Some applications of diophantine geometry and model theory to group theory.

Emmanuel Breuillard

Université Paris-Sud, Orsay, France

Oléron, June 6th, 2011

Plan of the talk:

Plan of the talk:

1. Effective Burnside-Schur theorems and the compactness theorem of first order logic.

Plan of the talk:

1. Effective Burnside-Schur theorems and the compactness theorem of first order logic.
2. Diophantine Geometry on character varieties and a height gap theorem.

Plan of the talk:

1. Effective Burnside-Schur theorems and the compactness theorem of first order logic.
2. Diophantine Geometry on character varieties and a height gap theorem.
3. A uniform Tits alternative.

Plan of the talk:

1. Effective Burnside-Schur theorems and the compactness theorem of first order logic.
2. Diophantine Geometry on character varieties and a height gap theorem.
3. A uniform Tits alternative.
4. Diameter of finite simple groups.

Plan of the talk:

1. Effective Burnside-Schur theorems and the compactness theorem of first order logic.
2. Diophantine Geometry on character varieties and a height gap theorem.
3. A uniform Tits alternative.
4. Diameter of finite simple groups.
5. Effective versions of Hrushovski's theorems on approximate groups.

Effective Burnside-Schur

Theorem (Restricted Burnside Problem; Kostrikin, Zelmanov)

Given natural integers r, n, there are only finitely many r-generated finite groups all of whose elements have order dividing n.

Effective Burnside-Schur

Theorem (Restricted Burnside Problem; Kostrikin, Zelmanov)

Given natural integers r, n, there are only finitely many r-generated finite groups all of whose elements have order dividing n.

For a symmetric set of generators $S = \{1, s_1^{\pm 1}, ..., s_r^{\pm 1}\}$ of a group $G = \langle S \rangle$, we denote by $S^k := S \cdot ... \cdot S$ the "ball of radius k" in the Cayley graph of G generated by S.

Effective Burnside-Schur

Theorem (Restricted Burnside Problem; Kostrikin, Zelmanov)

Given natural integers r, n, there are only finitely many r-generated finite groups all of whose elements have order dividing n.

For a symmetric set of generators $S = \{1, s_1^{\pm 1}, ..., s_r^{\pm 1}\}$ of a group $G = \langle S \rangle$, we denote by $S^k := S \cdot ... \cdot S$ the "ball of radius k" in the Cayley graph of G generated by S.

Conjecture (Effective restricted Burnside; Olshanskii)

Given r, n, does there exists $k(r, n) \in \mathbb{N}$ such that there are only finitely many r-generated finite groups $G = \langle S \rangle$ such that all elements in S^k have order dividing n ?

Effective Burnside-Schur

Theorem (Restricted Burnside Problem; Kostrikin, Zelmanov)

Given natural integers r, n, there are only finitely many r-generated finite groups all of whose elements have order dividing n.

For a symmetric set of generators $S = \{1, s_1^{\pm 1}, ..., s_r^{\pm 1}\}$ of a group $G = \langle S \rangle$, we denote by $S^k := S \cdot ... \cdot S$ the "ball of radius k" in the Cayley graph of G generated by S.

Conjecture (Effective restricted Burnside; Olshanskii)

Given r, n, does there exists $k(r, n) \in \mathbb{N}$ such that there are only finitely many r-generated finite groups $G = \langle S \rangle$ such that all elements in S^k have order dividing n ?

Remark (Olshanskii). The conjecture would solve a celebrated open problem of Gromov, i.e. show the existence of a non-residually finite Gromov hyperbolic group.

Effective Burnside-Schur

Theorem (Burnside 1904, Schur 1914)

Let K be a field and $S \subset \mathrm{GL}_d(K)$ a finite symmetric set. If every element of the subgroup $\langle S \rangle$ has finite order, then $\langle S \rangle$ is finite.

Effective Burnside-Schur

Theorem (Burnside 1904, Schur 1914)

Let K be a field and $S \subset \mathrm{GL}_d(K)$ a finite symmetric set. If every element of the subgroup $\langle S \rangle$ has finite order, then $\langle S \rangle$ is finite.

Corollary (1st effective version)

Olshanski's conjecture holds for subgroups of GL_d (d fixed). That is: given r, n, d, there exists $k(r, n, d) \in \mathbb{N}$ such that there are only finitely many r-generated finite groups $G = \langle S \rangle$ admitting an embedding in GL_d (over some field) such that all elements in S^k have order dividing n.

Effective Burnside-Schur

Corollary (1st effective version)

Olshanski's conjecture holds for subgroups of GL_d (d fixed). That is: given r, n, d, there exists $k(r, n, d) \in \mathbb{N}$ such that there are only finitely many r-generated finite groups $G = \langle S \rangle$ admitting an embedding in GL_d (over some field) such that all elements in S^k have order dividing n.

Proof. Arguing by contradiction, this follows easily from the Compactness Theorem and the Burnside-Schur theorem.

Effective Burnside-Schur

Corollary (1st effective version)

Olshanski's conjecture holds for subgroups of GL_d (d fixed). That is: given r, n, d, there exists $k(r, n, d) \in \mathbb{N}$ such that there are only finitely many r-generated finite groups $G = \langle S \rangle$ admitting an embedding in GL_d (over some field) such that all elements in S^k have order dividing n.

Proof. Arguing by contradiction, this follows easily from the Compactness Theorem and the Burnside-Schur theorem. Equivalent way to see it: use ultraproducts as follows.

Effective Burnside-Schur

Corollary (1st effective version)

Olshanski's conjecture holds for subgroups of GL_d (d fixed). That is: given r, n, d, there exists $k(r, n, d) \in \mathbb{N}$ such that there are only finitely many r-generated finite groups $G = \langle S \rangle$ admitting an embedding in GL_d (over some field) such that all elements in S^k have order dividing n.

Proof. Arguing by contradiction, this follows easily from the Compactness Theorem and the Burnside-Schur theorem.
Equivalent way to see it: use ultraproducts as follows. If conclusion fails, one can find a sequence of fields $\{K_k\}_{k \geqslant 0}$, a sequence of symmetric sets S_k of size r, such that every element in S_k^k has order dividing n, and yet $|\langle S_k \rangle| \to +\infty$.

Effective Burnside-Schur

Corollary (1st effective version)

Olshanski's conjecture holds for subgroups of GL_d (d fixed). That is: given r, n, d, there exists $k(r,n,d) \in \mathbb{N}$ such that there are only finitely many r-generated finite groups $G = \langle S \rangle$ admitting an embedding in GL_d (over some field) such that all elements in S^k have order dividing n.

