ASYMPTOTIC PROPERTIES OF SOLVABLE EQUATIONS IN GROUPS

Authors

Vitaly Roman'kov

Omsk State Dostoevskii University, Russia

joint with

Robert Gilman and **Alexei Myasnikov**

Stevens Institute of Technology, Hoboken, USA;
McGill University, Montreal, Canada

INTRODUCTION

Equations

$$u(x_1, \ldots, x_k) = 1$$

Free products

Usually the left side u of any equation $u = 1$ over any group G is

element of a free product

$$G_X = G * F(X),$$

where

$$X = \{x_1, \ldots, x_k\}$$

is considered as the set of variables

Free products in variety

We think that more naturally is to take free product in the variety $\mathcal{L} = Var(G)$ generated by G.

So we assume that $F(X) = F_{\mathcal{L}}(X)$ is a free group in the variety $\mathcal{L}$, and

$$G_X = G *_{\mathcal{L}} F(X)$$

is a free product in this variety.

Free products in variety

We think that more naturally is to take free product in the variety $\mathcal{L} = Var(G)$ generated by G.

So we assume that $F(X) = F_{\mathcal{L}}(X)$ is a free group in the variety $\mathcal{L}$, and

$$G_X = G *_{\mathcal{L}} F(X)$$

is a free product in this variety.

Equations

An **equation** $w = 1$ in k variables is defined by any element $w \in G_X$.

SAT and NSAT

An **equation** $w = 1$ **is SAT** if it is satisfiable (has a solution) in G.

An **equation** $w = 1$ **is NSAT** if it is non-satisfiable (has no solutions) in G.

Stratification

Let T be a countable set equipped with a *size* (or length) function $s : T \to \mathbb{N}$ such that for every $n \in \mathbb{N}$ the *ball*

$$B_n = \{t \in T \mid s(t) \leq n\}$$

is finite.

The size function s induces a volume stratification of the set T:

$$T = \cup_{r=0}^{\infty} B_r,$$

which gives a "direction" to infinity in T.

Stratification

Let T be a countable set equipped with a *size* (or length) function $s : T \to \mathbb{N}$ such that for every $n \in \mathbb{N}$ the *ball*

$$B_n = \{t \in T \mid s(t) \leq n\}$$

is finite.

The size function s induces a volume stratification of the set T:

$$T = \cup_{r=0}^{\infty} B_r,$$

which gives a "direction" to infinity in T.

Relative frequency

For a subset $A \subseteq T$ and a finite subset $B \subset T$ we define a relative frequency

$$d(A|B) = \frac{|A \cap B|}{|B|},$$

Now, one can define the r-frequency (or r-density) of A with respect to the stratification T (or the size function s) by

$$d_r(A) = d(A|B_r).$$

Relative frequency

For a subset $A \subseteq T$ and a finite subset $B \subset T$ we define a relative frequency

$$d(A|B) = \frac{|A \cap B|}{|B|},$$

Now, one can define the *r*-frequency (or *r*-density) of A with respect to the stratification T (or the size function s) by

$$d_r(A) = d(A|B_r).$$

Asymptotic density

Now, the asymptotic density of A with respect to the stratification T is defined as the following limit

$$ad(A) = \limsup_{r \to \infty} d_r(A)$$

If the actual limit

$$sad(A) = \lim_{r \to \infty} d_r(A)$$

exists then we call it the strict asymptotic density of A.
A is called generic if $sad(A) = 1$ and it is negligible if $sad(A) = 0$.

Asymptotic density

Now, the asymptotic density of A with respect to the stratification T is defined as the following limit

$$ad(A) = \limsup_{r \to \infty} d_r(A)$$

If the actual limit

$$sad(A) = \lim_{r \to \infty} d_r(A)$$

exists then we call it the strict asymptotic density of A.
A is called generic if $sad(A) = 1$ and it is negligible if $sad(A) = 0$.

Uniform asymptotic density of power sets in free abelian groups

The asymptotic density of any power set $\gamma\mathbb{Z}^k \subseteq \mathbb{Z}^k$ is almost obvious. But we need in estimates on the convergence rates that we could not find in the literature.

Proposition 1.

Let $\gamma, k \in \mathbb{N}^+$. Then
1) $sad(\gamma\mathbb{Z}^k) = 1/\gamma^k$;
2) $|d_r(\gamma\mathbb{Z}^k) - 1/\gamma^k| \leq \frac{2^{k+1}k}{r\gamma^{k-1}}$ for every $r \geq \gamma$,
3) $d_r(\gamma\mathbb{Z}^k)$ converges to $1/\gamma^k$ uniformly in γ.

