On random subgroups of free groups

Pascal Weil

LaBRI, CNRS and Université de Bordeaux

Workshop FREC, May 2013

Outline

- Preliminaries
- Random subgroups given by a tuple of generators
- Random subgroups given by a Stallings graph
- Generalizations of the tuple model: Markovian automata
- Generalizations of the tuple model: Bernoulli-like models

Random generation of subgroups of free groups 1/2

- **A variety of motivations**

Random generation of subgroups of free groups 1/2

- **A variety of motivations**
- The generic properties of subgroups of free groups

Random generation of subgroups of free groups 1/2

- **A variety of motivations**
- The generic properties of subgroups of free groups
- The generic properties of subgroups of certain other groups (towards cryptography)

Random generation of subgroups of free groups 1/2

- **A variety of motivations**
- The generic properties of subgroups of free groups
- The generic properties of subgroups of certain other groups (towards cryptography)
- The generic properties of group presentations

Random generation of subgroups of free groups 1/2

- **A variety of motivations**
- The generic properties of subgroups of free groups
- The generic properties of subgroups of certain other groups (towards cryptography)
- The generic properties of group presentations
- The generic properties of (finitely presented) groups (harder. . .)

Random generation of subgroups of free groups 1/2

- **A variety of motivations**
- The generic properties of subgroups of free groups
- The generic properties of subgroups of certain other groups (towards cryptography)
- The generic properties of group presentations
- The generic properties of (finitely presented) groups (harder. . .)
- There are by now classic results in both directions: on subgroups and on presentations

Random generation of subgroups of free groups 2/2

- **Two approaches**

Random generation of subgroups of free groups 2/2

- **Two approaches**
- One can pick a set of generators for the subgroup, or a set of relators for the presentation: Gromov (*most groups are hyperbolic*), Champetier, Ol'shanskiĭ, Arzhantseva, Ollivier, Miasnikov, Schupp, Shpilrain, Jitsukawa, and many more...

Random generation of subgroups of free groups 2/2

- **Two approaches**
- One can pick a set of generators for the subgroup, or a set of relators for the presentation: Gromov (*most groups are hyperbolic*), Champetier, Ol'shanskiĭ, Arzhantseva, Ollivier, Miasnikov, Schupp, Shpilrain, Jitsukawa, and many more...
- Or one can pick directly a Stallings graph: Bassino, Martino, Ventura, Nicaud, Weil

Stallings graph of a subgroup of a free group

$F(A) =$ reduced words on alphabet $\tilde{A} = A \sqcup A^{-1}$

Stallings graph of a subgroup of a free group

$F(A) =$ reduced words on alphabet $\tilde{A} = A \sqcup A^{-1}$
A graphical representation of the subgroups of $F(A)$

Stallings graph of a subgroup of a free group

$F(A) =$ reduced words on alphabet $\tilde{A} = A \sqcup A^{-1}$
A graphical representation of the subgroups of $F(A)$
$\Gamma(H)$, the Stallings graph of a finitely generated subgroup H

Stallings graph of a subgroup of a free group

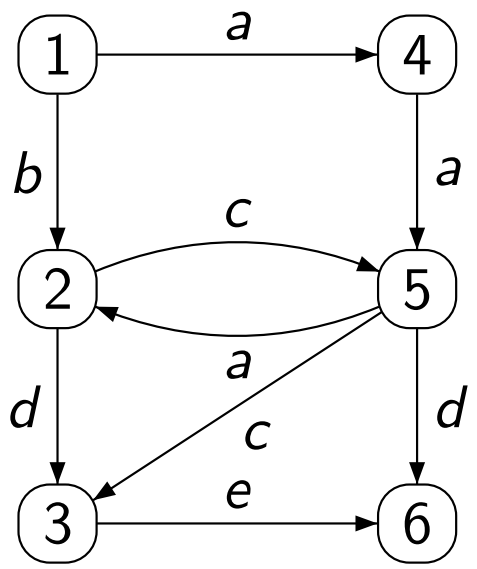
$F(A)$ = reduced words on alphabet $\tilde{A} = A \sqcup A^{-1}$
A graphical representation of the subgroups of $F(A)$
$\Gamma(H)$, the Stallings graph of a finitely generated subgroup H

$$H = \langle h_1, h_2, h_3, h_4 \rangle$$

$$h_1 = a^3 b^{-1}$$
$$h_2 = a^3 c a^{-2}$$
$$h_3 = a^2 c d^{-1} b^{-1}$$
$$h_4 = a^2 d e^{-1} d^{-1} b^{-1}$$

Stallings graph of a subgroup of a free group

$F(A)$ = reduced words on alphabet $\tilde{A} = A \sqcup A^{-1}$
A graphical representation of the subgroups of $F(A)$
$\Gamma(H)$, the Stallings graph of a finitely generated subgroup H



$$H = \langle h_1, h_2, h_3, h_4 \rangle$$

$$h_1 = a^3 b^{-1}$$
$$h_2 = a^3 c a^{-2}$$
$$h_3 = a^2 c d^{-1} b^{-1}$$
$$h_4 = a^2 d e^{-1} d^{-1} b^{-1}$$

Properties of interest (today!)

