Random subgroups of a free group

Frédérique Bassino

LIPN - Laboratoire d'Informatique de Paris Nord,
Université Paris 13 - CNRS

Joint work with Armando Martino, Cyril Nicaud, Enric Ventura et Pascal Weil

LIX – May, 2015

Introduction

- Any group is isomorphic to a quotient group of some free group.
- Study of algebraic properties of free groups by combinatorial methods
  - Graphical representation of subgroups : Stallings graphs
  - Combinatorial interpretation of parameters or properties like the rank, malnormality, Whitehead minimality, ...
- Quantitative study of finitely generated subgroups of a free group and analysis of related algorithms

Introduction

- Any group is isomorphic to a quotient group of some free group.
- Study of algebraic properties of free groups by combinatorial methods
  - Graphical representation of subgroups : Stallings graphs
  - Combinatorial interpretation of parameters or properties like the rank, malnormality, Whitehead minimality, ...
- Quantitative study of finitely generated subgroups of a free group and analysis of related algorithms

I. Free Group

Free group : a definition

- A group F is *free* if there is a subset A of F such that any element of F can be uniquely written as a finite product of elements of A and their inverses.
- The cardinality of A is the *rank* of the free group.
- Apart from the existence of inverses no other relation exists between the generators of a free group.

Basic properties

- The subgroups of a free group are free (Nielsen-Schreier Theorem).
- A free group with finite rank contains subgroups with any countable rank.

Free group : a definition

- A group F is *free* if there is a subset A of F such that any element of F can be uniquely written as a finite product of elements of A and their inverses.
- The cardinality of A is the *rank* of the free group.
- Apart from the existence of inverses no other relation exists between the generators of a free group.

Basic properties

- The subgroups of a free group are free (Nielsen-Schreier Theorem).
- A free group with finite rank contains subgroups with any countable rank.

Free group : a definition

- A group F is *free* if there is a subset A of F such that any element of F can be uniquely written as a finite product of elements of A and their inverses.
- The cardinality of A is the *rank* of the free group.
- Apart from the existence of inverses no other relation exists between the generators of a free group.

Basic properties

- The subgroups of a free group are free (Nielsen-Schreier Theorem).
- A free group with finite rank contains subgroups with any countable rank.

Free groups and reduced words

- Let A be a **finite** alphabet and $F = F(A)$ be the free group over A.
- The elements of $F(A)$ are uniquely represented by the *reduced* words over $A \cup A^{-1}$ where $A^{-1} = \{a^{-1} \mid a \in A\}$,
- A word is *reduced* if it does not contain factors of the form aa^{-1}
- Examples : $ab^{-1}b^{-1}aaba^{-1}$ is reduced,
  $aab^{-1}a^{-1}abcca^{-1}$ is not reduced
- Reduction of a word : replace **in any order** all occurrences of aa^{-1} by the empty word ϵ.
- Example :

$$aab^{-1}a^{-1}abcca^{-1} = aab^{-1}bcca^{-1} = aacca^{-1}$$

Free groups and reduced words

- Let A be a **finite** alphabet and $F = F(A)$ be the free group over A.
- The elements of $F(A)$ are uniquely represented by the *reduced* words over $A \cup A^{-1}$ where $A^{-1} = \{a^{-1} \mid a \in A\}$,
- A word is *reduced* if it does not contain factors of the form aa^{-1}
- Examples : $ab^{-1}b^{-1}aaba^{-1}$ is reduced,
  $aab^{-1}a^{-1}abcca^{-1}$ is not reduced
- Reduction of a word : replace **in any order** all occurrences of aa^{-1} by the empty word ϵ.
- Example :

$$aab^{-1}a^{-1}abcca^{-1} = aab^{-1}bcca^{-1} = aacca^{-1}$$

Free groups and reduced words

- Let A be a **finite** alphabet and $F = F(A)$ be the free group over A.
- The elements of $F(A)$ are uniquely represented by the *reduced* words over $A \cup A^{-1}$ where $A^{-1} = \{a^{-1} \mid a \in A\}$,
- A word is *reduced* if it does not contain factors of the form aa^{-1}
- Examples : $ab^{-1}b^{-1}aaba^{-1}$ is reduced,
  $aab^{-1}a^{-1}abcca^{-1}$ is not reduced
- Reduction of a word : replace **in any order** all occurrences of aa^{-1} by the empty word ϵ.
- Example :