Primitive and γ-primitive elements of free abelian groups

An element $x = x_1^{\gamma_1} \ldots x_k^{\gamma_k} \in A(X)$, where $A(X)$ is the free abelian group with basis X is called

primitive (visuable)

if and only if it is a member of some basis of $A(X)$, or, equivalently, $gcd(\gamma_1, \ldots, \gamma_k) = 1$.
It is called

γ-primitive ($\gamma-$visuable)

if and only if it is γ-power of some primitive element, or, equivalently, $gcd(\gamma_1, \ldots, \gamma_k) = \gamma$.

Asymptotic density of sets of $\gamma-$primitive elements in free abelian groups

Let $P_{k,\gamma}$ be the set of all γ-primitive elements in the free abelian group $A(X)$ of rank k.

The following result is well-known in number theory. In the case $k = 2$ it was proved by F. Mertens (1874), in full generality it is due to Christopher (1956). Below $\zeta(k) = \sum_{n=1}^{\infty} = 1/n^k$ denotes Riemann zeta-function.

Proposition 2.

For each $\gamma \in \mathbf{N}$ we have

$$sad(P_{k,\gamma}) = \frac{1}{\gamma^k \zeta(k)}.$$

Uniform asymptotic density of γ-primitive sets in free abelian groups

Also we need in estimates on the convergence rates for the sets $P_{k,\gamma}$.

Proposition 3.

Let $\gamma, k \in \mathbb{N}^+, \gamma \geq 2$. Then
1) For every $\varepsilon \geq 0$ there exists $r(\varepsilon) \in \mathbb{N}^+$ such that
$|d_r(P_{k,\gamma}) - \frac{1}{\gamma^k \zeta(k)}| \leq \frac{\varepsilon}{\gamma^{k-1}}$
for every $r \geq r(\varepsilon)$.
2) $d_r(P_{k,\gamma})$ converges to $\frac{1}{\gamma^k \zeta(k)}$ uniformly in γ.

FREE ABELIAN GROUPS

Equations

Let
$A = \mathbf{Z}^m$
be a free abelian group with basis $\{a_1, ..., a_m\}$ $(m \geq 1)$.

Now
$F(X) = \mathbf{Z}^k$
is the free abelian group with basis $\{x_1, ..., x_k\}$ $(k \geq 1)$,

and
$A_X = A \times F(X) = \mathbf{Z}^{m+k}$
is the free abelian group with basis $\{a_1, ..., a_m, x_1, ..., x_k\}$.

Satisfiable equations

Every element $w \in A_X$ can be uniquely written in the form

$$w = x_1^{\gamma_1} \ldots x_k^{\gamma_k} a_1^{\alpha_1} \ldots a_m^{\alpha_m},$$

where $\gamma_1, \ldots, \gamma_k, \alpha_1, \ldots, \alpha_m \in \mathbf{Z}$.
We call $\gamma = gcd(\gamma_1, \ldots, \gamma_k)$ the exponent of w and denote it as $\gamma = exp(w)$. In the exceptional case $\gamma_1 = \ldots = \gamma_k = 0$ we define $exp(u) = 0$.

Satisfiable equations

Lemma 1.

An equation $w = 1$ of non-zero exponent $\gamma = exp(u)$ has a solution in A if and only if $\gamma | gcd(\alpha_1, ..., \alpha_m)$. For $k = 1$ and $\gamma_1 = \pm\gamma \neq 0$ there is the unique solution $x_1 = a_1^{-\alpha_1/\gamma_1} ... a_m^{-\alpha_m/\gamma_1}$. When $exp(u) = 0$ a solution exists if and only if $\alpha_1 = ... = \alpha_m = 0$ (every tuple of k elements is a solution).

Stratification

For a free abelian group $\mathbf{Z}^q$ a length function $l : \mathbf{Z}^q \to \mathbf{N}$ will usually be the restriction to $\mathbf{Z}^q$ of $||\cdot||_\infty$−norm from $\mathbf{R}^q$.

The norm $||\cdot||$ of an element w is defined as

$$||w|| = max\{|\gamma_1|, ..., |\gamma_k|, |\alpha_1|, ..., |\alpha_m|\}.$$

The function $l : A_X \to \mathbf{N}$ is defined as $l(u) = ||u||$.
There are the boxes $B_r = \{w \in A_X : l(w) \leq r\}$, and their slices $B_r(\gamma) = \{w \in A_X : l(w) \leq r,\ exp(w) = \gamma\}$, for $\gamma = 0, 1, 2, ...$.

One-variable equations

Theorem 1.

For $r, m \in \mathbb{N}^+$

$$\mid d_r(SAT(A,1)) - \frac{\mathcal{Z}_r(m)}{r} \mid = O\left(\frac{\mathcal{Z}_r(m-1)}{r^2}\right),$$

where

$$\mathcal{Z}_r(k) = \sum_{n=1}^{r} = 1/n^k$$

One-variable equations

Corollary 1.

