Amalgamated products of groups: generation of normal forms

Liza Frenkel, Moscow State University

Manresa
July 11, 2011

Introduction

Paul Schupp in his lectures gave a review on a generic approach to computations in groups.
Namely, let I be a set of inputs with size function σ.
Define S_n, the sphere of radius n, by $S_n = \{w \mid w \in I, \sigma(w) \leq n\}$.

Let $f_n(R) = \dfrac{|R \cap S_n|}{|S_n|}$, where $|X|$ denotes the size of a set X.

Then, $R \subset I$ is said to have asymptotic density α, written $\rho(R) = \alpha$, if

$$\overline{\lim_{n\to\infty}} f_n(R) = \alpha.$$

Introduction

If the limit $\lim_{n \to \infty} f_n(R)$ exists and equal to 1, then R is called generic;

and if R has asymptotic density 0 it is negligible.

We say that R is exponentially generic if $|\rho(R) - f_n(R)| < \delta^n$, for some constant $0 < \delta < 1$ and all sufficiently large n.

Meanwhile, if $f_n(R) < \delta^n$ for large enough n then R is exponentially negligible.

Introduction

Let $\mathcal{P}$ be a problem. A partial algorithm, $\mathcal{A}$, for $\mathcal{P}$ generically solves $\mathcal{P}$ if the halting set $H_{\mathcal{A}}$ of $\mathcal{A}$ is a generic subset of the set of inputs I. In this case we say that $\mathcal{P}$ is generically solvable.

Introduction

Generic approach to an algorithm usually allows us to stratify the set of inputs onto three strata: generic subset, negligible subset and subset of intermediate density.

However, this approach is not sensitive enough. For instance, all finite sets and some infinite sets can have the same density.

The paper "Multiplicative measures on free groups"(Borovik, Miasnikov, Remeslennikov) introduced another approach to measuring in groups. Namely, a so-called $\lambda-$ measure of subsets $R \subseteq F = F(X)$ was defined, where $F(X)$ is a finitely generated free group and

$$\lambda(R) = \sum_{n=0}^{\infty} f_n(R), \text{ where } f_n(R) = \frac{|R \cap S_n|}{|S_n|}.$$

We say that R is *λ-measurable*, if $\lambda(R)$ is finite.

A set R is termed *exponentially λ-measurable* if $f_n(R) \leq q^n$ for all sufficiently large n.

The generating function for R is a formal series in $R[[t]]$:

Introduction

The main goal of this series of talks is to show some methods of calculation of different types of measures in combinatorial group theory, especially in free constructions of groups.

In particular, I will lay out several methods of calculation of $\lambda-$measure and generating function of groups based on the automata theory and the Perron-Frobenius theory. We use a generic approach to algorithms as well.

Introduction

From our (further “OUR = F, Miasnikov, Remeslennikov”) point of view, an algorithmic problem in G has a satisfactory solution if it has:

(i) satisfactory normal forms for elements of G;

(ii) convenient generators of random elements of G in normal forms;

(iii) atomic and probability measures on F for measuring elements and subsets of F;

(iv) results on stratification of inputs of algorithms (i.e. normal forms) at least on two strata: stratum of regular (or stable) elements on which algorithms works fast (i.e. in polynomial time) and another one of singular and unstable elements, on which the result of the algorithms work is unknown or it works slowly;

(v) asymptotic and probabilistic tools of estimation of these strata.

Introduction

Titles:

1. Amalgamated products of groups: generation of normal forms.
2. Measures on free products, free products with amalgamation and measuring of normal forms.
3. Search Algorithmic Problems and Algorithms.
4. Counting in free groups.
5. Asymptotic classification of regular sets.

Introduction

Literature:

- 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, p. 705 – 731.

- A. V. Borovik, A. G. Myasnikov and V. N. Remeslennikov, *The Conjugacy Problem in Amalgamated Products I: Regular Elements and Black Holes*, Intern. J. of Algebra and Computation, 17 (2007), no. 7, p. 1301 - 1335

- R. Gilman, A. G. Miasnikov, A. D. Myasnikov, A. Ushakov *Report on generic case complexity,* Herald of Omsk University, (2007), Special Issue p. 103 – 110

- E. Frenkel, A. G. Myasnikov and V. N. Remeslennikov, *Regular sets and counting in free groups*, Combinatorial and Geometric Group Theory, series “Trends in Mathematics”, p. 93 – 118, 2010 Birkhauser Verlag Basel/Switzerland

- E. Frenkel, A. G. Myasnikov and V. N. Remeslennikov, *Amalgamated Products of Groups II: Measures of Random Normal Forms*, to appear in "Fundamental and applied mathemtics”

Introduction

Let A, B, C be groups and $\varphi : C \to A$, $\psi : C \to B$ be monomorphisms.
Then, one can define a group $G = A \underset{C}{*} B$ called the amalgamated product of A and B over C (the monomorphisms φ, ψ are usually suppressed from notation).