- Rank of a subgroup H. The rank of H is $|E| - |V| + 1$ (edges $-$ vertices $+ 1$ in $\Gamma(H)$)

Properties of interest (today!)

- Rank of a subgroup H. The rank of H is $|E| - |V| + 1$ (edges $-$ vertices $+ 1$ in $\Gamma(H)$)
- Malnormality of H: for all $x \notin H$, $H^x \cap H = 1$

Properties of interest (today!)

- Rank of a subgroup H. The rank of H is $|E| - |V| + 1$ (edges $-$ vertices $+ 1$ in $\Gamma(H)$)
- Malnormality of H: for all $x \notin H$, $H^x \cap H = 1$
- In $\Gamma(H)$, no word labels a loop at two different vertices

Properties of interest (today!)

- Rank of a subgroup H. The rank of H is $|E| - |V| + 1$ (edges $-$ vertices $+ 1$ in $\Gamma(H)$)
- Malnormality of H: for all $x \notin H$, $H^x \cap H = 1$
- In $\Gamma(H)$, no word labels a loop at two different vertices
- Small cancellation: a tuple $\vec{h} = (h_i)_i$ of cyclically reduced words has property $C'(\lambda)$ if, whenever a word u has two occurrences as a factor of elements of $\vec{h}$ and $\vec{h}^{-1}$, say in h_i and h_j, then $|u| < \lambda \ \min(|h_i|, |h_j|)$

Properties of interest (today!)

- Rank of a subgroup H. The rank of H is $|E| - |V| + 1$ (edges $-$ vertices $+ 1$ in $\Gamma(H)$)
- Malnormality of H: for all $x \notin H$, $H^x \cap H = 1$
- In $\Gamma(H)$, no word labels a loop at two different vertices
- Small cancellation: a tuple $\vec{h} = (h_i)_i$ of cyclically reduced words has property $C'(\lambda)$ if, whenever a word u has two occurrences as a factor of elements of $\vec{h}$ and $\vec{h}^{-1}$, say in h_i and h_j, then $|u| < \lambda \ \min(|h_i|, |h_j|)$
- Property $C'(\frac{1}{6})$ implies hyperbolicity of $\langle A \mid \vec{h} \rangle$

Random subgroups

- Defining randomness (in this talk)

Random subgroups

- Defining randomness (in this talk)
- Agree on a notion of size, with a finite number of subgroups at each size

Random subgroups

- Defining randomness (in this talk)
- Agree on a notion of size, with a finite number of subgroups at each size
- Agree on a distribution on the set of size n subgroups (uniform, or not)

Random subgroups

- Defining randomness (in this talk)
- Agree on a notion of size, with a finite number of subgroups at each size
- Agree on a distribution on the set of size n subgroups (uniform, or not)
- *One option*: the subgroup is given by a tuple of generators $\vec{h} = (h_i)_i$, the size is $\max h_i$

Random subgroups

- Defining randomness (in this talk)
- Agree on a notion of size, with a finite number of subgroups at each size
- Agree on a distribution on the set of size n subgroups (uniform, or not)
- *One option*: the subgroup is given by a tuple of generators $\vec{h} = (h_i)_i$, the size is $\max h_i$
- Must specify the length of the vector ; works well with presentations too ; several tuples yield the same subgroup

Random subgroups

- Defining randomness (in this talk)
- Agree on a notion of size, with a finite number of subgroups at each size
- Agree on a distribution on the set of size n subgroups (uniform, or not)
- *One option*: the subgroup is given by a tuple of generators $\vec{h} = (h_i)_i$, the size is $\max h_i$
- Must specify the length of the vector ; works well with presentations too ; several tuples yield the same subgroup
- *Another option*: the subgroup is given by its Stallings graph, the size is the number of vertices

Random subgroups

- Defining randomness (in this talk)
- Agree on a notion of size, with a finite number of subgroups at each size
- Agree on a distribution on the set of size n subgroups (uniform, or not)
- *One option*: the subgroup is given by a tuple of generators $\vec{h} = (h_i)_i$, the size is $\max h_i$
- Must specify the length of the vector ; works well with presentations too ; several tuples yield the same subgroup
- *Another option*: the subgroup is given by its Stallings graph, the size is the number of vertices
- Why not for presentations?

