ and $k \geqslant 1$.
- Consider the free group $F_A = \langle a_1, \ldots, a_r \mid - \rangle$.
- In F_A we have the natural notion of size and balls.
- For $w_1, \ldots, w_k \in F_A$, let $G_{w_1,\ldots,w_k} = \langle a_1, \ldots, a_r \mid w_1, \ldots, w_k \rangle$.

Theorem (Arzhantseva-Ol'shanskii, '96)

$$\exists \quad \lim_{n\to\infty} \frac{|\{(w_1, \ldots, w_k) \in B(n)^k \mid G_{w_1,\ldots,w_k} \textit{ is infinite hyperbolic } \}|}{|B(n)|^k} = 1.$$

- Hence, generically many presentations present an infinite hyperbolic group.
- The proof is a detailed counting, using the notion of small cancelation.

Arzhantseva-Ol'shanskii's proof

- Fix $r \geqslant 2$ and $k \geqslant 1$.
- Consider the free group $F_A = \langle a_1, \ldots, a_r \mid - \rangle$.
- In F_A we have the natural notion of size and balls.
- For $w_1, \ldots, w_k \in F_A$, let $G_{w_1,\ldots,w_k} = \langle a_1, \ldots, a_r \mid w_1, \ldots, w_k \rangle$.

Theorem (Arzhantseva-Ol'shanskii, '96)

$$\exists \quad \lim_{n\to\infty} \frac{|\{(w_1, \ldots, w_k) \in B(n)^k \mid G_{w_1,\ldots,w_k} \text{ is infinite hyperbolic } \}|}{|B(n)|^k} = 1.$$

- Hence, generically many presentations present an infinite hyperbolic group.
- The proof is a detailed counting, using the notion of small cancelation.

Arzhantseva-Ol'shanskii's proof

- Fix $r \geqslant 2$ and $k \geqslant 1$.
- Consider the free group $F_A = \langle a_1, \ldots, a_r \mid - \rangle$.
- In F_A we have the natural notion of size and balls.
- For $w_1, \ldots, w_k \in F_A$, let $G_{w_1,\ldots,w_k} = \langle a_1, \ldots, a_r \mid w_1, \ldots, w_k \rangle$.

Theorem (Arzhantseva-Ol'shanskii, '96)

$$\exists \quad \lim_{n\to\infty} \frac{|\{(w_1, \ldots, w_k) \in B(n)^k \mid G_{w_1,\ldots,w_k} \text{ is infinite hyperbolic } \}|}{|B(n)|^k} = 1.$$

- Hence, generically many presentations present an infinite hyperbolic group.
- The proof is a detailed counting, using the notion of small cancelation.

Comments

- This fits the algebraic intuition: the longer the relations are, the closest will the group be to a free group.
- Problem-1: this counts r-generated, k-related groups, with r and k fixed.
- Problem-2: this counts presentations, not really groups !
- maybe different k-tuples $(w_1, \ldots, w_k) \neq (w'_1, \ldots, w'_k)$ generate the same subgroup $\langle w_1, \ldots, w_k \rangle = \langle w'_1, \ldots, w'_k \rangle$.
- maybe $\langle w_1, \ldots, w_k \rangle \neq \langle w'_1, \ldots, w'_k \rangle$, but they have the same normal closure $\langle\langle w_1, \ldots, w_k \rangle\rangle = \langle\langle w'_1, \ldots, w'_k \rangle\rangle$. .
- maybe even $\langle\langle w_1, \ldots, w_k \rangle\rangle \neq \langle\langle w'_1, \ldots, w'_k \rangle\rangle$, but $\langle a_1, \ldots, a_r \mid w_1, \ldots, w_k \rangle \simeq \langle a_1, \ldots, a_r \mid w'_1, \ldots, w'_k \rangle$.

Comments

- This fits the algebraic intuition: the longer the relations are, the closest will the group be to a free group.
- Problem-1: this counts r-generated, k-related groups, with r and k fixed.
- Problem-2: this counts presentations, not really groups !
- maybe different k-tuples $(w_1, \ldots, w_k) \neq (w'_1, \ldots, w'_k)$ generate the same subgroup $\langle w_1, \ldots, w_k \rangle = \langle w'_1, \ldots, w'_k \rangle$.
- maybe $\langle w_1, \ldots, w_k \rangle \neq \langle w'_1, \ldots, w'_k \rangle$, but they have the same normal closure $\langle\langle w_1, \ldots, w_k \rangle\rangle = \langle\langle w'_1, \ldots, w'_k \rangle\rangle$. .
- maybe even $\langle\langle w_1, \ldots, w_k \rangle\rangle \neq \langle\langle w'_1, \ldots, w'_k \rangle\rangle$, but $\langle a_1, \ldots, a_r \mid w_1, \ldots, w_k \rangle \simeq \langle a_1, \ldots, a_r \mid w'_1, \ldots, w'_k \rangle$.

Comments

- This fits the algebraic intuition: the longer the relations are, the closest will the group be to a free group.
- Problem-1: this counts r-generated, k-related groups, with r and k fixed.
- Problem-2: this counts presentations, not really groups !
- maybe different k-tuples $(w_1, \ldots, w_k) \neq (w'_1, \ldots, w'_k)$ generate the same subgroup $\langle w_1, \ldots, w_k \rangle = \langle w'_1, \ldots, w'_k \rangle$.
- maybe $\langle w_1, \ldots, w_k \rangle \neq \langle w'_1, \ldots, w'_k \rangle$, but they have the same normal closure $\langle\langle w_1, \ldots, w_k \rangle\rangle = \langle\langle w'_1, \ldots, w'_k \rangle\rangle$. . .
- maybe even $\langle\langle w_1, \ldots, w_k \rangle\rangle \neq \langle\langle w'_1, \ldots, w'_k \rangle\rangle$, but $\langle a_1, \ldots, a_r \mid w_1, \ldots, w_k \rangle \simeq \langle a_1, \ldots, a_r \mid w'_1, \ldots, w'_k \rangle$.

Comments

- This fits the algebraic intuition: the longer the relations are, the closest will the group be to a free group.
- Problem-1: this counts r-generated, k-related groups, with r and k fixed.
- Problem-2: this counts presentations, not really groups !
- maybe different k-tuples $(w_1, \ldots, w_k) \neq (w'_1, \ldots, w'_k)$ generate the same subgroup $\langle w_1, \ldots, w_k \rangle = \langle w'_1, \ldots, w'_k \rangle$.
- maybe $\langle w_1, \ldots, w_k \rangle \neq \langle w'_1, \ldots, w'_k \rangle$, but they have the same normal closure $\langle\langle w_1, \ldots, w_k \rangle\rangle = \langle\langle w'_1, \ldots, w'_k \rangle\rangle$. .
- maybe even $\langle\langle w_1, \ldots, w_k \rangle\rangle \neq \langle\langle w'_1, \ldots, w'_k \rangle\rangle$, but $\langle a_1, \ldots, a_r \mid w_1, \ldots, w_k \rangle \simeq \langle a_1, \ldots, a_r \mid w'_1, \ldots, w'_k \rangle$.

Comments

- This fits the algebraic intuition: the longer the relations are, the closest will the group be to a free group.
- Problem-1: this counts r-generated, k-related groups, with r and k fixed.
- Problem-2: this counts presentations, not really groups !
- maybe different k-tuples $(w_1, \ldots, w_k) \neq (w'_1, \ldots, w'_k)$ generate the same subgroup $\langle w_1, \ldots, w_k \rangle = \langle w'_1, \ldots, w'_k \rangle$.
- maybe $\langle w_1, \ldots, w_k \rangle \neq \langle w'_1, \ldots, w'_k \rangle$, but they have the same normal closure $\langle\langle w_1, \ldots, w_k \rangle\rangle = \langle\langle w'_1, \ldots, w'_k \rangle\rangle$.
- maybe even $\langle\langle w_1, \ldots, w_k \rangle\rangle \neq \langle\langle w'_1, \ldots, w'_k \rangle\rangle$, but $\langle a_1, \ldots, a_r \mid w_1, \ldots, w_k \rangle \simeq \langle a_1, \ldots, a_r \mid w'_1, \ldots, w'_k \rangle$.

Comments

- This fits the algebraic intuition: the longer the relations are, the closest will the group be to a free group.
- Problem-1: this counts r-generated, k-related groups, with r and k fixed.
- Problem-2: this counts presentations, not really groups !
- maybe different k-tuples $(w_1, \ldots, w_k) \neq (w'_1, \ldots, w'_k)$ generate the same subgroup $\langle w_1, \ldots, w_k \rangle = \langle w'_1, \ldots, w'_k \rangle$.
- maybe $\langle w_1, \ldots, w_k \rangle \neq \langle w'_1, \ldots, w'_k \rangle$, but they have the same normal closure $\langle\langle w_1, \ldots, w_k \rangle\rangle = \langle\langle w'_1, \ldots, w'_k \rangle\rangle$. .
- maybe even $\langle\langle w_1, \ldots, w_k \rangle\rangle \neq \langle\langle w'_1, \ldots, w'_k \rangle\rangle$, but $\langle a_1, \ldots, a_r \mid w_1, \ldots, w_k \rangle \simeq \langle a_1, \ldots, a_r \mid w'_1, \ldots, w'_k \rangle$.

Outline

A new point of view

Observation

Let $N = \langle w_1, \ldots, w_k \rangle \leqslant F_A$. Then,

$$\langle a_1, \ldots, a_r \mid w_1, \ldots, w_k \rangle \simeq \langle a_1, \ldots, a_r \mid N \rangle.$$

and let us count f.g. subgroups N of F_A, instead of counting k-tuples of words.

Advantages:

- r still fixed, but not k.
- less redundancy.
- it will be an equally natural way of counting.

... but with very different results... this is a very different direction to infinity.

A new point of view

Observation

Let $N = \langle w_1, \ldots, w_k \rangle \leqslant F_A$. Then,

$$\langle a_1, \ldots, a_r \mid w_1, \ldots, w_k \rangle \simeq \langle a_1, \ldots, a_r \mid N \rangle.$$

and let us count f.g. subgroups N of F_A, instead of counting k-tuples of words.

Advantages:

- r still fixed, but not k.
- less redundancy.
- it will be an equally natural way of counting.

... but with very different results... this is a very different direction to infinity.

