ON CONJUGACY GROWTH OF LINEAR GROUPS

EMMANUEL BREUILLARD, YVES DE CORNULIER, ALEXANDER LUBOTZKY, AND CHEN MEIRI

Abstract. We investigate the conjugacy growth of finitely generated linear groups. We show that finitely generated non-virtually-solvable subgroups of GL_d have uniform exponential conjugacy growth and in fact that the number of distinct polynomials arising as characteristic polynomials of the elements of the ball of radius n for the word metric has exponential growth rate bounded away from 0 in terms of the dimension d only.

1. introduction

Let Γ be a group, generated by a finite set Σ. Let $B_\Sigma(n) = (\Sigma \cup \Sigma^{-1})^n$ be the ball of radius n in the Cayley graph $\mathrm{Cay}(\Gamma, \Sigma)$ of Γ with respect to Σ, i.e., the set of elements in Γ that can be written as product of at most n elements of $\Sigma \cup \Sigma^{-1}$. We denote by $|\cdot|$ the cardinality of a finite set and define

$$\alpha_\Sigma := \lim_{n\to\infty} \frac{\log |B_\Sigma(n)|}{n}. \tag{1.1}$$

The group Γ is said to have exponential (word) growth if $\alpha_\Sigma > 0$ for some (hence every) Σ and uniform exponential growth if $\inf_\Sigma \alpha_\Sigma > 0$ when Σ ranges over finite generating subsets. It follows from the Tits alternative [28] and the Milnor-Wolf theorem [20, 30] that non-virtually-nilpotent linear groups have exponential growth. Uniform exponential growth of these groups was established by Eskin-Mozes-Oh [8] in characteristic zero and by Breuillard-Gelander in arbitrary characteristic [5].

A related question advertised by Guba and Sapir in [11] and also discussed in the book [18] consists in determining the *conjugacy growth* of a group Γ generated by a finite set Σ. Namely, we are interested in the asymptotics of the number $c_\Sigma(n)$ of conjugacy classes in Γ intersecting the word ball $B_\Sigma(n)$ of radius n. This question can be seen as a combinatorial analogue to the problem of counting the number of closed geodesics in a closed Riemannian manifold

Date: October 11, 2012.

2000 *Mathematics Subject Classification.* Primary 20E45; Secondary 11R04, 11R44, 20D06, 20G30, 20G40.

The authors are grateful for grants from the ERC and the NSF.

according to length, a problem much studied in the literature (see [11] and the references therein). Denote

$$\gamma_\Sigma := \liminf_{n\to\infty} \frac{\log c_\Sigma(n)}{n}$$

and say that Γ has exponential conjugacy growth if $\gamma_\Sigma > 0$ and uniform exponential conjugacy growth if $\inf_\Sigma \gamma_\Sigma > 0$.

Rivin [26, Obs. 12.4, §13] computed the asymptotics of $c_\Sigma(n)$ for free groups. Ivanov [22, §41.5] proved the existence of groups with exponential growth and finitely many conjugacy classes; Osin [23] improved the result to get only two conjugacy classes. The conjugacy growth can therefore be dramatically smaller than the word growth. Guba and Sapir gave many examples of groups with exponential conjugacy growth and asked about other families of groups. In this paper we answer their question for linear groups.

Theorem 1.1. *Let Γ be a linear group, i.e. isomorphic to a subgroup of $\mathrm{GL}_d(F)$ for some field F, and suppose that Γ is not virtually nilpotent. Then Γ has uniform exponential conjugacy growth.*

The case of virtually solvable groups, linear or not, was treated in [4] (and independently by M. Hull in [12] in the polycyclic case): such groups have uniform exponential conjugacy growth unless they are virtually nilpotent. So in this paper we focus on non-virtually-solvable linear groups. We actually consider the finer problem of counting, given a finitely generated subgroup Γ in $\mathrm{GL}_d(F)$, the number of GL_d-conjugacy classes in the balls of Γ, resulting in the following theorem, which immediately entails Theorem 1.1.

Theorem 1.2. *For every integer d, there exists a constant $c(d) > 0$ such that if F is a field and Σ a finite symmetric subset of $\mathrm{GL}_d(F)$ generating a non-virtually-solvable subgroup, then*

$$\liminf_{n\to\infty} \frac{1}{n} \log \chi_\Sigma(n) \geqslant c(d),$$

where $\chi_\Sigma(n)$ is the number of elements in $F[X]$ appearing as characteristic polynomials of elements of Σ^n.

Combining this with exponential conjugacy growth in the solvable case [4] and some further simple remarks in the solvable case (Proposition 9.3), we get the following trichotomy

Corollary 1.3. *Let F be any field and let Γ be a finitely generated subgroup of $\mathrm{GL}_d(F)$. Then exactly one of the following holds*

(i) Γ *is virtually nilpotent (so has polynomial growth);*

(ii) Γ *is virtually solvable but not virtually nilpotent; it has exponential conjugacy growth, while $\chi_\Sigma(n)$ is bounded above by a polynomial whose degree depends only on the subgroup Γ and not on Σ;*

(iii) Γ *is not virtually solvable and then* $\chi_\Sigma(n)$ *grows exponentially with a rate bounded below by a constant* $\mu > 0$ *depending only on* d*.*

This is summarized in the following table.

Γ	growth $\|B_\Sigma(n)\|$	conjugacy growth $b^c_\Sigma(n)$	characteristic polynomial growth $\chi_\Sigma(n)$
v. nilpotent	*polynomial*	*polynomial*	*polynomial*
v. solvable not v. nilpotent	*exponential*	*exponential*	*polynomial*
not v. solvable	*exponential*	*exponential*	*exponential*

Note that we have claimed here a strong form of uniformity, in which the rate of exponential conjugacy growth γ_Σ depends only on d and not on the subgroup Γ of GL_d nor the field F. We will make use here of the fact, proved by the first named author in [3] building on the earlier works [8, 5, 2] that non-virtually-solvable linear groups in GL_d have a word growth rate bounded from below by a positive lower bound depending only on d and not on the field of definition. This used as a key ingredient the main result of [2] which solved a semisimple analogue of the (still open) Lehmer conjecture from diophantine geometry. The uniformity for the whole class of solvable non-virtually-nilpotent subgroups of $\mathrm{GL}_2(\mathbb{C})$, for which a positive answer would imply the validity of the classical Lehmer conjecture [1], is still an open question.

About the proof. A standard specialization argument shows that it is enough to prove Theorem 1.2 in the case where $\mathbb{K}$ is a global field, i.e. isomorphic to a finite extension of $\mathbb{Q}$ or $\mathbb{F}_p(t)$. Besides, the proof essentially boils down to the case where the Zariski closure $\mathbf{G}$ of $\langle\Sigma\rangle$ in GL_d is semisimple. Then using strong approximation (Weisfeiler [29], Pink [24]) for Zariski-dense subgroups of simple algebraic groups, the more recent Product Theorem of Pyber-Szabó and Breuillard-Green-Tao [25, 7] on the classification of approximate subgroups of simple algebraic groups over finite fields, and a pigeonhole argument using classical results about the distribution of primes, we prove that for many prime ideals $\mathcal{P}$ of the ring of integers $\mathcal{O}_\mathbb{K}$ whose norm $|\mathcal{P}| := |\mathcal{O}_\mathbb{K}/\mathcal{P}|$ is exponential in n, the reduction map $\mathbf{G}(\mathcal{O}_\mathbb{K}) \to \mathbf{G}(\mathcal{O}_\mathbb{K}/\mathcal{P})$ is surjective when restricted to $B_\Sigma(Cn)$, where C is a constant depending on d only. At this point we use the fact that the number of distinct characteristic polynomials of elements of $\mathbf{G}(\mathcal{O}_\mathbb{K}/\mathcal{P})$ depends polynomially on $|\mathcal{P}|$ and thus is exponential in n.

In fact our methods can yield variants of Theorem 1.2, see Section 9. For example, if the Zariski closure $\mathbf{G}$ of Γ is a connected simple algebraic group and P is an arbitrary non-constant polynomial function on $\mathbf{G}$, then P achieves exponentially many values on $B_\Sigma(n)$, where the exponential rate of growth has a lower bound depending only on d. While it is possible to extend this latter result to the semisimple case using the same method, we do not include a proof in this paper for two reasons. Firstly some serious technicalities arise, in particular when applying strong approximation in positive characteristic due to the presence of Frobenius twists (see [24]). Secondly as shown to us by E. Hrushovski (private communication), it is possible to give a completely different treatment of this theorem (including an extension of Theorem 9.1 to semisimple groups). His approach avoids any appeal to strong approximation nor to the product theorem, but uses instead ideas from model theory and still reduces the counting problem to the ordinary word growth, hence to [3], as in Theorem 7.1 below.

Outline of the paper. The paper is organized as follows. In Section 2, we sketch the proof in the particular case of Zariski dense subgroups of $\mathrm{SL}_d(\mathbb{Z})$. In Section 4 we give a quantitative version of the fact that reduction modulo a large prime is injective on large finite subsets. In Section 6, we derive a fast generation result for the mod p quotients of Γ using the strong approximation theorem and the results on approximate groups mentioned above, which we recall in Section 5. In Section 7, we show that the ball of radius n in Γ cannot be covered by less than an exponential number of proper hypersurfaces of $\mathbf{G}$ of bounded degree. There we elaborate slightly more than what is needed for the immediate application to Theorem 1.2. We develop further applications in Section 9. The proof of 1.2 is completed in Section 8.