Proof. Arguing by contradiction, this follows easily from the Compactness Theorem and the Burnside-Schur theorem.
Equivalent way to see it: use ultraproducts as follows. If conclusion fails, one can find a sequence of fields $\{K_k\}_{k \geqslant 0}$, a sequence of symmetric sets S_k of size r, such that every element in S_k^k has order dividing n, and yet $|\langle S_k \rangle| \to +\infty$.
Then consider the ultraproduct $\prod_{\mathcal{U}} \langle S_k \rangle \subset \prod_{\mathcal{U}} \mathrm{GL}_d(K_k) = \mathrm{GL}_d(K)$, where

$$K = \prod_{\mathcal{U}} K_k.$$

Effective Burnside-Schur

Proof. Arguing by contradiction, this follows easily from the Compactness Theorem and the Burnside-Schur theorem.
Equivalent way to see it: use ultraproducts as follows. If conclusion fails, one can find a sequence of fields $\{K_k\}_{k\geqslant 0}$, a sequence of symmetric sets S_k of size r, such that every element in S_k^k has order dividing n, and yet $|\langle S_k\rangle| \to +\infty$.
Then consider the ultraproduct
$\prod_{\mathcal{U}}\langle S_k\rangle \subset \prod_{\mathcal{U}} \mathrm{GL}_d(K_k) = \mathrm{GL}_d(K)$, where

$$K = \prod_{\mathcal{U}} K_k.$$

Effective Burnside-Schur

Proof. Arguing by contradiction, this follows easily from the Compactness Theorem and the Burnside-Schur theorem.
Equivalent way to see it: use ultraproducts as follows. If conclusion fails, one can find a sequence of fields $\{K_k\}_{k\geqslant 0}$, a sequence of symmetric sets S_k of size r, such that every element in S_k^k has order dividing n, and yet $|\langle S_k\rangle| \to +\infty$.
Then consider the ultraproduct
$\prod_{\mathcal{U}}\langle S_k\rangle \subset \prod_{\mathcal{U}} \mathrm{GL}_d(K_k) = \mathrm{GL}_d(K)$, where

$$K = \prod_{\mathcal{U}} K_k.$$

The set $S := \prod_{\mathcal{U}} S_k$ has size r and yet for all $k \geqslant 1$, *every element of* S^k has order divisible by n.

Effective Burnside-Schur

Proof. Arguing by contradiction, this follows easily from the Compactness Theorem and the Burnside-Schur theorem.
Equivalent way to see it: use ultraproducts as follows. If conclusion fails, one can find a sequence of fields $\{K_k\}_{k\geqslant 0}$, a sequence of symmetric sets S_k of size r, such that every element in S_k^k has order dividing n, and yet $|\langle S_k\rangle| \to +\infty$.
Then consider the ultraproduct
$\prod_{\mathcal{U}}\langle S_k\rangle \subset \prod_{\mathcal{U}} \mathrm{GL}_d(K_k) = \mathrm{GL}_d(K)$, where

$$K = \prod_{\mathcal{U}} K_k.$$

The set $S := \prod_{\mathcal{U}} S_k$ has size r and yet for all $k \geqslant 1$, *every element of* S^k has order divisible by n.
But K is a field! so by the Burnside-Schur theorem, $\langle S\rangle$ is finite.

Effective Burnside-Schur

Proof. Arguing by contradiction, this follows easily from the Compactness Theorem and the Burnside-Schur theorem.
Equivalent way to see it: use ultraproducts as follows. If conclusion fails, one can find a sequence of fields $\{K_k\}_{k\geqslant 0}$, a sequence of symmetric sets S_k of size r, such that every element in S_k^k has order dividing n, and yet $|\langle S_k\rangle| \to +\infty$.
Then consider the ultraproduct
$\prod_{\mathcal{U}}\langle S_k\rangle \subset \prod_{\mathcal{U}} \mathrm{GL}_d(K_k) = \mathrm{GL}_d(K)$, where

$$K = \prod_{\mathcal{U}} K_k.$$

The set $S := \prod_{\mathcal{U}} S_k$ has size r and yet for all $k \geqslant 1$, *every element of* S^k has order divisible by n.
But K is a field! so by the Burnside-Schur theorem, $\langle S\rangle$ is finite.
In turn, this forces $\langle S_k\rangle$ to be bounded independently of k, contrary to the standing assumption. QED.

Effective Burnside-Schur

... in fact one can do better and switch two more quantifiers.

Effective Burnside-Schur

... in fact one can do better and switch two more quantifiers. We had

1st effective version: $\forall n$, $\exists k, K$ s.t. $\Big($every element in S^k has order $\leqslant n\Big) \Rightarrow |\langle S\rangle| \leqslant K$.

Effective Burnside-Schur

... in fact one can do better and switch two more quantifiers. We had

1st effective version: $\forall n$, $\exists k, K$ s.t. $\big($every element in S^k has order $\leqslant n\big) \Rightarrow |\langle S\rangle| \leqslant K$.

we prove the following stronger version:
2nd effective version: $\exists k = k(d)$ s.t. $\forall n$, $\exists K(n)$ s.t. $\big($every element in S^k has order $\leqslant n\big) \Rightarrow |\langle S\rangle| \leqslant K(n)$.

Effective Burnside-Schur

... in fact one can do better and switch two more quantifiers. We had

1st effective version: $\forall n, \exists k, K$ s.t. $\big($every element in S^k has order $\leqslant n\big) \Rightarrow |\langle S\rangle| \leqslant K$.

we prove the following stronger version:
2nd effective version: $\exists k = k(d)$ s.t. $\forall n, \exists K(n)$ s.t. $\big($every element in S^k has order $\leqslant n\big) \Rightarrow |\langle S\rangle| \leqslant K(n)$.
In particular:

Theorem (2nd effective version; B. '08)

There exists $k = k(d) \in \mathbb{N}$ such that if $S \subset \mathrm{GL}_d$ over some field, and every element of S^k has finite order, then $\langle S\rangle$ is finite.