$$aab^{-1}a^{-1}abcca^{-1} = aab^{-1}bcca^{-1} = aacca^{-1}$$

Free groups and reduced words

- Let A be a **finite** alphabet and $F = F(A)$ be the free group over A.
- The elements of $F(A)$ are uniquely represented by the *reduced* words over $A \cup A^{-1}$ where $A^{-1} = \{a^{-1} \mid a \in A\}$,
- A word is *reduced* if it does not contain factors of the form aa^{-1}
- Examples : $ab^{-1}b^{-1}aaba^{-1}$ is reduced,
  $aab^{-1}a^{-1}abcca^{-1}$ is not reduced
- Reduction of a word : replace **in any order** all occurrences of aa^{-1} by the empty word ϵ.
- Example :

$$aab^{-1}a^{-1}abcca^{-1} = aab^{-1}bcca^{-1} = aacca^{-1}$$

Free groups and reduced words

- Let A be a **finite** alphabet and $F = F(A)$ be the free group over A.
- The elements of $F(A)$ are uniquely represented by the *reduced* words over $A \cup A^{-1}$ where $A^{-1} = \{a^{-1} \mid a \in A\}$,
- A word is *reduced* if it does not contain factors of the form aa^{-1}
- Examples : $ab^{-1}b^{-1}aaba^{-1}$ is reduced,
  $aab^{-1}a^{-1}abcca^{-1}$ is not reduced
- Reduction of a word : replace **in any order** all occurrences of aa^{-1} by the empty word ϵ.
- Example :

$$aab^{-1}a^{-1}abcca^{-1} = aab^{-1}bcca^{-1} = aacca^{-1}$$

Finitely generated subgroups

We are interested in finitely generated free subgroups, *i.e.*, obtained from a finite set of generators.

- Finitely generated free subgroups can be represented in a unique way by a finite graph called its **Stallings graph** (Stallings 1983).
- This description is very useful, some properties of the subgroup can be directly obtained from its graph representation.

A 1st goal

To study algebraic properties of finitely generated subgroups of a free group with combinatorial methods.

Finitely generated subgroups

We are interested in finitely generated free subgroups, *i.e.*, obtained from a finite set of generators.

- Finitely generated free subgroups can be represented in a unique way by a finite graph called its **Stallings graph** (Stallings 1983).
- This description is very useful, some properties of the subgroup can be directly obtained from its graph representation.

A 1st goal

To study algebraic properties of finitely generated subgroups of a free group with combinatorial methods.

Finitely generated subgroups

We are interested in finitely generated free subgroups, *i.e.*, obtained from a finite set of generators.

- Finitely generated free subgroups can be represented in a unique way by a finite graph called its **Stallings graph** (Stallings 1983).
- This description is very useful, some properties of the subgroup can be directly obtained from its graph representation.

A 1st goal

To study algebraic properties of finitely generated subgroups of a free group with combinatorial methods.

Stallings foldings

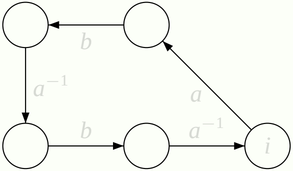
Let $Y = \{aba^{-1}ba^{-1}, b^2a^{-1}, b^3a^{-1}b^{-1}\}$.

Goal

Build a directed graph representing the free subgroup generated by Y

First step

Build a directed cycle labeled with $aba^{-1}ba^{-1}$ the first element of Y



Stallings foldings

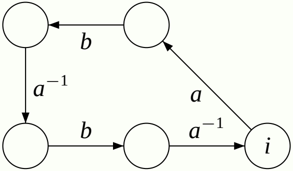
Let $Y = \{aba^{-1}ba^{-1}, b^2a^{-1}, b^3a^{-1}b^{-1}\}$.