A new point of view

Observation

Let $N = \langle w_1, \ldots, w_k \rangle \leqslant F_A$. *Then,*

$$\langle a_1, \ldots, a_r \mid w_1, \ldots, w_k \rangle \simeq \langle a_1, \ldots, a_r \mid N \rangle.$$

and let us count f.g. subgroups N of F_A, instead of counting k-tuples of words.

Advantages:

- r still fixed, but not k.
- less redundancy.
- it will be an equally natural way of counting.

... but with very different results... this is a very different direction to infinity.

A new point of view

Observation

Let $N = \langle w_1, \ldots, w_k \rangle \leqslant F_A$. *Then,*

$$\langle a_1, \ldots, a_r \mid w_1, \ldots, w_k \rangle \simeq \langle a_1, \ldots, a_r \mid N \rangle.$$

and let us count f.g. subgroups N of F_A, instead of counting k-tuples of words.

Advantages:

- r still fixed, but not k.
- less redundancy.
- it will be an equally natural way of counting.

... but with very different results... this is a very different direction to infinity.

A new point of view

Observation

Let $N = \langle w_1, \ldots, w_k \rangle \leqslant F_A$. *Then,*

$$\langle a_1, \ldots, a_r \mid w_1, \ldots, w_k \rangle \simeq \langle a_1, \ldots, a_r \mid N \rangle.$$

and let us count f.g. subgroups N of F_A, instead of counting k-tuples of words.

Advantages:

- r still fixed, but not k.
- less redundancy.
- it will be an equally natural way of counting.

... but with very different results... this is a very different direction to infinity.

A new point of view

Observation

Let $N = \langle w_1, \ldots, w_k \rangle \leqslant F_A$. *Then,*

$$\langle a_1, \ldots, a_r \mid w_1, \ldots, w_k \rangle \simeq \langle a_1, \ldots, a_r \mid N \rangle.$$

and let us count f.g. subgroups N of F_A, instead of counting k-tuples of words.

Advantages:

- r still fixed, but not k.
- less redundancy.
- it will be an equally natural way of counting.

... but with very different results... this is a very different direction to infinity.

A new point of view

Observation

Let $N = \langle w_1, \ldots, w_k \rangle \leqslant F_A$. Then,

$$\langle a_1, \ldots, a_r \mid w_1, \ldots, w_k \rangle \simeq \langle a_1, \ldots, a_r \mid N \rangle.$$

and let us count f.g. subgroups N of F_A, instead of counting k-tuples of words.

Advantages:

- r still fixed, but not k.
- less redundancy.
- it will be an equally natural way of counting.

... but with very different results... this is a very different direction to infinity.

Outline

Stallings automata

Definition

A Stallings automaton *is a finite A-labeled oriented graph with a distinguished vertex,* (X, v)*, such that:*

1- X *is connected,*

2- *no vertex of degree 1 except possibly* v *(*X *is a* core-graph*),*

3- *no two edges with the same label go out of (or in to) the same vertex.*

NO :

YES :

Stallings automata

Definition

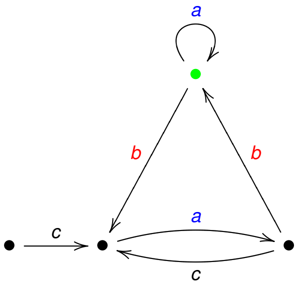
A *Stallings automaton* *is a finite A-labeled oriented graph with a distinguished vertex, (X, v), such that:*

1- *X is connected,*

2- *no vertex of degree 1 except possibly v (X is a core-graph),*

3- *no two edges with the same label go out of (or in to) the same vertex.*

NO :



YES :

Stallings automata

Definition

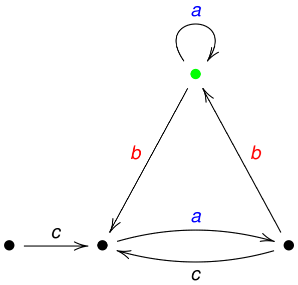
A Stallings automaton is a finite A-labeled oriented graph with a distinguished vertex, (X, v), such that:

1- *X is connected,*

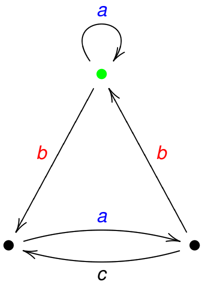
2- *no vertex of degree 1 except possibly v (X is a core-graph),*

3- *no two edges with the same label go out of (or in to) the same vertex.*

NO :



YES :



Stallings automata

In the influent paper

J. R. Stallings, Topology of finite graphs, Inventiones Math. 71 (1983), 551-565,

Stallings (building on previous works) gave a bijection between finitely generated subgroups of F_A and Stallings automata:

$$\{\text{f.g. subgroups of } F_A\} \quad \longleftrightarrow \quad \{\text{Stallings automata over } A\},$$

which is crucial for the modern understanding of the lattice of subgroups of F_A.

Stallings automata

In the influent paper

J. R. Stallings, Topology of finite graphs, Inventiones Math. 71 (1983), 551-565,

Stallings (building on previous works) gave a bijection between finitely generated subgroups of F_A and Stallings automata:

$$\{\text{f.g. subgroups of } F_A\} \quad \longleftrightarrow \quad \{\text{Stallings automata over } A\},$$

which is crucial for the modern understanding of the lattice of subgroups of F_A.

Stallings automata

In the influent paper

J. R. Stallings, Topology of finite graphs, Inventiones Math. 71 (1983), 551-565,

Stallings (building on previous works) gave a bijection between finitely generated subgroups of F_A and Stallings automata:

$$\{\text{f.g. subgroups of } F_A\} \quad \longleftrightarrow \quad \{\text{Stallings automata over } A\},$$

which is crucial for the modern understanding of the lattice of subgroups of F_A.

Definition

To any given (Stallings) automaton (X, v), we associate its fundamental group:

$$\pi(X, v) = \{ \text{labels of closed paths at } v\} \leqslant F_A,$$

clearly, a subgroup of F_A.

$$\pi(X, \bullet) = \{1, a, a^{-1}, bab, bc^{-1}b, babab^{-1}cb^{-1}, \ldots\}$$

$$\pi(X, \bullet) \not\ni bc^{-1}bcaa$$

Membership problem in $\pi(X, \bullet)$ is solvable.

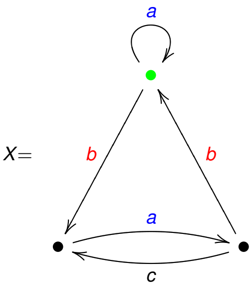
Reading the subgroup from the automata

Definition

To any given (Stallings) automaton (X, v), we associate its fundamental group:

$$\pi(X, v) = \{ \text{ labels of closed paths at } v \} \leqslant F_A,$$

clearly, a subgroup of F_A.



$$\pi(X, \bullet) = \{1, a, a^{-1}, bab, bc^{-1}b, babab^{-1}cb^{-1}, \ldots\}$$

$$\pi(X, \bullet) \not\ni bc^{-1}bcaa$$

Membership problem in $\pi(X, \bullet)$ is solvable.

A basis for $\pi(X, v)$

Proposition

For every Stallings automaton (X, v), the group $\pi(X, v)$ is free of rank $rk(\pi(X, v)) = 1 - |VX| + |EX|$.

Proof:

- Take a maximal tree T in X.
- Write $T[p, q]$ for the geodesic (i.e. the unique reduced path) in T from p to q.
- For every $e \in EX - ET$, $x_e = label(T[v, \iota e] \cdot e \cdot T[\tau e, v])$ belongs to $\pi(X, v)$.
- Not difficult to see that $\{x_e \mid e \in EX - ET\}$ is a basis for $\pi(X, v)$.
- And, $$\begin{aligned} |EX - ET| &= |EX| - |ET| \\ &= |EX| - (|VT| - 1) = 1 - |VX| + |EX|. \square \end{aligned}$$

A basis for $\pi(X, v)$

Proposition

For every Stallings automaton (X, v), the group $\pi(X, v)$ is free of rank $rk(\pi(X, v)) = 1 - |VX| + |EX|$.

Proof:

- Take a maximal tree T in X.
- Write $T[p, q]$ for the geodesic (i.e. the unique reduced path) in T from p to q.
- For every $e \in EX - ET$, $x_e = label(T[v, \iota e] \cdot e \cdot T[\tau e, v])$ belongs to $\pi(X, v)$.
- Not difficult to see that $\{x_e \mid e \in EX - ET\}$ is a basis for $\pi(X, v)$.
- And, $$\begin{aligned} |EX - ET| &= |EX| - |ET| \\ &= |EX| - (|VT| - 1) = 1 - |VX| + |EX|. \ \square \end{aligned}$$

A basis for $\pi(X, v)$

Proposition

For every Stallings automaton (X, v), the group $\pi(X, v)$ is free of rank $rk(\pi(X, v)) = 1 - |VX| + |EX|$.

Proof:

- Take a maximal tree T in X.
- Write $T[p, q]$ for the geodesic (i.e. the unique reduced path) in T from p to q.
- For every $e \in EX - ET$, $x_e = label(T[v, \iota e] \cdot e \cdot T[\tau e, v])$ belongs to $\pi(X, v)$.
- Not difficult to see that $\{x_e \mid e \in EX - ET\}$ is a basis for $\pi(X, v)$.
- And, $$\begin{aligned} |EX - ET| &= |EX| - |ET| \\ &= |EX| - (|VT| - 1) = 1 - |VX| + |EX|. \square \end{aligned}$$

A basis for $\pi(X, v)$

Proposition

For every Stallings automaton (X, v), the group $\pi(X, v)$ is free of rank $rk(\pi(X, v)) = 1 - |VX| + |EX|$.

Proof:

- Take a maximal tree T in X.
- Write $T[p, q]$ for the geodesic (i.e. the unique reduced path) in T from p to q.
- For every $e \in EX - ET$, $x_e = label(T[v, \iota e] \cdot e \cdot T[\tau e, v])$ belongs to $\pi(X, v)$.
- Not difficult to see that $\{x_e \mid e \in EX - ET\}$ is a basis for $\pi(X, v)$.
- And, $$\begin{aligned} |EX - ET| &= |EX| - |ET| \\ &= |EX| - (|VT| - 1) = 1 - |VX| + |EX|. \;\square \end{aligned}$$

A basis for $\pi(X, v)$

Proposition

For every Stallings automaton (X, v), the group $\pi(X, v)$ is free of rank $rk(\pi(X, v)) = 1 - |VX| + |EX|$.

