SOFIC PROFILE AND COMPUTABILITY OF CREMONA GROUPS

YVES CORNULIER

ABSTRACT. In this paper, we show that Cremona groups are sofic. We actually introduce a quantitative notion of soficity, called sofic profile, and show that the group of birational transformations of a d-dimensional variety has sofic profile at most polynomial of degree d. We also observe that finitely generated subgroups of the Cremona group have a solvable word problem. This provides examples of finitely generated groups with no embeddings into any Cremona group, answering a question of S. Cantat.

1. INTRODUCTION

Let K be a field. The *Cremona group* $\mathrm{Cr}_d(K)$ of K in dimension d is defined as the group of birational transformations of the d-dimensional K-affine space. It can also be described as the group of K-automorphisms of the field of rational functions $K(t_1, \ldots, t_d)$.

We are far from a global understanding of finitely generated subgroups of Cremona groups. They include, notably, linear groups (since we have an obvious inclusion $\mathrm{GL}_d(K) \subset \mathrm{Cr}_d(K)$), as well as examples of groups that are not linear over any field [CeD]. On the other hand, very few restrictions are known about these groups. In the case of $d = 2$, and sometimes assuming that K has characteristic zero, there has been a lot of recent progress including [Be, BeB, Bl1, Bl2, Bl3, Do, DoI1, DoI2], see notably the survey [Se2] about finite subgroups, and [Bl2, BlD1, BlD2, Can1, De] for other subgroups. For $d = 3$ there is much less information currently known, in this direction, see [Pr1, Pr2, PrS] concerning finite subgroups. For greater d, very little information is known; interesting methods have very recently been developed in [Can2].

We here provide the following.

Theorem 1.1. *The Cremona group $\mathrm{Cr}_d(K)$ is sofic for all d and all fields K. More generally, for any absolutely irreducible variety X over a field K, the group of birational transformations $\mathrm{Bir}_K(X)$ is sofic.*

Denoting by $\mathbf{N}$ the set of positive integers, recall that a group Γ is *sofic* if it satisfies the following: for every finite subset E of Γ and every $\varepsilon > 0$, there exists $n \in \mathbf{N}$ and a mapping $\phi : E \to \mathrm{Sym}_n$ satisfying

- $\mathsf{d}^n_{\mathrm{Ham}}(\phi(g)\phi(h), \phi(gh)) \le \varepsilon$ for all $g, h \in E$ such that $gh \in E$;
- $\phi(1) = 1$;
- $\mathsf{d}^n_{\mathrm{Ham}}(\phi(u), \phi(v)) \ge 1 - \varepsilon$ for all $u \ne v$,

where $\mathsf{d}^n_{\mathrm{Ham}}$ is the normalized Hamming distance on the symmetric group Sym_n:

$$(1.1) \qquad \mathsf{d}^n_{\mathrm{Ham}}(u, v) = \frac{1}{n} \#\{i : u(i) \ne v(i)\}.$$

Note that a group is sofic if and only if all its finitely generated subgroups are sofic. Sofic groups were independently introduced by B. Weiss [Wei] and Gromov [Gro]. Sofic groups notably include residually finite groups and amenable groups. For more on this topic, see also [ES2, Pe].

Soficity is a very weak way of approximating a group by finite groups. Theorem 1.1 was only known for $n = 1$ since then $\mathrm{Cr}_1(K) = \mathrm{PGL}_2(K)$ has all its finitely generated subgroups residually finite. There exists no example, at this time, of a group failing to be sofic, although it is likely to exist.

Nevertheless, the sofic property is interesting because of its various positive consequences. For instance, if G is a group and K is a field, a conjecture by Kaplansky asserts that the group algebra $K[G]$ is directly finite, i.e. satisfies $xy = 1 \Rightarrow yx = 1$. This conjecture is known to hold when G is sofic, by a result of Elek and Szabo [ES1]. Also another conjecture, by Gottschalk, is that if M is a finite set, any G-equivariant continuous injective map $M^G \to M^G$ is surjective (the product M^G being endowed with the product topology, which makes it a compact topological space); Gromov [Gro] proved that this is true when G is sofic.

The second restriction, of a totally different nature, is the following.

Theorem 1.2. *For every field K and integer $d \ge 0$, every finitely generated subgroup of $\mathrm{Cr}_d(K)$ has a solvable word problem.*

To avoid any reference to group presentations, here we define a group to have a solvable word problem if it is either finite or isomorphic to the set $\mathbf{N}$ endowed with a recursive group law, see §5.