Acknowledgements. The first two authors would like to thank the Hebrew University for its hospitality during their visit in the autumn of 2010. The first author acknowledges support from the European Research Council through grant no GADA-208091. So does the third author through grant no 226135. We are grateful to M. Sapir for bringing the problem of conjugacy growth of linear groups to our attention. We also thank A. Chambert-Loir, M. Brion and E. Hrushovski for useful conversations and A. Mann for his comments on an early version of this paper. Finally we thank G. Prasad, who spotted an inaccuracy in an earlier version of this article.

2. Sketch of proof: a particular case

We provide here a sketch of proof in the particular case of Zariski dense subgroups of $\mathrm{SL}_m(\mathbb{Z})$. It contains the highlights of the proof of the general case, although the latter is technically more involved.

Theorem 2.1. *For every $m \geq 2$, there exists a constant $c = c(m) > 0$ such that for every symmetric set Σ in $\mathrm{SL}_m(\mathbb{Z})$ generating a Zariski-dense subgroup of SL_m, there exists $N = N(\Sigma, m) \in \mathbb{N}$ such that for every $n \geq N(\Sigma, m)$ the number of traces of elements of the ball $B_\Sigma(n)$ is at least e^{cn}.*

The proof will use the following three theorems. We state each one here in the case of our specific situation. The first theorem asserts that $\mathrm{SL}_m(\mathbb{Z})$ and its Zariski-dense subgroups have uniform exponential growth in a uniform way:

Theorem 2.2 (Eskin-Mozes-Oh [8]). *For every $m \geq 2$, there exists $\alpha = \alpha(m) > 0$ such that $|B_\Sigma(n)| \geq e^{\alpha n}$ for every $n \in \mathbb{N}$ and every symmetric subset Σ in $\mathrm{SL}_m(\mathbb{Z})$ generating a Zariski-dense subgroup.*

Although Eskin-Mozes-Oh only state their theorem in [8] for a fixed subgroup of $\mathrm{SL}_m(\mathbb{Z})$, their proof carries over without any changes to yield the above result uniformly over the Zariski-dense subgroups of $\mathrm{SL}_m(\mathbb{Z})$. For the general case of our Theorem 1.1, we will require the more general uniformity result established in [3], where it is shown that the rate of growth can be bounded below by a uniform constant independently of the ring of definition.

The second is the recently established Product Theorem:

Theorem 2.3 (Breuillard-Green-Tao [7], Pyber-Szabó [25]). *For every $\delta > 0$ there exists a number $N_\delta = N_\delta(m) > 0$ such that for every prime number p and every symmetric generating subset A of $\mathrm{SL}_m(\mathbb{Z}/p\mathbb{Z})$ of size at least p^δ we have $A^{N_\delta} = \mathrm{SL}_m(\mathbb{Z}/p\mathbb{Z})$.*

The third is the Strong Approximation Theorem:

Theorem 2.4 (Matthews-Vaserstein-Weisfeiler [19]). *If Γ is a Zariski-dense subgroup of $\mathrm{SL}_m(\mathbb{Z})$, then for all but finitely many primes p, we have $\pi_p(\Gamma) = \mathrm{SL}_m(\mathbb{Z}/p\mathbb{Z})$, where π_p is the reduction mod p map.*

Let Σ be as in the statement of Theorem 2.1 and define $C := \max_{s\in\Sigma} \|s\|$ where $\|T\|$ denotes the operator norm of a matrix T. For every $n \in \mathbb{N}$ large enough, choose a symmetric subset B_n of $B_\Sigma(n)$ of size $e^{\alpha n}$ containing Σ, where α is given by Theorem 2.2.

We claim that there is $k_0 \in \mathbb{N}$ such that for $k \geq k_0$ there exists a prime number p in the interval $[e^{2\alpha k}, e^{4\alpha k}]$ such that the restriction of the map $\pi_p : \mathrm{SL}_m(\mathbb{Z}) \to \mathrm{SL}_m(\mathbb{Z}/p\mathbb{Z})$ to B_k is injective.

If k is large enough, by the distribution of the prime numbers (e.g. Chebyshev's estimate, see Theorem 3.3), there exist at least $e^{3\alpha k}$ prime numbers in the interval $[e^{2\alpha k}, e^{4\alpha k}]$. For each $(g, h) \in B_k \times B_k$, each nonzero entry of the matrix $gh^{-1} - I_m$ is at most C^{2k}, so the number of its prime divisors greater than $e^{2\alpha k}$ is at most $\frac{\log(C^{2k})}{\log(e^{2\alpha k})} = \frac{\log C}{\alpha}$. We have m^2 entries for each gh^{-1}, and $\leq e^{2\alpha k}$ possible pairs (g, h), so the number of primes greater than $e^{2\alpha k}$ dividing at least one nonzero entry of $gh^{-1} - I_m$ for some $(g, h) \in B_k \times B_k$ is $\leq \frac{\log C}{\alpha} m^2 e^{2\alpha k}$, which is less than $e^{3\alpha k}$ for k large enough. Thus, by the pigeonhole principle, if k is large enough, there exists a prime p in $[e^{2\alpha k}, e^{4\alpha k}]$ not dividing any nonzero entry of $gh^{-1} - I_m$ for any $(g, h) \in B_k \times B_k$. This means that B_k maps injectively into $\mathrm{SL}_m(\mathbb{Z}/p\mathbb{Z})$.

Let $N = N_{1/4}$ be the constant in Theorem 2.3. Let $n \geq N(k_0 + 1)$ and $k = \lfloor n/N \rfloor$; by the above we can fix a prime p so that $\pi_p|_{B_k}$ is injective. By Theorem 2.4, $\pi_p(B_k)$ generates $\mathrm{SL}_m(\mathbb{Z}/p\mathbb{Z})$ as soon as n is large enough. Moreover, we have $|\pi_p(B_k)| \geq e^{\alpha k} \geq p^{1/4}$, so Theorem 2.3 implies that $\pi_p(B_\Sigma(n)) = \mathrm{SL}_m(\mathbb{Z}/p\mathbb{Z})$. Since $m \geq 2$, every element of $\mathbb{Z}/p\mathbb{Z}$ is a trace of some matrix in $\mathrm{SL}_m(\mathbb{Z}/p\mathbb{Z})$; accordingly the number of traces of elements which belong to $B_\Sigma(n)$ is at least $p \geq e^{2\alpha k} \geq e^{\alpha n/N}$, and this yields the assertion of Theorem 2.1.

3. Preliminaries and notation

3.1. **Functions.** For real-valued functions, we write $f(x) \preceq g(x)$ or $f(x) = O(g(x))$ if for some constant $C > 0$ we have $f(x) \leq Cg(x)$ for all large x. If $f(x) \preceq g(x) \preceq f(x)$ we write $f(x) \approx g(x)$.

3.2. **Global fields.** The letter $\mathbb{K}$ will always denote a global field, that is, either a number field, i.e. a finite extension of $\mathbb{Q}$, or a function field, i.e. a finitely generated field of transcendence degree one over a finite field. We denote by $\overline{\mathbb{K}}$ an algebraic closure of $\mathbb{K}$. A place on $\mathbb{K}$ is the norm induced by the embedding of $\mathbb{K}$ into a nondiscrete locally compact field. We identify equivalent places, i.e. places inducing the same topology on $\mathbb{K}$.

Let S be a nonempty finite set of places on $\mathbb{K}$ including all Archimedean ones. The ring of S-integers of $\mathbb{K}$, defined as $\mathcal{O}_{\mathbb{K}}(S) = \{a \in \mathbb{K} : \forall v \notin S,\ v(a) \leq 1\}$ is a subring of $\mathbb{K}$ whose field of fractions is $\mathbb{K}$. Moreover, $\mathcal{O}_{\mathbb{K}}(S)$ is a finitely generated Dedekind domain. Let $\mathrm{Spec}(\mathcal{O}_{\mathbb{K}}(S))$ be the set of its prime ideals, consisting of $\{0\}$ along with infinitely many maximal ideals of finite index. If $\mathcal{P} \in \mathrm{Spec}(\mathcal{O}_{\mathbb{K}}(S))$ is nonzero, the size of the residue field $|\mathcal{P}| = |\mathcal{O}_{\mathbb{K}}(S)/\mathcal{P}|$ is called the norm of $\mathcal{P}$. If $\mathcal{P} = \{0\}$ we set $|\mathcal{P}| = 0$.

Let $V_{\mathbb{K}}$ be the set of all places of $\mathbb{K}$. For every $v \in V_{\mathbb{K}}$, let $\mathbb{K}_v$ be the completion of $\mathbb{K}$ with respect to v. Let $\mathbb{A} = \prod_{v\in S} \mathbb{K}_v$. If v is a place associated to a prime ideal $\mathcal{P}$ of $\mathcal{O}_{\mathbb{K}}$, we may choose for $|\cdot|_v$ the absolute value $|x|_v = q^{-\nu_{\mathcal{P}}(x)}$, where q is the size of the residue field $\mathcal{O}_{\mathbb{K}}/\mathcal{P}$ and $\nu_{\mathcal{P}}(x)$ the $\mathcal{P}$-valuation of x, so that the product formula holds for all $x \in \mathbb{K}^\times$, $\prod_{v\in V_{\mathbb{K}}} |x|_v = 1$. Let $\|\cdot\|_v$ be the standard norm on $\mathbb{K}_v^d$ relative to $|\cdot|_v$, i.e. the Euclidean (or Hermitian) norm if v is Archimedean and the supremum norm if v is non-Archimedean (i.e. $|x|_v = \max |x_i|_v$). We also denote by $\|\cdot\|_v$ the associated operator norm on $\mathrm{GL}_d(\mathbb{K}_v)$ and we let $\|(g_v)_v\| = \max \|g_v\|_v$ for all $g = (g_v)_v \in \mathrm{GL}_d(\mathbb{A})$ and $|a| = \max |a_v|_v$ for all $a = (a_v)_v \in \mathbb{A}$.

