Random subgroups of a free group and automata

Frédérique Bassino

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

Joint work with Cyril Nicaud (LIGM) and Pascal Weil (LaBRI)

Joint conference VMS-SMF, Hué – August, 2012

- Free group and group presentations (any group is isomorphic to a quotient group of some free group).
- Study of algebraic properties by combinatorial methods
  - Graphical representation of subgroups : Stallings graphs
  - Combinatorial interpretation of parameters or properties like the rank, malnormality
- Quantitative study of finitely generated subgroups of a free group and analysis of related algorithms
  - Gromov : ”Most” of groups with a fixed number of generators and relations and “long enough” relation length are hyperbolic. But what does a typical group look like ?
  - Generic (or average) complexity of algorithms handling groups or elements of a group.

Introduction

- Free group and group presentations (any group is isomorphic to a quotient group of some free group).
- Study of algebraic properties by combinatorial methods
  - Graphical representation of subgroups : Stallings graphs
  - Combinatorial interpretation of parameters or properties like the rank, malnormality
- Quantitative study of finitely generated subgroups of a free group and analysis of related algorithms
  - Gromov : "Most" of groups with a fixed number of generators and relations and "long enough" relation length are hyperbolic. But what does a typical group look like ?
  - Generic (or average) complexity of algorithms handling groups or elements of a group.

Introduction

- Free group and group presentations (any group is isomorphic to a quotient group of some free group).
- Study of algebraic properties by combinatorial methods
  - Graphical representation of subgroups : Stallings graphs
  - Combinatorial interpretation of parameters or properties like the rank, malnormality
- Quantitative study of finitely generated subgroups of a free group and analysis of related algorithms
  - Gromov : ”Most” of groups with a fixed number of generators and relations and “long enough” relation length are hyperbolic. But what does a typical group look like ?
  - Generic (or average) complexity of algorithms handling groups or elements of a group.

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 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 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 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 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 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**.
- 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**.
- 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**.
- 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

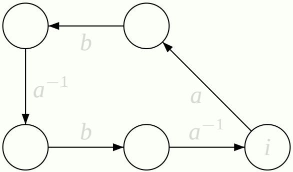
Let $Y = \{aba^{-1}ba^{-1}, b^2a^{-1}, b^3a^{-1}b^{-1}\}$.

Goal

To 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

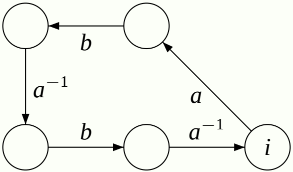
Let $Y = \{aba^{-1}ba^{-1}, b^2a^{-1}, b^3a^{-1}b^{-1}\}$.

Goal

To build a directed graph representing the free subgroup generated by Y

First step

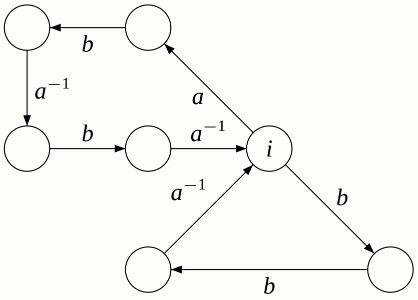
Build a directed cycle labeled with $aba^{-1}ba^{-1}$ the first element of Y



Stallings foldings

Second step

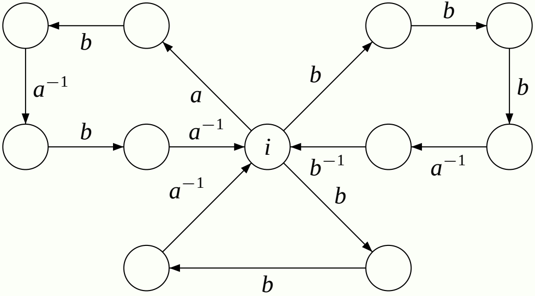
Build from the same vertex i a directed cycle labeled with b^2a^{-1} the second element of Y.



Stallings foldings

Third step

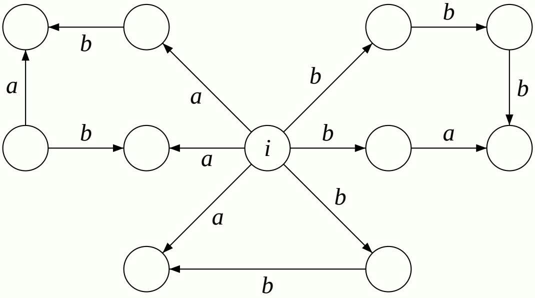
Build from the same vertex i a directed cycle labeled with $b^3a^{-1}b^{-1}$ the third and last element of Y.