This provides explicit examples of finitely generated – or even finitely presented – groups that are not subgroups of any Cremona group. (This answers a question of S. Cantat.)

Example 1.3. Let I be a subset of $\mathbf{N}$. If the group

$$G_I = \langle t, x \mid [t^n x t^{-n}, x] = 1, \ \forall n \in I \rangle, \qquad (\text{where } [g, h] = ghg^{-1}h^{-1})$$

has a solvable word problem then I is recursive. Indeed, an elementary argument shows that for $n \in \mathbf{N}$, we have $[t^n x t^{-n}, x] = 1$ in G_I if and only if $n \in I$, i.e. $([t^n x t^{-n}, x])_{n \in \mathbf{N}}$ is an independent family of relators [Bau1]. (It can be shown that, conversely, if I is recursive then G_I has a solvable word problem, but this is irrelevant here.) Thus by Theorem 5.3, if I is not recursive then G_I does not

embed into any Cremona group (if I is recursively enumerable then note that G_I is recursively presented).

Construction of *finitely presented* groups with an unsolvable word problem is considerably harder, and was done by Boone and Novikov. It follows from Theorem 5.3 that these groups do not embed into any Cremona group. Mark Sapir indicated to me that there exist, on the other hand, finitely presented groups, constructed in [BRS] whose word problem is solvable, but not in exponential time. Thus these groups do not embed into Cremona groups although they have a solvable word problem.

On the other hand, Miller III [Mi] improved the construction of Boone and Novikov by exhibiting nontrivial finitely presented groups all of whose nontrivial quotients have a non-solvable word problem. We deduce the following corollary.

Corollary 1.4. *There exists a nontrivial finitely presented group with no non-trivial homomorphism to any Cremona group over any field.*

However, Cantat's problem is in no way closed, as we are still far from even a rough understanding of the structure of subgroups of Cremona groups. Many natural instances of groups have an efficiently solvable word problem, and yet are not expected to embed into any Cremona group, e.g, when they fail to satisfy the Tits Alternative (which holds in $\mathrm{Cr}_2(\mathbf{C})$ by a result of Cantat [Can2]). For example, it is expected that if $n(d)$ is the smallest number such that $\mathrm{Cr}_{n(d)}$ contains a copy of the symmetric group on d letters, then $\lim_{d\to\infty} n(d) = \infty$. This would imply in particular that the group of finitely supported permutations of the integers (or any larger group) does not embed into any Cremona group.

Theorem 1.1 is proved in Section 2 in the case of Cremona groups, and in general in Section 4. Although the latter supersedes the former, the proof in the Cremona case is much less technical, so we include it. The main two steps are

(1) Reduction to finite fields;
(2) case of finite fields.

The second step uses the "quasi-action" on the set of points, using that the indeterminacy set being of positive codimension, its number of points over a given finite field can be bounded above in a quantitative way. The first step is fairly easy in the case of Cremona groups, and is much more technical in the general case.

No example is known of a non-sofic group; in particular, so far Theorem 1.1 provides no example of groups that cannot be embedded into any Cremona group. However, the proof provides a property stronger than soficity, namely that $\mathrm{Cr}_d(K)$ (or more generally $\mathrm{Bir}_K(X)$ when X is d-dimensional) has its "*sofic profile*" in $O(n^d)$ (see Corollary 4.5). This might result in new explicit examples of groups not embedding into Cremona groups, without exhibiting non-sofic groups, and with an efficiently solvable word problem. See Section 3, in which the sofic profile is defined, and related to the classical isoperimetric profile (or Følner function).

Outline of the paper. Section 2 contains the proof of soficity of the Cremona group $\mathrm{Cr}_d(K)$. Section 3 introduces the notion of sofic profile, yielding various examples. Then Section 4 proves Theorem 1.1 in full generality; although the proof uses only basic commutative algebra that are extensively used by algebraic geometers (generic flatness, openness conditions), these notions are not of the utmost common background for readers in geometric group theory, who can stick to Section 2 and 3. Section 3 can also be read independently, without reference to Cremona groups.

Finally, Section 5, which is also independent of the remainder, includes a proof of Theorem 1.2, as well as related remarks.

We end this introduction by the following open question:

Question 1.5. For $d \geq 2$, and any field K, is $\mathrm{Cr}_d(K)$ locally residually finite (i.e., is every finitely generated subgroup residually finite)? approximable by finite groups (see Definition 2.1)? (I heard the question of local residual finiteness for $\mathrm{Cr}_d(\mathbf{C})$ from S. Cantat.)