The few-generator model (Gromov, Ol'shanskii, Arzhantseva, Jutsikawa, and others): k generators, k fixed

- Draw uniformly at random $\vec{h} = (h_1, \ldots, h_k)$, reduced words of length at most n and consider $H = \langle \vec{h} \rangle$ as n tends to ∞

The few-generator model (Gromov, Ol'shanskii, Arzhantseva, Jutsikawa, and others): k generators, k fixed

- Draw uniformly at random $\vec{h} = (h_1, \ldots, h_k)$, reduced words of length at most n and consider $H = \langle \vec{h} \rangle$ as n tends to ∞
- *Use counting arguments on reduced words*

The few-generator model (Gromov, Ol'shanskii, Arzhantseva, Jutsikawa, and others): k generators, k fixed

- Draw uniformly at random $\vec{h} = (h_1, \ldots, h_k)$, reduced words of length at most n and consider $H = \langle \vec{h} \rangle$ as n tends to ∞
- *Use counting arguments on reduced words*
- Exponentially generically, very little initial cancellation (= cancellation of prefixes and suffixes): less than αn for any α

The few-generator model (Gromov, Ol'shanskii, Arzhantseva, Jutsikawa, and others): k generators, k fixed

- Draw uniformly at random $\vec{h} = (h_1, \ldots, h_k)$, reduced words of length at most n and consider $H = \langle \vec{h} \rangle$ as n tends to ∞
- *Use counting arguments on reduced words*
- Exponentially generically, very little initial cancellation (= cancellation of prefixes and suffixes): less than αn for any α
- A central tree, and k loops joining its leaves

The few-generator model (Gromov, Ol'shanskii, Arzhantseva, Jutsikawa, and others): k generators, k fixed

- Draw uniformly at random $\vec{h} = (h_1, \ldots, h_k)$, reduced words of length at most n and consider $H = \langle \vec{h} \rangle$ as n tends to ∞
- *Use counting arguments on reduced words*
- Exponentially generically, very little initial cancellation (= cancellation of prefixes and suffixes): less than αn for any α
- A central tree, and k loops joining its leaves
- $h_1, \ldots, h_k$ freely generate H (rank k)

The few-generator model (Gromov, Ol'shanskii, Arzhantseva, Jutsikawa, and others): k generators, k fixed

- Draw uniformly at random $\vec{h} = (h_1, \ldots, h_k)$, reduced words of length at most n and consider $H = \langle \vec{h} \rangle$ as n tends to ∞
- *Use counting arguments on reduced words*
- Exponentially generically, very little initial cancellation (= cancellation of prefixes and suffixes): less than αn for any α
- A central tree, and k loops joining its leaves
- $h_1, \ldots, h_k$ freely generate H (rank k)
- "uniqueness" of the basis of H

The few-generator model (Gromov, Ol'shanskii, Arzhantseva, Jutsikawa, and others): k generators, k fixed

- Draw uniformly at random $\vec{h} = (h_1, \ldots, h_k)$, reduced words of length at most n and consider $H = \langle \vec{h} \rangle$ as n tends to ∞
- *Use counting arguments on reduced words*
- Exponentially generically, very little initial cancellation (= cancellation of prefixes and suffixes): less than αn for any α
- A central tree, and k loops joining its leaves
- $h_1, \ldots, h_k$ freely generate H (rank k)
- "uniqueness" of the basis of H
- H is malnormal

The few-generator model (Gromov, Ol'shanskii, Arzhantseva, Jutsikawa, and others): k generators, k fixed

- Draw uniformly at random $\vec{h} = (h_1, \ldots, h_k)$, reduced words of length at most n and consider $H = \langle \vec{h} \rangle$ as n tends to ∞
- *Use counting arguments on reduced words*
- Exponentially generically, very little initial cancellation (= cancellation of prefixes and suffixes): less than αn for any α
- A central tree, and k loops joining its leaves
- $h_1, \ldots, h_k$ freely generate H (rank k)
- "uniqueness" of the basis of H
- H is malnormal
- Restricting to cyclically reduced words: $C'(\lambda)$ for any $\lambda < 1$: $G = \langle A \mid \vec{h} \rangle$ is hyperbolic

The density model (Gromov, Champetier, Olshanskii, Ollivier, . . .): exponential number of relators

- Fix $d < 1$, draw uniformly at random a tuple $\vec{h} = (h_1, \ldots, h_k)$ of density d in the sphere of radius n: roughly $(2r-1)^{dn}$ cyclically reduced words of length n, consider $G = \langle A \mid \vec{h} \rangle$ as n tends to ∞

