Measuring in free groups and amalgamated products of groups

Vladimir N. Remeslennikov
Alexei G. Myasnikov
Elizaveta V. Frenkel

Omsk
August 21, 2009

Outline

Object

- (1) Finitely generated free groups;
- (2) Amalgamated products $A_C * B$, where A, B, C as in (1).

Approach

Generic estimates of subsets of mentioned above objects.

Basis

- A. V. Borovik, A. G. Myasnikov and V. N. Remeslennikov, *Multiplicative measures on free groups*, Intern. J. of Algebra and Computation, 13 (2003), no. 6, pp. 705 – 731;
- E. Frenkel, A. G. Myasnikov and V. N. Remeslennikov, *Regular sets and counting in free groups*, to appear;
- E. Frenkel, A. G. Myasnikov and V. N. Remeslennikov, *Amalgamated products of groups II: Generation of random normal forms and estimates*, to appear;
- ....

Measuring in free groups

There are two known methods for measuring of subsets in free groups:

- with a help of **asymptotic densities**;
- with a help of **random walks**.

Asymptotic densities

Let $F = F(X)$ be a free group with basis $X = \{x_1, \ldots, x_m\}$.
Let R, L be subsets of the free group F, $R \subseteq L$ and $S_k = \{ w \in F \mid |w| = k \}$ the sphere of radius k in F. The fraction

$$f_k(R, L) = \frac{|R \cap S_k|}{|L \cap S_k|}$$

is the frequency of elements from R among the words of length k in F (relative to L).

Asymptotic densities

The asymptotic density $\rho(R)$ of R is defined by

$$\rho(R, L) = \limsup_{k \to \infty} f_k(R, L).$$

R is called generic (in L) if $\rho(R, L) = 1$, and negligible if $\rho(R, L) = 0$. If, in addition, there exists a positive constant $\delta < 1$ such that

$$1 - \delta^k < f_k(R, L) < 1$$

for all sufficiently large k then R is called exponentially generic (relative to L). Meanwhile, if $f_k(R, L) < \delta^k$ for large enough k then R is exponentially negligible.

Random walks on Cayley graph

Consider a no-return random walk W_s ($s \in (0,1]$) on the Cayley graph $C(F,X)$ of F with respect to the generating set X. We start at the identity element 1 and either do nothing with probability s (and return value 1 as the output of our random word generator), or move to one of the $2m$ adjacent vertices with equal probabilities $(1-s)/2m$. If we are at a vertex $v \neq 1$, we either stop at v with probability s (and return the value v as the output), or move, with probability $\frac{1-s}{2m-1}$, to one of the $2m-1$ adjacent vertices lying away from 1, thus producing a new freely reduced word $vx_i^{\pm 1}$. Since the Cayley graph $(C(F,X)$ is a tree and we never return to the word we have already visited, it is easy to see that the probability $\mu_s(w)$ for our process to terminate at a word w is given by the formula

$$\mu_s(w) = \frac{s(1-s)^{|w|}}{2m \cdot (2m-1)^{|w|-1}} \quad \text{for } w \neq 1 \tag{1}$$

and

$$\mu_s(1) = s. \tag{2}$$

Are we happy?

Question

We are started from the most common and easiest group, aren't we?

Are we happy?

Question

We are started from the most common and easiest group, aren't we?

Answer

Actually, we are not. At least, not completely.

Regular sets

Let now R be a subset in F and $n_k = n_k(R) = |R \cap S_k|$ be the number of elements of length k in R. The sequence $\{n_k(R)\}_{k=0}^{\infty}$ is called the *spherical growth sequence* of R. We assume, for the sake of minor technical convenience, that R does not contain the identity element 1, so that $n_0 = 0$. It is easy to see now that

$$\mu_s^*(R) = \sum_{k=0}^{\infty} n_k t^k.$$

One can view $\mu^*(R)$ as the generating function of the spherical growth sequence of the set R in variable t which is convergent for each $t \in [0, 1)$.

Regular sets

If the set R is an (unambiguous) context free language then, by a classical theorem of Chomsky and Schutzenberger (1963), the generating function $\mu^*(R) = \sum n_k t^k$, and hence the function $\mu(R)$, are algebraic functions of s.
Recall, that function y is called algebraic in n variables, if it solves a polynomial equation in $n+1$ variables:

$$P(y, x^1, \ldots, x^n) = 0$$

.