If $S \subset S'$ then $\mathcal{O}_{\mathbb{K}}(S')$ is a localization of $\mathcal{O}_{\mathbb{K}}(S)$ and $\mathrm{Spec}(\mathcal{O}_{\mathbb{K}}(S'))$ is the complement of a finite subset of $\mathrm{Spec}(\mathcal{O}_{\mathbb{K}}(S))$. Moreover, for any $\mathcal{P} \in \mathrm{Spec}(\mathcal{O}_{\mathbb{K}}(S'))$ there is a canonical field isomorphism between residual fields $\mathcal{O}_{\mathbb{K}}(S)/(\mathcal{P} \cap \mathcal{O}_{\mathbb{K}}(S)) \to \mathcal{O}_{\mathbb{K}}(S')/\mathcal{P}$. We thus write $\mathbb{K}_{\mathcal{P}} = \mathcal{O}_{\mathbb{K}}(S)/\mathcal{P}$. In particular, apart from finitely many primes, $\mathrm{Spec}(\mathcal{O}_{\mathbb{K}}(S))$ and its norm function do not depend on S and we thus speak of "primes of $\mathbb{K}$" whenever this finite indeterminacy is irrelevant. For instance we will use

Theorem 3.3 (Chebyshev, Landau [27, Theorem 5.12], [9, Theorem 7])**.** *Let $\mathbb{K}$ be a global field. Let $\pi(x)$ be the number of primes of $\mathbb{K}$ of norm $\leq x$. Then*

$$\pi(x) \approx \frac{x}{\log(x)} \quad (x \to +\infty).$$

This is a weak form of the prime number theorem, which asserts that $\frac{\pi(x)}{x/\log(x)}$ actually tends to 1. Theorem 3.3 has the following consequence.

Lemma 3.4. *Let $\mathbb{K}_0 \subset \mathbb{K}$ be an extension of global fields. Then the number of primes $\mathcal{P}$ of $\mathbb{K}$ of norm $\leq x$ such that $f_{\mathcal{P}} > 1$, where $f_{\mathcal{P}} = [\mathcal{O}_{\mathbb{K}}/\mathcal{P} : \mathcal{O}_{\mathbb{K}_0}/(\mathcal{P} \cap \mathcal{O}_{K_0})]$ is the residual degree, is $o(\sqrt{x})$. In particular, the number of primes of $\mathbb{K}$ of norm $\leq x$ and with $f_{\mathcal{P}} = 1$ is $\approx x/\log(x)$.*

Proof. Let $\mathfrak{p} = \mathcal{P} \cap \mathcal{O}_{\mathbb{K}_0}$ be the prime below $\mathcal{P}$. We have $|\mathcal{P}| = |\mathfrak{p}|^{f_{\mathcal{P}}}$. If $f_{\mathcal{P}} \geqslant 2$ and $|\mathcal{P}| \leqslant x$ it follows that $|\mathfrak{p}| \leqslant \sqrt{x}$. Since there are at most $[\mathbb{K} : \mathbb{K}_0]$ primes $\mathcal{P}$ above any given prime of $\mathcal{O}_{\mathbb{K}_0}$, by Chebyshev's theorem there are at most $O(\sqrt{x}/\log(x))$ primes $\mathcal{P}$ of $\mathbb{K}$ with $f_{\mathcal{P}} \geqslant 2$ and $|\mathcal{P}| \leqslant x$. We are done. □

3.5. **Reduction modulo a prime.** Let $\mathbb{K}$ be a global field. Let $\mathbf{G}$ be a linear algebraic group defined over $\mathbb{K}$. We want to define "reduction modulo $\mathcal{P}$" for $\mathbf{G}$. Let A be a finitely generated subdomain with $\mathbb{K}$ as field of fractions. We can write the ring of functions as $\mathbb{K}[\mathbf{G}] = M \otimes_{A_b} \mathbb{K}$, where A_b is a suitable localization of A and $M \subset \mathbb{K}[\mathbf{G}]$ a Hopf algebra over A_b. This choice being made, we write $A_b[\mathbf{G}]$ instead of M. Thus for any A_b-algebra B we can define functorially $\mathbf{G}(B) = \mathrm{Hom}(A_b[\mathbf{G}], B)$ which is naturally a group. In particular $\mathbf{G}(A/\mathcal{P})$ is well-defined for every $\mathcal{P} \in \mathrm{Spec}(A_b)$, and the reduction mod $\mathcal{P}$ map is the group homomorphism $\mathbf{G}(A_b) \to \mathbf{G}(A_b/\mathcal{P})$.

This depends on the choice of the Hopf algebra structure M over A_b; if two different choices M_i over A_{b_i} are made giving rise to forms $\mathbf{G}_i$ of $\mathbf{G}$ over A_{b_i}, the identity induces an isomorphism $M_1 \otimes_{A_{b_1}} \mathbb{K} \simeq M_2 \otimes_{A_{b_2}} \mathbb{K}$; such an isomorphism is actually defined over a suitable common localization A_b, and in particular, restricted to the class of A_b-algebras, the functors $B \mapsto \mathrm{Hom}(M_i, B)$ are equivalent for $i = 1, 2$. Given two fixed choices M_i over A_{b_i}, $i = 1, 2$, the group scheme structures will coincide for all but finitely many $\mathcal{P}$'s. Similarly, if Γ is a finitely generated subgroup of $\mathbf{G}(\mathbb{K})$, then for $\mathcal{P}$ large enough, we can talk about the homomorphism $\Gamma \to \mathbf{G}(\mathbb{K}_{\mathcal{P}})$, where $\mathbb{K}_{\mathcal{P}} = \mathcal{O}_{\mathbb{K}}(S)/\mathcal{P}$.

Moreover, $A_b[\mathbf{G}] \otimes_{A_b} \overline{\mathbb{K}}$ is a reduced ring and is a domain if $\mathbf{G}$ is connected. This continues to hold modulo $\mathcal{P}$ for $\mathcal{P}$ large enough, namely $\mathbf{G}$ is reduced over $\mathbb{K}_{\mathcal{P}}$, and is connected if $\mathbf{G}$ is connected. Indeed, since $A_b[\mathbf{G}]$ is a flat A_b-module (if we suppose as we may that A_b is Dedekind, then flat means torsion-free), "geometrically reduced" and "geometrically integral" are open properties on $\mathrm{Spec}(A_b)$ [10, 12.1.1].

Finer arguments of the same flavour show that if $\mathbf{G}$ is semisimple and simply connected, then this still holds over $\mathbb{K}_{\mathcal{P}}$ for large $\mathcal{P}$.

4. Finding many good prime ideals

In this section, we describe a pigeonhole argument (Corollary 4.2 below). In combination with Chebyshev's weak version of the prime number theorem for global fields, this will yield many good prime ideals modulo which the "ball" Σ^n will be preserved.

As above $\mathbb{K}$ denotes a global field and S a finite set of places including all Archimedean ones. Let $\{B_n\}_n$ be a family of finite subsets of $\mathrm{GL}_d(\mathcal{O}_{\mathbb{K}}(S))$ such that:

- $B_n \subset W^n(= W \cdot ... \cdot W)$ for some finite subset W of $\mathrm{GL}_d(\mathcal{O}_{\mathbb{K}}(S))$;
- $|B_n| \geqslant e^{\alpha n}$ for some fixed $\alpha > 0$.

The reader interested in a proof of Theorem 1.2 under the assumption that the Zariski closure of $\langle\Sigma\rangle$ is connected semisimple, can always suppose, in the forthcoming results, that $B_n = \Sigma^n$. This is, in particular, enough in order to obtain Theorem 1.1 (that is, exponential conjugacy growth without the uniformity in the field claimed in Theorem 1.2), because every non-virtually-solvable linear group has a finite index subgroup with a quotient isomorphic to a Zariski-dense subgroup of a simple algebraic group.

Given a prime ideal $\mathcal{P}$ not in S, let $\pi_{\mathcal{P}}$ be the reduction mod $\mathcal{P}$ map from $\mathrm{GL}_d(\mathcal{O}_{\mathbb{K}}(S))$ to $\mathrm{GL}_d(\mathbb{F}_q)$, where $\mathbb{F}_q = \mathcal{O}_{\mathbb{K}}/\mathcal{P}$.

Proposition 4.1. *Suppose that $B_n \subset W^n$ are sets as above. There exists a constant $C = C(W,S) > 0$ such that for all n, all $\gamma \in B_n^{-1}B_n$ and $\rho > 1$ we have*

$$\kappa_{\rho^n}(\gamma) \leq \frac{C}{\log(\rho)},$$

where $\kappa_{\rho^n}(\gamma)$ is the number of primes $\mathcal{P}$ with $|\mathcal{P}| \geqslant \rho^n$ such that $\pi_{\mathcal{P}}(\gamma) = 1$.