Suppose A and B are given by the presentations $A =< X \mid R_A = 1 >$, $B =< Y \,|R_B \ = 1 >$ and a generating set Z for the group C. We denote $\varphi(z) = u_z(x),\ \psi(z) = v_z(y)$ and then the group G has a presentation

$$G =< X \cup Y | R_A = 1, R_B = 1, u_z(x) = v_z(y), (z \in Z) > .$$

Introduction

Let A, B, C be free groups of finite ranks.

Denote by S and T fixed systems of right coset representatives of C in A and B and let the representative of C is the identity element 1.

For $g \in (A \cup B) \setminus C$, we define $F(g) = A$ if $g \in A$ and $F(g) = B$ if $g \in B$.

Representation of elements in G

- 1) in the **freely-reduced** form (in the alphabet $X \bigcup X^{-1} \bigcup Y \bigcup Y^{-1}$);
- 2) in the **reduced form**;
- 3) in the **canonical normal form** provided by systems of representatives S and T for a subgroup C in A and B correspondingly;
- 4) every element in the reduced form is a conjugate of an element in the **cyclically reduced form**.

Freely-reduced normal forms

Every element $g \in G$ can be written in a *freely-reduced normal form*

$$g = g_1 g_2 \dots g_n,$$

where $g_1, \dots, g_n$ are reduced words in $X \cup X^{-1}$ or in $Y \cup Y^{-1}$ and if $F(g_i) = A$, then $F(g_{i+1}) = B$ and vice versa.
This form is not unique (even the number n of multipliers can vary ad libitum).

Reduced normal forms

An element $g \in G$ is written in a *reduced normal form* if

$$g = g_1 g_2 \cdots g_k,$$

where $g_i \in (A \bigcup B) \setminus C$ and $F(g_i) \neq F(g_{i+1}),\ i = 1, \ldots, k$, if $k \geq 1$ and

$$g = c, \quad c \in C \text{ if } k = 0.$$

This form may not be unique, but the number k is uniquely determined by g.

Canonical normal forms

An element $g \in G$ is written in a **canonical normal form** provided by systems of representatives S and T for a subgroup C in A and B , if

$$g = cp_1 \dots p_k$$

where $c \in C,\ \ p_i \in (S \bigcup T)\ \setminus \{1\}$, and $F(p_i) \neq F(p_{i+1}),\ \ i = 1, \dots, l,\ \ l \geq 0$.

This form is unique up to representation of elements in A, B, C.

Cyclically reduced normal forms

A reduced form of an element $g \in G$ in a form

$$g = cg_1 \dots g_k$$

is called *cyclically reduced normal form*, if:

(i) $k = 0$, i.e. $g = c \in C$;

(ii) $k = 1$, then every element $g \in A \bigcup B$, that is not a conjugate of an element in C;

(iii) $k > 1$, then every g, such as k is even.

Random Generator of a canonical normal forms

The procedure RG_{cnf} depends on:

a given probability distribution $\theta : \mathbb{N} \bigcup \{0\} \to \mathbb{R}^+$,

two (fixed) probability distributions μ_A and μ_B on $A \setminus C$ and $B \setminus C$,

two probability distributions $\mu_{A,C}, \mu_{B,C}$, where C is viewed as a subgroup of A or B correspondingly.

Random Generator of a canonical normal form

INPUT: A natural number k chosen with respect to θ.

OUTPUT: A random canonical normal form v of length $s(v) = k$.

COMPUTATIONS:

1) Choose A or B with equal probability $\frac{1}{2}$ and do the following:
    a) if the choice in 1) is A then choose randomly an element c in C with respect to the probability $\mu_{A,C}$;
    b) if the choice in 1) is B then choose randomly an element c in C with respect to the probability $\mu_{B,C}$;

    If $k = 0$ then output $v = c$.

Random Generator of a canonical normal form

2) If $k \geq 1$

   a) if the choice in 1) is A then choose randomly an element $g_1 \in A \setminus C$ with the probability $\mu_A(Cg_1)$;
   represent it as $g_1 = cs_1$, where $c \in C$, $s_1 \in S$

   repeat this choosing alternatively $g_i \in A \smallsetminus C$ and $g_{i+1} \in B \smallsetminus C$ with probabilities $\mu_A(Cg_i)$, $\mu_B(Cg_{i+1})$ and represent $g_i = c_i s_i$, $g_{i+1} = c_{i+1} t_{i+1}$ until k elements are constructed.

