

GENERIC SUBGROUPS OF FREE PRODUCTS

Benjamin Fine
Alexei Myasnikov
Gerhard Rosenberger
(S. Ushakov)

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$ - $\text{T}\mathcal{E}\mathcal{X}$

TABLE OF CONTENTS

1. INTRODUCTION
2. THE GENERIC FREE GROUP PROPERTY
3. RELATIONSHIP TO CRYPTOGRAPHY
4. ASYMPTOTIC DENSITY
5. CHOOSING RANDOM ELEMENTS IN FREE PRODUCTS
6. THE RESULTS IN FREE PRODUCTS

1. INTRODUCTION

For many groups the structure of finitely generated subgroups is generically simple. That is with asymptotic density one a *randomly chosen* finitely generated subgroup has a particular well-known and easily analyzed structure.

For example a result of D.B.A.Epstein says that a finitely generated subgroup of $GL(n, \mathbb{R})$ is generically a free group.

Results of this type have a direct relevance to cryptography using nonabelian groups. Most of the cryptosystems developed with nonabelian groups as a platform - such as the Ko-Lee Scheme and the Anshel-Anshel-Goldfeld scheme use a random choice of a subgroup within a given platform group. For the above two schemes these involve braid groups. Whereas a subgroup of a platform group may be complicated, in many instances a generic subgroup has a simple structure which can be analyzed.

2. THE GENERIC FREE GROUP PROPERTY

If \mathcal{P} is a group property and G is a group then we say that subgroups of G are *generically* \mathcal{P} if a generic randomly chosen subgroup H of G has property \mathcal{P} . Equivalently this means that the asymptotic density of subgroups H of G that have property \mathcal{P} is one.

As an example a result of D.B.A.Epstein [E] says that a finitely generated subgroup of $GL(n, \mathbb{R})$ is generically a free group. In particular Epstein's result can be applied to the classical Modular group $PSL(2, \mathbb{Z})$ so that with asymptotic density one, n randomly chosen 2×2 projective integral matrices of determinant one generate a free group. Recall that group theoretically the Modular group $PSL(2, \mathbb{Z})$ is a nontrivial free product $\mathbb{Z}_2 \star \mathbb{Z}_3$.

Although this result and Epstein's proof seem specialized to linear groups this type of behavior turns out to be not uncommon. For many groups the structure of finitely generated subgroups is generically simple. That is with asymptotic density one a *randomly chosen* finitely generated subgroup has a particular well-known and easily analyzed structure.

In general we say that a group G has the **generic free group property** if a finitely generated subgroup is generically a free group. In this language Epstein's result is that the group $GL(n, \mathbb{R})$ satisfies the generic free group property.

G has the **strong generic free group property** if given randomly chosen elements g_1, \dots, g_n in G then generically they are a free basis for the free subgroup they generate.

G satisfies the **dominant Nielsen property** if given randomly chosen elements g_1, \dots, g_n in G then generically they are a minimal Nielsen basis for the free subgroup they generate.

(1) Jitsukawa [J] showed that finitely generated free groups have the strong generic free group property

(2) Myasnikov and Ushakov [MU] showed that pure braid groups have the strong generic free group property

(3) Gilman, Myasnikov and Osin showed that torsion-free hyperbolic groups have the strong generic free group property

MAIN RESULTS

Theorem I. *Let A and B be arbitrary finitely generated infinite groups and let $G = A \star B$ be their free product. Then a finitely generated subgroup of G is generically free. Thus an arbitrary free product of infinite groups has the generic free group property.*

Theorem II. *Let A and B be arbitrary finitely generated infinite groups and let $G = A \star B$ be their free product. Let $\{x_1, \dots, x_n\}$ be n randomly chosen elements from G . Then generically these elements are a free basis for the subgroup they generate. Thus an arbitrary free product of infinite groups has the strong generic free group property.*

Clearly Theorem II implies Theorem I however we give a slightly simpler proof for Theorem I than for Theorem II.

With some restrictions these results can be extended to more general amalgams – free products with amalgamation and HNN extensions of infinite groups.