Effective Burnside-Schur

... in fact one can do better and switch two more quantifiers. We had

1st effective version: $\forall n$, $\exists k, K$ s.t. $\big($every element in S^k has order $\leqslant n\big) \Rightarrow |\langle S\rangle| \leqslant K$.

we prove the following stronger version:
2nd effective version: $\exists k = k(d)$ s.t. $\forall n$, $\exists K(n)$ s.t. $\big($every element in S^k has order $\leqslant n\big) \Rightarrow |\langle S\rangle| \leqslant K(n)$.
In particular:

Theorem (2nd effective version; B. '08)

There exists $k = k(d) \in \mathbb{N}$ such that if $S \subset \mathrm{GL}_d$ over some field, and every element of S^k has finite order, then $\langle S\rangle$ is finite.

Open pb: find optimal upper bounds for $K(n)$

Effective Burnside-Schur

... in fact one can do better and switch two more quantifiers. We had

1st effective version: $\forall n$, $\exists k, K$ s.t. $\big($every element in S^k has order $\leqslant n\big) \Rightarrow |\langle S\rangle| \leqslant K$.

we prove the following stronger version:
2nd effective version: $\exists k = k(d)$ s.t. $\forall n$, $\exists K(n)$ s.t. $\big($every element in S^k has order $\leqslant n\big) \Rightarrow |\langle S\rangle| \leqslant K(n)$.
In particular:

Theorem (2nd effective version; B. '08)

There exists $k = k(d) \in \mathbb{N}$ such that if $S \subset \mathrm{GL}_d$ over some field, and every element of S^k has finite order, then $\langle S\rangle$ is finite.

Open pb: find optimal upper bounds for $K(n)$ (proof shows $K(n) \leqslant e^{n^{C(d)}}$).

Heights on character varieties

This time, the compactness theorem is not enough...

Heights on character varieties

This time, the compactness theorem is not enough... we need some diophantine geometry.

Heights on character varieties

This time, the compactness theorem is not enough... we need some diophantine geometry.
Let $\mathbf{G}$ be a reductive algebraic group over $\overline{\mathbb{Q}}$. Say $\mathbf{G} = \mathrm{GL}_d$. We are going to build a height function $\widehat{h}$ on the "character variety" $\mathbf{G}^r//\mathbf{G}$ = "$\mathbf{G}^r$ modulo the diagonal action by conjugation".

Heights on character varieties

This time, the compactness theorem is not enough... we need some diophantine geometry.
Let $\mathbf{G}$ be a reductive algebraic group over $\overline{\mathbb{Q}}$. Say $\mathbf{G} = \mathrm{GL}_d$. We are going to build a height function $\widehat{h}$ on the "character variety" $\mathbf{G}^r//\mathbf{G} =$ "$\mathbf{G}^r$ modulo the diagonal action by conjugation".

Recall the definition of the logarithmic Weil height on $\overline{\mathbb{Q}}^\times$.

Heights on character varieties

This time, the compactness theorem is not enough... we need some diophantine geometry.
Let $\mathbf{G}$ be a reductive algebraic group over $\overline{\mathbb{Q}}$. Say $\mathbf{G} = \mathrm{GL}_d$. We are going to build a height function $\widehat{h}$ on the "character variety" $\mathbf{G}^r//\mathbf{G}$ = "$\mathbf{G}^r$ modulo the diagonal action by conjugation".

Recall the definition of the logarithmic Weil height on $\overline{\mathbb{Q}}^\times$. Let $K \leqslant \overline{\mathbb{Q}}^\times$ be a number field.

$$\text{For } x \in K, \text{ set } h(x) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in V_K} n_v \log^+ |x|_v,$$

where, as usual, V_K =set of places of K, $n_v = [K_v : \mathbb{Q}_v]$, and $\log^+ = \max\{\log, 0\}$.

Heights on character varieties

For a $d \times d$ matrix $A \in M_{d,d}(\overline{\mathbb{Q}}^{\times})$, we set

Heights on character varieties

For a $d \times d$ matrix $A \in M_{d,d}(\overline{\mathbb{Q}}^{\times})$, we set

$$h(A) = \frac{1}{[K : \mathbb{Q}]} \sum_{v \in V_K} n_v \log^+ ||A||_v,$$

Heights on character varieties

For a $d \times d$ matrix $A \in M_{d,d}(\overline{\mathbb{Q}}^{\times})$, we set

$$h(A) = \frac{1}{[K : \mathbb{Q}]} \sum_{v \in V_K} n_v \log^+ ||A||_v,$$

where $||A||_v$ is the operator norm associated to the standard norm on K_v^d (i.e. ℓ^2 if v is archimedean, ℓ^∞ is v is non-archimedean).

Given $S \in \mathrm{GL}_d(K)^r$, we set

Heights on character varieties

For a $d \times d$ matrix $A \in M_{d,d}(\overline{\mathbb{Q}}^{\times})$, we set

$$h(A) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in V_K} n_v \log^+ ||A||_v,$$

where $||A||_v$ is the operator norm associated to the standard norm on K_v^d (i.e. ℓ^2 if v is archimedean, ℓ^∞ is v is non-archimedean).

Given $S \in \mathrm{GL}_d(K)^r$, we set

$$h(S) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in V_K} n_v \log^+ ||S||_v,$$

where

$$||S||_v := \max\{||s||_v, s \in S\}.$$

Heights on character varieties

Given $S \in \mathrm{GL}_d(K)^r$, we set

$$h(S) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in V_K} n_v \log^+ ||S||_v,$$

where

$$||S||_v := \max\{||s||_v, s \in S\}.$$

Heights on character varieties

Given $S \in \mathrm{GL}_d(K)^r$, we set

$$h(S) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in V_K} n_v \log^+ ||S||_v,$$

where

$$||S||_v := \max\{||s||_v, s \in S\}.$$

Definition

We call **normalized height** the quantity

$$\widehat{h}(S) := \lim_{n \to +\infty} \frac{1}{n} h(S^n),$$

where $S^n = S \cdot \ldots \cdot S$ is the n-th fold product set.

Heights on character varieties

properties of $\widehat{h}(S) \leftrightarrow$ group theoretic properties of $\langle S \rangle$.

Heights on character varieties

properties of $\widehat{h}(S) \leftrightarrow$ group theoretic properties of $\langle S \rangle$.

Theorem (B. '08)

(i) (height zero points) $\widehat{h}(S) = 0 \iff \langle S \rangle$ *is virtually unipotent.*

Heights on character varieties

properties of $\widehat{h}(S) \leftrightarrow$ group theoretic properties of $\langle S \rangle$.