Proof:

- Take a maximal tree T in X.
- Write $T[p, q]$ for the geodesic (i.e. the unique reduced path) in T from p to q.
- For every $e \in EX - ET$, $x_e = label(T[v, \iota e] \cdot e \cdot T[\tau e, v])$ belongs to $\pi(X, v)$.
- Not difficult to see that $\{x_e \mid e \in EX - ET\}$ is a basis for $\pi(X, v)$.
- And, $$\begin{aligned} |EX - ET| &= |EX| - |ET| \\ &= |EX| - (|VT| - 1) = 1 - |VX| + |EX|. \ \square \end{aligned}$$

A basis for $\pi(X, v)$

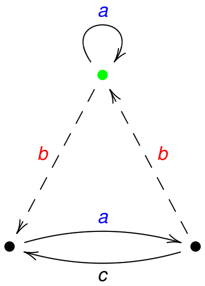
Proposition

For every Stallings automaton (X, v), *the group* $\pi(X, v)$ *is free of rank* $rk(\pi(X, v)) = 1 - |VX| + |EX|$.

Proof:

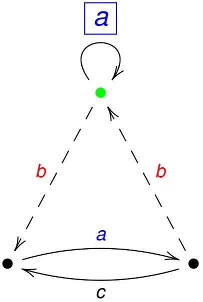
- Take a maximal tree T in X.
- Write $T[p, q]$ for the geodesic (i.e. the unique reduced path) in T from p to q.
- For every $e \in EX - ET$, $x_e = label(T[v, \iota e] \cdot e \cdot T[\tau e, v])$ belongs to $\pi(X, v)$.
- Not difficult to see that $\{x_e \mid e \in EX - ET\}$ is a basis for $\pi(X, v)$.
- And, $$\begin{aligned} |EX - ET| &= |EX| - |ET| \\ &= |EX| - (|VT| - 1) = 1 - |VX| + |EX|. \ \square \end{aligned}$$

Example



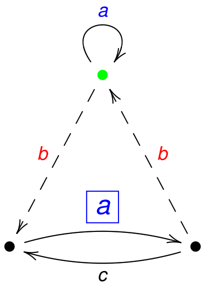
$H = \langle \quad \rangle$

Example



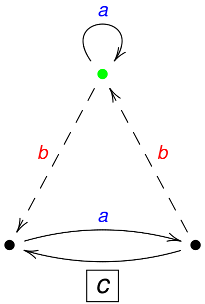
$H = \langle a, \quad \rangle$

Example



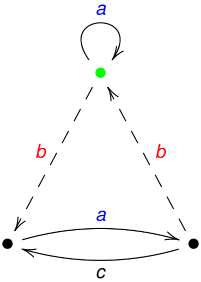
$H = \langle a,\ bab,\quad \rangle$

Example



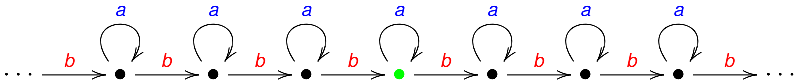
$H = \langle a,\ bab,\ b^{-1}cb^{-1} \rangle$

Example



$H = \langle a,\ bab,\ b^{-1}cb^{-1} \rangle$
$rk(H) = 1 - 3 + 5 = 3.$

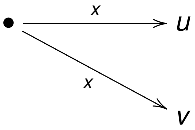
Example-2



$$F_{\aleph_0} \simeq H = \langle \ldots, b^{-2}ab^2, b^{-1}ab, a, bab^{-1}, b^2ab^{-2}, \ldots \rangle \leqslant F_2.$$

Constructing the automata from the subgroup

In any automaton containing the following situation, for $x \in A^{\pm 1}$,

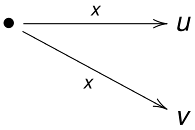


we can fold and identify vertices u and v to obtain

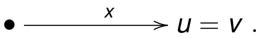
This operation, $(X, v) \rightsquigarrow (X', v)$, is called a Stallings folding.

Constructing the automata from the subgroup

In any automaton containing the following situation, for $x \in A^{\pm 1}$,

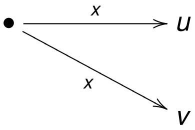


we can fold and identify vertices u and v to obtain

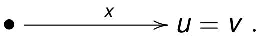


This operation, $(X, v) \rightsquigarrow (X', v)$, is called a Stallings folding.

In any automaton containing the following situation, for $x \in A^{\pm 1}$,



we can fold and identify vertices u and v to obtain



This operation, $(X, v) \rightsquigarrow (X', v)$, is called a Stallings folding.

Lemma (Stallings)

If $(X, v) \rightsquigarrow (X', v')$ is a Stallings folding then $\pi(X, v) = \pi(X', v')$.

Given a f.g. subgroup $H = \langle w_1, \ldots w_m \rangle \leqslant F_A$ (we assume w_i are reduced words), do the following:

1- *Draw the flower automaton,*

2- *Perform successive foldings until obtaining a Stallings automaton, denoted $\Gamma(H)$.*

Constructing the automata from the subgroup

Lemma (Stallings)

If $(X, v) \rightsquigarrow (X', v')$ is a Stallings folding then $\pi(X, v) = \pi(X', v')$.

Given a f.g. subgroup $H = \langle w_1, \ldots w_m \rangle \leqslant F_A$ (we assume w_i are reduced words), do the following:

1- *Draw the flower automaton,*

2- *Perform successive foldings until obtaining a Stallings automaton, denoted $\Gamma(H)$.*

Constructing the automata from the subgroup

Lemma (Stallings)

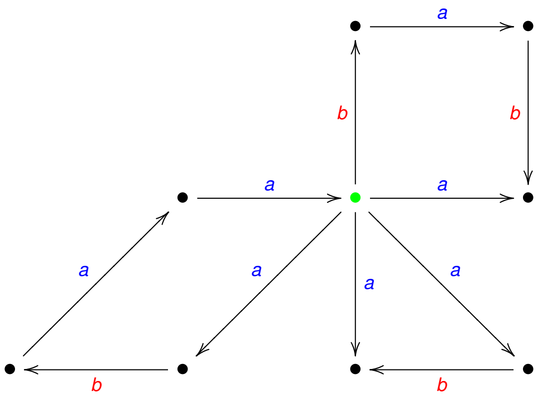
If $(X, v) \rightsquigarrow (X', v')$ is a Stallings folding then $\pi(X, v) = \pi(X', v')$.

Given a f.g. subgroup $H = \langle w_1, \ldots w_m \rangle \leqslant F_A$ (we assume w_i are reduced words), do the following:

1- *Draw the flower automaton,*

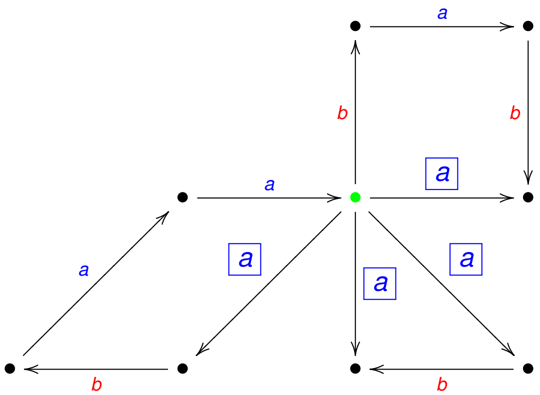
2- *Perform successive foldings until obtaining a Stallings automaton, denoted $\Gamma(H)$.*

Example: $H = \langle baba^{-1}, aba^{-1}, aba^2 \rangle$



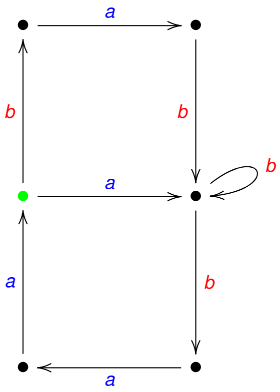
Flower(H)

Example: $H = \langle baba^{-1}, aba^{-1}, aba^2 \rangle$



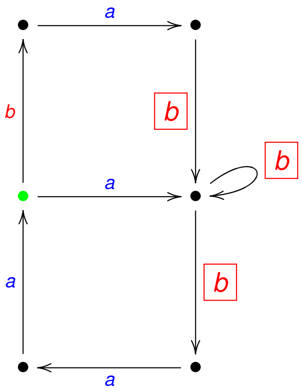
Flower(H)

Example: $H = \langle baba^{-1}, aba^{-1}, aba^2 \rangle$



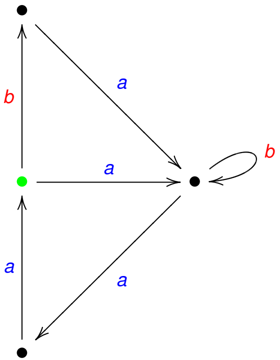
Folding #1

Example: $H = \langle baba^{-1}, aba^{-1}, aba^2 \rangle$



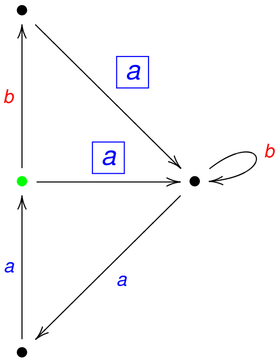
Folding $\#1$.

Example: $H = \langle baba^{-1}, aba^{-1}, aba^2 \rangle$



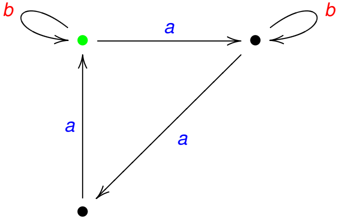
Folding #2.

Example: $H = \langle baba^{-1}, aba^{-1}, aba^2 \rangle$



Folding #2.

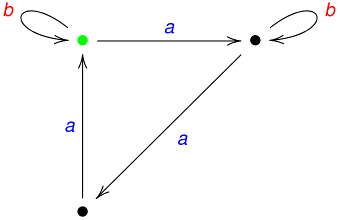
Example: $H = \langle baba^{-1}, aba^{-1}, aba^2 \rangle$



Folding #3. $\Gamma(H)$

By Stallings Lemma, $\pi(\Gamma(H), \bullet) = \langle baba^{-1}, aba^{-1}, aba^2 \rangle$

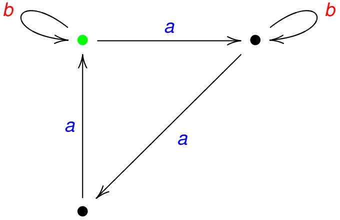
Example: $H = \langle baba^{-1}, aba^{-1}, aba^2 \rangle$



Folding $\#3$. $\Gamma(H)$

By Stallings Lemma, $\pi(\Gamma(H), \bullet) = \langle baba^{-1}, aba^{-1}, aba^2 \rangle$

Example: $H = \langle baba^{-1}, aba^{-1}, aba^2 \rangle$



Folding $\#3$. $\Gamma(H)$

By Stallings Lemma, $\pi(\Gamma(H), \bullet) = \langle baba^{-1}, aba^{-1}, aba^2 \rangle$
$= \langle b, aba^{-1}, a^3 \rangle$

Local confluence

It can be shown that

Proposition

The automaton $\Gamma(H)$ does not depend on the sequence of foldings.