Proof. We make use of the following easy consequence of the product formula: if $\mathcal{P}$ is a prime ideal in $\mathcal{O}_{\mathbb{K}}(S)$, then $|x|^{|S|} \geqslant |\mathcal{P}|$ for any $x \in \mathcal{P}\setminus\{0\}$. Similarly, if $g \in \mathrm{GL}_d(\mathcal{O}_{\mathbb{K}}(S))$, $g \neq 1$, and $g-1 \in M_d(\mathcal{P}_i)$ for k distinct primes ideals $\mathcal{P}_1$,...,$\mathcal{P}_k$ not in S, then $\|g-1\|^{|S|} \geqslant |\mathcal{P}_1|...|\mathcal{P}_k|$. So if $\pi_{\mathcal{P}_i}(\gamma) = 1$ for each $\mathcal{P}_1$,...,$\mathcal{P}_k$, then $\|\gamma-1\|^{|S|} \geqslant \rho^{nk}$. But $\|\gamma-1\| \leqslant 1+M^{2n} \leqslant M^{3n}$, where $M := \max\{\|g\|, g \in W\}$. Hence the result. □

We then derive:

Corollary 4.2. *With probability tending to 1 as n tends to infinity, a prime $\mathcal{P}$ of $\mathbb{K}$ whose norm $|\mathcal{P}|$ lies in the interval $[e^{3\alpha n}, e^{4\alpha n}]$ must satisfy $|\pi_{\mathcal{P}}(B_n)| \geqslant |\mathcal{P}|^{\frac{1}{4}}$.*

Proof. Let P_n be a subset of B_n of size $e^{\alpha n}$. If $\pi_{\mathcal{P}}$ is not injective on P_n, then there must exist $\gamma \in P_n^{-1}P_n$ such that $\pi_{\mathcal{P}}(\gamma) = 1$ while $\gamma \neq 1$. However by the last proposition, there are at most $\kappa := C/3\alpha$ such primes $\mathcal{P}$ with norm $|\mathcal{P}| \geqslant e^{3\alpha n}$. Hence there are at most $\kappa |P_n|^2 = O(e^{2\alpha n})$ possibilities for such a prime. However, by Chebyshev's theorem (Theorem 3.3 above), there are $\approx e^{4\alpha n}/n$ primes with norm in $[e^{3\alpha n}, e^{4\alpha n}]$. Hence for most such primes $\pi_{\mathcal{P}}$ is injective on P_n, and thus $|\pi_{\mathcal{P}}(B_n)| \geqslant e^{\alpha n} \geqslant |\mathcal{P}|^{\frac{1}{4}}$. □

5. Approximate subgroups and fast generation in semisimple algebraic groups

One of the key ingredients in the proof of our main theorem, is the following recent result regarding approximate subgroups of simple algebraic groups over finite fields.

Let $\mathbf{G} \subset \mathrm{GL}_d$ be an algebraic group defined over an algebraically closed field k. We will say that a closed algebraic subvariety $\mathcal{V}$ of $\mathbf{G}$ has bounded *complexity* (say bounded by $M \geqslant 1$) if it is defined as the set of zeros of at most M polynomial maps on $\mathbf{G}$ of degree at most M. We will also say that a subset of $\mathbf{G}$ is M-sufficiently Zariski dense if it is not contained in a proper closed algebraic subvariety of $\mathbf{G}$ of complexity at most M. For more details about this definition, we refer the reader to [7] especially Section 3 and Appendix A therein. The following was obtained in [7].

Theorem 5.1 (Product Theorem)**.** *Let $\mathbf{G}$ be a (connected) almost simple linear algebraic group of dimension d defined over an algebraically closed field k. There exist constants $\varepsilon, C > 0$, depending only on d and not on k, such that the following holds. Let A be a finite subset of $\mathbf{G}(k)$, then*

- *either $\langle A\rangle$ is not C-sufficiently Zariski-dense in $\mathbf{G}$, that is A is contained in a proper algebraic subgroup of $\mathbf{G}$ of complexity at most C.*
- *or $|AAA| \geqslant \min\{|\langle A\rangle|, |A|^{1+\varepsilon}\}$.*

The above was obtained independently by Pyber and Szabó ([25]) in the case when $k = \overline{\mathbb{F}_p}$ and A generates $\mathbf{G}(\mathbb{F}_q)$, which is the hardest case and the only one we will use in this paper. As a direct consequence, we get:

Corollary 5.2. *Let $\mathbf{H}$ be a simple algebraic group defined over a finite field $\mathbb{F}_q$, of dimension at most d. Let $\beta > 0$. Then there is $D = D(\beta, d) > 0$ such that the following holds: if A is a finite generating subset of $\mathbf{H}(\mathbb{F}_q)$ such that $|A| \geqslant q^{\beta}$, then $A^D = \mathbf{H}(\mathbb{F}_q)$.*

6. Strong approximation

To apply Corollary 5.2, we need to know that Γ maps onto many mod $\mathcal{P}$ quotients. This is a consequence of the so-called "strong approximation", a result due to Weisfeiler [29], except some tricky cases due to the existence of "non-standard isogenies" in characteristic two or three, and the general result is due to Pink [24]. We have:

Theorem 6.1. *Let $\mathbb{K}$ be a global field of characteristic p (possibly $p = 0$) and $\mathbf{G} \subset \mathrm{GL}_d$ be a simply connected absolutely simple $\mathbb{K}$-subgroup. Let Γ be a finitely generated Zariski dense subgroup of $\mathbf{G}$ contained in $\mathbf{G}(\mathbb{K})$. Then with probability tending to one when $x \to \infty$, if $\mathcal{P}$ is a prime of $\mathbb{K}$ with norm $\leq x$, then $\pi_{\mathcal{P}}(\Gamma) = \mathbf{G}(\mathbb{K}_{\mathcal{P}})$.*

Proof. By Weisfeiler's theorem [29, Theorem 1.1] (or Pink's version [24] in case of characteristic 2 and 3) there exists a finitely generated subfield $\mathbb{K}_0$ of $\mathbb{K}$ (namely the subfield generated by the traces of $\mathrm{Ad}(\Gamma)$ in characteristic 0) and a $\mathbb{K}_0$-structure on $\mathbf{G}$ such that $\Gamma \subset \mathbf{G}(\mathbb{K}_0)$ and for all $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_{\mathbb{K}_0})$ large enough we have $\pi_{\mathfrak{p}}(\Gamma) = \mathbf{G}((\mathbb{K}_0)_{\mathfrak{p}})$. Let $\mathcal{P}$ be a prime of $\mathcal{O}_{\mathbb{K}}$ of norm $\leq x$, with residual degree $f_{\mathcal{P}} = [\mathcal{O}_{\mathbb{K}}/\mathcal{P} : \mathcal{O}_{\mathbb{K}_0}/\mathfrak{p}]$, where $\mathfrak{p} = \mathcal{P} \cap \mathcal{O}_{\mathbb{K}_0}$. We can suppose that $f_{\mathcal{P}} = 1$, since this holds with probability tending to one by Lemma 3.4. Hence

$$\pi_{\mathcal{P}}(\Gamma) \supseteq \pi_{\mathfrak{p}}(\Gamma) = \mathbf{G}(\mathcal{O}_{\mathbb{K}_0}/\mathfrak{p}) = \mathbf{G}(\mathcal{O}_{\mathbb{K}}/\mathcal{P}).$$

□

Combining Theorem 6.1, Corollary 5.2, and Corollary 4.2, we obtain

Corollary 6.2. *For every d and $\alpha > 0$ there exists $D = D(d, \alpha)$ such that the following holds. Let $\mathbb{K}$ be a global field and $\mathbf{H}$ be a simply connected absolutely simple $\mathbb{K}$-group. Let Γ be a finitely generated Zariski-dense subgroup of $\mathbf{H}(\mathbb{K})$ and $W \subset \mathrm{GL}_d(\mathbb{K})$ a finite subset. Let $(B_n)_n$ be a family of subsets of $\mathbf{H}(\mathbb{K})$ such that*

- *$B_n \subset W^n$ for every $n \geqslant 1$,*
- *$\Gamma \subset \langle B_n \rangle$ for all n large enough,*
- *$|B_n| \geqslant e^{\alpha n}$.*

Then, with probability tending to one as $n \to \infty$, if $\mathcal{P}$ is a prime of $\mathbb{K}$ of norm in $[e^{3\alpha n}, e^{4\alpha n}]$, we have

$$\pi_{\mathcal{P}}(B_n^D) = \mathbf{H}(\mathbb{K}_{\mathcal{P}}).$$

Proof. By Corollary 4.2, with probability tending to one as n tends to $+\infty$, a prime $\mathcal{P}$ with norm $|\mathcal{P}| \in [e^{3\alpha n}, e^{4\alpha n}]$ satisfies $|\pi_{\mathcal{P}}(B_n)| \geq |\mathcal{P}|^{\frac{1}{4}}$. By Corollary 5.2, there exists $D > 0$ depending only on d such that, provided $\pi_{\mathcal{P}}(\Gamma) = \mathbf{H}(\mathbb{K}_{\mathcal{P}})$ for all i, we have $\pi_{\mathcal{P}}(B_n^D) = \mathbf{H}(\mathbb{K}_{\mathcal{P}})$. Finally, the condition $\pi_{\mathcal{P}}(\Gamma) = \mathbf{H}(\mathbb{K}_{\mathcal{P}})$ holds with probability tending to one by Theorem 6.1. □

7. Covering balls by subvarieties

The following theorem indicates that in a simple algebraic group, large balls cannot be covered by a small number of subvarieties of bounded complexity. Let $\mathbf{G}$ be a connected simple algebraic group defined over a global field $\mathbb{K}$ with $d = \dim \mathbf{G}$. We fix a linear $\mathbb{K}$-embedding $\mathbf{G} \leqslant \mathrm{GL}_d$. Suppose that Γ is a Zariski dense subgroup of $\mathbf{G}(\mathbb{K})$. Let $W \subset \mathrm{GL}_d(\mathbb{K})$ be a finite subset. Now let (B_n) be a family of finite sets of $\mathbf{G}(\mathbb{K})$ such that

- $B_n \subset W^n$ for every $n \geqslant 1$,
- $\Gamma \subset \langle B_n \rangle$ for all n large enough,
- $|B_n| \geqslant e^{\alpha n}$ for some fixed $\alpha > 0$.