Theorem (B. '08)

(i) (height zero points) $\widehat{h}(S) = 0 \iff \langle S \rangle$ *is virtually unipotent.*
(ii) (Bogomolov-type Height Gap Theorem) $\exists \varepsilon = \varepsilon(d) > 0$ *such that, unless* $\langle S \rangle$ *is virtually solvable, we have*

$$\widehat{h}(S) > \varepsilon.$$

Heights on character varieties

properties of $\widehat{h}(S) \leftrightarrow$ group theoretic properties of $\langle S \rangle$.

Theorem (B. '08)

(i) (height zero points) $\widehat{h}(S) = 0 \iff \langle S \rangle$ *is virtually unipotent.*
(ii) (Bogomolov-type Height Gap Theorem) $\exists \varepsilon = \varepsilon(d) > 0$ *such that, unless* $\langle S \rangle$ *is virtually solvable, we have*

$$\widehat{h}(S) > \varepsilon.$$

(iii) (Comparison with heights of eigenvalues) if $\langle S \rangle$ *is Zariski-dense in* $\mathbf{G}$*, then for some* $C = C(d), c = c(d) > 0$,

$$\frac{1}{C}\widehat{h(S)} \leqslant \max\{h(\lambda); \lambda \text{ eigenvalue of some } g \in S^c\} \leqslant C\widehat{h}(S).$$

Heights on character varieties

Theorem (B. '08)

(i) (height zero points) $\widehat{h}(S) = 0 \iff \langle S \rangle$ *is virtually unipotent.*
(ii) (Bogomolov-type Height Gap Theorem) $\exists \varepsilon = \varepsilon(d) > 0$ *such that unless* $\langle S \rangle$ *is virtually solvable, we have*

$$\widehat{h}(S) > \varepsilon.$$

(iii) (Comparison with heights of eigenvalues) if $\langle S \rangle$ *is Zariski-dense in* $\mathbf{G}$*, then for some* $C = C(d), c = c(d) > 0$,

$$\frac{1}{C}\widehat{h(S)} \leqslant \max\{h(\lambda); \lambda \text{ eigenvalue of some } g \in S^c\} \leqslant C\widehat{h}(S).$$

Heights on character varieties

Theorem (B. '08)

(i) (height zero points) $\widehat{h}(S) = 0 \iff \langle S \rangle$ *is virtually unipotent.*
(ii) (Bogomolov-type Height Gap Theorem) $\exists \varepsilon = \varepsilon(d) > 0$ *such that unless* $\langle S \rangle$ *is virtually solvable, we have*

$$\widehat{h}(S) > \varepsilon.$$

(iii) (Comparison with heights of eigenvalues) if $\langle S \rangle$ *is Zariski-dense in* $\mathbf{G}$*, then for some* $C = C(d), c = c(d) > 0$,

$$\frac{1}{C}\widehat{h(S)} \leqslant \max\{h(\lambda); \lambda \text{ eigenvalue of some } g \in S^c\} \leqslant C\widehat{h}(S).$$

The 2nd effective version of Burnside-Schur follows easily from Properties (i) and (iii) of $\widehat{h}(S)$.

Heights on character varieties

Theorem (B. '08)

(i) (height zero points) $\widehat{h}(S) = 0 \iff \langle S \rangle$ *is virtually unipotent.*
(ii) (Bogomolov-type Height Gap Theorem) $\exists \varepsilon = \varepsilon(d) > 0$ *such that unless* $\langle S \rangle$ *is virtually solvable, we have*

$$\widehat{h}(S) > \varepsilon.$$

(iii) (Comparison with heights of eigenvalues) if $\langle S \rangle$ *is Zariski-dense in* $\mathbf{G}$*, then for some* $C = C(d), c = c(d) > 0$,

$$\frac{1}{C}\widehat{h(S)} \leqslant \max\{h(\lambda); \lambda \text{ eigenvalue of some } g \in S^c\} \leqslant C\widehat{h}(S).$$

The 2nd effective version of Burnside-Schur follows easily from Properties (i) and (iii) of $\widehat{h}(S)$.

Heights on character varieties

Some ingredients of the proof:
1) a geometric reformulation of the problem in terms of minimal displacement of S on each symmetric space or Bruhat-Tits building associated to $\mathbf{G}(K_v)$.

Heights on character varieties

Some ingredients of the proof:
1) a geometric reformulation of the problem in terms of minimal displacement of S on each symmetric space or Bruhat-Tits building associated to $\mathbf{G}(K_v)$.
2) some geometry of symmetric spaces and buildings, in particular we make use of non-positive curvature.

Heights on character varieties

Some ingredients of the proof:
1) a geometric reformulation of the problem in terms of minimal displacement of S on each symmetric space or Bruhat-Tits building associated to $\mathbf{G}(K_v)$.
2) some geometry of symmetric spaces and buildings, in particular we make use of non-positive curvature.
3) a "spectral radius formula" for several matrices that relates the growth of $||S^n||_v$ to that of eigenvalues of S^n.

Heights on character varieties

Some ingredients of the proof:
1) a geometric reformulation of the problem in terms of minimal displacement of S on each symmetric space or Bruhat-Tits building associated to $\mathbf{G}(K_v)$.
2) some geometry of symmetric spaces and buildings, in particular we make use of non-positive curvature.
3) a "spectral radius formula" for several matrices that relates the growth of $||S^n||_v$ to that of eigenvalues of S^n.
4) Bilu's theorem on equidistribution of Galois orbits of small points on tori.

Heights on character varieties

Some ingredients of the proof:
1) a geometric reformulation of the problem in terms of minimal displacement of S on each symmetric space or Bruhat-Tits building associated to $\mathbf{G}(K_v)$.
2) some geometry of symmetric spaces and buildings, in particular we make use of non-positive curvature.
3) a "spectral radius formula" for several matrices that relates the growth of $||S^n||_v$ to that of eigenvalues of S^n.
4) Bilu's theorem on equidistribution of Galois orbits of small points on tori.
5) The Bogomolov conjecture for tori (Zhang's theorem).

Uniform Tits Alternative

... in fact the above theorem allows to show more than the effective Burnside-Schur result...