Goal

Build a directed graph representing the free subgroup generated by Y

First step

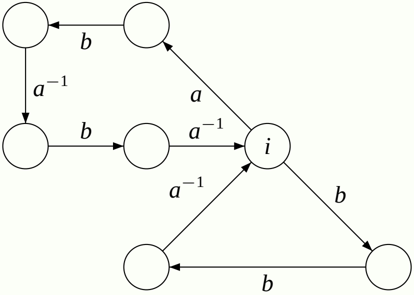
Build a directed cycle labeled with $aba^{-1}ba^{-1}$ the first element of Y



Stallings foldings

Second step

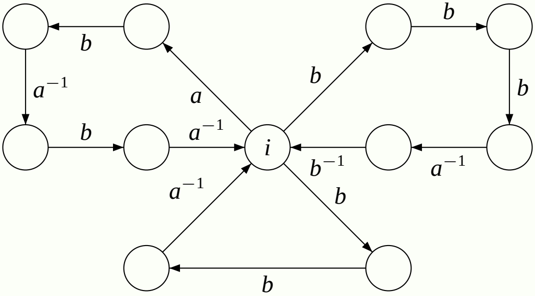
Build from the same vertex i a directed cycle labeled with b^2a^{-1} the second element of Y.



Stallings foldings

Third step

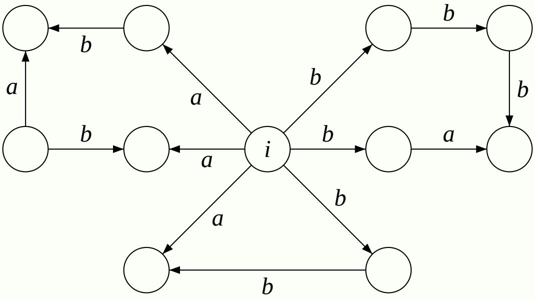
Build from the same vertex i a directed cycle labeled with $b^3a^{-1}b^{-1}$ the third and last element of Y.



Stallings foldings

Formal inverses

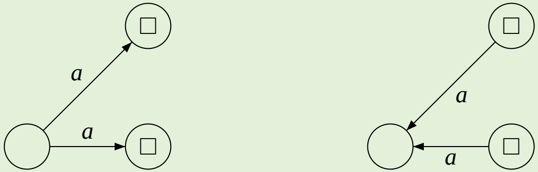
Reverse all edges labeled by a^{-1} are and replace their label by a.



Stallings foldings

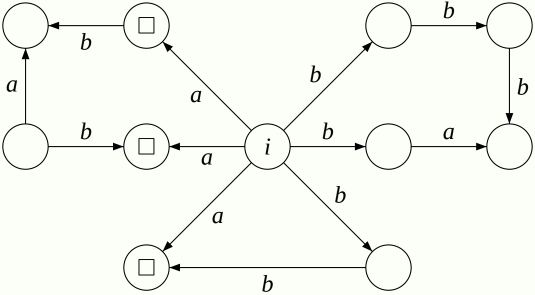
Foldings to obtain determinism and codeterminism

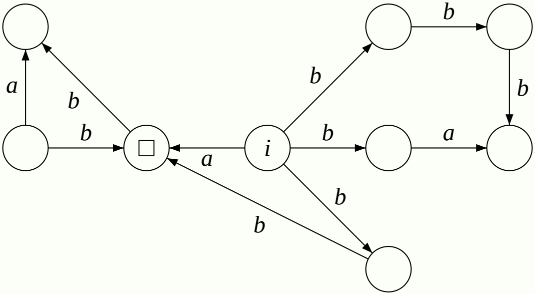
Apply as many times as possible the following rules of merging (or folding) :



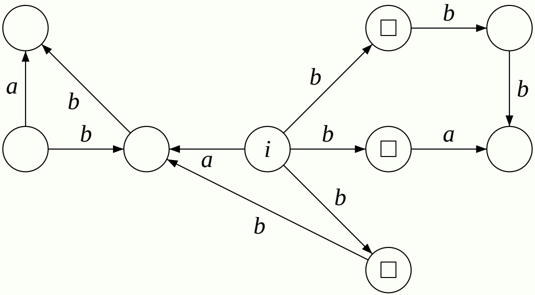
The result does not depend on the order in which the transformations are performed.