Theorem 7.1. *Given B_n and $\alpha > 0$ as above and $M > 0$ there exist $D = D(d, \alpha) \geqslant 1$ (independent of M) and $n_0 = n_0(d, \alpha, M) \geqslant 1$, such that the following holds. Let Θ_n be the smallest $k \geqslant 1$ such that there are proper subvarieties $\mathcal{V}_1, ..., \mathcal{V}_k$ of $\mathbf{G}$ with complexity bounded by M such that*

$$B_n^D \subset \bigcup_{1 \leq i \leq k} \mathcal{V}_i.$$

Then $\Theta_n \geqslant e^{\alpha n}$ for every $n \geqslant n_0$.

Remark 7.2. Upon hearing of the above theorem E. Hrushovski (personal communication) kindly supplied an alternative argument for it using the methods of model theory. While our proof makes use of [7] (which in turn is inspired by [14]), his derivation uses the Larsen-Pink estimates [14] more directly.

We will use the following estimate on the number of points on a variety over a finite field.

Proposition 7.3. *Let d, m be positive integers. There exists a constant $c = c(d, m)$ such that for every finite field $\mathbb{F}_q$ and every closed r-dimensional subvariety X of the d-dimensional affine space over $\mathbb{F}_q$ of complexity $\leq m$ we have*

$$\# X(\mathbb{F}_q) \leq c q^r.$$

This is probably well known to experts (modulo the definition of complexity), but in a lack of reference we provide a proof based on the Lang-Weil estimates, although they are probably also not needed for this upper bound.

Proof. A much more precise asymptotic behavior with upper and lower bounds is given by the Lang-Weil theorem [13], but it requires the assumption that the variety is absolutely irreducible. As we will see below, there is no asymptotic lower bound by q^r in case the variety is irreducible but not absolutely irreducible.

Let us check however that the theorem follows from the original statement in [13]. We argue by induction on the integer $r \in [0, d]$. Let us suppose that the theorem is proved for all $r' < r$ and let X have dimension r. First, because of the bound on the complexity, we have a bound on the number of irreducible components [7, Lemma A.4], and therefore it is enough to prove the theorem when X is irreducible over $\mathbb{F}_q$ and r-dimensional.

- Suppose that X is absolutely irreducible. Then the Lang-Weil Theorem (as stated in [13]) directly provides the desired upper bound.
- Suppose that X is not absolutely irreducible. Let $X_1, \dots, X_k$ be the irreducible components of X. By [7, Lemma A.4] the integer k can be bounded in terms of d, m. The components X_i are defined over some finite extension of $\mathbb{F}_q$. This is a Galois extension, and X is irreducible over $\mathbb{F}_q$, so the action of the Galois group on these components is transitive. Moreover, $X(\mathbb{F}_q)$ is contained in $Y = \bigcap X_i$. By assumption, $k \geq 2$, so $Y = \bigcap X_i$ has dimension $< r$ and is defined over $\mathbb{F}_q$ and has complexity bounded by some constant depending only on m and k, hence of d and m. So by induction we get $\#Y(\mathbb{F}_q) \leq c'q^{r-1}$ for some constant $c' = c(m, d)$ and
$$\#X(\mathbb{F}_q) \leq \#Y(\mathbb{F}_q) \leq c'q^{r-1} \leq c'q^r.$$

Note that the induction has only d steps, hence the constant c eventually remains controlled by (d, m). □

Proof of Theorem 7.1. To apply Corollary 6.2, we need to assume that $\mathbf{G}$ is simply connected. So first assume that the theorem is proved when $\mathbf{G}$ is simply connected and let us prove it in general. Let $\kappa : \tilde{\mathbf{G}} \to \mathbf{G}$ be the simply connected covering of $\mathbf{G}$; it is defined over $\mathbb{K}$; its kernel has cardinality bounded by some number only depending on d, and it has bounded degree. Now $\kappa^{-1}(B_n)$ is also a family of generating subsets of $\kappa^{-1}(\Gamma)$ satisfying the required assumptions, and a covering of B_n by k proper subvarieties pulls pack to a covering of $\kappa^{-1}(B_n)$ by k proper subvarieties. We can therefore assume that $\mathbf{G}$ is simply connected.

Let S be some non-empty finite set of valuations on $\mathbb{K}$ including the Archimedean ones and such that $W \subset \mathrm{GL}_d(\mathcal{O}_{\mathbb{K}}(S))$. By Lemma 7.4 below, if we choose S large enough, then $A = \mathcal{O}_{\mathbb{K}}(S)$ is a principal ideal ring.

Enlarging S again if necessary, we can ensure that $A[\mathbf{G}] \otimes_A A/\mathcal{P}$ is a reduced ring for all primes $\mathcal{P}$ (a priori this holds for all but finitely many $\mathcal{P}$'s, see §3.5). We may also fix an A-structure on $\mathbf{G}$, i.e. we fix an isomorphism $\mathbb{K}[\mathbf{G}] = A[\mathbf{G}] \otimes_A \mathbb{K}$, where $A[\mathbf{G}] \subset \mathbb{K}[\mathbf{G}]$ is a Hopf A-subalgebra.

Now suppose that $B_n^D \subset \bigcup_{i=1}^{k_n} X_i$ with X_i of complexity $\leq M$. We can suppose without loss of generality that X_i is given as a proper hypersurface $\{f_i = 0\}$ in $\mathbb{K}[\mathbf{G}]$.

Now multiplying by a suitable nonzero element of $\mathbb{K}$ we can even assume that $f_i \in A[\mathbf{G}]$. Moreover, if $f_i \in aA[\mathbf{G}]$ for some $a \in A - \{0\}$ then we can replace

f_i by $a^{-1}f_i$ without changing its set of zeros. Since $A[\mathbf{G}]$ is Noetherian, we can suppose that $f_i \notin aA[\mathbf{G}]$ for any $a \in A$ not invertible in $A[\mathbf{G}]$ (or equivalently in A: because of the co-unity $A[\mathbf{G}] \to A$, if $a \in A$ is not invertible then it remains non-invertible in $A[\mathbf{G}]$).

We have the following claim: *for every prime ideal $\mathcal{P}$ of A, f_i defines a proper hypersurface $X_i^{\mathcal{P}}$ of $\mathbb{K}_{\mathcal{P}}[\mathbf{G}]$.*

Let us first finish the proof of Theorem 7.1, granting the claim for a moment. For all $\mathcal{P}$'s we have

$$\pi_{\mathcal{P}}(B_n^D) \subset \bigcup_{i=1}^{k_n} X_i^{\mathcal{P}}(\mathbb{K}_{\mathcal{P}}).$$

By Corollary 6.2, with probability tending to one as n tends to $+\infty$, if $\mathcal{P}$ is has norm in $[e^{3\alpha n}, e^{4\alpha n}]$, then $\pi_{\mathcal{P}}(B_n^D) = \mathbf{G}(\mathbb{K}_{\mathcal{P}})$. For such a prime, we get

$$|\mathbf{G}(\mathbb{K}_{\mathcal{P}})| \leq k_n \sup_i |X_i^{\mathcal{P}}(\mathbb{K}_{\mathcal{P}})|.$$

If d is the dimension of $\mathbf{G}$, using the shorthand $q := |\mathcal{P}|$, then the Lang-Weil upper bound in Theorem 7.3 gives $|X_i^{\mathcal{P}}(\mathbb{K}_{\mathcal{P}})| \leq cq^{d-1}$; while the Lang-Weil theorem in its original form (using that $\mathbf{G}$ is absolutely irreducible) yields $|\mathbf{G}(\mathbb{K}_{\mathcal{P}})| \geq c'q^d$; here c, c' are positive constants depending only on d and M. Thus $c'q^d \leq k_n cq^{d-1}$, hence $k_n \geq \frac{c'}{c}q \geq \frac{c'}{c}e^{3\alpha n}$ and this ends the proof of the theorem modulo the claim.

Let us verify the claim. If $f_i = 0$ is all of $\mathbf{G}$ modulo $\mathcal{P}$, this means that f_i is nilpotent in $A[\mathbf{G}] \otimes_A A/\mathcal{P}$. Since the latter is a reduced ring, this means that f_i is zero in $A[\mathbf{G}] \otimes_A A/\mathcal{P} = A[\mathbf{G}]/\mathcal{P}A[\mathbf{G}]$, i.e. that $f_i \in \mathcal{P}A[\mathbf{G}]$. But A is a principal ideal ring, so we can write $\mathcal{P} = pA$, so $f_i \in pA[\mathbf{G}]$. By our choice of f_i, this implies that p is invertible in A, a contradiction. □

We made use of the following classical lemma. Since we did not find a reference, we include a proof.