Proposition

The automaton $\Gamma(H)$ does not depend on the generators of H.

Theorem

The following is a bijection:

$$\begin{array}{ccc} \{f.g.\ subgroups\ of\ F_A\} & \longleftrightarrow & \{Stallings\ automata\} \\ H & \to & \Gamma(H) \\ \pi(X,v) & \leftarrow & (X,v) \end{array}$$

Local confluence

It can be shown that

Proposition

The automaton $\Gamma(H)$ does not depend on the sequence of foldings.

Proposition

The automaton $\Gamma(H)$ does not depend on the generators of H.

Theorem

The following is a bijection:

$$\begin{array}{rcl} \{\text{f.g. subgroups of } F_A\} & \longleftrightarrow & \{\text{Stallings automata}\} \\ H & \to & \Gamma(H) \\ \pi(X, v) & \leftarrow & (X, v) \end{array}$$

Local confluence

It can be shown that

Proposition

The automaton $\Gamma(H)$ does not depend on the sequence of foldings.

Proposition

The automaton $\Gamma(H)$ does not depend on the generators of H.

Theorem

The following is a bijection:

$$\begin{array}{rcl} \{\text{f.g. subgroups of } F_A\} & \longleftrightarrow & \{\text{Stallings automata}\} \\ H & \to & \Gamma(H) \\ \pi(X, v) & \leftarrow & (X, v) \end{array}$$

Corollary (Nielsen-Schreier)

Every subgroup of F_A is free.

- Finite automata work for the finitely generated case, but everything extends easily to the general case (using infinite graphs).
- The original proof (1920's) is combinatorial and much more technical.

Nielsen-Schreier Theorem

Corollary (Nielsen-Schreier)

Every subgroup of F_A is free.

- Finite automata work for the finitely generated case, but everything extends easily to the general case (using infinite graphs).
- The original proof (1920's) is combinatorial and much more technical.

Nielsen-Schreier Theorem

Corollary (Nielsen-Schreier)

Every subgroup of F_A is free.

- Finite automata work for the finitely generated case, but everything extends easily to the general case (using infinite graphs).
- The original proof (1920's) is combinatorial and much more technical.

Outline

Stallings' graphs as partial injections

Definition

Let Γ be a Stallings graph. Every letter in A determines a partial injection of the set of vertices $V\Gamma$: $a(i) = j$ *iff* $i \xrightarrow{a} j$.

$\Gamma=$

$a: V$	$\to$	V	$b: V$	$\to$	V	$c: V$	$\to$	V
1	$\mapsto$	1	1	$\mapsto$	2	1		
2	$\mapsto$	3	2			2		
3			3	$\mapsto$	1	3	$\mapsto$	2

Observation

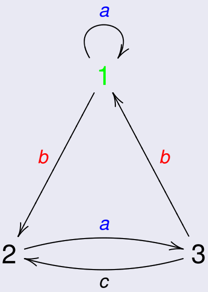
And the r partial injections $a_1, \ldots, a_r$ determine back the graph Γ.

Stallings' graphs as partial injections

Definition

Let Γ be a Stallings graph. Every letter in A determines a partial injection of the set of vertices $V\Gamma$: $a(i) = j$ *iff* $i \xrightarrow{a} j$.

$\Gamma =$



$a: V$	$\to$	V
1	$\mapsto$	1
2	$\mapsto$	3
3		

$b: V$	$\to$	V
1	$\mapsto$	2
2		
3	$\mapsto$	1

$c: V$	$\to$	V
1		
2		
3	$\mapsto$	2

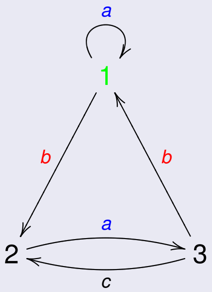
Observation

And the r partial injections $a_1, \ldots, a_r$ determine back the graph Γ.

Definition

Let Γ be a Stallings graph. Every letter in A determines a partial injection of the set of vertices $V\Gamma$: $a(i) = j$ iff $i \xrightarrow{a} j$.

$\Gamma =$



a:	V	$\to$	V		b:	V	$\to$	V		c:	V	$\to$	V
	1	$\mapsto$	1			1	$\mapsto$	2			1		
	2	$\mapsto$	3			2					2		
	3					3	$\mapsto$	1			3	$\mapsto$	2

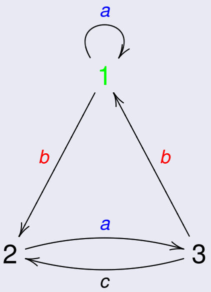
Observation

And the r partial injections $a_1, \ldots, a_r$ determine back the graph Γ.

Stallings' graphs as partial injections

Definition

Let Γ be a Stallings graph. Every letter in A determines a partial injection of the set of vertices $V\Gamma$: $a(i) = j$ iff $i \xrightarrow{a} j$.

$\Gamma =$ 

a:	V	$\to$	V	b:	V	$\to$	V	c:	V	$\to$	V
	1	$\mapsto$	1		1	$\mapsto$	2		1		
	2	$\mapsto$	3		2				2		
	3				3	$\mapsto$	1		3	$\mapsto$	2

Observation

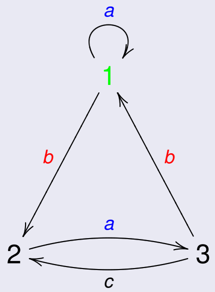
And the r partial injections $a_1, \ldots, a_r$ determine back the graph Γ.

Stallings' graphs as partial injections

Definition

Let Γ be a Stallings graph. Every letter in A determines a partial injection *of the set of vertices $V\Gamma$: $a(i) = j$ iff $i \xrightarrow{a} j$.*

$\Gamma =$



$a\colon V$	$\to$	V	$b\colon V$	$\to$	V	$c\colon V$	$\to$	V
1	$\mapsto$	1	1	$\mapsto$	2	1		
2	$\mapsto$	3	2			2		
3			3	$\mapsto$	1	3	$\mapsto$	2

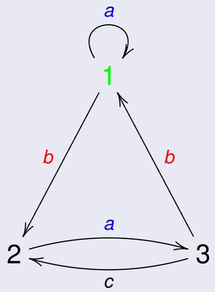
Observation

And the r partial injections $a_1, \ldots, a_r$ determine back the graph Γ.

Stallings' graphs as partial injections

Definition

Let Γ be a Stallings graph. Every letter in A determines a partial injection of the set of vertices $V\Gamma$: $a(i) = j$ iff $i \xrightarrow{a} j$.

$\Gamma=$ 

$a\colon V$	$\to$	V	$b\colon V$	$\to$	V	$c\colon V$	$\to$	V
1	$\mapsto$	1	1	$\mapsto$	2	1		
2	$\mapsto$	3	2			2		
3			3	$\mapsto$	1	3	$\mapsto$	2

Observation

And the r partial injections $a_1, \ldots, a_r$ determine back the graph Γ.

Stallings' graphs as partial injections

Definition

Let I_n be the set of partial injections of $[n] = \{1, 2, \ldots, n\}$.

A Stallings graph (over A) with n vertices can be thought as a r-tuple of partial injections, plus a base-point, $\sigma \in I_n^r \times [n]$, such that

- *the corresponding graph $\Gamma(\sigma)$ is connected,*
- *and without degree 1 vertices, except possibly the base-point.*

Observation

There are at most $|I_n|^r \cdot n$ Stallings graphs with n vertices (over A).

Stallings' graphs as partial injections

Definition

Let I_n be the set of partial injections of $[n] = \{1, 2, \ldots, n\}$.

A Stallings graph (over A) with n vertices can be thought as a r-tuple of partial injections, plus a base-point, $\sigma \in I_n^r \times [n]$, such that

- *the corresponding graph $\Gamma(\sigma)$ is connected,*
- *and without degree 1 vertices, except possibly the base-point.*

Observation

There are at most $|I_n|^r \cdot n$ Stallings graphs with n vertices (over A).

Stallings' graphs as partial injections

Definition

Let I_n be the set of partial injections of $[n] = \{1, 2, \ldots, n\}$.

A Stallings graph (over A) with n vertices can be thought as a r-tuple of partial injections, plus a base-point, $\sigma \in I_n^r \times [n]$, such that

- *the corresponding graph $\Gamma(\sigma)$ is connected,*
- *and without degree 1 vertices, except possibly the base-point.*

Observation

There are at most $|I_n|^r \cdot n$ Stallings graphs with n vertices (over A).

Stallings' graphs as partial injections

Definition

Let I_n be the set of partial injections of $[n] = \{1, 2, \ldots, n\}$.

A Stallings graph (over A) with n vertices can be thought as a r-tuple of partial injections, plus a base-point, $\sigma \in I_n^r \times [n]$, such that

- *the corresponding graph $\Gamma(\sigma)$ is connected,*
- *and without degree 1 vertices, except possibly the base-point.*

Observation

There are at most $|I_n|^r \cdot n$ Stallings graphs with n vertices (over A).

Stallings' graphs as partial injections

Definition

Let I_n be the set of partial injections of $[n] = \{1, 2, \ldots, n\}$.

A Stallings graph (over A) with n vertices can be thought as a r-tuple of partial injections, plus a base-point, $\sigma \in I_n^r \times [n]$, such that

- *the corresponding graph $\Gamma(\sigma)$ is connected,*
- *and without degree 1 vertices, except possibly the base-point.*

Observation

There are at most $|I_n|^r \cdot n$ Stallings graphs with n vertices (over A).