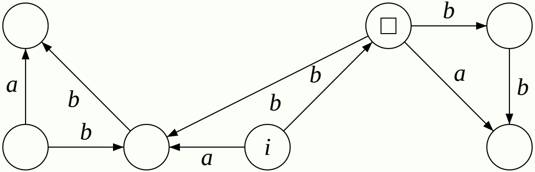
Stallings foldings - 1st folding



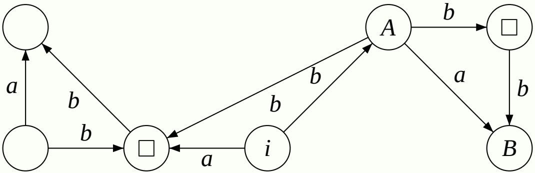


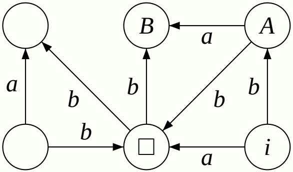
Stallings foldings - 2nd folding



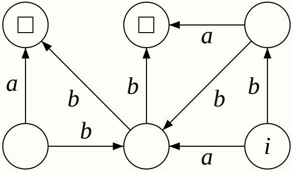


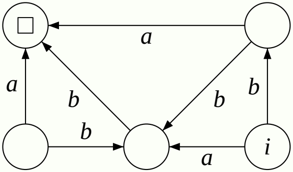
Stallings foldings - 3rd folding



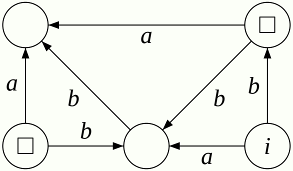


Stallings foldings - 4th folding



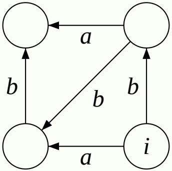


Stallings foldings - Last folding and Stallings graph



The Stallings graph representing the free subgroup generated by

$$Y = \{aba^{-1}ba^{-1}, b^2a^{-1}, b^3a^{-1}b^{-1}\}.$$



Stallings graphs : a definition

The graph (with a distinguished vertex *i*) obtained is a *Stallings graph*.

Stallings graph

- It is deterministic and co-deterministic : each letter acts like a **partial injection** on the set of states.
- it is connected
- all but the distinguished state *i* have degree at least two

Unicity of the representation

A Stallings graph represents in a unique way a finitely generated subgroup of the free group generated by the alphabet of the labels.

Stallings graphs : a definition

The graph (with a distinguished vertex i) obtained is a *Stallings graph*.

Stallings graph

- It is deterministic and co-deterministic : each letter acts like a **partial injection** on the set of states.
- it is connected
- all but the distinguished state i have degree at least two

Unicity of the representation

A Stallings graph represents in a unique way a finitely generated subgroup of the free group generated by the alphabet of the labels.

Stallings graphs : a definition

The graph (with a distinguished vertex i) obtained is a *Stallings graph*.

Stallings graph

- It is deterministic and co-deterministic : each letter acts like a **partial injection** on the set of states.
- it is connected
- all but the distinguished state i have degree at least two

Unicity of the representation

A Stallings graph represents in a unique way a finitely generated subgroup of the free group generated by the alphabet of the labels.

Stallings graphs – examples of use

- One can check whether a (reduced) word belongs the subgroup or not.
  Check if there exists a cycle labeled by the word beginning in i
- One can compute a basis and the rank of the subgroup

$$rank = |E| - (|V| - 1)$$

  To obtain a basis, choose a spanning tree of the Stallings graph. Each edge e that is not in the tree corresponds to a generator of the base : the label of a cycle beginning in i using e and edges in the spanning tree.
- One can check whether the subgroup has finite index or not.
  All letters act like permutations on the set of vertices

Stallings graphs – examples of use

- One can check whether a (reduced) word belongs the subgroup or not.
  Check if there exists a cycle labeled by the word beginning in i
- One can compute a basis and the rank of the subgroup

$$rank = |E| - (|V| - 1)$$

  To obtain a basis, choose a spanning tree of the Stallings graph. Each edge e that is not in the tree corresponds to a generator of the base : the label of a cycle beginning in i using e and edges in the spanning tree.
- One can check whether the subgroup has finite index or not.
  All letters act like permutations on the set of vertices