Uniform Tits Alternative

... in fact the above theorem allows to show more than the effective Burnside-Schur result... we get an uniform Tits alternative:

Uniform Tits Alternative

... in fact the above theorem allows to show more than the effective Burnside-Schur result... we get an uniform Tits alternative:

Theorem (Uniform Tits Alternative, B. '08)

There is $N = N(d) \in \mathbb{N}$ such that if S is a finite symmetric set in GL_d (over any field), then

Uniform Tits Alternative

... in fact the above theorem allows to show more than the effective Burnside-Schur result... we get an uniform Tits alternative:

Theorem (Uniform Tits Alternative, B. '08)

There is $N = N(d) \in \mathbb{N}$ such that if S is a finite symmetric set in GL_d (over any field), then
(i) either $\langle S \rangle$ has a solvable subgroup of finite index,

Uniform Tits Alternative

... in fact the above theorem allows to show more than the effective Burnside-Schur result... we get an uniform Tits alternative:

Theorem (Uniform Tits Alternative, B. '08)

There is $N = N(d) \in \mathbb{N}$ such that if S is a finite symmetric set in GL_d (over any field), then
(i) either $\langle S \rangle$ has a solvable subgroup of finite index,
(ii) or S^N contains two elements a, b, such that $\langle a, b \rangle$ is a non-abelian free group.

Uniform Tits Alternative

... in fact the above theorem allows to show more than the effective Burnside-Schur result... we get an uniform Tits alternative:

Theorem (Uniform Tits Alternative, B. '08)

There is $N = N(d) \in \mathbb{N}$ such that if S is a finite symmetric set in GL_d (over any field), then
(i) either $\langle S \rangle$ has a solvable subgroup of finite index,
(ii) or S^N contains two elements a, b, such that $\langle a, b \rangle$ is a non-abelian free group.

Remark: The proof uses the Tits "ping-pong method" (extending earlier work of Eskin-Mozes-Oh and Breuillard-Gelander) and relies crucially on the Bogomolov-type result for $\widehat{h}(S)$ presented above.

Theorem (Uniform Tits Alternative, B. '08)

There are $N = N(d), M = M(d) \in \mathbb{N}$ such that if S is a finite symmetric set in $\mathrm{GL}_d(\mathbb{C})$, then
(i) either $\langle S \rangle$ has a solvable subgroup of index at most M,
(ii) or S^N contains two elements a, b, such that $\langle a, b \rangle$ is a non-abelian free group.

Note:
(i) is an algebraic condition on S in GL_d^r, equivalent to

$$S \in \mathcal{V} := \text{“}\langle S \rangle \text{ has a solvable sugroup of finite index”}$$

Theorem (Uniform Tits Alternative, B. '08)

There are $N = N(d), M = M(d) \in \mathbb{N}$ such that if S is a finite symmetric set in $\mathrm{GL}_d(\mathbb{C})$, then
(i) either $\langle S \rangle$ has a solvable subgroup of index at most M,
(ii) or S^N contains two elements a, b, such that $\langle a, b \rangle$ is a non-abelian free group.

Note:
(i) is an algebraic condition on S in GL_d^r, equivalent to

$$S \in \mathcal{V} := \text{“}\langle S \rangle \text{ has a solvable sugroup of finite index”}$$

(ii) is a countable union of algebraic conditions, each equivalent to

$S \in \mathcal{W}_n :=$ “every two words in S^N have a relation of length $\leqslant n$”

Theorem (Uniform Tits Alternative, B. '08)

There are $N = N(d), M = M(d) \in \mathbb{N}$ such that if S is a finite symmetric set in $\mathrm{GL}_d(\mathbb{C})$, then
(i) either $\langle S \rangle$ has a solvable subgroup of index at most M,
(ii) or S^N contains two elements a, b, such that $\langle a, b \rangle$ is a non-abelian free group.

Note:
(i) is an algebraic condition on S in GL_d^r, equivalent to

$$S \in \mathcal{V} := \text{“}\langle S \rangle \text{ has a solvable sugroup of finite index”}$$

(ii) is a countable union of algebraic conditions, each equivalent to

$S \in \mathcal{W}_n :=$ “every two words in S^N have a relation of length $\leqslant n$”

Then Uniform Tits reads:

Theorem (Uniform Tits Alternative, B. '08)

There are $N = N(d), M = M(d) \in \mathbb{N}$ such that if S is a finite symmetric set in $\mathrm{GL}_d(\mathbb{C})$, then
(i) either $\langle S \rangle$ has a solvable subgroup of index at most M,
(ii) or S^N contains two elements a, b, such that $\langle a, b \rangle$ is a non-abelian free group.

Note:
(i) is an algebraic condition on S in GL_d^r, equivalent to

$$S \in \mathcal{V} := \text{“}\langle S \rangle \text{ has a solvable sugroup of finite index”}$$

(ii) is a countable union of algebraic conditions, each equivalent to

$S \in \mathcal{W}_n :=$ “every two words in S^N have a relation of length $\leqslant n$”

Then Uniform Tits reads:

$$\mathcal{V} = \bigcup_n \mathcal{W}_n$$

Then Uniform Tits reads:

$$\mathcal{V} = \bigcup_n \mathcal{W}_n$$

But $\mathcal{V}$ and $\mathcal{W}_n$ are algebraic subvarieties in $\mathbf{G}^{|S|}$.

Then Uniform Tits reads:

$$\mathcal{V} = \bigcup_n \mathcal{W}_n$$

But $\mathcal{V}$ and $\mathcal{W}_n$ are algebraic subvarieties in $\mathbf{G}^{|S|}$. Hence in fact:

$$\mathcal{V}(\mathbb{C}) = \mathcal{W}_n(\mathbb{C}),$$

for all n large enough.

Then Uniform Tits reads:

$$\mathcal{V} = \bigcup_n \mathcal{W}_n$$

But $\mathcal{V}$ and $\mathcal{W}_n$ are algebraic subvarieties in $\mathbf{G}^{|S|}$. Hence in fact:

$$\mathcal{V}(\mathbb{C}) = \mathcal{W}_n(\mathbb{C}),$$

for all n large enough.

Since $\mathcal{V}$ and $\mathcal{W}_n$ are defined over $\mathbb{Z}$, this equality holds also for algebraically closed fields of characteristic p if p is large enough, say $p \geqslant p(n)$.

Then Uniform Tits reads:

$$\mathcal{V} = \bigcup_n \mathcal{W}_n$$

But $\mathcal{V}$ and $\mathcal{W}_n$ are algebraic subvarieties in $\mathbf{G}^{|S|}$. Hence in fact:

$$\mathcal{V}(\mathbb{C}) = \mathcal{W}_n(\mathbb{C}),$$

for all n large enough.

Since $\mathcal{V}$ and $\mathcal{W}_n$ are defined over $\mathbb{Z}$, this equality holds also for algebraically closed fields of characteristic p if p is large enough, say $p \geqslant p(n)$.

Problem: Find the best bound on $p(n)$.