Stallings' graphs as partial injections

Theorem (Bassino, Nicaud, Weil, 2008)

a) $\frac{|\{\sigma \in {I_n}^r \times [n] \quad | \quad \Gamma(\sigma) \text{ not connected } \}|}{|I_n|^r \cdot n} = \mathcal{O}(\frac{1}{n^{r-1}})$.

b) $\frac{|\{\sigma \in {I_n}^r \times [n] \quad | \quad \Gamma(\sigma) \text{ has a deg. 1 vertex} \neq \text{bspt.}\}|}{|I_n|^r \cdot n} = o(1)$.

Corollary

Generically, a Stallings graph (over A) with n vertices is just a r-tuple of partial injections, plus a base-point, ${I_n}^r \times [n]$.

Hence, counting Stallings graphs reduces to count partial injections: a purely combinatorial matter.

Stallings' graphs as partial injections

Theorem (Bassino, Nicaud, Weil, 2008)

a) $\frac{|\{\sigma \in {I_n}^r \times [n] \quad | \quad \Gamma(\sigma) \text{ not connected } \}|}{|I_n|^r \cdot n} = \mathcal{O}(\frac{1}{n^{r-1}})$.

b) $\frac{|\{\sigma \in {I_n}^r \times [n] \quad | \quad \Gamma(\sigma) \text{ has a deg. 1 vertex} \neq \text{bspt.}\}|}{|I_n|^r \cdot n} = o(1)$.

Corollary

Generically, a Stallings graph (over A) with n vertices is just a r-tuple of partial injections, plus a base-point, ${I_n}^r \times [n]$.

Hence, counting Stallings graphs reduces to count partial injections: a purely combinatorial matter.

Stallings' graphs as partial injections

Theorem (Bassino, Nicaud, Weil, 2008)

a) $\frac{|\{\sigma \in {I_n}^r \times [n] \quad | \quad \Gamma(\sigma) \text{ not connected } \}|}{|I_n|^r \cdot n} = \mathcal{O}(\frac{1}{n^{r-1}})$.

b) $\frac{|\{\sigma \in {I_n}^r \times [n] \quad | \quad \Gamma(\sigma) \text{ has a deg. 1 vertex} \neq \text{bspt.}\}|}{|I_n|^r \cdot n} = o(1)$.

Corollary

Generically, a Stallings graph (over A) with n vertices is just a r-tuple of partial injections, plus a base-point, ${I_n}^r \times [n]$.

Hence, counting Stallings graphs reduces to count partial injections: a purely combinatorial matter.

Stallings' graphs as partial injections

Theorem (Bassino, Nicaud, Weil, 2008)

a) $\frac{|\{\sigma \in {I_n}^r \times [n] \quad | \quad \Gamma(\sigma) \text{ not connected } \}|}{|I_n|^r \cdot n} = \mathcal{O}(\frac{1}{n^{r-1}})$.

b) $\frac{|\{\sigma \in {I_n}^r \times [n] \quad | \quad \Gamma(\sigma) \text{ has a deg. 1 vertex} \neq \text{bspt.}\}|}{|I_n|^r \cdot n} = o(1)$.

Corollary

Generically, a Stallings graph (over A) with n vertices is just a r-tuple of partial injections, plus a base-point, ${I_n}^r \times [n]$.

Hence, counting Stallings graphs reduces to count partial injections: a purely combinatorial matter.

Counting partial injections

Observation

Any partial injection $\sigma \in I_n$ decomposes in orbits of two types: closed and open (i.e. cycles and segments).

Definition

A partial injection $\sigma \in I_n$ is called a

- *permutation if all its orbits are closed,*
- *fragmented permutation if all its orbits are open.*

Let S_n and J_n, resp., be the sets of permutations and fragmented permutations in I_n.

Observation

Every partial injection is the disjoint union of a permutation and a fragmented permutation. In particular, $|I_n| = \sum_{k=0}^{n} \binom{n}{k} |S_k||J_{n-k}| = \sum_{k=0}^{n} \frac{n!}{(n-k)!} |J_{n-k}|$.

Counting partial injections

Observation

Any partial injection $\sigma \in I_n$ decomposes in orbits of two types: closed and open (i.e. cycles and segments).

Definition

A partial injection $\sigma \in I_n$ is called a

- *permutation if all its orbits are closed,*
- *fragmented permutation if all its orbits are open.*

Let S_n and J_n, resp., be the sets of permutations and fragmented permutations in I_n.

Observation

Every partial injection is the disjoint union of a permutation and a fragmented permutation. In particular, $|I_n| = \sum_{k=0}^{n} \binom{n}{k} |S_k||J_{n-k}| = \sum_{k=0}^{n} \frac{n!}{(n-k)!} |J_{n-k}|$.

Counting partial injections

Observation

Any partial injection $\sigma \in I_n$ decomposes in orbits of two types: closed and open (i.e. cycles and segments).

Definition

A partial injection $\sigma \in I_n$ is called a

- *permutation if all its orbits are closed,*
- *fragmented permutation if all its orbits are open.*

Let S_n and J_n, resp., be the sets of permutations and fragmented permutations in I_n.

Observation

Every partial injection is the disjoint union of a permutation and a fragmented permutation. In particular, $|I_n| = \sum_{k=0}^{n} \binom{n}{k} |S_k||J_{n-k}| = \sum_{k=0}^{n} \frac{n!}{(n-k)!} |J_{n-k}|$.

Counting partial injections

Observation

Any partial injection $\sigma \in I_n$ decomposes in orbits of two types: closed and open (i.e. cycles and segments).

Definition

A partial injection $\sigma \in I_n$ is called a

- *permutation if all its orbits are closed,*
- *fragmented permutation if all its orbits are open.*

Let S_n and J_n, resp., be the sets of permutations and fragmented permutations in I_n.

Observation

Every partial injection is the disjoint union of a permutation and a fragmented permutation. In particular, $|I_n| = \sum_{k=0}^{n} \binom{n}{k} |S_k||J_{n-k}| = \sum_{k=0}^{n} \frac{n!}{(n-k)!} |J_{n-k}|$.

Counting partial injections

Observation

Any partial injection $\sigma \in I_n$ decomposes in orbits of two types: closed and open (i.e. cycles and segments).

Definition

A partial injection $\sigma \in I_n$ is called a

- *permutation if all its orbits are closed,*
- *fragmented permutation if all its orbits are open.*

Let S_n and J_n, resp., be the sets of permutations and fragmented permutations in I_n.

Observation

Every partial injection is the disjoint union of a permutation and a fragmented permutation. In particular, $|I_n| = \sum_{k=0}^{n} \binom{n}{k} |S_k||J_{n-k}| = \sum_{k=0}^{n} \frac{n!}{(n-k)!} |J_{n-k}|$.

Counting partial injections

Definition

a) The EGS for partial injections: $I(z) = \sum_{n=0}^{\infty} \frac{|I_n|}{n!} z^n$.

b) The EGS for permutations: $S(z) = \sum_{n=0}^{\infty} \frac{|S_n|}{n!} z^n = \sum_{n=0}^{\infty} z^n = \frac{1}{1-z}$.

c) The EGS for fragmented permutations: $J(z) = \sum_{n=0}^{\infty} \frac{|J_n|}{n!} z^n$.

Theorem

a) $I(z) = \frac{1}{1-z} e^{\frac{z}{1-z}} = 1 + 2z + \frac{7}{2} z^2 + \frac{17}{3} z^3 + \cdots$.

b) $\frac{|I_n|}{n!} = \frac{e^{2\sqrt{n}}}{2\sqrt{\pi e}} n^{-\frac{1}{4}} (1 + o(1))$.

Theorem

a) $J(z) = e^{\frac{z}{1-z}} = 1 + z + \frac{3}{2} z^2 + \frac{13}{6} z^3 + \cdots$.

b) $\frac{|J_n|}{n!} = \frac{e^{2\sqrt{n}}}{2\sqrt{\pi e}} n^{-\frac{3}{4}} (1 + o(1))$.

Hence, $\frac{|J_n|}{|I_n|} = \mathcal{O}(\frac{1}{n^{1/2}})$.

Counting partial injections

Definition

a) The EGS for partial injections: $I(z) = \sum_{n=0}^{\infty} \frac{|I_n|}{n!} z^n$.
b) The EGS for permutations: $S(z) = \sum_{n=0}^{\infty} \frac{|S_n|}{n!} z^n = \sum_{n=0}^{\infty} z^n = \frac{1}{1-z}$.
c) The EGS for fragmented permutations: $J(z) = \sum_{n=0}^{\infty} \frac{|J_n|}{n!} z^n$.

Theorem

a) $I(z) = \frac{1}{1-z} e^{\frac{z}{1-z}} = 1 + 2z + \frac{7}{2}z^2 + \frac{17}{3}z^3 + \cdots$.
b) $\frac{|I_n|}{n!} = \frac{e^{2\sqrt{n}}}{2\sqrt{\pi e}} n^{-\frac{1}{4}} (1 + o(1))$.

Theorem

a) $J(z) = e^{\frac{z}{1-z}} = 1 + z + \frac{3}{2}z^2 + \frac{13}{6}z^3 + \cdots$.
b) $\frac{|J_n|}{n!} = \frac{e^{2\sqrt{n}}}{2\sqrt{\pi e}} n^{-\frac{3}{4}} (1 + o(1))$.

Hence, $\frac{|J_n|}{|I_n|} = \mathcal{O}(\frac{1}{n^{1/2}})$.

Counting partial injections

Definition

a) The EGS for partial injections: $I(z) = \sum_{n=0}^{\infty} \frac{|I_n|}{n!} z^n$.
b) The EGS for permutations: $S(z) = \sum_{n=0}^{\infty} \frac{|S_n|}{n!} z^n = \sum_{n=0}^{\infty} z^n = \frac{1}{1-z}$.
c) The EGS for fragmented permutations: $J(z) = \sum_{n=0}^{\infty} \frac{|J_n|}{n!} z^n$.

Theorem

a) $I(z) = \frac{1}{1-z} e^{\frac{z}{1-z}} = 1 + 2z + \frac{7}{2}z^2 + \frac{17}{3}z^3 + \cdots$.
b) $\frac{|I_n|}{n!} = \frac{e^{2\sqrt{n}}}{2\sqrt{\pi e}} n^{-\frac{1}{4}}(1 + o(1))$.

Theorem

a) $J(z) = e^{\frac{z}{1-z}} = 1 + z + \frac{3}{2}z^2 + \frac{13}{6}z^3 + \cdots$.
b) $\frac{|J_n|}{n!} = \frac{e^{2\sqrt{n}}}{2\sqrt{\pi e}} n^{-\frac{3}{4}}(1 + o(1))$.