The density model (Gromov, Champetier, Olshanskii, Ollivier, . . .): exponential number of relators

- Fix $d < 1$, draw uniformly at random a tuple $\vec{h} = (h_1, \ldots, h_k)$ of density d in the sphere of radius n: roughly $(2r-1)^{dn}$ cyclically reduced words of length n, consider $G = \langle A \mid \vec{h} \rangle$ as n tends to ∞
- Using counting arguments again: generically

The density model (Gromov, Champetier, Olshanskii, Ollivier, . . .): exponential number of relators

- Fix $d < 1$, draw uniformly at random a tuple $\vec{h} = (h_1, \ldots, h_k)$ of density d in the sphere of radius n: roughly $(2r-1)^{dn}$ cyclically reduced words of length n, consider $G = \langle A \mid \vec{h} \rangle$ as n tends to ∞
- Using counting arguments again: generically
- if $d > \frac{1}{2}$, $|G| \leq 2$ — there will be words in $\vec{h}$ which differ only in their last letter (some variant of the birthday paradox)

The density model (Gromov, Champetier, Olshanskii, Ollivier, . . .): exponential number of relators

- Fix $d < 1$, draw uniformly at random a tuple $\vec{h} = (h_1, \ldots, h_k)$ of density d in the sphere of radius n: roughly $(2r-1)^{dn}$ cyclically reduced words of length n, consider $G = \langle A \mid \vec{h} \rangle$ as n tends to ∞
- Using counting arguments again: generically
- if $d > \frac{1}{2}$, $|G| \leq 2$ — there will be words in $\vec{h}$ which differ only in their last letter (some variant of the birthday paradox)
- If $d < \frac{\lambda}{2}$, $\vec{h}$ satisfies $C'(\lambda)$, and if $d > \frac{\lambda}{2}$, $\vec{h}$ does not satisfy $C'(\lambda)$

The density model (Gromov, Champetier, Olshanskii, Ollivier, . . .): exponential number of relators

- Fix $d < 1$, draw uniformly at random a tuple $\vec{h} = (h_1, \ldots, h_k)$ of density d in the sphere of radius n: roughly $(2r-1)^{dn}$ cyclically reduced words of length n, consider $G = \langle A \mid \vec{h} \rangle$ as n tends to ∞
- Using counting arguments again: generically
- if $d > \frac{1}{2}$, $|G| \leq 2$ — there will be words in $\vec{h}$ which differ only in their last letter (some variant of the birthday paradox)
- If $d < \frac{\lambda}{2}$, $\vec{h}$ satisfies $C'(\lambda)$, and if $d > \frac{\lambda}{2}$, $\vec{h}$ does not satisfy $C'(\lambda)$
- If $d < \frac{1}{12}$, G is hyperbolic

The density model (Gromov, Champetier, Olshanskii, Ollivier, . . .): exponential number of relators

- Fix $d < 1$, draw uniformly at random a tuple $\vec{h} = (h_1, \ldots, h_k)$ of density d in the sphere of radius n: roughly $(2r-1)^{dn}$ cyclically reduced words of length n, consider $G = \langle A \mid \vec{h} \rangle$ as n tends to ∞
- Using counting arguments again: generically
- if $d > \frac{1}{2}$, $|G| \leq 2$ — there will be words in $\vec{h}$ which differ only in their last letter (some variant of the birthday paradox)
- If $d < \frac{\lambda}{2}$, $\vec{h}$ satisfies $C'(\lambda)$, and if $d > \frac{\lambda}{2}$, $\vec{h}$ does not satisfy $C'(\lambda)$
- If $d < \frac{1}{12}$, G is hyperbolic
- In fact, if $d < \frac{1}{2}$, G is hyperbolic — by a higher-dimensional counting argument (on van Kampen diagrams)

Use Stallings graphs to draw fg subgroups (Bassino, Martino, Nicaud, Ventura, Weil)

- Stallings graphs are in bijection with fg subgroups, so draw uniformly at random a Stallings graph with n vertices

Use Stallings graphs to draw fg subgroups (Bassino, Martino, Nicaud, Ventura, Weil)

- Stallings graphs are in bijection with fg subgroups, so draw uniformly at random a Stallings graph with n vertices
- and consider what happens when n tends to ∞

Use Stallings graphs to draw fg subgroups (Bassino, Martino, Nicaud, Ventura, Weil)

- Stallings graphs are in bijection with fg subgroups, so draw uniformly at random a Stallings graph with n vertices
- and consider what happens when n tends to ∞
- But... how *do* we draw a Stallings graph at random?