Stallings foldings

Formal inverses

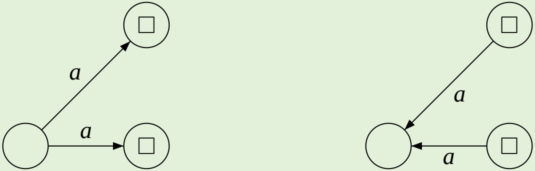
Reverse all edges labeled by a^{-1} are and replace their label by a.



Stallings foldings

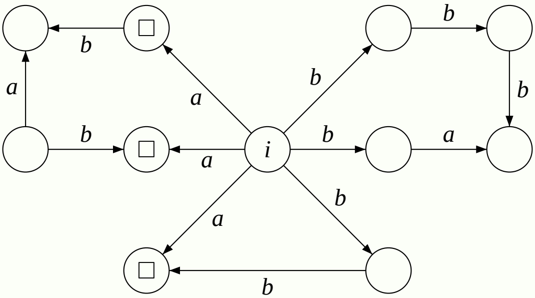
Foldings to obtain determinism and codeterminism

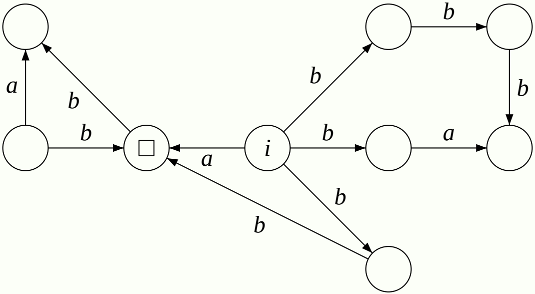
Apply as many times as possible the following rules of merging (or folding) :



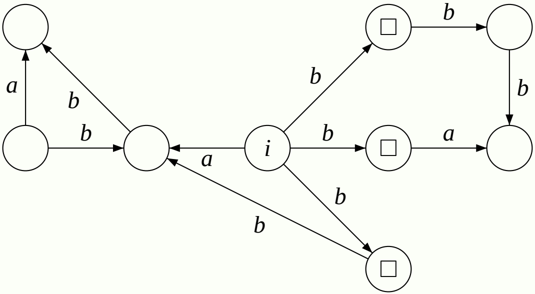
The result does not depend on the order in which the transformations are performed.

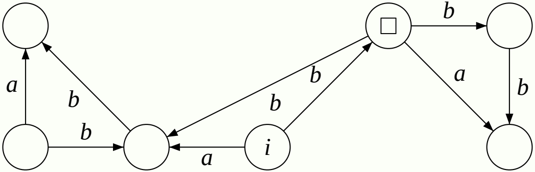
Stallings foldings - 1st folding



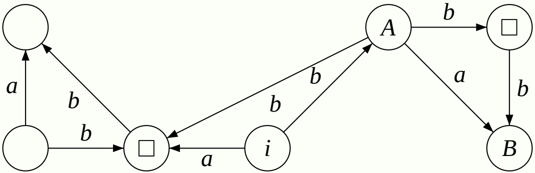


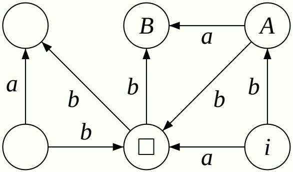
Stallings foldings - 2nd folding



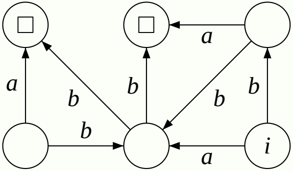


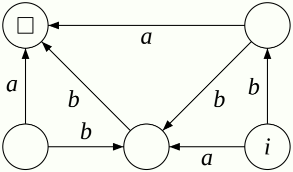
Stallings foldings - 3rd folding



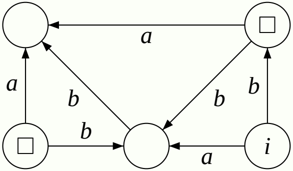


Stallings foldings - 4th folding



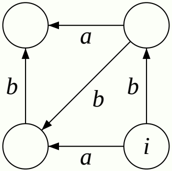


Stallings foldings - Last folding and Stallings graph



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*.

- 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

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

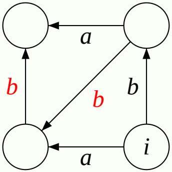
- One can check whether a (reduced) word belongs the subgroup or not.
  Check if there exists a cycle labeled by the word beginning in i
- One can compute a basis and the rank of the subgroup

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

  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.