   Output $v = cs_1 t_2 s_3 t_4 \ldots p_k$.

   b) if the choice in 1) is B then choose randomly an element $g_1 \in B \setminus C$ with the probability $\mu_B(Cg_1)$
   represent it as $g_1 = ct_1$, where $c \in C$, $t_1 \in T$
   repeat as in 2a).

   Output $v = ct_1 s_2 t_3 s_4 \ldots p_k$.

Measures

- Measures of subsets in free groups.
- Measures of free products of sets:
  - $\mathcal{EF} = A * B$;
  - $\mathcal{RF} = (A \setminus C) * (B \setminus C)$;
  - $\mathcal{CNF} = C \underset{t}{\circ} (S * T)$.

Measures

Consider a certain set F, and let $\mathcal{P}(F)$ be the set of all subsets of F and $\mathcal{A} \subset \mathcal{P}(\mathcal{F})$. A real non-negative additive function $\mu : \mathcal{A} \to \mathbb{R}^+$ is called a *pseudo-measure on F* if $\mathcal{A}$ is closed under complements.

If $\mathcal{A}$ is a subalgebra of $\mathcal{P}(F)$ then μ is a *measure*.

Let $F = F(X)$ be a free group. Let μ be an atomic pseudo-measure on F. Recall, that a measure μ on the countable set P is called *atomic*, if every subset $Q \subseteq P$ is measurable; or equivalently if $\mu(Q) = \sum\limits_{q \in Q} \mu(q)$.

Measures on elements

Consider a no-return random walk W_s ($s \in (0,1]$) on the Cayley graph $C(F,X)$, where $|X| = m$.

We start at the root vertex 1 and either do nothing with probability s and return value 1 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,

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 $vx_i^{\pm 1}$.

Measures on elements

The probability $\mu_s(w)$ for our process to terminate at a word w is given by the formula

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

and

$$\mu_s(1) = s.$$

By $\mu(R)$ we denote the function

$$\begin{aligned} \mu(R) : (0,1) &\rightarrow \mathbb{R} \\ s &\mapsto \mu_s(R) = \sum_{w \in R} \mu_s(w); \end{aligned}$$

and we call it a measure of R with respect to the family of distributions μ_s.

Measuring of canonical normal forms

Suppose A, B and C are finitely generated free groups.

The probability to obtain the canonical normal form $v = cp_1 p_2 \dots p_k$, $k \geq 0$ on the output of our generator is equal to

$$\mu_k(v) = \frac{1}{2}\mu_C(c)\mu_1(p_1)\mu_2(p_2)\dots\mu_k(p_k),$$

where $\mu_i(p_i) = \mu_{F(p_i)}(Cp_i)$ and $\mu_C(c) = \mu_{A,C}$ if C is viewed as a subgroup of A, and $\mu_C(c) = \mu_{B,C}$ otherwise.

Clearly, μ_k is an atomic probability measure on the set $\mathcal{NF}_k$ of all normal forms of length k.

Now, one can introduce a probability measure μ on the set $\mathcal{NF}$ of all normal forms setting

$$\mu(v) = \theta(k)\mu_k(v)$$

if $v \in \mathcal{NF}_k$, where $\theta(k)$ is a fixed probability distribution on $\mathbf{N}$.

$L-$measure in free groups

For subsets R, L of F define their *size ratio* at length k by

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

The *relative asymptotic density* of R relative to L is defined by

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

R is called *negligible* relative to L if $\rho(R, L) = 0$.

A set R is termed *exponentially L-negligible* if there exists a positive constant $q < 1$ $f_k(R, L) \leq q^k$ for all sufficiently large k.

A set R is termed *exponentially L-generic* if $1 - q^k \leq f_k(R, L) < 1$ for all sufficiently large k.

λ_L-measure in free groups

For subsets R, L of F there is another natural measure defined by random walks on an automaton for R coherent with L.

$$\lambda_L(R) = \sum_{w\in R} \lambda_L(w) = \sum_{k=0}^{\infty} f'_k(R, L),$$

where

$$f'_k(R, L) = \sum_{w\in R\cap S_k} \lambda_L(w),$$

and $\lambda_L(w), f'_k(R, L)$ defined by a random walk on an automaton for L.

λ_L-measure in free groups

We say that R is *λ_L-measurable*, if $\lambda_L(R)$ is finite.

A set R is termed *exponentially λ_L-measurable*, if $f'_k(R, L) \leq q^k$ for all sufficiently large k.