Stallings graphs – examples of use

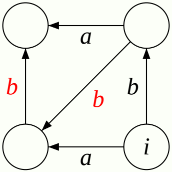
- One can check whether a (reduced) word belongs the subgroup or not.
  Check if there exists a cycle labeled by the word beginning in i
- One can compute a basis and the rank of the subgroup

  $$rank = |E| - (|V| - 1)$$

  To obtain a basis, choose a spanning tree of the Stallings graph. Each edge e that is not in the tree corresponds to a generator of the base : the label of a cycle beginning in i using e and edges in the spanning tree.
- One can check whether the subgroup has finite index or not.
  All letters act like permutations on the set of vertices

Example for the rank

The Stallings graph of the subgroup genrated by
$Y = \{aba^{-1}ba^{-1}, b^2a^{-1}, b^3a^{-1}b^{-1}\}$:



Therefore $\{b^2a^{-1}, aba^{-1}b^{-1}\}$ is a basis of the subgroup and the rank is 2.

Stallings graphs – algorithmic point of view

- Stalling foldings can be computed in $O(n \log^* n)$ where n is the total length of the generators. The algorithm due Touikan (2006) makes use of ”Union and Find”.
- The intersection (resp. union) of two subgroups can be computed in time and space $O(n_1 \times n_2)$ where n_1 (resp. n_2) is the size (here the number of vertices) of the first (resp. second) Stallings graph.

II. Distributions on Subgroups

A graph-based distribution on subgroups

- A random subgroup is given by choosing uniformly at random a **Stallings graph of size** n
- Studied by Bassino, Nicaud, Weil (2008, 2013, 2015)
- What does the Stallings graph of such a random subgroup look like ?

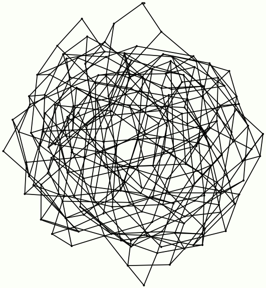


FIGURE: A random subgroup with 200 vertices for the graph-based distribution (The alphabet is of size 2).

The classical word-based distribution on subgroups

- A random subgroup is given by choosing randomly and uniformly k generators of length at most n, where k is fixed
- Studied by Gromov (1987), Arzhantseva and Ol'shanskiĭ (1996), Jitsukawa (2002), ...
- What does the Stallings graph of such a random subgroup look like ?

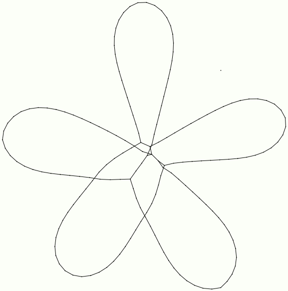


FIGURE: A random subgroup for the word-based distribution with 5 words of lengths at most 40 (The alphabet is of size 2.)

A word-based distribution (few generators)

- Fix the number k of generators and the maximal length n of each generator.
- Consider the uniform distribution over the k-tuples of reduced words of length at most n.
- Let R_n the number of reduced words of length n,

$$R_n = 2r(2r-1)^{n-1}$$

- The length of word in a random k-tuple is near to n.

A word-based distribution (few generators)

- Fix the number k of generators and the maximal length n of each generator.
- Consider the uniform distribution over the k-tuples of reduced words of length at most n.
- Let R_n the number of reduced words of length n,

$$R_n = 2r(2r-1)^{n-1}$$

- The length of word in a random k-tuple is near to n.

A word-based distribution (few generators)

Length, prefixes and suffixes

- Let $0 < \alpha < 1$. A reduced word in R_n has length greater than αn with probability that tends toward 1 when n tends toward $+\infty$.
- Let $0 < \beta < \alpha/2$. A k-uple of reduced words of R_n is such that the prefixes of length βn of all words and their inverses are pairwise distinct with probability that tends toward 1 when n tends toward $+\infty$.

Consequence

Each of the k reduced words has an outer loop of length at least $n(\alpha - 2\beta)$ with probability that tends to 1 when n tends to $+\infty$.

A graph-based distribution : Probabilistic results

Theorem (Bassino, Nicaud, Weil 2008)

The probability for a random r-tuple of partial injections of size n to form a Stallings graph tends toward 1 when n tends toward $+\infty$.