Then Uniform Tits reads:

$$\mathcal{V} = \bigcup_n \mathcal{W}_n$$

But $\mathcal{V}$ and $\mathcal{W}_n$ are algebraic subvarieties in $\mathbf{G}^{|S|}$. Hence in fact:

$$\mathcal{V}(\mathbb{C}) = \mathcal{W}_n(\mathbb{C}),$$

for all n large enough.

Since $\mathcal{V}$ and $\mathcal{W}_n$ are defined over $\mathbb{Z}$, this equality holds also for algebraically closed fields of characteristic p if p is large enough, say $p \geqslant p(n)$.

Problem: Find the best bound on $p(n)$.

Classical effective versions of the Hilbert Nullstellensatz give $p(n) \leqslant \exp(n^A)$ for some $A > 1$.

Classical effective versions of the Hilbert Nullstellensatz give $p(n) \leqslant \exp(n^A)$ for some $A > 1$.

So $\mathcal{V} = \mathcal{W}_n$ in char p for $p > p(n) \simeq exp(n^A)$.

Classical effective versions of the Hilbert Nullstellensatz give $p(n) \leqslant \exp(n^A)$ for some $A > 1$.

So $\mathcal{V} = \mathcal{W}_n$ in char p for $p > p(n) \simeq exp(n^A)$.

In particular we have proved:

Corollary (uniform exponential growth)

There are $e, c, N, M > 0$ depending on d only such that if $S \subset \mathrm{GL}_d(\mathbb{F}_p)$ and $\langle S \rangle$ has no solvable subgroup of index at most M, then
(i) $\exists a, b \in S^N$ with no relation up to length $(\log p)^e$.
(ii) $|S^n| > \exp(cn)$ for every $n \leqslant (\log p)^e$.

Applications: diameter of finite simple groups

Let G be a finite simple group, S a finite symmetric generating set, and $\mathcal{C}ay(G,S)$ its *Cayley graph*.

Applications: diameter of finite simple groups

Let G be a finite simple group, S a finite symmetric generating set, and $\mathcal{C}ay(G,S)$ its *Cayley graph*.

Let $diam(G,S)$ be the diameter of $\mathcal{C}ay(G,S)$ and

$$diam(G) := \sup_S diam(G,S).$$

Applications: diameter of finite simple groups

Let G be a finite simple group, S a finite symmetric generating set, and $\mathcal{C}ay(G,S)$ its *Cayley graph*.

Let $diam(G,S)$ be the diameter of $\mathcal{C}ay(G,S)$ and

$$diam(G) := \sup_S diam(G,S).$$

Conjecture (Uniform logarithmic diameter for FSG's of Lie type, folklore)

Let $r \in \mathbb{N}$. There is a constant $C_r > 0$ such that

$$diam(G) \leqslant C_r \log |G|,$$

for an arbitrary finite simple group of Lie type G with rank $\leqslant r$.

Conjecture (Uniform logarithmic diameter for FSG's of Lie type, folklore)

Let $r \in \mathbb{N}$. There is a constant $C_r > 0$ such that

$$diam(G) \leqslant C_r \log |G|,$$

for an arbitrary finite simple group of Lie type G with rank $\leqslant r$.

In Breuillard-Gamburd (2010), using the uniform Tits alternative, we gave the first example of such a family among finite simple groups: we showed that $G_n = \mathrm{PSL}_2(\mathbb{F}_{p_n})$ for some infinite family of primes p_n satisfies the conjecture and indeed are uniform expanders.

Conjecture (Uniform logarithmic diameter for FSG's of Lie type, folklore)

Let $r \in \mathbb{N}$. There is a constant $C_r > 0$ such that

$$diam(G) \leqslant C_r \log |G|,$$

for an arbitrary finite simple group of Lie type G with rank $\leqslant r$.

In Breuillard-Gamburd (2010), using the uniform Tits alternative, we gave the first example of such a family among finite simple groups: we showed that $G_n = \mathrm{PSL}_2(\mathbb{F}_{p_n})$ for some infinite family of primes p_n satisfies the conjecture and indeed are uniform expanders.

In fact, it is not obvious to find even one infinite family $\{G_n\}$ of finite groups for which $diam(G_n) \ll \log |G_n|$ (a question Lubotzky's)

Diameter of finite simple groups

Using recent results on approximate groups by Hrushovski, Pyber-Szabo and Breuillard-Green-Tao, one can now push the method of Breuillard-Gamburd to obtain:

Diameter of finite simple groups

Using recent results on approximate groups by Hrushovski, Pyber-Szabo and Breuillard-Green-Tao, one can now push the method of Breuillard-Gamburd to obtain:

Theorem (There can be only few exceptions to Conjecture 3)

Given $r, k, \varepsilon > 0$ *there is an explicit* $C = C(r, k, \varepsilon) > 0$ *such that*

Diameter of finite simple groups

Using recent results on approximate groups by Hrushovski, Pyber-Szabo and Breuillard-Green-Tao, one can now push the method of Breuillard-Gamburd to obtain:

Theorem (There can be only few exceptions to Conjecture 3)

Given $r, k, \varepsilon > 0$ there is an explicit $C = C(r, k, \varepsilon) > 0$ such that if $\mathcal{P}_{good}$ denotes the set of prime numbers p such that

$$diam(G) \leqslant C \log |G|$$

for all finite simple groups of Lie type of the form $G = \mathbf{G}(\mathbb{F}_{p^s})$, where $s \leqslant k$, $\mathbf{G}$ is a simple algebraic group of rank at most r,

Diameter of finite simple groups

Using recent results on approximate groups by Hrushovski, Pyber-Szabo and Breuillard-Green-Tao, one can now push the method of Breuillard-Gamburd to obtain:

Theorem (There can be only few exceptions to Conjecture 3)

Given $r, k, \varepsilon > 0$ there is an explicit $C = C(r, k, \varepsilon) > 0$ such that if $\mathcal{P}_{good}$ denotes the set of prime numbers p such that

$$diam(G) \leqslant C \log |G|$$

for all finite simple groups of Lie type of the form $G = \mathbf{G}(\mathbb{F}_{p^s})$, where $s \leqslant k$, $\mathbf{G}$ is a simple algebraic group of rank at most r, Then for all $X \geqslant 1$, $|\{p \notin \mathcal{P}_{good}, p \leqslant X\}| \leqslant X^{\varepsilon}$.

Now some words about proofs.

Now some words about proofs.