For every $w \in F$ the set $C_L(w) = L \cap C(w)$ is called an L-cone.

A cone $C_L(w)$ is called *L-small*, if it is exponentially λ_L-measurable.

Theorem (Frenkel, Miasnikov, Remeslennikov, 2009). 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.

Free product of subsets

Let $F = A * B$ be a free product of finitely generated groups A and B, R be a nonempty subset of A, and S be a nonempty subset of B. Then the *free product* $R * S$ is the set of all elements in F having the form

$$f = f_1 f_2 \dots f_k,$$

where $k = 1, 2, \dots;\ f_i \in R \bigcup S,\ i = \{1, \dots k\},\ f_i \neq 1$ if $i \geq 2$ and for all $i \in \{1,\ k-1\}$ elements f_i and f_{i+1} belong to different factors of F.
The number $k = s(f)$ is called the *syllable length* of f.

Free product of subsets

Let μ_A and μ_B be atomic pseudo-measures on A and B correspondingly and $\mu_A(1) = \mu_B(1)$. We also fix a probability distribution $\theta : \mathbb{N} \to \mathbb{R}^+$, i.e. $\sum\limits_{n=1}^{\infty} \theta(n) = 1$.
We define an atomic (pseudo) measure μ on G in the following way.
Let

$$f = f_1 \dots f_k, \text{ where} \tag{1}$$

$f_i \in A \bigcup B,\ i = 1, \dots, k,\ f_i \neq 1$, if $i \geq 2$ and for all $i \in 1, \dots, k-1$ elements f_i and f_{i+1} belong to different factors of F.

Set by definition,

$$\mu(f) = \frac{1}{2}\theta(k)\mu_{F_1}(f_1)\dots\mu_{F_k}(f_k), \tag{2}$$

where $F_i = A$, if $f_i \in A$, or $F_i = B$, if $f_i \in B$; $i = 1, \dots, k$.

If $R \subseteq F$ then

$$\mu(R) = \sum_{f \in R} \mu(f).$$

We will say that R is a *$\mu-$measurable* set, if $\mu(R) < \infty$.

Free products of subsets

Denote by M_φ the set of all $\mu-$measurable subsets of F :

$$M_\varphi = \{R \subseteq F | \mu(R) < \infty\}$$

Example. Let μ_A, μ_B be pseudo-measures on A and B, defined by the cardinality functions on A and B and let $\theta(n) = \dfrac{6}{\pi^2 n^2}$ be a probability distribution on $\mathbb{N}$. Then $M_{\mu_A} = \mathcal{F}(A)$ and $M_{\mu_B} = \mathcal{F}(B)$, where $\mathcal{F}(A)$ and $\mathcal{F}(B)$ are the sets of all finite subsets of A and B. But $M_\mu \supset \mathcal{F}(F)$ is a strict inclusion (where $\mathcal{F}(F)$ is a set of all finite subsets of F. Indeed, let $R \subseteq F$ and $R_k = R \bigcap F_k$. Then $R \in M_\mu$ iff the series $\sum \dfrac{|R_k|}{k^2}$ converges.

Bidimensional asymptotic density

Let $T = A_0 * B_0 \subseteq F = A * B$ and suppose Q is a subset of T. For a pair of natural numbers (n,k) we define a (n, k)-*ball*:

$$T_{n,k} = \{f = f_1 \dots f_k \in T : s(f) = k, |f_i| \leq n, i = 1, \dots, k\}.$$

We call $T = \bigcup\limits_{k=0,n=0}^{\infty} T_{n,k}$ the *bidimensional decomposition*.

A function $\rho_{\mu}^{n,k}(Q, T) = \dfrac{\mu(Q \cap T_{n,k})}{\mu(T_{n,k})}$ is called the frequency function of Q relative to T.

Bidimensional asymptotic density

By *direction function* $d(n, k)$ we mean one-to-one correspondence between n and k which parametrize a path from $(1, 1)$ to (∞, ∞) such that the arguments n and k tend to ∞ while $d(n, k) \to \infty$.

Let $d(n, k)$ be some direction function.

Asymptotic behavior of Q relative to T we will characterize by a *bidimensional asymptotic density*:

$$\rho_\mu(Q, T) = \overline{\lim_{d(n,k)\to\infty}} \rho_\mu^{n,k}(Q, T).$$

If this limit exists and does not depend on a choice of a direction function, we denote it by $\rho^e_\mu(Q, T)$.

Bidimensional asymptotic density

We say that Q is *μ-generic* relative to T , if $\rho^e_\mu(Q, T) = 1$,

and *μ-negligible* relative to T, if $\rho^e_\mu(Q, T) = 0$.