Hence, $\frac{|J_n|}{|I_n|} = \mathcal{O}(\frac{1}{n^{1/2}})$.

Counting partial injections

Definition

a) The EGS for partial injections: $I(z) = \sum_{n=0}^{\infty} \frac{|I_n|}{n!} z^n$.

b) The EGS for permutations: $S(z) = \sum_{n=0}^{\infty} \frac{|S_n|}{n!} z^n = \sum_{n=0}^{\infty} z^n = \frac{1}{1-z}$.

c) The EGS for fragmented permutations: $J(z) = \sum_{n=0}^{\infty} \frac{|J_n|}{n!} z^n$.

Theorem

a) $I(z) = \frac{1}{1-z} e^{\frac{z}{1-z}} = 1 + 2z + \frac{7}{2} z^2 + \frac{17}{3} z^3 + \cdots$.

b) $\frac{|I_n|}{n!} = \frac{e^{2\sqrt{n}}}{2\sqrt{\pi e}} n^{-\frac{1}{4}} (1 + o(1))$.

Theorem

a) $J(z) = e^{\frac{z}{1-z}} = 1 + z + \frac{3}{2} z^2 + \frac{13}{6} z^3 + \cdots$.

b) $\frac{|J_n|}{n!} = \frac{e^{2\sqrt{n}}}{2\sqrt{\pi e}} n^{-\frac{3}{4}} (1 + o(1))$.

Hence, $\frac{|J_n|}{|I_n|} = \mathcal{O}(\frac{1}{n^{1/2}})$.

Counting partial injections

Definition

a) The EGS for partial injections: $I(z)=\sum_{n=0}^{\infty}\frac{|I_n|}{n!}z^n$.
b) The EGS for permutations: $S(z)=\sum_{n=0}^{\infty}\frac{|S_n|}{n!}z^n=\sum_{n=0}^{\infty}z^n=\frac{1}{1-z}$.
c) The EGS for fragmented permutations: $J(z)=\sum_{n=0}^{\infty}\frac{|J_n|}{n!}z^n$.

Theorem

a) $I(z)=\frac{1}{1-z}e^{\frac{z}{1-z}}=1+2z+\frac{7}{2}z^2+\frac{17}{3}z^3+\cdots$.
b) $\frac{|I_n|}{n!}=\frac{e^{2\sqrt{n}}}{2\sqrt{\pi e}}n^{-\frac{1}{4}}(1+o(1))$.

Theorem

a) $J(z)=e^{\frac{z}{1-z}}=1+z+\frac{3}{2}z^2+\frac{13}{6}z^3+\cdots$.
b) $\frac{|J_n|}{n!}=\frac{e^{2\sqrt{n}}}{2\sqrt{\pi e}}n^{-\frac{3}{4}}(1+o(1))$.

Hence, $\frac{|J_n|}{|I_n|}=\mathcal{O}(\frac{1}{n^{1/2}})$.

Counting partial injections

Definition

a) The *EGS for partial injections*: $I(z) = \sum_{n=0}^{\infty} \frac{|I_n|}{n!} z^n$.
b) The *EGS for permutations*: $S(z) = \sum_{n=0}^{\infty} \frac{|S_n|}{n!} z^n = \sum_{n=0}^{\infty} z^n = \frac{1}{1-z}$.
c) The *EGS for fragmented permutations*: $J(z) = \sum_{n=0}^{\infty} \frac{|J_n|}{n!} z^n$.

Theorem

a) $I(z) = \frac{1}{1-z} e^{\frac{z}{1-z}} = 1 + 2z + \frac{7}{2} z^2 + \frac{17}{3} z^3 + \cdots$.
b) $\frac{|I_n|}{n!} = \frac{e^{2\sqrt{n}}}{2\sqrt{\pi e}} n^{-\frac{1}{4}} (1 + o(1))$.

Theorem

a) $J(z) = e^{\frac{z}{1-z}} = 1 + z + \frac{3}{2} z^2 + \frac{13}{6} z^3 + \cdots$.
b) $\frac{|J_n|}{n!} = \frac{e^{2\sqrt{n}}}{2\sqrt{\pi e}} n^{-\frac{3}{4}} (1 + o(1))$.

Hence, $\frac{|J_n|}{|I_n|} = \mathcal{O}(\frac{1}{n^{1/2}})$.

Counting partial injections

Definition

a) The EGS for partial injections: $I(z) = \sum_{n=0}^{\infty} \frac{|I_n|}{n!} z^n$.
b) The EGS for permutations: $S(z) = \sum_{n=0}^{\infty} \frac{|S_n|}{n!} z^n = \sum_{n=0}^{\infty} z^n = \frac{1}{1-z}$.
c) The EGS for fragmented permutations: $J(z) = \sum_{n=0}^{\infty} \frac{|J_n|}{n!} z^n$.

Theorem

a) $I(z) = \frac{1}{1-z} e^{\frac{z}{1-z}} = 1 + 2z + \frac{7}{2} z^2 + \frac{17}{3} z^3 + \cdots$.
b) $\frac{|I_n|}{n!} = \frac{e^{2\sqrt{n}}}{2\sqrt{\pi e}} n^{-\frac{1}{4}} (1 + o(1))$.

Theorem

a) $J(z) = e^{\frac{z}{1-z}} = 1 + z + \frac{3}{2} z^2 + \frac{13}{6} z^3 + \cdots$.
b) $\frac{|J_n|}{n!} = \frac{e^{2\sqrt{n}}}{2\sqrt{\pi e}} n^{-\frac{3}{4}} (1 + o(1))$.

Hence, $\frac{|J_n|}{|I_n|} = \mathcal{O}(\frac{1}{n^{1/2}})$.

Counting partial injections

Definition

a) The EGS for partial injections: $I(z) = \sum_{n=0}^{\infty} \frac{|I_n|}{n!} z^n$.
b) The EGS for permutations: $S(z) = \sum_{n=0}^{\infty} \frac{|S_n|}{n!} z^n = \sum_{n=0}^{\infty} z^n = \frac{1}{1-z}$.
c) The EGS for fragmented permutations: $J(z) = \sum_{n=0}^{\infty} \frac{|J_n|}{n!} z^n$.

Theorem

a) $I(z) = \frac{1}{1-z} e^{\frac{z}{1-z}} = 1 + 2z + \frac{7}{2} z^2 + \frac{17}{3} z^3 + \cdots$.
b) $\frac{|I_n|}{n!} = \frac{e^{2\sqrt{n}}}{2\sqrt{\pi e}} n^{-\frac{1}{4}} (1 + o(1))$.

Theorem

a) $J(z) = e^{\frac{z}{1-z}} = 1 + z + \frac{3}{2} z^2 + \frac{13}{6} z^3 + \cdots$.
b) $\frac{|J_n|}{n!} = \frac{e^{2\sqrt{n}}}{2\sqrt{\pi e}} n^{-\frac{3}{4}} (1 + o(1))$.

Hence, $\frac{|J_n|}{|I_n|} = \mathcal{O}(\frac{1}{n^{1/2}})$.

Outline

1. A claim due to Gromov
2. Arzhantseva-Ol'shanskii's proof
3. A new point of view
4. Stallings' graphs
5. Counting Stallings' graphs: partial injections
6. **Most groups are trivial**
7. Proof of the combinatorial theorem

Most groups are trivial

Definition

Let $\sigma \in I_n$. Define $\gcd(\sigma)$ as the gcd *of the lengths of the closed orbits of σ (if $\sigma \in J_n$, put $\gcd(\sigma) = \infty$).*

Key observation

Let $\sigma = (\sigma_1, \ldots, \sigma_r, j) \in {I_n}^r \times [n]$, let $\Gamma(\sigma)$ be the corresponding (Stallings) graph, and let $G = \langle a_1, \ldots, a_r \mid \pi(\Gamma(\sigma)) \rangle$. We have,

- *if $\gcd(\sigma_i) = 1$ then $a_i = 1$ in G,*
- *if $\gcd(\sigma_1) = \cdots = \gcd(\sigma_r) = 1$ then $G = 1$.*

Most groups are trivial

Definition

Let $\sigma \in I_n$. Define $\mathrm{gcd}(\sigma)$ *as the* gcd *of the lengths of the closed orbits of σ (if $\sigma \in J_n$, put* $\mathrm{gcd}(\sigma) = \infty$*).*

Key observation

Let $\sigma = (\sigma_1, \ldots, \sigma_r, j) \in {I_n}^r \times [n]$, let $\Gamma(\sigma)$ be the corresponding (Stallings) graph, and let $G = \langle a_1, \ldots, a_r \mid \pi(\Gamma(\sigma)) \rangle$. We have,

- *if* $\mathrm{gcd}(\sigma_i) = 1$ *then $a_i = 1$ in G,*
- *if* $\mathrm{gcd}(\sigma_1) = \cdots = \mathrm{gcd}(\sigma_r) = 1$ *then $G = 1$.*

Most groups are trivial

Definition

Let $\sigma \in I_n$. Define $\mathrm{gcd}(\sigma)$ *as the* gcd *of the lengths of the closed orbits of* σ *(if* $\sigma \in J_n$*, put* $\mathrm{gcd}(\sigma) = \infty$*).*

Key observation

Let $\sigma = (\sigma_1, \ldots, \sigma_r, j) \in I_n{}^r \times [n]$*, let* $\Gamma(\sigma)$ *be the corresponding (Stallings) graph, and let* $G = \langle a_1, \ldots, a_r \mid \pi(\Gamma(\sigma)) \rangle$*. We have,*

- *if* $\mathrm{gcd}(\sigma_i) = 1$ *then* $a_i = 1$ *in* G*,*
- *if* $\mathrm{gcd}(\sigma_1) = \cdots = \mathrm{gcd}(\sigma_r) = 1$ *then* $G = 1$*.*

Most groups are trivial

Definition

Let $\sigma \in I_n$. Define $\text{gcd}(\sigma)$ *as the* gcd *of the lengths of the closed orbits of σ (if $\sigma \in J_n$, put* $\text{gcd}(\sigma) = \infty$*).*

Key observation

Let $\sigma = (\sigma_1, \ldots, \sigma_r, j) \in {I_n}^r \times [n]$, let $\Gamma(\sigma)$ be the corresponding (Stallings) graph, and let $G = \langle a_1, \ldots, a_r \mid \pi(\Gamma(\sigma)) \rangle$. We have,