AN INTERPRETATION OF EPSTEIN'S RESULT

Before looking at our results we look heuristically at Epstein's result for linear groups.

$GL(n, \mathbb{R})$ lives in R^{n^2} that is n^2 -dimensional space. Consider standard measure on this space and let $E_n(\mathbb{R})$ be the set of all real $n \times n$ matrices. Since

$$\det : E_n(\mathbb{R}) \rightarrow \mathbb{R}$$

is a continuous function it follows that the set of singular matrices has measure zero and therefore $GL(n, \mathbb{R})$ is generically n^2 -dimensional. Suppose M_1, \dots, M_k are k randomly chosen matrices in $GL(n, \mathbb{R})$. If they did not generate a free group then there is a nontrivial relation on M_1, \dots, M_k and hence a nontrivial word W with $W(M_1, \dots, M_k) = I$. This imposes an algebraic relation on the elements in M_1, \dots, M_k and thus implies that as elements of R^{n^2} live in a nontrivial algebraic variety and hence a lower dimensional space. It follows that in this case, that is M_1, \dots, M_k do not generate a free group, the group generated by M_1, \dots, M_k must have measure zero. Although not exactly the same our proof will use that elements of bounded syllable length in a free product have asymptotic density 0.

3. RELATION TO CRYPTOGRAPHY

These results have implications in nonabelian group cryptography.

In cryptographic methods using nonabelian groups encryption is usually done within subgroups of given finitely presented groups. As one way functions for cryptography, "hard" group theoretical problems such as the conjugator search problem are used. Random choices of subgroups are made. In many cases, even though the overall group theoretical problem is hard to solve generically the subgroups have a nice structure in which the problem can be solved. This affects the security of the cryptosystem and must be dealt with in both implementing the cryptosystem and in devising parameters for the implementation (see [BMS]). Cryptosystems involving these methods employing groups that have either the generic free group property or the strong generic free group property are subject to length based attacks similar to attacks on pure free group cryptosystems (see [SU]).

4. ASYMPTOTIC DENSITY

we first explain the concept of asymptotic density and generic subgroups and then describe how we choose random elements and random finitely generated subgroups in free products. These methods carry through to more general amalgams.

Asymptotic density is general method to compute densities and/or probabilities on infinite discrete sets where each individual outcome is tacitly assumed to be equally likely. The method can also be used where some probability distribution is assumed on the elements. It has been effectively applied to determining densities within infinite discrete finitely generated groups where random elements are considered as being generated from random walks on the Cayley graph of the group. The paper by Borovik, Myasnikov and Shpilrain [BMS] provides a good general description of this method in group theory. Let \mathcal{P} be a group property and let G be a finitely generated group. We want to determine the measure of the set of elements which satisfy \mathcal{P} . For each positive integer n let B_n denote the n -ball in G . Let $|B_n|$ denote the actual size of B_n (which is an integer since G is finitely generated) or the measure of $|B_n|$ if a distribution has been placed on the elements of G . Let S be the set of elements in G satisfying \mathcal{P} . The asymptotic density of S is then

$$\lim_{n \rightarrow \infty} \frac{|S \cap B_n|}{|B_n|}$$

provided this limit exists. We say that the property \mathcal{P} is **generic** if the asymptotic density of the set S of elements satisfying \mathcal{P} is one.

This concept can be easily extended to properties of finitely generated subgroups, We consider the asymptotic density of finite sets of elements that generate subgroups that have a considered property. For example to say that a group has the generic free

group property we mean that

$$\lim_{m,n \rightarrow \infty} \frac{|S_m \cap B_n|}{|B_n|} = 1$$

where S_m is the collection of finite sets of elements of size m that generate a free subgroup.

5. CHOOSING RANDOM ELEMENTS IN FREE PRODUCTS

We now describe how to choose random elements and random finitely generated subgroups in free product. Let $G = A \star B$ where A and B are finitely generated infinite groups.