The set $SAT(A, 1)$ is negligible, and $NSAT(A, 1)$ is generic.

Multi-variable equations

Theorem 2.

Assume that $k \geq 2, m \geq 1$. Then the set $SAT(A,k)$ has the asymptotic density

$$sad(SAT(A,k)) = \frac{\zeta(k+m)}{\zeta(k)}.$$

FREE NILPOTENT GROUPS

Free nilpotent groups

Let

$$N = N_{mc}$$

be a free nilpotent group of rank m and class c with basis $\{a_1, \dots, a_m\}$.

Now

$$F(X) = F_{\mathcal{N}_c}(X) = N_{kc}$$

is the free nilpotent group of rank k and class c with basis $\{x_1, \dots, x_k\}$.

Normal forms

Then every element $u \in N_X$ can be uniquely written in the form:

$$u = x_1^{\gamma_1} \ldots x_k^{\gamma_k} \; a_1^{\alpha_1} \ldots a_m^{\alpha_m} \; \prod_{j=1}^{p} b_j^{\delta_j}.$$

where $b_1 < \ldots < b_p$ denote the set of all basic commutators of weights ≥ 2 on $a_1, \ldots, a_m, x_1, \ldots, x_k.$. We assume that the ordering of all basic commutators of weight $j \geq 2$ is such that first s_{j-1} ones depend in a_i only, and other $p_{j-1} - s_{j-1}$ of them occur at least one of x_j.

Norm

The norm $||\cdot||$ of an element $u \in N_X$ is defined as

$$||u|| = max\{|\gamma_i|, |\alpha_l|, |\delta_j| \ (i = 1, ..., k; l = 1, ..., m; j = 1, ..., p)\}.$$

The function $l : N_X \to \mathbb{N}$ is defined as $l(u) = ||u||$. There are the boxes: $B_r = \{u \in N_X : l(u) \leq r\}$, and the slices: $B_{r,\gamma} = \{u \in N_X : l(u) \leq r, \gamma = exp(u) = gcd(\gamma_1, ..., \gamma_k)$ (or 0 if $\gamma_1 = ... = \gamma_k = 0)\}$.

Norm

The norm $||\cdot||$ of an element $u \in N_X$ is defined as

$$||u|| = max\{|\gamma_i|, |\alpha_l|, |\delta_j| \ (i = 1, ..., k; l = 1, ..., m; j = 1, ..., p)\}.$$

The function $l : N_X \to \mathbb{N}$ is defined as $l(u) = ||u||$. There are the boxes: $B_r = \{u \in N_X : l(u) \leq r\}$, and the slices: $B_{r,\gamma} = \{u \in N_X : l(u) \leq r, \gamma = exp(u) = gcd(\gamma_1, ..., \gamma_k)$ (or 0 if $\gamma_1 = ... = \gamma_k = 0)\}$.

Main theorem

Now we can formulate our main assertions for nilpotent case.

Theorem 3.

Assume that $k, m \geq 2, c \geq 2$. Then the set $SAT(N, k)$ has the asymptotic density

$$ad(SAT(N, k)) \geq \frac{\zeta(k + m + s)}{\zeta(k)}, \quad (1)$$

where s denote the total number of all basic commutators at $a_1, \ldots, a_m$ of weights $2, \ldots, c - 1$.

FREE GROUPS

Preliminaries

Let

$$F = F_m$$

be a free group of rank $m \geq 2$ with basis $\mathcal{F} = \mathcal{F}_m = \{f_1, \ldots, f_m\}$, and

$$F(X) = F_k$$

is the free group of rank $k \geq 1$ with basis $X = \{x_1, \ldots, x_k\}$. Then

$$F_X = F * F(X) = F_{m+k}$$

is a space of all equations with variables from X and constants from F.

As before, F_X has the ball and spherical stratifications:

$$\cup_{r=0}^{\infty} B_r = F_X, \cup_{r=0}^{\infty} S_r = F_X,$$

relative to basis $\mathcal{F} \cup X$.

Connection between solvability of equations in free and free abelian groups

As usual, $A_X = A \times A(X)$ is the free abelian group of rank $m + k$, the standard epimorphic image for $\mu : F_X \to F_X / F'_X = A_X$. A basis of A_X is taken as $\{a_1, ..., a_m\}$, and $\mu(f_i) = a_i, \mu(x_j) = x_j$.
For $a \in A$ put

$$S_r(a) = \{f \in S_r : \mu(f) = a\} = \mu^{-1}(a) \cap S_r.$$

Connection between solvability of equations in free and free abelian groups

We need to recall two known results that relate asymptotics in F_q and A_q.