Lemma 7.4. *There exists a finitely generated principal ideal subring A of $\mathbb{K}$ containing $\mathcal{O}_{\mathbb{K}}(S)$.*

Proof. Recall that if B is a domain with field of fractions K, a fractional ideal of B is by definition a nonzero finitely generated B-submodule of K. Under multiplication, they form a commutative semigroup with unity; if this is actually a group, B is called a Dedekind domain and the quotient of this group by its subgroup consisting of nonzero principal ideals is called the class group of B and is denoted by $\mathrm{Cl}(B)$.

Observe that if B is a Dedekind domain and D any multiplicative subset of $B - \{0\}$, $D^{-1}B$ is a Dedekind domain and the natural homomorphism $\mathrm{Cl}(B) \to \mathrm{Cl}(D^{-1}B)$ is surjective. Moreover, if I is a (finitely generated) ideal of B and $D \cap I \neq \varnothing$ then the image $D^{-1}I$ of I in $\mathrm{Cl}(D^{-1}B)$ is trivial.

Now assume that $B = \mathcal{O}_{\mathbb{K}}(S)$, so $K = \mathbb{K}$. Then B is a Dedekind domain and $\mathrm{Cl}(B)$ is finitely generated (it is finite in characteristic zero [21, Theorem I.6.3] and finite-by-cyclic in positive characteristic [27, Lemma 5.6]). Pick ideals $I_1, \dots, I_k$ of B which are representatives of generators of $\mathrm{Cl}(B)$, and let $s_j \in I_j \setminus \{0\}$ for each $j = 1, ..., k$ and $s = s_1 \cdot \ldots \cdot s_k$. Then it follows from the remarks above that the image of each I_j in $\mathrm{Cl}(B[1/s])$ is trivial and since $\mathrm{Cl}(B) \to \mathrm{Cl}(B[1/s])$ is surjective, we deduce that $\mathrm{Cl}(B[1/s])$ is the trivial group, i.e. $A = B[1/s]$ is a principal ideal domain. □

8. Proof of uniform exponential conjugacy growth

In this section, we prove Theorem 1.2, relying on Theorem 7.1. First, we show that without loss of generality, we may assume that the field of definition F is a global field (specialization step). Then we reduce to the reductive case and finally prove the theorem by intersecting the ball with the semisimple part using Theorem 7.1 to count conjugacy classes inside the semisimple part.

Specialization step.

In proving Theorem 1.2, the first step is to reduce the proof to the case when the field F is a global field $\mathbb{K}$. Since Σ is a finite set, the ring generated by the matrix entries of the elements of Σ is a finitely generated commutative ring R. Such rings have lots of homomorphisms to global fields $\mathbb{K}$. The proposition below says that we can choose such a ring homomorphism with the property that the image of $\langle\Sigma\rangle$ under the induced homomorphism on $\langle\Sigma\rangle$ into $\mathrm{GL}_d(\mathbb{K})$ remains non-virtually solvable. This process is traditionally called *specialization*, because the ring homomorphism from R to $\mathbb{K}$ is defined by specializing the values of a transcendence basis for R to algebraic values.

Proposition 8.1 (Specialization). *Let F be any field and R be a finitely generated subring of F. Let Σ be a finite symmetric subset of $\mathrm{GL}_d(R)$, which generates a non-virtually solvable subgroup $\langle\Sigma\rangle$. Then there exists a global field $\mathbb{K}$, with $\mathrm{char}(\mathbb{K}) = \mathrm{char}(F)$ and a ring homomorphism $\varphi : R \to \mathbb{K}$ inducing a group homomorphism $\overline{\varphi} : \langle\Sigma\rangle \to \mathrm{GL}_d(\mathbb{K})$ such that $\overline{\varphi}(\langle\Sigma\rangle)$ is non-virtually solvable.*

Proof. This is now classical. See for example [16, Proposition 2.2], [15, Theorem 4] and also [8, §4] or [5, Lemma 3.1]. □

This proposition allows us to assume that the field F is a global field $\mathbb{K}$ in the proof of Theorem 1.2, because if $g \in \langle\Sigma\rangle$, then the characteristic polynomial $\chi_{\overline{\varphi}(g)}$ coincides with $\varphi(\chi_g)$, so there are at least as many distinct characteristic polynomials arising from elements in Σ^n as there are from elements in $\overline{\varphi}(\Sigma)^n$.

Reduction to a reductive group.

Let $\mathbf{G}$ be the Zariski-closure of $\langle\Sigma\rangle$ in GL_d. Recall, by definition, that a reductive algebraic group is an algebraic group with no non-trivial unipotent normal subgroup. Note that we do not require reductive groups to be connected here. We have:

Lemma 8.2 (Going to the reductive part)**.** *Let $\mathbf{G} \subset \mathrm{GL}_d$ be an algebraic group defined over a field $\mathbb{K}$. There is a homomorphism of algebraic groups $\rho : \mathbf{G} \to \mathrm{GL}_d$ defined over a finite extension $\mathbb{K}'$ of $\mathbb{K}$, and with unipotent kernel, such that $\rho(\mathbf{G})$ is a reductive algebraic subgroup of GL_d defined over $\mathbb{K}'$ and such that $\chi(\rho(g)) = \chi(g)$, for every $g \in \mathbf{G}(\mathbb{K})$, where $\chi(g)$ is the characteristic polynomial of g in GL_d.*

Proof. Let $\mathbf{U}$ be the maximal normal unipotent subgroup of $\mathbf{G}$. It is a $\mathbb{K}$-closed algebraic subgroup and is thus defined over a finite extension $\mathbb{K}'$ of $\mathbb{K}$. Let $V = \mathbb{K}'^d$. Being unipotent, $\mathbf{U}$ admits a non-trivial subspace of fixed points V_1 in V, and in fact stabilizes a flag $V_1 \subsetneq V_2 \subsetneq ... \subsetneq V_r = V$, such that V_i/V_{i-1} consists of the $\mathbf{U}$-fixed points in V/V_{i-1}. Then $\mathbf{G}$ leaves each V_i invariant and its action on V_i/V_{i-1} factors through $\mathbf{G}/\mathbf{U}$. Replace the original representation by its semi-simplification, i.e. the representation ρ on $V = \oplus_i V_i/V_{i-1}$. It is easy to see that the new representation consists of the diagonal blocks of the old one and gives rise to the same characteristic polynomial as the old one, and that the kernel of ρ is unipotent. □

Accordingly, to prove Theorem 1.2, it is enough to do it under the additional assumptions that the field F is a global field, and the Zariski closure of Σ is reductive (possibly not connected): indeed applying Lemma 8.2 to the Zariski closure of the subgroup generated by Σ, since the kernel of ρ is nilpotent, the image of Σ still generates a non-virtually-solvable subgroup. What we actually show is the following. Recall that α_Σ was defined in (1.1).

Proposition 8.3. *For every d, there exists a constant $\eta(d) > 0$ such that if $\mathbb{K}$ is a global field and Σ a finite symmetric subset of $\mathrm{GL}_d(\mathbb{K})$ generating a non-virtually-solvable subgroup with (not necessarily connected) reductive Zariski closure $\mathbf{G}$, then*

$$\liminf_{n\to\infty} \frac{1}{n} \log \chi_\Sigma(n) \geqslant \eta(d)\alpha_\Sigma.$$

According to the uniform exponential growth of linear groups [3], α_Σ can be bounded below by a positive constant $c(d)$, not depending on $\mathbb{K}$ nor on the subgroup generated by Σ. Therefore, in view of the reductions above, Theorem 1.2 follows from Proposition 8.3, which we now proceed to prove.

Proof of Proposition 8.3. Let $\mathbf{G}^0$ be the connected component of the identity in $\mathbf{G}$, and let $\mathbf{H} := [\mathbf{G}^0, \mathbf{G}^0]$ be the commutator subgroup of $\mathbf{G}^0$. Then $\mathbf{H}$ is a connected semisimple algebraic group. Let $\pi : \mathbf{G} \to \mathbf{G}/\mathbf{H}$ be the quotient homomorphism; we have $\ker \pi = \mathbf{H}$. Let also $\mathbf{S}_i$ be the absolutely simple factors of $\mathbf{H}$ and $\pi_i : \mathbf{G}^0 \to \mathbf{S}_i$ the canonical projections. Up to passing to a finite extension of $\mathbb{K}$ if necessary, we may assume that the $\mathbf{S}_i$ and the projection maps π_i are defined over $\mathbb{K}$.

Since $\mathbf{G}/\mathbf{H}$ is virtually abelian, the growth of $|\pi(\Sigma^n)|$ is at most polynomial, say $\leq Cn^\kappa$. By the pigeonhole principle, there must exist a coset of $\mathbf{H}$ whose intersection with Σ^n has at least $|\Sigma^n|/Cn^\kappa$ elements. It follows that $|\Sigma^{2n} \cap \mathbf{H}| \geq |\Sigma^n|/Cn^\kappa$. Moreover, setting $\alpha_\Sigma(i) := \liminf_{n\to\infty} \frac{1}{n} \log |\pi_i(\Sigma^{2n} \cap \mathbf{H})|$, we have,

$$d \max_i \alpha_\Sigma(i) \geqslant \sum_i \alpha_\Sigma(i) \geqslant \liminf_{n\to\infty} \frac{1}{n} \log |\Sigma^{2n} \cap \mathbf{H}| \geqslant \alpha_\Sigma.$$

Let j be an index such that $\alpha_\Sigma(j) = \max_i \alpha_\Sigma(i)$. Let $B_n = \pi_j(\Sigma^{2n} \cap \mathbf{H})$. We have:

$$\liminf_{n\to\infty} \frac{1}{n} \log |B_n| \geqslant \frac{1}{d}\alpha_\Sigma$$

We are going to apply Theorem 7.1 to the simple group $\mathbf{S}_j$, the B_n's and the subvarieties of $\mathbf{S}_j$ defined by $\mathcal{V}_f := \overline{\pi_j(\{g \in \mathbf{H}, \chi_g = f\})}$, where $f \in \mathbb{K}[X]$ is an arbitrary polynomial and χ_g denotes the characteristic polynomial of g. Let $\alpha < \frac{1}{d}\alpha_\Sigma$. We now check that the assumptions of that theorem do hold.