Now assume that $A = \langle a_1, \dots, a_N \rangle$ and $B = \langle b_1, \dots, b_M \rangle$ but we make no assumption on the distributions in A and B . Essentially choosing a random element in $A \star B$ is a random walk on the Bass-Serre tree with a random choice from each vertex. To randomly choose an element we do the following. Choose a 0 or a 1 - to see whether an element starts with an A element or a B elements. We then randomly choose a integer n to be the syllable length. To pick an element pick 0 or 1, Suppose its 0 so A is picked first. We then randomly pick an A element followed by a random B element and so on. The probability of choosing A elements and B elements depends on the distribution of elements within the factors. Syllable length is random on the natural numbers even if we don't know the distribution in the factors.

To permit some counting we are going to randomly choose within the total random choice in finite balls in A and B . (These choices will depend on the distribution in the factors but will not affect our final densities.)

To choose a random element we make 4 random choices:

- (1) $n =$ syllable length
- (2) $m =$ total length in the alphabet on the generators
- (3) An n -partition k_1, \dots, k_n of m with no $k_i = 0$
- (4) Choose 0 or 1

To then pick a random element we do the following:

The 0 or 1 pick says that you're starting with either A or B . Suppose its 0 so we pick first from A . We choose a random k_1 length element in A . Notice that this depends on the distribution

in A but that doesn't affect our final result. We then pick a random k_2 length element in B and so on.

Notice the probabilities of picking elements in A and B of shorter lengths may not be the same as longer lengths or vice versa but all we are interested in is the relative picking of fixed syllable length versus arbitrary syllable length.

Randomly choosing a finitely generated subgroup is equivalent to randomly choosing an integer m and then randomly choosing m elements.

6. GENERIC SUBGROUPS OF FREE PRODUCTS

We first outline the proof of Theorem II.

Theorem II. *Let A and B be arbitrary finitely generated infinite groups and let $G = A \star B$ be their free product. Let $\{x_1, \dots, x_n\}$ be n randomly chosen elements from G . Then generically these elements are a free basis for the subgroup they generate. That is an arbitrary free product of f.g. infinite groups satisfies the strong generic free group property,*

To prove the theorem we need the following lemmas:

Lemma 1. *In $G = A \star B$ the asymptotic density of elements of syllable length one is zero*

Corollary. *If S is a finite set then the asymptotic density of S is zero if S has any elements of syllable length one.*

Lemma 2. *Let $S = \{x_1, \dots, x_n\}$ be a finite set of elements. Then*

$$P(\{x_1, \dots, x_n\} \text{ is a free basis}) = P(\{x_1, \dots, x_n\} \text{ is a free basis} \mid x_1, \dots, x_n \text{ all have syllable length} > 1)$$

In essence this lemma says that we may assume that in choosing a finitely generated subgroup each generator has syllable length > 1 .

Lemma 3. *Let A be an infinite f.g. group. Then the probability of picking two random elements a, b and having $a = b^{-1}$ is zero.*

This follows from a result of Olshanki's. If $A = F/N$ is infinite then the asymptotic density of randomly choosing an element in F and its being in N is zero.

Lemma 4. *Let $x_1, \dots, x_n \in G = A \star B$ be all of syllable length > 1 .
Then*

$$P(\{x_1, \dots, x_n\} \text{ are a free basis}) = 1$$

Here by a free basis we mean a free basis for the subgroup they generate.

We now give an alternative proof of the weaker result that an arbitrary free product of infinite groups has the generic free group property.

Theorem I. *Let A and B be arbitrary finitely generated infinite groups and let $G = A \star B$ be their free product. Then G satisfies the generic free group property.*

Proof. Let $H = \langle g_1, \dots, g_n \rangle$ be a randomly chosen finitely generated subgroup of $A \star B$. From the Kurosh theorem H must have the following structure

$$H = F \star A_1 \star B_1 \star \dots \star B_K$$

where F is a free group and each A_i is a conjugate of a subgroup of A and each B_j is a conjugate of a subgroup of B . An easy modification of Lemma 1 above shows that randomly choosing a conjugate of a subgroup of A or B must have asymptotic density zero. Therefore generically H is F the free group part.

We could also further formalize this by randomly choosing Kurosh bases.