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, 2010)
- What does the Stallings graph of such a random subgroup look like ?

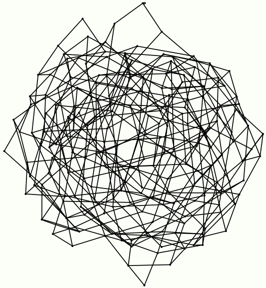


FIGURE: A random subgroup with 200 vertices for the graph-based distribution (The alphabet is of size 2).

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 Jitsukawa (2002), Ol'sanskiĭ (1992), …
- What does the Stallings graph of such a random subgroup look like ?

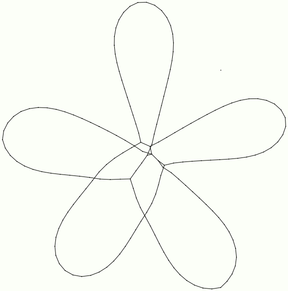
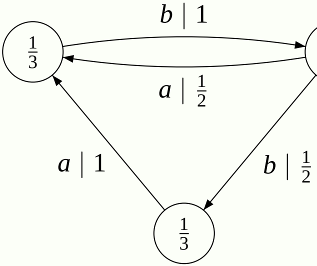


FIGURE: A random subgroup for the word-based distribution with 5 words of lengths at most 40 (The alphabet is of size 2.)

Markovian automata

- We use Markovian automata, which are kind of hidden Markov chains, with labels (letters) on edges to generate words of a given length.



- We just require that the underlying Markov chain is ergodic.

A generalized word-based distribution on subgroups

- Classical : k (fixed) uniform reduced words of length at most n
- k is not fixed anymore, it is a random variable K_n.
- The length of each word also follows a random variable L_n, with $\mathbb{E}[L_n] = n$.
- Each word is generated by a Markovian automaton.

A generalized word-based distribution on subgroups

- Classical : k (fixed) uniform reduced words of length at most n
- k is not fixed anymore, it is a random variable K_n.
- The length of each word also follows a random variable L_n, with $\mathbb{E}[L_n] = n$.
- Each word is generated by a Markovian automaton.

IV. Statistical properties of the random subgroups generated

Genericity

- 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 ∞.

Theorem (B., Nicaud, Weil 2012)

Most generic properties of the classical word-based model are still generic for the generalized word-based model under mild hypotheses.

Set mild hypotheses :

- Long words in average : $\mathbb{E}(L_n) = n$,
- No small words : Generically, $L_n > \mu(n)$, with $\lim \mu(n) = \infty$; e.g. $\mu(n) = \log^d(n)$ $(d > 0)$, n^d $(0 < d < 1)$, αn $(0 < \alpha < 1)$
- At most a polynomial number of generators : Generically, $K_n < \nu(n)$; e.g. $\nu(n) = K$ $(K > 1)$, $\log^d n$ $(d > 0)$, n^d $(d > 0)$
- The Markovian chain is ergodic

Genericity

- 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 ∞.

Theorem (B., Nicaud, Weil 2012)

Most generic properties of the classical word-based model are still generic for the generalized word-based model under mild hypotheses.

Set mild hypotheses :

- Long words in average : $\mathbb{E}(L_n) = n$,
- No small words : Generically, $L_n > \mu(n)$, with $\lim \mu(n) = \infty$; e.g. $\mu(n) = \log^d(n)$ $(d > 0)$, n^d $(0 < d < 1)$, αn $(0 < \alpha < 1)$
- At most a polynomial number of generators : Generically, $K_n < \nu(n)$; e.g. $\nu(n) = K$ $(K > 1)$, $\log^d n$ $(d > 0)$, n^d $(d > 0)$
- The Markovian chain is ergodic

Genericity

- 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 ∞.

Theorem (B., Nicaud, Weil 2012)

Most generic properties of the classical word-based model are still generic for the generalized word-based model under mild hypotheses.

Set mild hypotheses :

- Long words in average : $\mathbb{E}(L_n) = n$,
- No small words : Generically, $L_n > \mu(n)$, with $\lim \mu(n) = \infty$; e.g. $\mu(n) = \log^d(n)$ $(d > 0)$, n^d $(0 < d < 1)$, αn $(0 < \alpha < 1)$
- At most a polynomial number of generators : Generically, $K_n < \nu(n)$; e.g. $\nu(n) = K$ $(K > 1)$, $\log^d n$ $(d > 0)$, n^d $(d > 0)$
- The Markovian chain is ergodic

Properties of the random bases

Theorem (initial cancellation - common prefixes or suffixes)