Stallings graph

- It is deterministic and co-deterministic : each letter acts like a **partial injection** on the set of states.
- it is connected
- all but the distinguished state i have degree at least two

The proof

- is a study of partial injections
- basically uses the saddle-point method

A graph-based distribution : Probabilistic results

Theorem (Bassino, Nicaud, Weil 2008)

The probability for a random r-tuple of partial injections of size n to form a Stallings graph tends toward 1 when n tends toward $+\infty$.

Stallings graph

- It is deterministic and co-deterministic : each letter acts like a **partial injection** on the set of states.
- it is connected
- all but the distinguished state i have degree at least two

The proof

- is a study of partial injections
- basically uses the saddle-point method

A graph-based distribution : Probabilistic results

Theorem (Bassino, Nicaud, Weil 2008)

The probability for a random r-tuple of partial injections of size n to form a Stallings graph tends toward 1 when n tends toward $+\infty$.

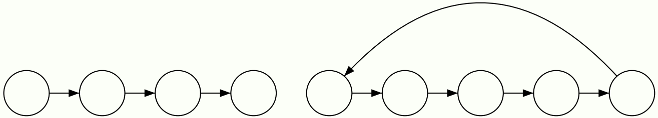
Stallings graph

- It is deterministic and co-deterministic : each letter acts like a **partial injection** on the set of states.
- it is connected
- all but the distinguished state i have degree at least two

The proof

- is a study of partial injections
- basically uses the saddle-point method

A graph-based distribution : Partial injections



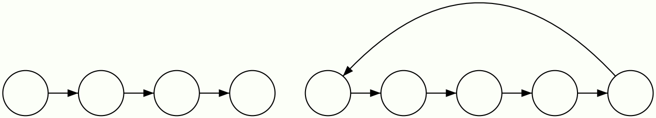
- A partial injection can be seen as a set of cycles and of non-empty sequences.
- Set(Cycle or non-empty Sequences)
- With the symbolic method :

$$I(z) = \sum_{n \geq 0} \frac{I_n}{n!} z^n = \exp\left(\log \frac{1}{1-z} + \frac{z}{1-z}\right) = \frac{1}{1-z} e^{z/(1-z)}$$

- With the saddle point method :

$$\frac{I_n}{n!} \sim \frac{e^{-\frac{1}{2}}}{2\sqrt{\pi}} e^{2\sqrt{n}} n^{-\frac{1}{4}}$$

A graph-based distribution : Partial injections



- A partial injection can be seen as a set of cycles and of non-empty sequences.
- Set(Cycle or non-empty Sequences)
- With the symbolic method :

$$I(z) = \sum_{n \geq 0} \frac{I_n}{n!} z^n = \exp\left(\log \frac{1}{1-z} + \frac{z}{1-z}\right) = \frac{1}{1-z} e^{z/(1-z)}$$

- With the saddle point method :

$$\frac{I_n}{n!} \sim \frac{e^{-\frac{1}{2}}}{2\sqrt{\pi}} e^{2\sqrt{n}} n^{-\frac{1}{4}}$$

Connectedness

Theorem

The probability for r partial injections of size n to form a connected graph is

$$p_n = 1 - \frac{2^r}{n^{r-1}} + o\left(\frac{1}{n^{r-1}}\right)$$

Proof

Let $J(z) = \sum_{n>0} j_n z^n = \sum_{n>0} I_n^r z^n / n!$.
Then $1 + J(z) = \exp(C(z))$ and $C(z) = \log(1 + J(z))$.
From a Bender theorem (1974) it is enough to check that $j_n = o(j_{n-1})$ and that for some $s \geq 1$, $\sum_{k=s}^{n-s} |j_k j_{n-k}| = O(j_{n-s})$, to obtain that

$$c_n = j_n \left(1 - \frac{2^r}{n^{r-1}} + o\left(\frac{1}{n^{r-1}}\right)\right)$$