Moreover, if R is regular then $\mu(R)$ is a rational function with rational coefficients.
An important class of example of algebraic subsets is provided by:

[Theorem, Muller and Schupp, 2001]

A normal subgroup $R \triangleleft F$ is a context free language if and only if the factor group F/R is free-by-finite. For the derived subgroup $R = [F, F]$ of the free group of rank 2, the measure $\mu(R)$ is not an algebraic function.

Regular sets

It is well known that singular points of an algebraic function are either poles or branching points. Since $\mu(R)$ is bounded for $s \in (0,1)$, this means that, for a context-free set R, the function $\mu(R)$ has no singularity at 0 or has a branching point at 0. A standard result on analytic functions allows us to expand $\mu_s(R)$ as a fractional power series:

$$\mu_s(R) = m_0 + m_1 s^{1/n} + m_2 s^{2/n} + \cdots ,$$

n being the branching index.

If R is regular, than we actually have the usual power series expansion:

$$\mu_s(R) = m_0 + m_1 s + m_2 s^2 + \cdots ;$$

in particular, $\mu(R)$ can be analytically extended in the neighbourhood of 0 and R is smooth.

Regular sets

By numbering the states by numbers $1, \ldots, n$, we can associate with the automaton $\mathcal{A}$ its *adjacency matrix* A by taking an $n \times n$ matrix and writing the number of arrows from state i to state j in the position (i, j). It is easy to see that the number of different paths of length l from state i to state j is $(A^l)_{ij}$ and the measure of the set of labels on these paths is $t^l(A^l)_{ij}$. Let I and J be the sets of initial and accept states. If we denote $T = tA$ then it follows that

$$\mu_s^*(\mathcal{L}) = \sum_{i \in I, j \in J} ((T)_{ij} + (T^2)_{ij} + \cdots).$$

In particular, the series on the right converges for every given s. Denote by $B = T + T^2 + \cdots$ the matrix with entries from the ring of formal power series $\mathbb{R}[[t]]$, then, obviously,

$$\mu^*(\mathcal{L}) = \sum_{i \in I, j \in J} B_{ij}$$

and

$$B = (I_n - T)^{-1} - I_n.$$

Regular sets

Since we consider the automaton $\mathcal{A}^*$ where an initial state is never an accept state, we can simplify the formula and write

$$\mu^*(\mathcal{L}) = \sum_{i \in I, j \in J} ((I_n - T)^{-1})_{ij}.$$

We come to the following formula:

$$\mu^*(\mathcal{L}) = \sum_{i \in I, j \in J} ((I_n - T)^{-1} - I_n)_{ij}.$$

We have as a corollary the following result.

Theorem

The measure $\mu^*(R)$ (and hence the probability measure $\mu(R)$) of a regular subset of F is a rational function in t (and hence in s) with rational coefficients.

Regular sets

[Theorem,??]

Let R be a regular subset of F. Then the following estimate for $f_k(R)$ holds:

$$f_k \sim P(k)\beta^k + O(B^k),$$

where $P(k)$ is polynomial, β is maximal eigenvalue of T and B: $0 < B < \beta$.

But in practical needs this estimates doesn't really work because of different reasons:

- It is difficult to estimate maximal eigenvalue β of matrix T;
- Sometimes it doesn't work ...

Amalgamated products

Goal

To describe some generic properties of normal forms in $A_C * B$.

Why?

Amalgamated product of groups

There are a lot of explanations of our interest, for example:

- (1) Daily leaving needs of algorithmic problems;
- (2) Several results on "generic decidability" of well-known algorithmic problems.

Stratification of the set of inputs

For example, if cyclically reduced forms of elements are regular, then the Conjugacy Search Problem in amalgamated product is decidable:

[Theorem, BMR, 2005]

Let $G = A_C * B$ be a free product of finitely presented groups A and B amalgamated over a finitely generated subgroup C. Assume also that there are algorithms for A and B, solving the following problems:

- Coset Representative Search Problem for the subgroup C.
- Cardinality Search Problem for $\Phi(Sub(C), A)$ in A and for $\Phi(Sub(C), B) inB$.
- Conjugacy Search Problem in A and in B.
- Conjugacy Membership Search Problem for C in A and B.