Contents

2. Soficity of Cremona groups

We begin by the notion of approximation, studied in a much wider context by Malcev in [Ma2] and classical in model theory.

Definition 2.1. Let $\mathcal{C}$ be a class of groups. We say that a group G is *approximable by the class $\mathcal{C}$* (or *initially sub-$\mathcal{C}$* in Gromov's terminology [Gro]) if for every finite symmetric subset S of G containing 1, there exists a group $H \in \mathcal{C}$ and an abstract injective map $\phi : S \to H$ such that $\phi(1) = 1$ and for all $x, y, z \in S$ we have $\phi(x)\phi(y) = \phi(z)$ whenever $xy = z$ (in particular $\phi(x^{-1}) = \phi(x)^{-1}$ for all $x \in S$). Equivalently, G is approximable by the class $\mathcal{C}$ if and only if it is isomorphic to a subgroup of an ultraproduct of groups of the class $\mathcal{C}$.

Note that plainly, if a group is approximable by $\mathcal{C}$ then so are all its subgroups, and conversely if all its finitely generated subgroups are approximable by $\mathcal{C}$, then so is the whole group.

It is straightforward from the definition that if a group is approximable by sofic groups, then it is sofic as well. Therefore the first part of Theorem 1.1 follows from the following two propositions.

Proposition 2.2. *For any field K and d, the Cremona group $\mathrm{Cr}_d(K)$ is approximable by the family*

$$\{\mathrm{Cr}_d(\mathbf{F}) : \mathbf{F} \text{ finite field}\}.$$

Proposition 2.3. *For any finite field $\mathbf{F}$ and d, the Cremona group $\mathrm{Cr}_d(\mathbf{F})$ is sofic.*

Remark 2.4. A strengthening of Proposition 2.2 would be the assertion that for every field K, the group $\mathrm{Cr}_d(K)$ is "locally residually Cr_d of a finite field", in the sense that every finitely generated subgroup embeds into a product of groups of the form $\mathrm{Cr}_d(\mathbf{F})$ with $\mathbf{F}$ finite field; we do not know if this assertion holds. On the other hand, it is clear that every finitely generated subgroup of $\mathrm{Cr}_d(K)$ is contained in $\mathrm{Cr}_d(L)$ for some finitely generated subfield L of K.

To prove the propositions, we begin by some basic material about birational transformations of affine spaces. Consider $f = (f_1, \ldots, f_d)$, where $f_i \in K(t_1, \ldots, t_d)$. Its (affine) *indeterminacy*[1] *set* X_f is by definition the union of the zero sets of the denominators of the f_i (written in irreducible form). To such a d-tuple corresponds to the regular map defined outside its singular set mapping, for any extension L of K

$$(x_1, \ldots, x_d) \in L^d \smallsetminus X_f(L) \quad \text{to} \quad (f_1(x_1, \ldots, x_d), \ldots, f_d(x_1, \ldots, x_d)).$$

We say that f is non-degenerate if f has a Zariski-dense image. If g is another d-tuple and f is non-degenerate, we can define the composition $g \circ f$ by

$$\left(g_1\big(f_1(t_1, \ldots, t_d), \ldots, f_d(t_1, \ldots, t_d)\big), \ldots, g_d(\ldots) \right) \in K(t_1, \ldots, t_d).$$

The non-degenerate d-tuples thus form a semigroup under composition, and by definition the Cremona group $\mathrm{Cr}_d(K)$ is the set of invertible elements of this semigroup. If $f \in \mathrm{Cr}_d(K)$ and f' is its inverse (which will be written f^{-1} in the sequel, but not in the next line in order to avoid a confusion with the inverse image by the map f defined outside X_f), we define the *singular set* $Z_f = X_f \cup f^{-1}(X_{f'})$. Then f induces a bijection, for every extension L of K

$$L^d \smallsetminus Z_f \to L^d \smallsetminus Z_{f^{-1}}.$$

---

[1]The notion of indeterminacy set is sensitive to our choice to work in affine coordinates; here the indeterminacy set usually has codimension 1, while in projective coordinates the indeterminacy set has codimension at least 2.

Proof of Proposition 2.2. Since any field extension $K \subset L$ induces a group embedding $\mathrm{Cr}_d(K) \subset \mathrm{Cr}_d(L)$, it is enough to prove the proposition when K is algebraically closed.