Stallings graphs as combinatorial structures

- a size n subgroup is a tuple of partial injections $[n] \to [n]$, one for each $a \in A$: given by the a-labeled edges in $\Gamma(H)$ – subject to certain conditions

Stallings graphs as combinatorial structures

- a size n subgroup is a tuple of partial injections $[n] \to [n]$, one for each $a \in A$: given by the a-labeled edges in $\Gamma(H)$ – subject to certain conditions
- Draw independently these partial injections

Stallings graphs as combinatorial structures

- a size n subgroup is a tuple of partial injections $[n] \to [n]$, one for each $a \in A$: given by the a-labeled edges in $\Gamma(H)$ – subject to certain conditions
- Draw independently these partial injections
- A partial injection is a disjoint union of orbits that are either cycles, or sequences

Stallings graphs as combinatorial structures

- a size n subgroup is a tuple of partial injections $[n] \to [n]$, one for each $a \in A$: given by the a-labeled edges in $\Gamma(H)$ – subject to certain conditions
- Draw independently these partial injections

- A partial injection is a disjoint union of orbits that are either cycles, or sequences
- Compute the distribution of sizes of orbits (cycles and sequences), and the distribution of cycles vs. sequences for each size of orbits

Stallings graphs as combinatorial structures

- a size n subgroup is a tuple of partial injections $[n] \to [n]$, one for each $a \in A$: given by the a-labeled edges in $\Gamma(H)$ – subject to certain conditions
- Draw independently these partial injections

- A partial injection is a disjoint union of orbits that are either cycles, or sequences
- Compute the distribution of sizes of orbits (cycles and sequences), and the distribution of cycles vs. sequences for each size of orbits
- Draw a size m of an orbit, decide whether it is a cycle or a sequence; and draw another random partial injection of size $n - m$

Stallings graphs as combinatorial structures

- a size n subgroup is a tuple of partial injections $[n] \to [n]$, one for each $a \in A$: given by the a-labeled edges in $\Gamma(H)$ – subject to certain conditions
- Draw independently these partial injections
- It may happen that the resulting graph is not connected, or that it has vertices of degree 1 (not acceptable in Stallings graphs)

Stallings graphs as combinatorial structures

- a size n subgroup is a tuple of partial injections $[n] \to [n]$, one for each $a \in A$: given by the a-labeled edges in $\Gamma(H)$ – subject to certain conditions
- Draw independently these partial injections

- It may happen that the resulting graph is not connected, or that it has vertices of degree 1 (not acceptable in Stallings graphs)
- Either situation is generically negligible, so a rejection algorithm will work in an average of $1 + o(1)$ rounds [BNW]

Counting edges [BNW]

- Main tool: exponential generating series and analytic combinatorics

Counting edges [BNW]

- Main tool: exponential generating series and analytic combinatorics
- We can study the distribution of the number of sequences in a size n partial injection

Counting edges [BNW]

- Main tool: exponential generating series and analytic combinatorics
- We can study the distribution of the number of sequences in a size n partial injection
- Expected number of sequences: $\mathbb{E}(\mathit{sequence}) = \sqrt{n}$ with standard deviation $o(\sqrt{n})$

Counting edges [BNW]

- Main tool: exponential generating series and analytic combinatorics
- We can study the distribution of the number of sequences in a size n partial injection
- Expected number of sequences: $\mathbb{E}(\mathit{sequence}) = \sqrt{n}$ with standard deviation $o(\sqrt{n})$
- Expected number of a-labeled edges: $n - \sqrt{n}$ (whereas in the word-based distribution, Stallings graph have few edges)

Counting edges [BNW]

- Main tool: exponential generating series and analytic combinatorics
- We can study the distribution of the number of sequences in a size n partial injection
- Expected number of sequences: $\mathbb{E}(sequence) = \sqrt{n}$ with standard deviation $o(\sqrt{n})$
- Expected number of a-labeled edges: $n - \sqrt{n}$ (whereas in the word-based distribution, Stallings graph have few edges)
- Expected rank of H:

$$\mathbb{E}(rank(H)) = \mathbb{E}(edges) - n + 1 = (r-1)n - r\sqrt{n} + 1$$

with standard deviation $o(\sqrt{n})$

Malnormality is negligible [BMNVW]

- Recall: H is *not* malnormal if and only if some word u labels a loop at two distinct vertices in $\Gamma(H)$

Malnormality is negligible [BMNVW]

- Recall: H is *not* malnormal if and only if some word u labels a loop at two distinct vertices in $\Gamma(H)$
- Study the distribution of the lengths of cycles and of the number of cycles in a size n partial injection

Malnormality is negligible [BMNVW]

- Recall: H is *not* malnormal if and only if some word u labels a loop at two distinct vertices in $\Gamma(H)$
- Study the distribution of the lengths of cycles and of the number of cycles in a size n partial injection
- With probability equivalent to $1 - \frac{1}{\sqrt{n}}$, each letter a labels several cycles, or one cycle of length at least 2