Then the Conjugacy Search Problem in G is decidable for elements from the set of all conjugates in G of cyclically reduced regular elements.

[Corollary, BMR, 2005]

Let $G = A_C * B$ be a free product of free groups A and B with amalgamated finitely generated subgroup C. Then the Conjugacy Search Problem in G is decidable for elements from the set of all conjugates in G of cyclically reduced regular elements.

Normal forms of elements of amalgamated product of groups

Let $G = A \underset{C}{*} B$ be a free product of a free group A with a finite basis X and a group B with a finite basis Y, amalgamated over a subgroup C of finite rank. There are four main methods to represent an element of G :

- 1) by a word in the alphabet $X \bigcup X^{-1} \bigcup Y \bigcup Y^{-1}$;
- 2) in the reduced form;
- 3) in the cyclically reduced form;
- 4)in the canonical normal form.

Canonical normal forms

Recall that an element g in G written in the *canonical normal form*, if:

$$g = cp_1 \dots p_k, \quad \text{where} \quad k = 0, 1, 2, \dots, \tag{3}$$

where $c \in C$, $p_i \in (S \bigcup T) \setminus 1$, $i = 1, \dots, k$ and neighboring elements in (3) are lying in different factors.

The normal form of an element g in G is unique up to the equality of words p_i, $i = 0, \dots, k$ inside the groups A and B.

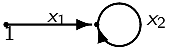
Work with normal forms

Good fortune

All natural subsets we have to deal with are rather "good" (i.e. regular).

Subgroup graphs, coset graphs and Shreier Systems of Representatives

Let $F = F(X)$ be a free group with basis $X = \{x_1, \ldots, x_n\}$. Let $C = \langle h_1, \ldots, h_m \rangle$ be a subgroup of F generated by finitely many elements $h_1, \ldots, h_m \in F$.
One can associate with C *the subgroup graph* $\Gamma = \Gamma_C$. For our purposes, the crucial property of Γ is that it is a directed finite connected graph with edges labeled by elements from X. For example, this is the graph for the subgroup generated by $x_1 x_2 x_1^{-1}$:

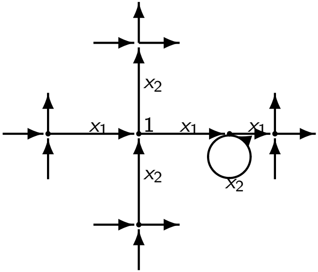


Pic. 1.

Reading labels on all paths in Γ without backtracking which start and end at 1, we get all reduced words which belong to C.

The *extended subgroup graph* Γ^* of Γ is made from Γ by the following procedure: for every vertex v of Γ and every letter $x \in X$ such that there is no edge in Γ which starts at v and has label x, we attach to v an edge labeled x which leads outside of Γ, and then continue this edge by attaching a tree with every possible label in such a way that the resulting graph is folded.

Here is the fragment of the graph Γ^* for the previous example $C = \left\langle x_1 x_2 x_1^{-1} \right\rangle$:



Pic. 2.

Simple observation

- Reading labels on all paths in T^{ast} without backtracking which start at 1 and end at T^{ast}, we get all reduced words which belong some Shreier transversal $S_{T^{ast}}$ of C in F
- (Subgroup C has a finite index in F) $\Leftrightarrow$ (the subgroup graph Γ isomorphic to the extended graph Γ^*)

Remark

Here T^* is a maximal subtree of Γ^*. Transversal S is called Shreier, if every initial segment of a representative from S again belongs to S.

Subgroup graphs, coset graphs and Shreier Systems of Representatives

It is allows to "identify" elements from a given Shreier transversal S of C with the vertices of the graph Γ^*.

- A representative $s \in S$ is called *internal* if corresponding to s path ends at $V(\Gamma)$. By S_{int} we denote the set of all internal representatives in S;
- Elements from $S_{ext} = S \setminus S_{int}$ are called *external* representatives in S.

Subgroup graphs, coset graphs and Shreier Systems of Representatives

Definition

Let S be a transversal of C in A.