There are two periods in the growth of a Cayley graph ball $B(n)$ for $G = \mathbf{G}(\mathbb{F}_{p^s})$.

Now some words about proofs.

There are two periods in the growth of a Cayley graph ball $B(n)$ for $G = \mathbf{G}(\mathbb{F}_{p^s})$.

1) an early period,

Now some words about proofs.

There are two periods in the growth of a Cayley graph ball $B(n)$ for $G = \mathbf{G}(\mathbb{F}_{p^s})$.

1) an early period, when the growth is exponential: $|B(n)| \geqslant exp(cn)$,

Now some words about proofs.

There are two periods in the growth of a Cayley graph ball $B(n)$ for $G = \mathbf{G}(\mathbb{F}_{p^s})$.

1) an early period, when the growth is exponential: $|B(n)| \geqslant exp(cn)$,

2) and a later period,

Now some words about proofs.

There are two periods in the growth of a Cayley graph ball $B(n)$ for $G = \mathbf{G}(\mathbb{F}_{p^s})$.

1) an early period, when the growth is exponential: $|B(n)| \geqslant exp(cn)$,

2) and a later period, when the growth is no longer exponential but still $\gg exp(n^\alpha)$ for some $\alpha < 1$

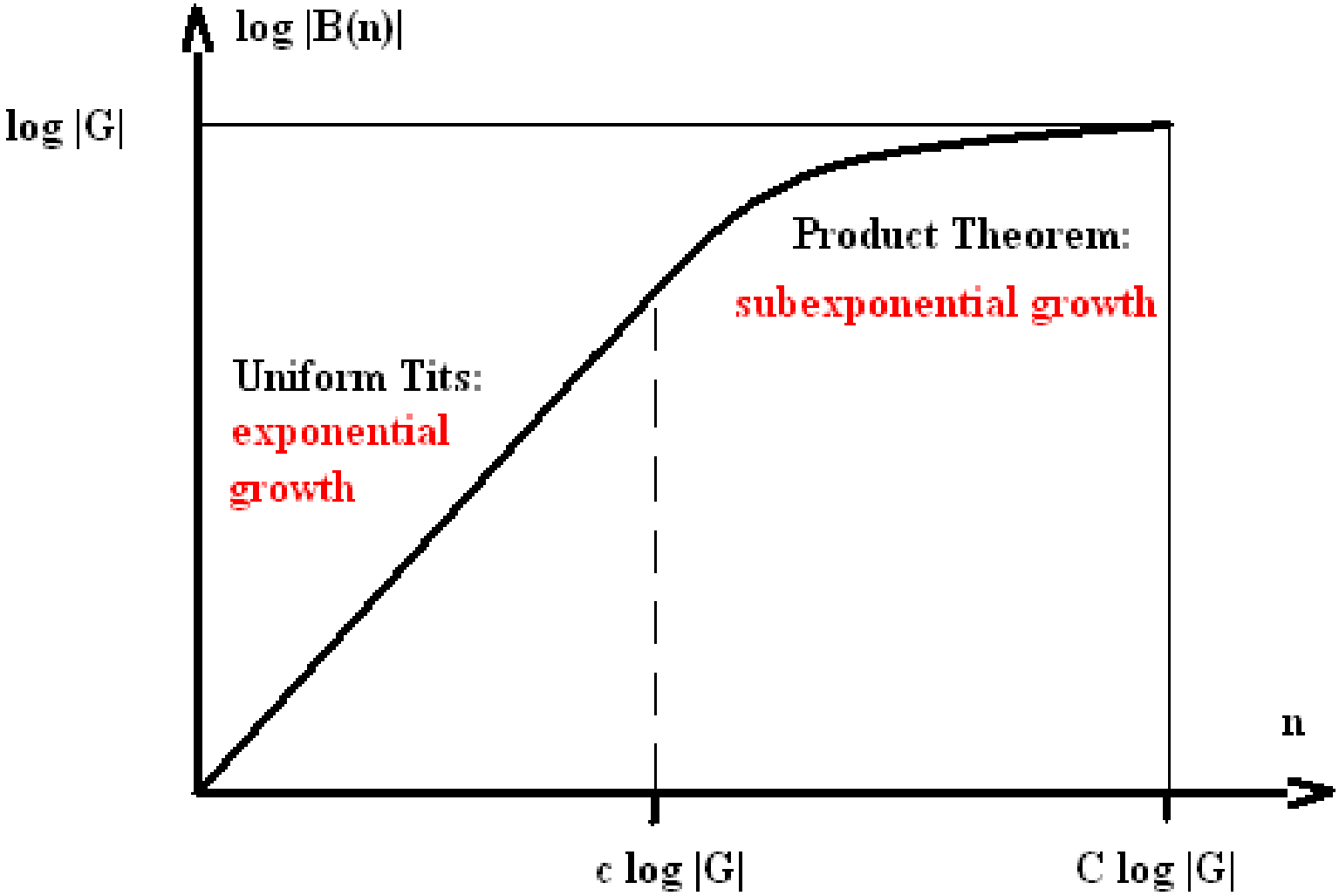
Now some words about proofs.

There are two periods in the growth of a Cayley graph ball $B(n)$ for $G = \mathbf{G}(\mathbb{F}_{p^s})$.

1) an early period, when the growth is exponential: $|B(n)| \geqslant exp(cn)$,

2) and a later period, when the growth is no longer exponential but still $\gg exp(n^\alpha)$ for some $\alpha < 1$

then we reach $B(n) = G$.



Growth of the ball of radius n, B(n), in a finite simple group of Lie type G.

Exponential growth in the *early period* follows from the uniform Tits alternative as outlined above.

Exponential growth in the *early period* follows from the uniform Tits alternative as outlined above.

The poor bounds on the size of first prime $p = p(n)$ for which $\mathcal{V} = \mathcal{W}_n$ holds also in characteristic p obtained in Corollary 11 (and gotten from the effective Nullstellensatz) need to be bootstrapped using a pigeonhole argument at the expense of loosing a small (but perhaps infinite) family of primes.

Exponential growth in the *early period* follows from the uniform Tits alternative as outlined above.

The poor bounds on the size of first prime $p = p(n)$ for which $\mathcal{V} = \mathcal{W}_n$ holds also in characteristic p obtained in Corollary 11 (and gotten from the effective Nullstellensatz) need to be bootstrapped using a pigeonhole argument at the expense of loosing a small (but perhaps infinite) family of primes.