A set Q is said to be *exponentially $\mu-$negligible* relative to T if Q is μ-negligible and there exists a positive constant $\delta < 1$ such that $\rho^{n,k}_\mu(Q, T) \leq \delta^k$ for all sufficiently large k.

A set Q is termed *exponentially $\mu-$generic* relative to T if Q is $\mu-$generic and there exists a positive constant $\delta < 1$ such that $1 - \delta^k < \rho^{n,k}_\mu(Q, T) < 1$ for large enough k.

Stratification of normal forms

Inspired by needs of the classical algorithmic problems of combinatorial group theory, we must know some properties of the obtained elements. For example, if cyclically reduced forms of elements are regular, then the Conjugacy Search Problem in the amalgamated product of groups is decidable:

Theorem (Borovik, Miasnikov, Remeslennikov, 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 $\Phi(Sub(C), B)$ in B.
- 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.

Stratification of normal forms

Corollary (Borovik, Miasnikov, Remeslennikov, 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.

In this way we subdivide the set of inputs of the algorithms into two parts: "good" and "bad" inputs.

On the "good" part our algorithm works fast (for example, in polynomial time) and on the "bad" part it works slowly or does not work at all.

The main idea of this stratification of the algorithm's inputs is to show that the "good" strata is large enough (i.e. generic) in the set of all inputs and the bad one is a very small set (or so called negligible set).

Stratification of representatives

Let S be a fixed system of right coset representatives 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 $S_{\mathrm{nst}} = S \setminus S_{\mathrm{st}}$.

Asymptotic estimates

An element $g \in G$ in normal form is called *regular* if at least one of the elements g_i or p_i; $i = 1, \ldots, s(g)$ is regular.

Otherwise g is called *singular*.

An element $g \in G$ in normal form is called *stable* if at least one of the elements g_i or p_i; $i = 1, \ldots, s(g)$ is stable.
Otherwise g is called *unstable*.

Asymptotic estimates

Denote $\mathcal{NF}_{\mathrm{sin}}$ the set of all singular normal forms; $\mathcal{NF}_{\mathrm{uns}}$ the set of all unstable normal forms;
$\mathcal{NF}_{\mathrm{s}}$ the set of all stable normal forms;
$\mathcal{NF}_{\mathrm{r}}$ the set of all regular normal forms.

Let $\mathcal{EF}$ be the set of all freely-reduced normal forms of elements in G;
$\mathcal{RF}$ be the set of all reduced normal forms in G;
$\mathcal{CNF}$ be the set of all canonical normal forms in G;
$\mathcal{CRF}$ be the set of all cyclically reduced normal forms in G.

Asymptotic estimates: λ_L-measure

Theorem A. (F, Miasnikov, Remeslennikov). Let $G = A \underset{C}{*} B$ be an amalgamated product, where A, B, C are free groups of finite rank. Then for every set of normal forms $\mathcal{NF} = \{\mathcal{EF}, \mathcal{RF}, \mathcal{CNF}, \mathcal{CRF}\}$

(i) If C has a finite index in A and in B, then every normal form is singular and unstable, i.e. $\mathcal{NF}_{\rm sin} = \mathcal{NF}_{\rm uns} = \mathcal{NF}$;

(ii) If C of infinite index either in A or in B, then $\mathcal{NF}_r$ and $\mathcal{NF}_s$ are exponentially $\mu-$generic relative to $\mathcal{NF}$, and $\mathcal{NF}_{\rm sin}$ and $\mathcal{NF}_{\rm uns}$ are exponentially $\mu-$negligible relative to $\mathcal{NF}$ in the following cases:

  (ii.1) μ is defined by pseudo-measures μ_A and μ_B, which are cardinality functions on A and B correspondingly; in this case ρ_μ is a bidimensional asymptotic density;

  (ii.2) μ is defined by atomic probability measures $\mu_{A,l}$ and $\mu_{B,l}$ on A and B correspondingly; in this case ρ^C is a bidimensional Cesaro asymptotic density.

Asymptotic estimates: λ_L−measure

Theorem B. (F, Miasnikov, Remeslennikov). Let $G = A \underset{C}{*} B$ be an amalgamated product, where A, B, C are free groups of finite rank. If C of infinite index either in A or in B, then sets of all unstable $\mathcal{NF}_{\mathrm{uns}}$ and all singular $\mathcal{NF}_{\mathrm{sin}}$ normal forms are exponentially $\lambda_{\mathcal{NF}}$−measurable, where $\mathcal{NF} = \{\mathcal{EF}, \mathcal{RF}, \mathcal{CNF}, \mathcal{CRF}\}$.