- *if* $\text{gcd}(\sigma_i) = 1$ *then $a_i = 1$ in G,*
- *if* $\text{gcd}(\sigma_1) = \cdots = \text{gcd}(\sigma_r) = 1$ *then $G = 1$.*

Most groups are trivial

Theorem (Bassino, Martino, Nicaud, V., Weil, 2010)

$$\frac{|\{\sigma \in I_n \mid \gcd(\sigma) > 1\}|}{|I_n|} = \mathcal{O}(\frac{1}{n^{1/6}})$$

Corollary

$$\frac{|\{\sigma \in {I_n}^r \times [n] \mid \Gamma(\sigma) \text{ St. gr. } \& \ G \neq 1\}|}{|\{\sigma \in {I_n}^r \times [n] \mid \Gamma(\sigma) \text{ St. gr. }\}|} = \mathcal{O}(\frac{1}{n^{1/6}}).$$

Proof.

$$= \frac{|{I_n}^r| \cdot n}{|\{\sigma \in {I_n}^r \times [n] \mid \Gamma(\sigma) \text{ St. gr. }\}|} \cdot \frac{|\{\sigma \in {I_n}^r \times [n] \mid \Gamma(\sigma) \text{ St. gr. } \& \ G \neq 1\}|}{|{I_n}^r| \cdot n}$$

$$\leqslant 2 \cdot \frac{r \cdot |I_n|^{r-1} \cdot n \cdot |\{\sigma \in I_n \mid \gcd(\sigma) > 1\}|}{|I_n|^r \cdot n} =$$

Most groups are trivial

Theorem (Bassino, Martino, Nicaud, V., Weil, 2010)

$$\frac{|\{\sigma \in I_n \mid \gcd(\sigma) > 1\}|}{|I_n|} = \mathcal{O}(\frac{1}{n^{1/6}})$$

Corollary

$$\frac{|\{\sigma \in {I_n}^r \times [n] \mid \Gamma(\sigma) \textit{ St. gr. } \& \ G \neq 1\}|}{|\{\sigma \in {I_n}^r \times [n] \mid \Gamma(\sigma) \textit{ St. gr. }\}|} = \mathcal{O}(\frac{1}{n^{1/6}}).$$

Proof.

$$= \frac{|{I_n}^r| \cdot n}{|\{\sigma \in {I_n}^r \times [n] \mid \Gamma(\sigma) \textit{ St. gr. }\}|} \cdot \frac{|\{\sigma \in {I_n}^r \times [n] \mid \Gamma(\sigma) \textit{ St. gr. } \& \ G \neq 1\}|}{|{I_n}^r| \cdot n}$$

$$\leqslant 2 \cdot \frac{r \cdot |I_n|^{r-1} \cdot n \cdot |\{\sigma \in I_n \mid \gcd(\sigma) > 1\}|}{|I_n|^r \cdot n} =$$

Most groups are trivial

Theorem (Bassino, Martino, Nicaud, V., Weil, 2010)

$$\frac{|\{\sigma \in I_n \mid \gcd(\sigma) > 1\}|}{|I_n|} = \mathcal{O}(\frac{1}{n^{1/6}})$$

Corollary

$$\frac{|\{\sigma \in {I_n}^r \times [n] \mid \Gamma(\sigma) \textit{ St. gr. \& } G \neq 1\}|}{|\{\sigma \in {I_n}^r \times [n] \mid \Gamma(\sigma) \textit{ St. gr. }\}|} = \mathcal{O}(\frac{1}{n^{1/6}}).$$

Proof.

$$= \frac{|{I_n}^r| \cdot n}{|\{\sigma \in {I_n}^r \times [n] \mid \Gamma(\sigma) \textit{ St. gr. }\}|} \cdot \frac{|\{\sigma \in {I_n}^r \times [n] \mid \Gamma(\sigma) \textit{ St. gr. \& } G \neq 1\}|}{|{I_n}^r| \cdot n}$$

$$\leqslant 2 \cdot \frac{r \cdot |I_n|^{r-1} \cdot n \cdot |\{\sigma \in I_n \mid \gcd(\sigma) > 1\}|}{|I_n|^r \cdot n} =$$

Most groups are trivial

Theorem (Bassino, Martino, Nicaud, V., Weil, 2010)

$$\frac{|\{\sigma \in I_n \mid \gcd(\sigma) > 1\}|}{|I_n|} = \mathcal{O}(\frac{1}{n^{1/6}})$$

Corollary

$$\frac{|\{\sigma \in {I_n}^r \times [n] \mid \Gamma(\sigma) \textit{ St. gr. \& } G \neq 1\}|}{|\{\sigma \in {I_n}^r \times [n] \mid \Gamma(\sigma) \textit{ St. gr. }\}|} = \mathcal{O}(\frac{1}{n^{1/6}}).$$

Proof.

$$= \frac{|{I_n}^r| \cdot n}{|\{\sigma \in {I_n}^r \times [n] \mid \Gamma(\sigma) \textit{ St. gr. }\}|} \cdot \frac{|\{\sigma \in {I_n}^r \times [n] \mid \Gamma(\sigma) \textit{ St. gr. \& } G \neq 1\}|}{|{I_n}^r| \cdot n}$$

$$\leqslant 2 \cdot \frac{r \cdot |I_n|^{r-1} \cdot n \cdot |\{\sigma \in I_n \mid \gcd(\sigma) > 1\}|}{|I_n|^r \cdot n} =$$

Most groups are trivial

$$= 2r\frac{|\{\sigma \in I_n \mid \gcd(\sigma) > 1\}|}{|I_n|} = \mathcal{O}(\frac{1}{n^{1/6}}). \quad \square$$

So, we are reduced to proof the purely combinatorial result:

$$\frac{|\{\sigma \in I_n \mid \gcd(\sigma) > 1\}|}{|I_n|} = \mathcal{O}(\frac{1}{n^{1/6}}).$$

Most groups are trivial

$$= 2r \frac{|\{\sigma \in I_n \mid \gcd(\sigma) > 1\}|}{|I_n|} = \mathcal{O}(\frac{1}{n^{1/6}}). \quad \square$$

So, we are reduced to proof the purely combinatorial result:

$$\frac{|\{\sigma \in I_n \mid \gcd(\sigma) > 1\}|}{|I_n|} = \mathcal{O}(\frac{1}{n^{1/6}}).$$

Outline

Proof of the combinatorial theorem

Theorem (Bassino, Martino, Nicaud, V., Weil, 2010)

$$\frac{|\{\sigma \in I_n \mid \gcd(\sigma) > 1\}|}{|I_n|} = \mathcal{O}(\frac{1}{n^{1/6}})$$

The permutation case

Definition

For a prime p, let $S_n^{(p)}$ be the set of permutations $\sigma \in S_n$ with all its cycles having length multiple of p. Clearly, $S_n^{(p)} \neq \emptyset \quad \Rightarrow p|n$.

Lemma

Let $n \geqslant 2$, and p be a prime divisor of n. Then,

$$|S_n^{(p)}| \leqslant 2n!n^{\frac{1}{p}-1}.$$

Proof of the combinatorial theorem

Theorem (Bassino, Martino, Nicaud, V., Weil, 2010)

$$\frac{|\{\sigma \in I_n \mid \gcd(\sigma) > 1\}|}{|I_n|} = \mathcal{O}(\frac{1}{n^{1/6}})$$

The permutation case

Definition

For a prime p, let $S_n^{(p)}$ be the set of permutations $\sigma \in S_n$ with all its cycles having length multiple of p. Clearly, $S_n^{(p)} \neq \emptyset \quad \Rightarrow p|n$.

Lemma

Let $n \geqslant 2$, and p be a prime divisor of n. Then,

$$|S_n^{(p)}| \leqslant 2n!n^{\frac{1}{p}-1}.$$

Proof of the combinatorial theorem

Theorem (Bassino, Martino, Nicaud, V., Weil, 2010)

$$\frac{|\{\sigma \in I_n \mid \gcd(\sigma) > 1\}|}{|I_n|} = \mathcal{O}(\frac{1}{n^{1/6}})$$

The permutation case

Definition

For a prime p, let $S_n^{(p)}$ be the set of permutations $\sigma \in S_n$ with all its cycles having length multiple of p. Clearly, $S_n^{(p)} \neq \emptyset \quad \Rightarrow p|n$.

Lemma

Let $n \geqslant 2$, and p be a prime divisor of n. Then,

$$|S_n^{(p)}| \leqslant 2n! n^{\frac{1}{p}-1}.$$

Proof of the combinatorial theorem

Theorem (Bassino, Martino, Nicaud, V., Weil, 2010)

$$\frac{|\{\sigma \in I_n \mid \gcd(\sigma) > 1\}|}{|I_n|} = \mathcal{O}(\frac{1}{n^{1/6}})$$

The permutation case

Definition

For a prime p, let $S_n^{(p)}$ be the set of permutations $\sigma \in S_n$ with all its cycles having length multiple of p.Clearly, $S_n^{(p)} \neq \emptyset \quad \Rightarrow p|n$.

Lemma

Let $n \geqslant 2$, and p be a prime divisor of n. Then,

$$|S_n^{(p)}| \leqslant 2n!n^{\frac{1}{p}-1}.$$

Proof of the combinatorial theorem

Theorem (Bassino, Martino, Nicaud, V., Weil, 2010)

$$\frac{|\{\sigma \in I_n \mid \gcd(\sigma) > 1\}|}{|I_n|} = \mathcal{O}(\frac{1}{n^{1/6}})$$

The permutation case

Definition

For a prime p, let $S_n^{(p)}$ be the set of permutations $\sigma \in S_n$ with all its cycles having length multiple of p.Clearly, $S_n^{(p)} \neq \emptyset \quad \Rightarrow p|n$.

Lemma

Let $n \geqslant 2$, and p be a prime divisor of n. Then,

$$|S_n^{(p)}| \leqslant 2n!n^{\frac{1}{p}-1}.$$

Proof of the combinatorial theorem

Lemma

Let $Q_n = \{\sigma \in S_n \mid \gcd(\sigma) > 1\}$. *Then,*

$$\frac{|Q_n|}{n!} \leqslant \frac{2}{\sqrt{n}} + 2\frac{\log_3(n)}{n^{2/3}} = \mathcal{O}(\frac{1}{\sqrt{n}}).$$

The general case

Lemma

$\frac{|J_n|}{n!}$ *is strictly increasing for* $n \geqslant 1$.