Let W be a finite symmetric subset of $\mathrm{Cr}_d(K)$ containing 1. Write each coordinate of every element of W as a quotient of two polynomials. Let c_1 be the product in K of all nonzero coefficients of denominators of coordinates of elements of WW; let c_2 be the product of all nonzero coefficients of numerators of coordinates of elements of the form $u - v$, when (u, v) ranges over pairs of distinct elements of W. Let A be the domain generated by all coefficients of elements of W, so $c = c_1 c_2 \in A - \{0\}$. Since the ring A is residually a finite field [Ma1], there exists a finite quotient field $\mathbf{F}$ of A in which $\bar{c} \neq 0$, where $x \mapsto \bar{x}$ is the natural projection $A \to \mathbf{F}$. If $u \in \mathbf{F}$, we can view u as an element of $\mathbf{F}(t_1, \ldots, t_d)^d$ as above (the denominator does not vanish because $\bar{c}_1 \neq 0$). Also, the condition $\bar{c}_1 \neq 0$ implies that whenever $uv = w$, we also have $\bar{u}\bar{v} = \bar{w}$. In particular, since W is symmetric and contains 1, it follows that the elements $\bar{u}$ are invertible, i.e. belong to $\mathrm{Cr}_d(\mathbf{F})$. Finally, whenever $u \neq v$, since $\bar{c}_2 \neq 0$, we have $\bar{u} \neq \bar{v}$. $\qquad\square$

Remark 2.5. It follows from the proof that $\mathrm{Cr}_d(K)$ is approximable by some suitable subclasses of the class of d-Cremona groups over finite fields: if K has characteristic p it is enough to restrict to finite fields of characteristic p, and if K has characteristic 0 it is enough to restrict to the class of finite fields of characteristic $p \geq p_0$ for any fixed p_0. Also, if $K = \mathbf{Q}$, it is enough to restrict to the class of cyclic fields $\mathbf{Z}/p\mathbf{Z}$ (for $p \geq p_0$).

Proof of Proposition 2.3. Write $\mathbf{F} = \mathbf{F}_q$. Let W be a finite symmetric subset of $\mathrm{Cr}_d(\mathbf{F}_q)$ containing 1.

For any $u \in \mathrm{Cr}_d(\mathbf{F}_q)$ and for every $\mathbf{F}_q$-field L, u induces a bijection from $L^d - Z_u$ to $L^d - Z_{u'}$. We extend it arbitrarily (for each given L) to a permutation $\hat{u}$ of L^d.

Note that for all u, v, the permutations $\hat{u}\hat{v}$ and $\widehat{uv}$ coincide on the complement of $Z_v \cup v^{-1}(Z_u)$.

Then there exists a constant $C > 0$ such that for all $u \in W$ and all m we have $\#Z_u(\mathbf{F}_{q^m}) \leq C q^{m(d-1)}$ (this is a standard consequence, for instance, of the Lang-Weil estimates [LW] but can be checked directly).

So, when $L = \mathbf{F}_{q^m}$ the Hamming distance in $\mathrm{Sym}(L^d)$ between $\hat{u}\hat{v}$ and $\widehat{uv}$ is $\leq 2Cq^{-m}$, which tends to 0 when m tends to $+\infty$.

Also, by considering the zero set D_{uv} of the numerator of $u - v$, we obtain that if $u \neq v$, the Hamming distance from $\hat{u}$ and $\hat{v}$ is $\geq 1 - 2C'q^{-m}$, for some fixed constant C' and for all m. We thus proved that $\mathrm{Cr}_d(K)$ is sofic. $\qquad\square$

Remark 2.6. We actually proved that for every field K, the group $\mathrm{Cr}_d(K)$ satisfies the following property: for every finite subset $S \subset \mathrm{Cr}_d(K)$ there is a constant $c_S > 0$ such that for every integer n there exists $k \leq n$ and a map $S \to \mathrm{Sym}_k$ satisfying

- $\mathsf{d}_{\mathrm{Ham}}^k(\phi(g)\phi(h), \phi(gh)) \leq c_S n^{-1/d}$ for all $g, h \in S$ such that $gh \in S$;

- $\phi(1) = 1$ and $\phi(g) = \phi(g^{-1})$ for all $g \in S$;
- $\mathsf{d}_{\text{Ham}}^k(\phi(u), \phi(v)) \geq 1 - c_S n^{-1/d}$ for all $u \neq v$.

where $\mathsf{d}_{\text{Ham}}^k$ is the normalized Hamming distance on the symmetric group Sym_k. (In Section 3, we will interpret this by saying that the "sofic profile" of $\text{Cr}_d(K)$ is in $O(n^d)$.) Note that for every integer $m \geq 1$ there exists a distance-preserving homomorphism $(\text{Sym}_k, \mathsf{d}_{\text{Ham}}^k) \to (\text{Sym}_{mk}, \mathsf{d}_{\text{Ham}}^{mk})$; in particular k can be chosen so that $k \geq n/2$.