Malnormality is negligible [BMNVW]

- Recall: H is *not* malnormal if and only if some word u labels a loop at two distinct vertices in $\Gamma(H)$
- Study the distribution of the lengths of cycles and of the number of cycles in a size n partial injection
- With probability equivalent to $1 - \frac{1}{\sqrt{n}}$, each letter a labels several cycles, or one cycle of length at least 2
- Malnormality is negligible, with probability $\mathcal{O}(n^{-\frac{r}{2}})$

Groups presented by a Stallings graph are generically trivial

- The idea: instead of giving a finite set of relators, as a k-tuple of words, let us give instead the Stallings graph Γ of a fg subgroup H of relators: $G = \langle A \mid \Gamma \rangle$

Groups presented by a Stallings graph are generically trivial

- The idea: instead of giving a finite set of relators, as a k-tuple of words, let us give instead the Stallings graph Γ of a fg subgroup H of relators: $G = \langle A \mid \Gamma \rangle$
- Study the distribution of the lengths of cycles in a partial injection

Groups presented by a Stallings graph are generically trivial

- The idea: instead of giving a finite set of relators, as a k-tuple of words, let us give instead the Stallings graph Γ of a fg subgroup H of relators: $G = \langle A \mid \Gamma \rangle$
- Study the distribution of the lengths of cycles in a partial injection
- Generically, the gcd of the lengths of the cycles of a partial injection is 1

Groups presented by a Stallings graph are generically trivial

- The idea: instead of giving a finite set of relators, as a k-tuple of words, let us give instead the Stallings graph Γ of a fg subgroup H of relators: $G = \langle A \mid \Gamma \rangle$
- Study the distribution of the lengths of cycles in a partial injection
- Generically, the gcd of the lengths of the cycles of a partial injection is 1
- Generically, each letter $a \in A$ is in the normal subgroup generated by H:

Groups presented by a Stallings graph are generically trivial

- The idea: instead of giving a finite set of relators, as a k-tuple of words, let us give instead the Stallings graph Γ of a fg subgroup H of relators: $G = \langle A \mid \Gamma \rangle$
- Study the distribution of the lengths of cycles in a partial injection
- Generically, the gcd of the lengths of the cycles of a partial injection is 1
- Generically, each letter $a \in A$ is in the normal subgroup generated by H:
- Generically, $G = \langle A \mid \Gamma \rangle = 1$

Generalizing the tuple model, Markovian automata 1/2

- Allow the length of the tuple $\vec{h}$ to grow with n (polynomially, exponentially, etc.)

Generalizing the tuple model, Markovian automata 1/2

- Allow the length of the tuple $\vec{h}$ to grow with n (polynomially, exponentially, etc.)
- Allow a non uniform distribution of the words of given length using a Markovian scheme

Generalizing the tuple model, Markovian automata 1/2

- Allow the length of the tuple $\vec{h}$ to grow with n (polynomially, exponentially, etc.)
- Allow a non uniform distribution of the words of given length using a Markovian scheme
- Take an ordinary (deterministic) finite state automaton: states, transitions labeled by letters in $\tilde{A}$,

Generalizing the tuple model, Markovian automata 1/2

- Allow the length of the tuple $\vec{h}$ to grow with n (polynomially, exponentially, etc.)
- Allow a non uniform distribution of the words of given length using a Markovian scheme
- Take an ordinary (deterministic) finite state automaton: states, transitions labeled by letters in $\tilde{A}$,
- and add probability weights on the transitions – in such a way that, at each state q, the sum of probabilities of the transitions out of state q is equal to 1.

Generalizing the tuple model, Markovian automata 1/2

- Allow the length of the tuple $\vec{h}$ to grow with n (polynomially, exponentially, etc.)
- Allow a non uniform distribution of the words of given length using a Markovian scheme
- Take an ordinary (deterministic) finite state automaton: states, transitions labeled by letters in $\tilde{A}$,
- and add probability weights on the transitions – in such a way that, at each state q, the sum of probabilities of the transitions out of state q is equal to 1.
- For each n, this gives a probability law on the set of words of length n

Generalizing the tuple model, Markovian automata 2/2

- Example: the (uniform) distribution on all reduced words

Generalizing the tuple model, Markovian automata 2/2

- Example: the (uniform) distribution on all reduced words
- Example: the (uniform) distribution on all positive words

Generalizing the tuple model, Markovian automata 2/2

- Example: the (uniform) distribution on all reduced words
- Example: the (uniform) distribution on all positive words
- Example: the (uniform) distribution on the geodesics of $PSL_2(\mathbb{Z}) = \langle a, b \mid a^2, b^3 \rangle$: all reduced words without a squared letter