The $\mathcal{V}_f$ are subvarieties of $\mathbf{S}_j$ whose complexity is bounded in terms of d only and in particular independently of f. Let us check that they are proper subvarieties too. Let T be a maximal torus of $\mathbf{H}$ and λ_i's be characters of T in the ambient linear representation of $\mathbf{H}$, so that for every $t \in T$, $\chi_t(X) = \prod_i(\lambda_i(t) - X)$. Write $T = T_1T_2$, where $T_1 \cap T_2$ is finite and T_1 is isogenous via π_j to a maximal torus of $\mathbf{S}_j$. If $\mathcal{V}_f$ were not proper, then for a dense set of $t_1 \in T_1$, there would exist a $t_2 \in T_2$ such that $\chi_{t_1t_2}(X) = f = \prod_i(\lambda_i - X)$. We would thus have $\lambda_i(t_1t_2) = \lambda_i$ for all i. But recall that if $t \in T$, then $\lambda_i(t) = 1$ for all i implies $t = 1$. Since $T_1 \cap T_2$ is finite, this implies that T_1 is finite, which is impossible. We conclude that the $\mathcal{V}_f$'s are proper subvarieties of $\mathbf{S}_j$.

The B_n's form an increasing family of symmetric subsets of $\mathbf{S}_j$ with $|B_n| \geqslant e^{\alpha n}$ for all n large enough. Moreover, observe that $\Lambda := \langle\Sigma\rangle \cap \mathbf{G}^0$ is finitely generated since $\mathbf{G}^0$ has finite index in $\mathbf{G}$. It follows from the Reidemeister-Schreier rewriting process (see [17, sec 2.3]) that there exists a finite set of generators W_0 of Λ such that for every $\gamma \in \Lambda$ one has $\ell_{W_0}(\gamma) \leqslant \ell_\Sigma(\gamma)$, where ℓ_{W_0} and ℓ_Σ denote the word length with respect to the generating sets W_0 and Σ. Taking $W := W_0W_0$, we get a finite set $W \subset \langle\Sigma\rangle \cap \mathbf{G}^0$ such that $\Sigma^{2n} \cap \mathbf{G}^0 \subset W^n$, and hence $B_n \subset \pi_j(W)^n$. It now only remains to check that $\langle B_n\rangle$ eventually contains some fixed Zariski-dense subgroup Γ of $\mathbf{S}_j$. We require the following lemma:

Lemma 8.4. *Let $\mathbf{H}$ be a connected semisimple algebraic group defined over a global field $\mathbb{K}$ and Δ be a Zariski-dense subgroup of $\mathbf{H}(\mathbb{K})$. Then Δ contains a finitely generated Zariski-dense subgroup Γ.*

Proof. The argument is standard. For each simple factor $\mathbf{S_i}$ of $\mathbf{H}$, one can find an element σ_i in Δ whose projection to $\mathbf{S_i}$ has infinite order (note that $\mathbb{K}$ has only finitely many roots of unity). If the connected component $\mathbf{L}$ of the Zariski closure of the subgroup generated by the σ_i is normal in $\mathbf{H}$ we are done, because it maps nontrivially on all $\mathbf{S_i}$'s. If not, then one can find $\gamma_j \in \Delta$ such that the Zariski closure of $\langle \mathbf{L}, \gamma_j \mathbf{L} \gamma_j^{-1} \rangle$ has dimension $> \dim \mathbf{L}$. This process must stop after at most $\dim \mathbf{H}$ steps, and the σ_i's together with the $\gamma_j \sigma_i \gamma_j^{-1}$'s generate a Zariski dense subgroup of $\mathbf{H}$. □

Note that $\langle \Sigma \rangle \cap \mathbf{H}$ is Zariski-dense in $\mathbf{H}$ because $\langle \Sigma \rangle \cap \mathbf{G}^0$ is Zariski-dense in $\mathbf{G}^0$ and the commutator map is surjective from $\mathbf{G}^0 \times \mathbf{G}^0$ to $\mathbf{H}$. Thus the lemma applied to $\Delta := \langle \Sigma \rangle \cap \mathbf{H}$ implies that $\langle \Sigma \rangle \cap \mathbf{H}$ contains a finitely generated Zariski dense subgroup in $\mathbf{H}$, and hence $\pi_j(\langle \Sigma \rangle \cap \mathbf{H})$ contains a finitely generated subgroup Γ which is Zariski dense in $\mathbf{S}_j$. Hence $\langle B_n \rangle$ will eventually contain Γ. We have now checked that the assumptions of Theorem 7.1 hold in our situation and we can conclude that

$$\chi_\Sigma(2Dn) \geqslant \Theta_n \geqslant e^{\alpha n},$$

as soon as n is large enough. This implies

$$\liminf_{n \to \infty} \frac{1}{n} \log \chi_\Sigma(n) \geqslant \frac{\alpha}{2D};$$

since this holds whenever $\alpha < \frac{1}{d} \alpha_\Sigma$. This completes the proof of Proposition 8.3. □

Remark 8.5. It would have been more elegant to reduce to the semisimple case by finding a subset $\Sigma' \subset \Sigma^N \cap \mathbf{H}$ such that Σ' generates a Zariski-dense subgroup of $\mathbf{H}$. Unless the characteristic is zero, we cannot afford doing this here, because $\mathbf{G}/\mathbf{G}^0$ and hence N cannot be uniformly bounded in terms of d only and proceeding in this way would ruin the uniformity in Theorem 1.2.

9. Concluding remarks and suggestions for further research

Images of balls under regular maps. In this subsection, we give some further applications of the method of this paper. Using Theorem 7.1 and working directly with subvarieties of the simple group $\mathbf{G}$, the proof of Theorem 1.2 generalizes straightforwardly to yield:

Theorem 9.1. *Let $d \geqslant 1$. There exists a constant $c = c(d) > 0$ such that the following holds. Let F be a field, $\mathbf{G}$ a d-dimensional absolutely simple algebraic* *group defined over F and Γ a Zariski-dense subgroup of $\mathbf{G}$ generated by a finite set Σ. Let f be a regular function on $\mathbf{G}$ defined over F. Assume that f is nonconstant on $\mathbf{G}$. Then the image of the Σ^n under f grows at an exponential rate at least c, i.e.*

$$\liminf_{n\to\infty} \frac{1}{n} \log |f(\Sigma^n)| \geq c.$$

Proof. Applying [15, Theorem 4], we may specialize as in Proposition 8.1 to a global field $\mathbb{K}$ with the additional property that the image of Γ under the specialization map is still Zariski-dense in $\mathbf{G}$. Then the conditions of Theorem 7.1 are fulfilled with $B_n = \Sigma^n$, $W = \Sigma$, the $\mathcal{V}_i$ being level sets of the regular map f, and $\alpha > 0$ gotten from uniform exponential growth [3]. Setting $c = \alpha/D$, where D is the constant obtained in Theorem 7.1, we are done. □

This can be applied for example to the trace function:

Corollary 9.2. *Assume $\mathbf{G} \leqslant \mathrm{GL}_d$ is a connected simple algebraic group over a field F on which the restriction of the trace function $g \mapsto \mathrm{Trace}(g)$ is not constant. Then for every finite $\Sigma \subset \mathbf{G}(F)$ generating a Zariski dense subgroup in $\mathbf{G}$, we have*

$$\liminf_{n\to\infty} \frac{1}{n} \log |\{\mathrm{Trace}(g); g \in \Sigma^n\}| \geq c,$$

for some constant $c > 0$ depending only on d (and not on F nor Σ).

It can happen that the trace function is constant on some simple groups, e.g. if the characteristic is p and $\mathbf{G} = \mathrm{SL}_n$ is embedded diagonally in SL_{np}. But one can show that if $\mathbf{G}$ is any Zariski connected algebraic subgroup of GL_d, which is not unipotent, then if the characteristic of F is either 0 or finite and more than d, then the trace function is not constant on $\mathbf{G}$.

Solvable groups. In [4] it was proved that virtually solvable groups have exponential conjugacy growth unless they are virtually nilpotent. By way of contrast, this does not hold when we look at GL_d-conjugacy classes.

Proposition 9.3. *Let Σ be a finite subset of GL_d over any field, generating a virtually solvable group Γ. Then the number of characteristic polynomials $\chi_\Sigma(n)$ is polynomially bounded. Moreover, it is bounded if and only if Γ is virtually unipotent.*

Proof. It will be convenient to prove the following equivalent statement. Let Γ be a group with a finite generating subset Σ and let $\rho : \Gamma \to \mathrm{GL}_d$ be a linear representation over any field, with virtually solvable image. Let $\chi_\Sigma^\rho(n)$ be the number of distinct characteristic polynomials in $\rho(B_\Sigma(n))$. Then $\chi_\Sigma^\rho(n)$ is polynomially bounded with respect to n. Moreover, it is bounded if and only if $\rho(\Gamma)$ is virtually unipotent.