Theorem by Sharp (2001). Let $a \in A_q$ and $r \in \mathbb{N}$. Then

$\lim_{r\to\infty} |\sigma^q r^{q/2}(\frac{|S_r(a)|}{|S_r|} + \frac{|S_{r+1}(a)|}{|S_{r+1}|}) - \frac{2}{(2\pi)^{q/2}} e^{-||a||_2^2/2\sigma^2 r}| = 0,$
uniformly in $a \in A$.

Here $\sigma^2 = \frac{1}{\sqrt{2q-1}}(1 + (\frac{q+\sqrt{2q-1}}{q-\sqrt{2q-1}})^{1/2})$.

Corollary

Corollary 1. There is a constant $c \in \mathbb{N}$ such that for any $a \in A_q$ and $r \in \mathbb{N}$ $\frac{|S_{2r+\delta_a}(a)|}{|S_{2r+\delta_a}|} \leq \frac{c}{r^{q/2}}$,

where $\delta_a = 0$ if $||a||_1$ is even, and $\delta_a = 1$ if $||a||_1$ is odd.

Rivin's theorem

Theorem by Rivin (1999). For any $D \subseteq \mathbb{R}^q, q \geq 2$,

$$\lim_{r\to\infty} \frac{1}{|S_r|}|\{w \in S_r | \mu(w)/r^{1/2} \in D\}| = \frac{1}{(2\pi)^{q/2}\sigma^q} \int_D e^{-||t||_2^2/2\sigma^2} dt.$$

Asymptotic of one-variable equations

Theorem 4.

The set $SAT(F,1)$ is negligible relative to both ball and spherical stratifications, so $sad(SAT(F,1)) = 0, sad(NSAT(F,1)) = 1.$

Split equations

We say that an equation $u = 1$, $u \in F_X$, splits if $u = vg^{-1}$, and so it is equivalent to equation

$$v = v(x_1, ..., x_k) = g,$$

where $v = v(x_1, ..., x_k) \in F(X)$ and $g \in F$.
Denote by $V(F, k)$ the set of all split equations in k variables over F. Also let

$$SAT_V(F, k)$$

and

$$NSAT_V(F, k)$$

be the sets of all satisfiable and all unsatisfiable split equations from $V(F, k)$.

Conditions of satisfiability

The image of an element $u \in F_X$ under $\mu : F_X \to A_X$ can be uniquely written as

$$u^{\mu} = x_1^{\gamma_1} \ldots x_k^{\gamma_k} a_1^{\alpha_1} \ldots a_m^{\alpha_m}.$$

We define $exp(u) = \exp(u^{\mu}) = gcd(\gamma_1, \ldots, \gamma_k)$.

Lemma 2.

Let $u \in V(F, k)$. If $exp(u) = 1$ then $u \in SAT_V(F, k)$.

Conditions of satisfiability

The image of an element $u \in F_X$ under $\mu : F_X \to A_X$ can be uniquely written as

$$u^{\mu} = x_1^{\gamma_1} \dots x_k^{\gamma_k} a_1^{\alpha_1} \dots a_m^{\alpha_m}.$$

We define $exp(u) = \exp(u^{\mu}) = gcd(\gamma_1, \dots, \gamma_k)$.

Lemma 2.

Let $u \in V(F, k)$. If $exp(u) = 1$ then $u \in SAT_V(F, k)$.

Lemma

Lemma 3.

Let $k \geq m$. Then for every $\varepsilon > 0$ there exists $0 < \alpha < 1$ and a number $r_0 = r(\varepsilon, \alpha) \in \mathbb{N}$ such that for every $r \geq r_0$ the following inequality holds

$$\frac{|V_\alpha(F,k) \cap S_r|}{|V(F,k) \cap S_r|} \leq \varepsilon.$$

Here $V_\alpha(F,k) = \{vg \in V(F,k) | \ |g| \leq \alpha |vg|\}$.

Main theorem

Assume that $k \geq 2$ and $k \geq m$. Then the asymptotic density of the set $SAT_V(F,k)$ can be estimated as follows:

Theorem 5.

$ad(SAT_V(F,k)) \geq \frac{2}{(2k-1)\zeta(k)}$.

The set $NSAT(F,k)$ can be estimated too.

Main theorem

Assume that $k \geq 2$ and $k \geq m$. Then the asymptotic density of the set $SAT_V(F, k)$ can be estimated as follows:

Theorem 5.

$ad(SAT_V(F, k)) \geq \frac{2}{(2k-1)\zeta(k)}$.

The set $NSAT(F, k)$ can be estimated too.