Now we are ready to proof the theorem

Proof of the combinatorial theorem

Lemma

Let $Q_n = \{\sigma \in S_n \mid \gcd(\sigma) > 1\}$*. Then,*

$$\frac{|Q_n|}{n!} \leqslant \frac{2}{\sqrt{n}} + 2\frac{\log_3(n)}{n^{2/3}} = \mathcal{O}(\frac{1}{\sqrt{n}}).$$

The general case

Lemma

$\frac{|J_n|}{n!}$ *is strictly increasing for* $n \geqslant 1$.

Now we are ready to proof the theorem

Proof of the combinatorial theorem

Lemma

Let $Q_n = \{\sigma \in S_n \mid \gcd(\sigma) > 1\}$*. Then,*

$$\frac{|Q_n|}{n!} \leqslant \frac{2}{\sqrt{n}} + 2\frac{\log_3(n)}{n^{2/3}} = \mathcal{O}(\frac{1}{\sqrt{n}}).$$

The general case

Lemma

$\frac{|J_n|}{n!}$ *is strictly increasing for* $n \geqslant 1$*.*

Now we are ready to proof the theorem

Proof of the combinatorial theorem

Theorem (Bassino, Martino, Nicaud, V., Weil, 2010)

$$\frac{|\{\sigma \in I_n \mid \gcd(\sigma) > 1\}|}{|I_n|} = \mathcal{O}(\frac{1}{n^{1/6}})$$

Proof.

- *Every such $\sigma \in I_n$ is the disjoint union of a permutation in S_k and a fragmented permutation in J_{n-k}, for some $k = 0, \ldots, n$.*
- *Let's distinguish between k "short" and k "long".*

$$\frac{|\{\sigma \in I_n \mid \gcd(\sigma) > 1\}|}{|I_n|} = \frac{1}{|I_n|} \sum_{k=0}^{n} \binom{n}{k} |Q_k||J_{n-k}|$$

$$\leqslant \frac{1}{|I_n|} \sum_{k=0}^{\lfloor n^{1/3} \rfloor} \frac{n!}{(n-k)!} |J_{n-k}| + \frac{1}{|I_n|} \sum_{k=\lceil n^{1/3} \rceil}^{n} \frac{n!}{(n-k)!} \frac{M}{\sqrt{k}} |J_{n-k}|$$

Proof of the combinatorial theorem

Theorem (Bassino, Martino, Nicaud, V., Weil, 2010)

$$\frac{|\{\sigma \in I_n \mid \gcd(\sigma) > 1\}|}{|I_n|} = \mathcal{O}(\frac{1}{n^{1/6}})$$

Proof.

- *Every such $\sigma \in I_n$ is the disjoint union of a permutation in S_k and a fragmented permutation in J_{n-k}, for some $k = 0, \ldots, n$.*
- *Let's distinguish between k "short" and k "long".*

$$\frac{|\{\sigma \in I_n \mid \gcd(\sigma) > 1\}|}{|I_n|} = \frac{1}{|I_n|} \sum_{k=0}^{n} \binom{n}{k} |Q_k||J_{n-k}|$$

$$\leqslant \frac{1}{|I_n|} \sum_{k=0}^{\lfloor n^{1/3} \rfloor} \frac{n!}{(n-k)!} |J_{n-k}| + \frac{1}{|I_n|} \sum_{k=\lceil n^{1/3} \rceil}^{n} \frac{n!}{(n-k)!} \frac{M}{\sqrt{k}} |J_{n-k}|$$

Proof of the combinatorial theorem

Theorem (Bassino, Martino, Nicaud, V., Weil, 2010)

$$\frac{|\{\sigma \in I_n \mid \gcd(\sigma) > 1\}|}{|I_n|} = \mathcal{O}(\frac{1}{n^{1/6}})$$

Proof.

- *Every such $\sigma \in I_n$ is the disjoint union of a permutation in S_k and a fragmented permutation in J_{n-k}, for some $k = 0, \ldots, n$.*
- *Let's distinguish between k "short" and k "long".*

$$\frac{|\{\sigma \in I_n \mid \gcd(\sigma) > 1\}|}{|I_n|} = \frac{1}{|I_n|} \sum_{k=0}^{n} \binom{n}{k} |Q_k||J_{n-k}|$$

$$\leqslant \frac{1}{|I_n|} \sum_{k=0}^{\lfloor n^{1/3} \rfloor} \frac{n!}{(n-k)!} |J_{n-k}| + \frac{1}{|I_n|} \sum_{k=\lceil n^{1/3} \rceil}^{n} \frac{n!}{(n-k)!} \frac{M}{\sqrt{k}} |J_{n-k}|$$

Proof of the combinatorial theorem

Theorem (Bassino, Martino, Nicaud, V., Weil, 2010)

$$\frac{|\{\sigma \in I_n \mid \gcd(\sigma) > 1\}|}{|I_n|} = \mathcal{O}\left(\frac{1}{n^{1/6}}\right)$$

Proof.

- *Every such $\sigma \in I_n$ is the disjoint union of a permutation in S_k and a fragmented permutation in J_{n-k}, for some $k = 0, \ldots, n$.*
- *Let's distinguish between k "short" and k "long".*

$$\frac{|\{\sigma \in I_n \mid \gcd(\sigma) > 1\}|}{|I_n|} = \frac{1}{|I_n|} \sum_{k=0}^{n} \binom{n}{k} |Q_k||J_{n-k}|$$

$$\leqslant \frac{1}{|I_n|} \sum_{k=0}^{\lfloor n^{1/3} \rfloor} \frac{n!}{(n-k)!} |J_{n-k}| + \frac{1}{|I_n|} \sum_{k=\lceil n^{1/3} \rceil}^{n} \frac{n!}{(n-k)!} \frac{M}{\sqrt{k}} |J_{n-k}|$$

Proof of the combinatorial theorem

Theorem (Bassino, Martino, Nicaud, V., Weil, 2010)

$$\frac{|\{\sigma \in I_n \mid \gcd(\sigma) > 1\}|}{|I_n|} = \mathcal{O}(\frac{1}{n^{1/6}})$$

Proof.

- *Every such $\sigma \in I_n$ is the disjoint union of a permutation in S_k and a fragmented permutation in J_{n-k}, for some $k = 0, \ldots, n$.*
- *Let's distinguish between k "short" and k "long".*

$$\frac{|\{\sigma \in I_n \mid \gcd(\sigma) > 1\}|}{|I_n|} = \frac{1}{|I_n|} \sum_{k=0}^{n} \binom{n}{k} |Q_k||J_{n-k}|$$

$$\leqslant \frac{1}{|I_n|} \sum_{k=0}^{\lfloor n^{1/3} \rfloor} \frac{n!}{(n-k)!} |J_{n-k}| + \frac{1}{|I_n|} \sum_{k=\lceil n^{1/3} \rceil}^{n} \frac{n!}{(n-k)!} \frac{M}{\sqrt{k}} |J_{n-k}|$$

Proof of the combinatorial theorem

$$\leqslant \frac{1}{|I_n|} n!(1+\lfloor n^{1/3}\rfloor)\frac{|J_n|}{n!} + \frac{M}{|I_n|\cdot n^{1/6}} \sum_{k=\lceil n^{1/3}\rceil}^{n} \frac{n!}{(n-k)!}|J_{n-k}|$$

$$\leqslant (1+\lfloor n^{1/3}\rfloor)\frac{|J_n|}{|I_n|} + \frac{M}{|I_n|\cdot n^{1/6}} \sum_{k=0}^{n} \frac{n!}{(n-k)!k!} k!|J_{n-k}|$$

$$\leqslant \mathcal{O}(\frac{n^{1/3}}{n^{1/2}}) + \mathcal{O}(\frac{1}{n^{1/6}})$$

$$= \mathcal{O}(\frac{1}{n^{1/6}}). \quad \square$$

Proof of the combinatorial theorem

$$\leqslant \frac{1}{|I_n|} n!(1+\lfloor n^{1/3}\rfloor)\frac{|J_n|}{n!} + \frac{M}{|I_n|\cdot n^{1/6}} \sum_{k=\lceil n^{1/3}\rceil}^{n} \frac{n!}{(n-k)!}|J_{n-k}|$$

$$\leqslant (1+\lfloor n^{1/3}\rfloor)\frac{|J_n|}{|I_n|} + \frac{M}{|I_n|\cdot n^{1/6}} \sum_{k=0}^{n} \frac{n!}{(n-k)!k!}k!|J_{n-k}|$$

$$\leqslant \mathcal{O}(\frac{n^{1/3}}{n^{1/2}}) + \mathcal{O}(\frac{1}{n^{1/6}})$$

$$= \mathcal{O}(\frac{1}{n^{1/6}}). \quad \square$$

Proof of the combinatorial theorem

$$\leqslant \frac{1}{|I_n|} n!(1+\lfloor n^{1/3} \rfloor)\frac{|J_n|}{n!} + \frac{M}{|I_n| \cdot n^{1/6}} \sum_{k=\lceil n^{1/3} \rceil}^{n} \frac{n!}{(n-k)!} |J_{n-k}|$$

$$\leqslant (1+\lfloor n^{1/3} \rfloor)\frac{|J_n|}{|I_n|} + \frac{M}{|I_n| \cdot n^{1/6}} \sum_{k=0}^{n} \frac{n!}{(n-k)!k!} k!|J_{n-k}|$$

$$\leqslant \mathcal{O}(\frac{n^{1/3}}{n^{1/2}}) + \mathcal{O}(\frac{1}{n^{1/6}})$$

$$= \mathcal{O}(\frac{1}{n^{1/6}}). \quad \square$$

Proof of the combinatorial theorem

$$\leqslant \frac{1}{|I_n|} n!(1+\lfloor n^{1/3} \rfloor)\frac{|J_n|}{n!} + \frac{M}{|I_n| \cdot n^{1/6}} \sum_{k=\lceil n^{1/3} \rceil}^{n} \frac{n!}{(n-k)!} |J_{n-k}|$$

$$\leqslant (1+\lfloor n^{1/3} \rfloor)\frac{|J_n|}{|I_n|} + \frac{M}{|I_n| \cdot n^{1/6}} \sum_{k=0}^{n} \frac{n!}{(n-k)!k!} k!|J_{n-k}|$$

$$\leqslant \mathcal{O}(\frac{n^{1/3}}{n^{1/2}}) + \mathcal{O}(\frac{1}{n^{1/6}})$$

$$= \mathcal{O}(\frac{1}{n^{1/6}}). \quad \square$$

Thanks