Let us prove the latter statement. First, let π be the semisimplification of ρ (see the proof of Lemma 8.2). Then $\chi^{\rho}_{\Sigma} = \chi^{\pi}_{\Sigma}$ and π has virtually solvable image (since $\ker \pi \supset \ker \rho$). Now let G be the Zariski closure of $\pi(\Gamma)$; since its action is semisimple, G is reductive, and since G is virtually solvable, it is therefore virtually abelian. So $\pi(\Gamma)$ is virtually abelian and hence has polynomial growth. It follows that χ^{ρ}_{Σ} is polynomially bounded.

For the last statement of the proposition, observe that if $\rho(\Gamma)$ is virtually unipotent then $\pi(G)$ has finite image; conversely if $\rho(\Gamma)$ is not virtually unipotent, then Γ contains some element with an eigenvalue which is not a root of unity, hence χ^{ρ}_{Σ} is unbounded. □

Since in GL_d there are at most $O_d(1)$ conjugacy classes with a given characteristic polynomial, we deduce

Corollary 9.4. *If Γ is a virtually solvable subgroup of GL_d then the number of GL_d-conjugacy classes met by the n-ball in Γ is polynomially bounded.*

New questions arise if we ask about the number of $\mathbf{G}$-conjugacy classes in Σ^n, especially when $\mathbf{G}$ is the Zariski closure of Γ. Let us provide two examples where different phenomena appear.

Example 9.5. Let $\mathbf{G}$ be the group of upper triangular 3×3 matrices (a_{ij}) with $a_{11} = a_{33} = 1$. Set $\Gamma = \mathbf{G}(\mathbb{Z}[1/2])$. Then the reader can check that Γ is finitely generated and Zariski dense in $\mathbf{G}$. Moreover, its conjugacy growth is exponential, as the elements $\begin{pmatrix} 1 & 0 & k \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, for $k = 0, 1, \ldots, 2^n$ have word length $O(n)$ but are pairwise non-conjugate in $\mathbf{G}$. ◇

Example 9.6. We present an example where the type of conjugacy growth depends on the field. Let $\mathbf{G}$ be either SL_2 or its subgroup consisting of upper triangular matrices. Let Γ be the subgroup generated by $\begin{pmatrix} 2 & 0 \\ 0 & 1/2 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Then the elements $\begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix}$ for p prime in $[0, 2^n]$ (there are exponentially many such elements) have word length $O(n)$ and are pairwise non-conjugate in $\mathbf{G}(\mathbb{Q})$. On the other hand, every element in the n-ball is conjugate in $\mathbf{G}(\mathbb{C})$ to $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ or $\begin{pmatrix} 2^k & 0 \\ 0 & 2^{-k} \end{pmatrix}$ for some k with $-n \leq k \leq n$. So Γ has exponential $\mathbf{G}(\mathbb{Q})$-conjugacy growth but linear $\mathbf{G}(\mathbb{C})$-conjugacy growth. ◇

On the rate of exponential growth. We record here a related open problem. Let Γ be a group and Σ a symmetric generating subset. In general, we have

$$\gamma_\Sigma := \liminf_{n\to\infty} \frac{\log c_\Sigma(n)}{n} \leq \limsup_{n\to\infty} \frac{\log c_\Sigma(n)}{n} \leq \lim_{n\to\infty} \frac{\log |B_\Sigma(n)|}{n} = \alpha_\Sigma.$$

As we saw in the introduction, Osin's groups provide examples for which the inequality on the right-hand side is strict. We are not aware of any example for which inequality on the left-hand side is strict, but constructions of the same spirit might provide examples. On the other hand, for non-virtually-solvable linear groups, does $\gamma_\Sigma = \alpha_\Sigma$ hold? in fact, in this case, we do not know if any of those two inequalities can be sharp. For instance, in a free group over Σ, it is easy to check that both are equalities.

In case $\mathbb{K}$ is a global field and Γ is a non-virtually-solvable subgroup of $\mathrm{GL}_d(\mathbb{K})$ whose Zariski closure is reductive, Proposition 8.3 implies that $\gamma_\Sigma \geq \eta(d)\alpha_\Sigma$, where $\eta(d) > 0$ only depends on d. It would be interesting to investigate if these assumptions (i.e. $\mathbb{K}$ be a global field, the Zariski closure be reductive) could be relaxed to weaker hypotheses.

References

[1] E. Breuillard, *On uniform exponential growth for solvable groups*, Pure Appl. Math. Q. **3**, Margulis Volume, (2007), no. 4, part 1, 949–967.

[2] E. Breuillard, *A height gap theorem for nonvirtually solvable subgroups of* $\mathrm{GL}_n(\overline{\mathbb{Q}})$, Ann. of Math. (2) **174** (2011), no. 2, 1057–1110.

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

[4] E. Breuillard, Y. Cornulier, *On conjugacy growth for solvable groups.* Illinois J. Math. 54(1) (2010), 389–395.

[5] E. Breuillard and T. Gelander, *Uniform independence for linear groups*, Invent. Math. **173** (2008), no. 2, 225–263.

[6] E. Breuillard, B. J. Green and T. C. Tao, *Linear approximate groups,* Electron. Res. Announc. Math. Sci **17** (2010), 57–67.

[7] E. Breuillard, B. J. Green and T. C. Tao, *Approximate subgroups of linear groups*, Geom. Funct. Anal. **21** (2011), no. 4, 774–819.

[8] A. Eskin, S. Mozes and H. Oh, *On uniform exponential growth for linear groups*, Invent. Math. **160** (2005), no. 1, 1–30.

[9] G.H. Hardy, E.M. Wright, *An introduction to the Theory of Numbers*, 5th ed. Oxford Science Publ. (1979).

[10] A. Grothendieck. *Étude locale des schémas et des morphismes de schémas, Troisième partie,* in *Éléments de géométrie algébrique. IV.* Publ. Math. Inst. Hautes Études Sci., 28 (1966), p. 5–255.

[11] V. Guba and M. Sapir, *On the conjugacy growth functions of groups.* Illinois J. Math. 54(1) (2010), 301–313.

[12] M. Hull, *Conjugacy Growth in Polycyclic Groups*, Arch. Math. (Basel) **96** (2011), no. 2, 131–134.

[13] S. Lang and A. Weil, *Number of points of varieties in finite fields,* Amer. J. Math. **76**, (1954). 819–827.

[14] M. Larsen and R. Pink, *Finite subgroups of algebraic groups*, J. Amer. Math. Soc. **24** (2011), no. 4, 1105–1158.

[15] A. Lubotzky, M. Larsen *Normal subgroup growth of Linear groups, the G_2, F_4, E_8 case*, in Algebraic groups and arithmetic, Raghunathan volume, Tata Institute Publ., 440–468 (2004).

[16] A. Lubotzky, A. Mann, *On groups of polynomial subgroup growth*, Invent. Math. 104, 521–533 (1991).

[17] W. Magnus, A. Karass and D. Solitar, *Combinatorial group theory*, Dover Publ. New York (1976).

[18] A. Mann, *How Groups Grow*, London Mathematical Society Lecture Note Series, **395**, Cambridge University Press, Cambridge, (2012), 199 pp.

[19] C. R. Matthews, L. N. Vaserstein and B. Weisfeiler, *Congruence properties of Zariski-dense subgroups. I*, Proc. London Math. Soc. (3) **48** (1984), no. 3, 514–532.

[20] J. Milnor, *Growth of finitely generated solvable groups*, J. Diff. Geom. 2, 447–449 (1968).

[21] J. Neukirch, *Algebraic Number theory*, 2nd ed. Springer-Verlag, Berlin, Heidelberg (1999).

[22] A.Yu. Ol'shanskii, *Geometry of defining relations in groups*, Translated from the 1989 Russian original by Yu. A. Bakhturin. Mathematics and its Applications (Soviet Series), 70. Kluwer Academic Publishers Group, Dordrecht, (1991) 505 pp.

[23] D. Osin, *Small cancellations over relatively hyperbolic groups and embedding theorems*, Annals of Math. 172 (2010), 1–39.

[24] R. Pink, *Strong approximation for Zariski-dense subgroups over arbitrary global fields*, Comment. Math. Helv. 75 (2000), 608–643.

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

[26] I. Rivin, *Growth in free groups (and other stories)*, arXiv math/9911076 (preprint 1999)

[27] M. Rosen, *Number theory in function fields*, Springer-Verlag, New-York (2002).

[28] J. Tits, *Free subgroups in linear groups*, Journal of Algebra, **20** (1972), 250–270.

[29] B. Weisfeiler, *Strong approximation for Zariski-dense subgroups of semi-simple algebraic groups*, Annals of Math. 120 (1984), 271–315.

[30] J. Wolf, *Growth of finitely generated solvable groups and curvature of Riemannian manifolds*, J. Diff. Geom. 2, 421–446 (1968).

(E.B. and Y.C.) Laboratoire de Mathématiques, Bâtiment 425, Université Paris-Sud 11, 91405 Orsay, FRANCE

E-mail address: emmanuel.breuillard@math.u-psud.fr

E-mail address: yves.cornulier@math.u-psud.fr

(A.L. and C.M.) Einstein institute of mathematics, Hebrew University, Jerusalem 91904, ISRAEL

E-mail address: alexlub@math.huji.ac.il

E-mail address: chen.meiri@mail.huji.ac.il