Connectedness

Theorem

The probability for r partial injections of size n to form a connected graph is

$$p_n = 1 - \frac{2^r}{n^{r-1}} + o\left(\frac{1}{n^{r-1}}\right)$$

Proof

Let $J(z) = \sum_{n>0} j_n z^n = \sum_{n>0} I_n^r z^n / n!$.
Then $1 + J(z) = \exp(C(z))$ and $C(z) = \log(1 + J(z))$.
From a Bender theorem (1974) it is enough to check that $j_n = o(j_{n-1})$ and that for some $s \geq 1$, $\sum_{k=s}^{n-s} |j_k j_{n-k}| = O(j_{n-s})$, to obtain that

$$c_n = j_n \left(1 - \frac{2^r}{n^{r-1}} + o\left(\frac{1}{n^{r-1}}\right)\right)$$

Vertices with zero or one outgoing or ingoing edge

- If x is a vertex with 0 or 1 edge, then x must be **isolated** for $r-1$ injections and **an endpoint** for the remaining injection.
- The probability it is isolated for an injection is $\frac{I_{n-1}}{I_n}$, which is smaller than $\frac{1}{n}$.
- Let $I_{n,k}$ be the number of size-n injections **having** k **sequences**, and let $I(z,u)$ be the bivariate generating function defined by :

$$I(z,u) = \exp\left(\frac{zu}{1-z} + \log\left(\frac{1}{1-z}\right)\right) = \frac{1}{1-z}\exp\left(\frac{zu}{1-z}\right)$$

Using the **saddle point theorem** we obtain that the expected number of sequences is $\frac{1}{\sqrt{n}}$ and that the probability that a given vertex is an endpoint is in $\mathcal{O}(\frac{1}{\sqrt{n}})$.

Trimness

Therefore

- A given vertex has degree 0 or 1 with probability $\mathcal{O}(n^{-r+1/2})$,
- there is such a vertex with probability $\mathcal{O}(n^{-r+3/2})$
- **with probability at least $\mathcal{O}(n^{-1/2})$ the graph has no such vertex.**

IV. How to compare the two distributions

Méthod

- A property P is *generic* for (X_n) when the probability for an element of X_n to satisfy P tends toward 1 when n tends toward ∞.
- A property P is *negligible* for (X_n) when the probability for an element of X_n to satisfy P tends toward O when n tends toward ∞.
- In the following, we present generic or negligible algebraic properties for each distribution.

Méthod

- A property P is *generic* for (X_n) when the probability for an element of X_n to satisfy P tends toward 1 when n tends toward ∞.
- A property P is *negligible* for (X_n) when the probability for an element of X_n to satisfy P tends toward O when n tends toward ∞.
- In the following, we present generic or negligible algebraic properties for each distribution.

Experimental results

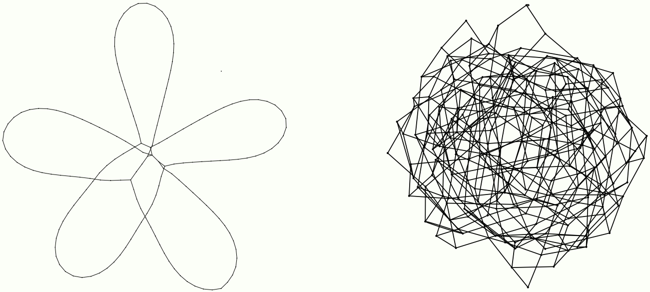


FIGURE: On the left, a random subgroup for the word-based distribution with 5 words of lengths at most 40. On the right, a random subgroup with 200 vertices for the graph-based distribution (The alphabet is of size 2).

Rank

- One can compute the rank of a finitely generated subgroup from its Stallings graph

$$rank = |E| - (|V| - 1)$$

- In the word based distribution (k words of maximal length n), the average rank is k
- In the graph based distribution the average rank is $(|A| - 1)n - |A|\sqrt{n} + 1$.

Rank

- One can compute the rank of a finitely generated subgroup from its Stallings graph

$$rank = |E| - (|V| - 1)$$

- In the word based distribution (k words of maximal length n), the average rank is k
- In the graph based distribution the average rank is $(|A| - 1)n - |A|\sqrt{n} + 1$.

Malnormality

- A subgroup H of G is **normal** when for any $g \in G$, $g^{-1}Hg = H$.
- A subgroup is **malnormal** when for any $g \notin H$, $g^{-1}Hg \cap H = 1$.