- A representative $s \in S$ is called *singular* if it belongs to the generalized normalizer $N_F^*(C) = \{f \in F | f^{-1}Cf \bigcap C \neq 1\}$ of C. All other representatives from S are called *regular*. By S_{sing} and, respectively, S_{reg} we denote the subsets of singular and regular representatives in S.

- A representative $s \in S$ is called *stable* if $sc \in S$ for any $c \in C$. By S_{st} we denote the set of all stable representatives in S, and the set of all *unstable* elements by $S_{\mathrm{nst}} = S \setminus S_{\mathrm{st}}$.

Normal form is unstable (or singular) if it contains some unstable (or singular) elements.

Subgroup graphs, coset graphs and Shreier

A *L- cone* $C_L(u)$ defined by (or based at) an element $u \in F$ is a set of all reduced words in L that start with u.

We will write $C(u)$ for $C_F(u)$.

Subgroup graphs, coset graphs and Shreier Systems of Representatives

[Lemma, FMR]

Let S be a Shreier transversal for C, so $S = S_T$ for some maximal subtree T of Γ. Then the following statements hold:

- 1) $|S_{\rm int}| = |V(\Gamma)|$.
- 2) $S_{\rm ext}$ is the union of finitely many coni that are centered at vertices in $\Gamma^* \smallsetminus \Gamma$ which are immediate neighbours of vertices from Γ.
- 3) $S_{\rm sing}$ is a finite union of double cosets $Cs_1s_2^{-1}C$ of C, where $s_1, s_2 \in S_{\rm int}$.
- 4) $S_{\rm nst}$ is a finite union of left cosets of C of the type $s_1s_2^{-1}C$, where $s_1, s_2 \in S_{\rm int}$.

Subgroup graphs, coset graphs and Shreier Systems of Representatives

[Lemma, FMR]

Let C be a finitely generated subgroup of infinite index in F and S a Schreier transversal for C. Then the following hold:

- 1) The set of singular representatives S_{sin} is exponentially negligible in S.
- 2) The set S_{uns} of unstable representatives is exponentially negligible in S.

Problems

But even in such a lucky situation it is still difficult to measure what you want!

For example:
Asymptotic classification of regular subsets of F:

[Theorem]

- 1) Every negligible regular subset of F is strongly negligible.
- 2) A regular subset of F is thick if and only if its prefix closure contains a cone.
- 3) Every regular subset of F is either thick or strongly negligible.

Problems

But what should we do in "relativized" case? What about analogue to previous theorem?

Problem

How to estimate a measure of an arbitrary subset $R \subseteq L$, where $R, L \subseteq F$ relative not only a free group F, but relative to L?

Realistic Problem

How to estimate a measure of an regular subset $R \subseteq L$, where $R, L \subseteq F$ relative to regular subset L?

First step

That was precisely the same estimates that we have done for the set of all unstable and singular representatives in Shreier transversal S.

Problems

Observation

This is exactly the same thing that we should do with a set of normal forms of elements in $G = A_C * B$!

Example

Let $G = A_C * B$ and S and T are Shreier transversals of C in A and B correspondingly. We have to estimate the set of all canonical normal forms $\mathcal{NF}$:

$$\mathcal{NF} = C \underset{t}{\circ} (S * T).$$

This set is regular.

T

he set of all singular representatives in this case can be written as

$$\mathcal{NF}_{sin} = C \underset{t}{\circ} (S_{sin} * T_{sin})$$

and therefore also regular (where S_{sin} and T_{sin} are singular representatives in S and T.

Deciding of problems

On this way two following seminal results was shown:

[Theorem, FMR]

Let R be a regular subset of a prefix-closed regular set L in a free group F. Then either the prefix closure $\overline{R}$ of R in L contains a non-small $L-$cone or $\overline{R}$ is exponentially λ_L-measurable.

Deciding of problems

[Theorem, FMR]

Let $G = A \underset{C}{*} B$ be an amalgamated product, where A, B, C are free groups of finite ranks. If C of infinite index in both A and B, then sets of all unstable $\mathcal{NF}_{nr}$ and all singular $\mathcal{NF}_{ns}$ normal forms are exponentially $\mathcal{NF}-$measurable.