Let T_n be the number of initial cancellations. Let $0 < \alpha < 1$ and let $\tau(n)$ be a function such that $\tau(n) \leq \alpha\mu(n)$ and $\lim \tau(n) = \infty$. Any one of the following conditions implies that $T_n \leq \tau(n)$ **generically** :

- $\nu(n)$ is bounded ;
- $\nu(n) = \mathcal{O}(\log^d n)$ for some $d > 0$, $\mathbb{P}[L_n < \mu(n)] = o(\frac{1}{\log^{2d} n})$ and $\tau(n)$ grows faster than $\log \log n$;
- $\nu(n) = \mathcal{O}(n^d)$ for some $d > 0$, $\mathbb{P}[L_n < \mu(n)] = o(n^{-2d})$ and $\tau(n)$ grows faster than $\log n$.

- With stronger hypotheses, we get information on error term
- Same kind of result for the multiple occurrences of long factors

Some Results

- The rank can be seen on Stallings graphs by computing $|E| - |V| + 1$
- Claim : the rank of a subgroup is generically its number of generators
- In particular, the rank is k in the classical model

- A subgroup H is malnormal when for every $x \notin H$, $x^{-1}Hx \cap H = \{1\}$
- On the Stallings graph of H : no non-trivial word u labels a loop on two distincts vertices of the graph
- Claim : generically, a random subgroup is malnormal

Some Results

- The rank can be seen on Stallings graphs by computing $|E| - |V| + 1$
- Claim : the rank of a subgroup is generically its number of generators
- In particular, the rank is k in the classical model

- A subgroup H is malnormal when for every $x \notin H$, $x^{-1}Hx \cap H = \{1\}$
- On the Stallings graph of H : no non-trivial word u labels a loop on two distincts vertices of the graph
- Claim : generically, a random subgroup is malnormal

Some More Results - Group presentation

- A set of cyclically reduced words $C = \{c_1, \ldots, c_k\}$ satisfies the small cancellation property $C'(\frac{1}{6})$, when if u is a factor of two distincts cyclic conjugates x_1 and x_2 of C, then $|u| \leq \min(\frac{1}{6}|x_1|\frac{1}{6}|x_2|)$.
- If a set of relators satisfies the $C'(\frac{1}{6})$ property then the presented group enjoys a lot of properties : it is torsion-free, word-hyperbolic, has solvable word problem, ...
- Gromov (1993) studied the case of an exponential number of long relators.

In our setting,

- Generically, reducing cyclically a random reduced word only remove a small number of letters
- Generically, a set of long reduced words satisfies the $C'(\frac{1}{6})$ property
- Generically, the quotient of a free group of finite rank by the normal closure of a random subgroup is torsion-free, word-hyperbolic, has solvable word problem, ...

Some More Results - Group presentation

- A set of cyclically reduced words $C = \{c_1, \ldots, c_k\}$ satisfies the small cancellation property $C'(\frac{1}{6})$, when if u is a factor of two distincts cyclic conjugates x_1 and x_2 of C, then $|u| \leq \min(\frac{1}{6}|x_1|\frac{1}{6}|x_2|)$.
- If a set of relators satisfies the $C'(\frac{1}{6})$ property then the presented group enjoys a lot of properties : it is torsion-free, word-hyperbolic, has solvable word problem, …
- Gromov (1993) studied the case of an exponential number of long relators.

In our setting,

- Generically, reducing cyclically a random reduced word only remove a small number of letters
- Generically, a set of long reduced words satisfies the $C'(\frac{1}{6})$ property
- Generically, the quotient of a free group of finite rank by the normal closure of a random subgroup is torsion-free, word-hyperbolic, has solvable word problem, …

Some More Results - Group presentation

- A set of cyclically reduced words $C = \{c_1, \ldots, c_k\}$ satisfies the small cancellation property $C'(\frac{1}{6})$, when if u is a factor of two distincts cyclic conjugates x_1 and x_2 of C, then $|u| \leq \min(\frac{1}{6}|x_1| \frac{1}{6}|x_2|)$.
- If a set of relators satisfies the $C'(\frac{1}{6})$ property then the presented group enjoys a lot of properties : it is torsion-free, word-hyperbolic, has solvable word problem, …
- Gromov (1993) studied the case of an exponential number of long relators.

In our setting,

- Generically, reducing cyclically a random reduced word only remove a small number of letters
- Generically, a set of long reduced words satisfies the $C'(\frac{1}{6})$ property
- Generically, the quotient of a free group of finite rank by the normal closure of a random subgroup is torsion-free, word-hyperbolic, has solvable word problem, …

Thank you for your attention !