Theorem (combinatorial characterization)

A subgroup of a free group is **non-malnormal** if and only, in its Stallings graph, if there exists two vertices $x \neq y$ and a non-empty reduced word u, such that

u is the label of a loop on x and of a loop on y.

Malnormality

- A subgroup H of G is **normal** when for any $g \in G$, $g^{-1}Hg = H$.
- A subgroup is **malnormal** when for any $g \notin H$, $g^{-1}Hg \cap H = 1$.

Theorem (combinatorial characterization)

A subgroup of a free group is **non-malnormal** if and only, in its Stallings graph, if there exists two vertices $x \neq y$ and a non-empty reduced word u, such that
u is the label of a loop on x and of a loop on y.

Malnormality

Theorem

For the word-based distribution, malnormality is **generic**, but it is **negligible** for the graph-based.

Proof

- The proof in the word-based distribution is due to Jitsukawa (2002). Basically loops are long enough to be distinct with high probability.
- The probability that a partial injection contains at most one cycle and that the length of this cycle is 1 is $\sim \frac{e}{\sqrt{n}}$.

Malnormality

Theorem

For the word-based distribution, malnormality is **generic**, but it is **negligible** for the graph-based.

Proof

- The proof in the word-based distribution is due to Jitsukawa (2002). Basically loops are long enough to be distinct with high probability.
- The probability that a partial injection contains at most one cycle and that the length of this cycle is 1 is $\sim \frac{e}{\sqrt{n}}$.

Finite presentation

- The idea is to quotient the free group by a normal finitely generated subgroup. Let E be an arbitrary subset, and $N(E)$ be its normal closure, that is the smallest normal subgroup containing E.
- Equivalently each word x of E becomes a relator $x = 1$.
- In the word-based distribution generically the quotient subgroup is infinite (Jitsukawa, 2002).
- But in the graph-based distribution, the quotient group is generically trivial.

Finite presentation

- The idea is to quotient the free group by a normal finitely generated subgroup. Let E be an arbitrary subset, and $N(E)$ be its normal closure, that is the smallest normal subgroup containing E.
- Equivalently each word x of E becomes a relator $x = 1$.
- In the word-based distribution generically the quotient subgroup is infinite (Jitsukawa, 2002).
- But in the graph-based distribution, the quotient group is generically trivial.

Finite presentation

- The idea is to quotient the free group by a normal finitely generated subgroup. Let E be an arbitrary subset, and $N(E)$ be its normal closure, that is the smallest normal subgroup containing E.
- Equivalently each word x of E becomes a relator $x = 1$.
- In the word-based distribution generically the quotient subgroup is infinite (Jitsukawa, 2002).
- But in the graph-based distribution, the quotient group is generically trivial.

Finite presentation

- The idea is to quotient the free group by a normal finitely generated subgroup. Let E be an arbitrary subset, and $N(E)$ be its normal closure, that is the smallest normal subgroup containing E.
- Equivalently each word x of E becomes a relator $x = 1$.
- In the word-based distribution generically the quotient subgroup is infinite (Jitsukawa, 2002).
- But in the graph-based distribution, the quotient group is generically trivial.

Finite presentation

Theorem

Generically the gcd of the lengths of the cycles of a **partial injection** of size n is 1.

Theorem

Generically the gcd of the lengths of the cycles of a **permutation** of size n is 1.

Permutation part of an injection

Generically the permutation part of a size n injection is greater than $n^{1/3}$ and the gcd of the length of the cycles is 1.

Finite presentation

Theorem

Generically the gcd of the lengths of the cycles of a **partial injection** of size n is 1.

Theorem

Generically the gcd of the lengths of the cycles of a **permutation** of size n is 1.

Permutation part of an injection

Generically the permutation part of a size n injection is greater than $n^{1/3}$ and the gcd of the length of the cycles is 1.

Finite presentation

Theorem

Generically the gcd of the lengths of the cycles of a **partial injection** of size n is 1.

Theorem

Generically the gcd of the lengths of the cycles of a **permutation** of size n is 1.

Permutation part of an injection

Generically the permutation part of a size n injection is greater than $n^{1/3}$ and the gcd of the length of the cycles is 1.

Thank you for your attention !