Generalizing the tuple model, Markovian automata 2/2

- Example: the (uniform) distribution on all reduced words
- Example: the (uniform) distribution on all positive words
- Example: the (uniform) distribution on the geodesics of $PSL_2(\mathbb{Z}) = \langle a, b \mid a^2, b^3 \rangle$: all reduced words without a squared letter
- Usually require ergodicity of the Markovian automaton, that is, *strong connectedness* and *the loops have relatively prime lengths*

The properties of the few-relator model are preserved

- Assume an ergodic Markovian automaton and use probabilistic arguments (rather than counting)

The properties of the few-relator model are preserved

- Assume an ergodic Markovian automaton and use probabilistic arguments (rather than counting)
- If $\vec{h}$ consists of **sub-exponentially many** reduced words of length at most n and $H = \langle \vec{h} \rangle$, then super-polynomially generically:

The properties of the few-relator model are preserved

- Assume an ergodic Markovian automaton and use probabilistic arguments (rather than counting)
- If $\vec{h}$ consists of **sub-exponentially many** reduced words of length at most n and $H = \langle \vec{h} \rangle$, then super-polynomially generically:
- $\Gamma(H)$ has a central tree of linear height, and consists of one loop for each h_i, connecting the leaves of the tree

The properties of the few-relator model are preserved

- Assume an ergodic Markovian automaton and use probabilistic arguments (rather than counting)
- If $\vec{h}$ consists of **sub-exponentially many** reduced words of length at most n and $H = \langle \vec{h} \rangle$, then super-polynomially generically:
- $\Gamma(H)$ has a central tree of linear height, and consists of one loop for each h_i, connecting the leaves of the tree
- $\vec{h}$ freely generates H

The properties of the few-relator model are preserved

- Assume an ergodic Markovian automaton and use probabilistic arguments (rather than counting)
- If $\vec{h}$ consists of **sub-exponentially many** reduced words of length at most n and $H = \langle \vec{h} \rangle$, then super-polynomially generically:
- $\Gamma(H)$ has a central tree of linear height, and consists of one loop for each h_i, connecting the leaves of the tree
- $\vec{h}$ freely generates H
- H is malnormal

The properties of the few-relator model are preserved

- Assume an ergodic Markovian automaton and use probabilistic arguments (rather than counting)
- If $\vec{h}$ consists of **sub-exponentially many** reduced words of length at most n and $H = \langle \vec{h} \rangle$, then super-polynomially generically:
- $\Gamma(H)$ has a central tree of linear height, and consists of one loop for each h_i, connecting the leaves of the tree
- $\vec{h}$ freely generates H
- H is malnormal
- $\vec{h}$ satisfies $C'(\lambda)$

The properties of the few-relator model are preserved

- Assume an ergodic Markovian automaton and use probabilistic arguments (rather than counting)
- If $\vec{h}$ consists of **sub-exponentially many** reduced words of length at most n and $H = \langle \vec{h} \rangle$, then super-polynomially generically:
- $\Gamma(H)$ has a central tree of linear height, and consists of one loop for each h_i, connecting the leaves of the tree
- $\vec{h}$ freely generates H
- H is malnormal
- $\vec{h}$ satisfies $C'(\lambda)$
- All this *exponentially generically* if $\vec{h}$ consists of polynomially many reduced words

Digression: a very small central tree if k generators, k fixed

- Back to k generators, taken uniformly at random among reduced words of length at most n

Digression: a very small central tree if k generators, k fixed

- Back to k generators, taken uniformly at random among reduced words of length at most n
- Initial cancellation (= size of the central tree) is generically much smaller than linear:

Digression: a very small central tree if k generators, k fixed

- Back to k generators, taken uniformly at random among reduced words of length at most n
- Initial cancellation (= size of the central tree) is generically much smaller than linear:
- generically, it is smaller than any function $\mu(n)$ such that $\lim \mu(n) = \infty$ (*e.g.* $\log n$, or $\log \log n$, or ...)

Digression: a very small central tree if k generators, k fixed

- Back to k generators, taken uniformly at random among reduced words of length at most n
- Initial cancellation (= size of the central tree) is generically much smaller than linear:
- generically, it is smaller than any function $\mu(n)$ such that $\lim \mu(n) = \infty$ (*e.g.* $\log n$, or $\log \log n$, or ...)
- super-polynomially generically if $\log n = o(\mu(n)$ (*e.g.* $\log^{1+\varepsilon} n$, or $\log n \log \log n$, or ...)