Open problem: can one take $p(n) \leqslant \exp(Cn)$? (currently we know $p(n) \leqslant exp(n^C)$).

Approximate groups

Subexponential growth in the *later period* follows from the aforementioned results on *Approximate groups*. Namely:

Approximate groups

Subexponential growth in the *later period* follows from the aforementioned results on *Approximate groups*. Namely:

Theorem (Product Theorem, Hrushovski, Pyber-Szabo and Breuillard-Green-Tao)

Let $r \in \mathbb{N}$. There exists a constant $\gamma = \gamma(r) > 0$ such that

$$|AAA| \geqslant \min\{|A|^{1+\gamma}, |G|\},$$

for every generating subset A of any finite simple group of Lie type G of rank at most r.

Approximate groups

Subexponential growth in the *later period* follows from the aforementioned results on *Approximate groups*. Namely:

Theorem (Product Theorem, Hrushovski, Pyber-Szabo and Breuillard-Green-Tao)

Let $r \in \mathbb{N}$. There exists a constant $\gamma = \gamma(r) > 0$ such that

$$|AAA| \geqslant \min\{|A|^{1+\gamma}, |G|\},$$

for every generating subset A of any finite simple group of Lie type G of rank at most r.

As a consequence, for every Cayley graph of G, either $|B(3n)| \geqslant |B(n)|^{1+\gamma}$ or $B(3n) = G$. Hence we get:

Approximate groups

Subexponential growth in the *later period* follows from the aforementioned results on *Approximate groups*. Namely:

Theorem (Product Theorem, Hrushovski, Pyber-Szabo and Breuillard-Green-Tao)

Let $r \in \mathbb{N}$. There exists a constant $\gamma = \gamma(r) > 0$ such that

$$|AAA| \geqslant \min\{|A|^{1+\gamma}, |G|\},$$

for every generating subset A of any finite simple group of Lie type G of rank at most r.

As a consequence, for every Cayley graph of G, either $|B(3n)| \geqslant |B(n)|^{1+\gamma}$ or $B(3n) = G$. Hence we get:
a) subexponential lower bound on the growth in the later period.

Approximate groups

Subexponential growth in the *later period* follows from the aforementioned results on *Approximate groups*. Namely:

Theorem (Product Theorem, Hrushovski, Pyber-Szabo and Breuillard-Green-Tao)

Let $r \in \mathbb{N}$. There exists a constant $\gamma = \gamma(r) > 0$ such that

$$|AAA| \geqslant \min\{|A|^{1+\gamma}, |G|\},$$

for every generating subset A of any finite simple group of Lie type G of rank at most r.

As a consequence, for every Cayley graph of G, either $|B(3n)| \geqslant |B(n)|^{1+\gamma}$ or $B(3n) = G$. Hence we get:
a) subexponential lower bound on the growth in the later period.
b) that $diam(G) \leqslant (\log |G|)^C$ for some $C > 0$ depending only on $rank(G)$...

Approximate groups

Subexponential growth in the *later period* follows from the aforementioned results on *Approximate groups*. Namely:

Theorem (Product Theorem, Hrushovski, Pyber-Szabo and Breuillard-Green-Tao)

Let $r \in \mathbb{N}$. There exists a constant $\gamma = \gamma(r) > 0$ such that

$$|AAA| \geqslant \min\{|A|^{1+\gamma}, |G|\},$$

for every generating subset A of any finite simple group of Lie type G of rank at most r.

As a consequence, for every Cayley graph of G, either $|B(3n)| \geqslant |B(n)|^{1+\gamma}$ or $B(3n) = G$. Hence we get:
a) subexponential lower bound on the growth in the later period.
b) that $diam(G) \leqslant (\log |G|)^C$ for some $C > 0$ depending only on $rank(G)$... but not enough for $\leqslant C \cdot \log |G|$!

Approximate groups

The above product theorem can be reformulated in terms of "approximate groups" (T. Tao), that is finite subsets A of a group G, such that AA can be covered by a small amount of translates of A.

Approximate groups

The above product theorem can be reformulated in terms of "approximate groups" (T. Tao), that is finite subsets A of a group G, such that AA can be covered by a small amount of translates of A.

In 2009, using model theory, Hrushovski obtained the first general results on the structure of approximate groups.

Approximate groups

The above product theorem can be reformulated in terms of "approximate groups" (T. Tao), that is finite subsets A of a group G, such that AA can be covered by a small amount of translates of A.

In 2009, using model theory, Hrushovski obtained the first general results on the structure of approximate groups.

For approximate subgroups of simple algebraic groups, he obtained essentially complete results. Namely, approximate groups are close to genuine subgroups unless they are trapped in a proper algebraic subgroup.

Approximate groups

The above product theorem can be reformulated in terms of "approximate groups" (T. Tao), that is finite subsets A of a group G, such that AA can be covered by a small amount of translates of A.

In 2009, using model theory, Hrushovski obtained the first general results on the structure of approximate groups.

For approximate subgroups of simple algebraic groups, he obtained essentially complete results. Namely, approximate groups are close to genuine subgroups unless they are trapped in a proper algebraic subgroup.

The aforementioned subsequent works of Pyber-Szabo and Breuillard-Green-Tao aim at giving a better bound on how close to a genuine group is a given approximate group, resulting in the above stated theorem.

References: Heights on character varieties, uniform Tits

E. Breuillard, *A Height Gap Theorem for finite subsets of* $\mathrm{GL}_d(\overline{\mathbb{Q}})$ *and non amenable subgroups*, to appear Annals of Math (2011).

E. Breuillard, *A strong Tits alternative*, preprint, arXiv:0804.1395.

E. Breuillard, *Heights on* SL_2 *and free subgroups*, Zimmer Volume, Chicago Univ. Press (2011).

E. Breuillard and A. Gamburd, *Strong uniform expansion in* $\mathrm{SL}(2,p)$, Geom. Anal. Func. Anal. Vol. 20-5 (2010), 1201-1209.

References: Approximate groups and applications to finite groups

E. Breuillard, B. J. Green and T. C. Tao, *Approximate subgroups of linear groups*, to appear Geom. Anal. Func. Anal. (2011).

H. A. Helfgott, *Growth and generation in* $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, Ann. of Math. (2) **167** (2008), no. 2, 601–623.

E. Hrushovski, *Stable group theory and approximate subgroups*, preprint (2009), arXiv:0909.2190.

L. Pyber and E. Szabó, *Growth in finite simple groups of Lie type*, preprint (2010), arXiv:1001.4556.

Thank you!