What about the properties of the density model? 1/2

- Interesting results using an almost memoryless (Bernoulli-like) model

What about the properties of the density model? 1/2

- Interesting results using an almost memoryless (Bernoulli-like) model
- A Markovian automaton where the same spectrum of probabilities $\vec{p} = (p_b)_b \in B$ is available out of every state (even if not ergodic)

What about the properties of the density model? 1/2

- Interesting results using an almost memoryless (Bernoulli-like) model
- A Markovian automaton where the same spectrum of probabilities $\vec{p} = (p_b)_b \in B$ is available out of every state (even if not ergodic)
- Examples: all reduced words; all geodesics of $PSL(2, \mathbb{Z})$

What about the properties of the density model? 1/2

- Interesting results using an almost memoryless (Bernoulli-like) model
- A Markovian automaton where the same spectrum of probabilities $\vec{p} = (p_b)_b \in B$ is available out of every state (even if not ergodic)
- Examples: all reduced words; all geodesics of $PSL(2, \mathbb{Z})$
- Two parameters seem to play a role: $\vec{p}_{max} = \max_{b \in B} p_b$ and $\vec{p}_e = \prod_{b \in B} p_b^{p_b}$ (which is $-\log(entropy)$ of the Bernoulli source). Note that $\vec{p}_e \leq \vec{p}_{max}$ and the two are equal if $\vec{p}$ is uniform

What about the properties of the density model? 2/2

- If $\vec{h}$ is a vector of cyclically reduced words of length n and $G = \langle A \mid \vec{h} \rangle$, then:

What about the properties of the density model? 2/2

- If $\vec{h}$ is a vector of cyclically reduced words of length n and $G = \langle A \mid \vec{h} \rangle$, then:
- If $\vec{h}$ has $\vec{p_e}^{\,-dn}$ elements with $d > \frac{1}{2}$, then G is degenerate

What about the properties of the density model? 2/2

- If $\vec{h}$ is a vector of cyclically reduced words of length n and $G = \langle A \mid \vec{h} \rangle$, then:
- If $\vec{h}$ has $\vec{p}_e{}^{-dn}$ elements with $d > \frac{1}{2}$, then G is degenerate
- If $\vec{h}$ has $\vec{p}_e{}^{-dn}$ elements with $d > \frac{\lambda}{2}$, then **not** $C'(\lambda)$

What about the properties of the density model? 2/2

- If $\vec{h}$ is a vector of cyclically reduced words of length n and $G = \langle A \mid \vec{h} \rangle$, then:
- If $\vec{h}$ has $\vec{p}_e{}^{-dn}$ elements with $d > \frac{1}{2}$, then G is degenerate
- If $\vec{h}$ has $\vec{p}_e{}^{-dn}$ elements with $d > \frac{\lambda}{2}$, then **not** $C'(\lambda)$
- If $\vec{h}$ has $\vec{p}_{max}{}^{-dn}$ elements with $d < \frac{\lambda}{2}$, then $C'(\lambda)$

What about the properties of the density model? 2/2

- If $\vec{h}$ is a vector of cyclically reduced words of length n and $G = \langle A \mid \vec{h} \rangle$, then:
- If $\vec{h}$ has $\vec{p}_e{}^{-dn}$ elements with $d > \frac{1}{2}$, then G is degenerate
- If $\vec{h}$ has $\vec{p}_e{}^{-dn}$ elements with $d > \frac{\lambda}{2}$, then **not** $C'(\lambda)$
- If $\vec{h}$ has $\vec{p}_{max}{}^{-dn}$ elements with $d < \frac{\lambda}{2}$, then $C'(\lambda)$
- What if the number of elements is between $\vec{p}_{max}{}^{-\frac{n}{12}}$ and $\vec{p}_e{}^{-\frac{n}{12}}$?

What about the properties of the density model? 2/2

- If $\vec{h}$ is a vector of cyclically reduced words of length n and $G = \langle A \mid \vec{h} \rangle$, then:
- If $\vec{h}$ has $\vec{p_e}^{\,-dn}$ elements with $d > \frac{1}{2}$, then G is degenerate
- If $\vec{h}$ has $\vec{p_e}^{\,-dn}$ elements with $d > \frac{\lambda}{2}$, then **not** $C'(\lambda)$
- If $\vec{h}$ has $\vec{p}_{max}^{\,-dn}$ elements with $d < \frac{\lambda}{2}$, then $C'(\lambda)$
- What if the number of elements is between $\vec{p}_{max}^{\,-\frac{n}{12}}$ and $\vec{p_e}^{\,-\frac{n}{12}}$?
- And between $\vec{p_e}^{\,-\frac{n}{12}}$ and $\vec{p_e}^{\,-\frac{n}{2}}$?

Thank you for your attention!