3. SOFIC PROFILE

3.1. Isoperimetric profile.

Let us first recall the classical notion of isoperimetric profile (or Følner function) of a group G (see [PiS] for a more detailed survey). If S, X are subsets of G, define $\partial_S X = SX - X$. Following Vershik [V], define the isoperimetric profile of (G, S) as the nondecreasing function $\alpha_{G,S}$ defined for $r > 1$ by

$$\alpha_{G,S}(r) = \inf\{n \geq 1 : \exists E \subset G, \#(E) = n, \#(\partial_S(E))/\#(E) < r^{-1}\},$$

where $\inf \emptyset = +\infty$. The group G is *amenable* if $\alpha_{G,S}(r) < +\infty$ for every finite subset $S \subset G$ and all $r > 1$. The equivalence between this definition and the original definition of amenability by von Neumann [vNe] is due to Følner [Fol].

Note that the isoperimetric profile of (G, S) is bounded for every finite subset S (i.e., $\forall S$ finite, $\sup_r \alpha_{G,S}(r) < \infty$) if and only if G is locally finite.

A convenient fact is that the asymptotics of $\alpha_{G,S}$ does not depend on S, when the latter is assumed to be a symmetric generating subset of G.

If $u, v :]1, \infty[\to [0, \infty]$ are nondecreasing functions, we write $u \preceq v$ if there exist positive real constants such that $u(r) \leq Cv(C'r) + C''$ for all $r \geq 1$, and we write $u \simeq v$ if $u \preceq v \preceq u$.

Remark 3.1. If G is a finitely generated group and S, T are finite subsets, with S a symmetric generating subset, then $\alpha_{G,S} \succeq \alpha_{G,T}$. In particular, if T is also a symmetric generating subset then $\alpha_{G,S} \simeq \alpha_{G,T}$. Thus if G is finitely generated, the $\simeq$-class of the function $\alpha_{G,S}$ does not depend on the finite symmetric generating subset S. It is usually called the *isoperimetric profile* of G (and is $\simeq \infty$ if and only if G is non-amenable).

By a result of Coulhon and Saloff-Coste [CouS], the isoperimetric profile grows at least as fast as the volume growth.

If $G = \mathbf{Z}^d$, the isoperimetric profile is $\simeq r^d$ and this is optimal; the same estimate holds for groups of polynomial growth of degree d. If G has exponential growth, then the isoperimetric profile is $\succeq \exp(r)$ and this is optimal for polycyclic groups [Pi].

Let us mention that the isoperimetric profile is closely related to the non-increasing function $I_{G,S}$ (also called "isoperimetric profile" in some papers) defined by

$$I_{G,S}(n) = \inf\{\#(\partial_S(E))/\#(E) : \ E \subset G, \ 0 < \#(E) \le n\}.$$

We check immediately that for all reals $r \ge 1$ and integers $n \ge 1$ we have $\alpha_{G,S}(r) \le n \Leftrightarrow r < I_{G,S}(n)^{-1}$. Thus $\alpha_{G,S}$ and $1/I_{G,S}$ are essentially inverse functions to each other. For instance, if G is a polycyclic group of exponential growth then $I_{G,S}$ grows as $1/\log(n)$ whenever S is a finite symmetric generating subset.

3.2. **Sofic profile and basic properties.** Here we introduce a notion of *sofic profile*, intuitively associated to a group, but more formally associated to its finite pieces, or "chunks". A similar, but different notion of "sofic dimension growth" of a finitely generated group was independently introduced by Arzhantseva and Cherix (see Remark 3.13 for the precise definition and comments).

Definition 3.2. Let us call *chunk* a finite set E, endowed with a basepoint 1_E and a subset D of $E \times E \times E$ satisfying the condition $(x,y,z), (x,y,z') \in D$ implies $z = z'$. So we can view it as a partially defined composition law $(x,y) \mapsto z$ and we write $xy = z$ to mean that $(x,y,z) \in D$.

If E is an abstract chunk and G is a group, we call *representation* of E into G a mapping $f : E \to G$ such that $f(1_E) = 1_G$ and $f(x)f(y) = f(z)$ whenever $xy = z$.

If E is a subset of a group G with $1_G \in E$, it is naturally a chunk with basepoint 1_G by setting $xy = z$ whenever this holds in the group G. We call it a chunk of G (symmetric chunk if E is symmetric in G).

This allows the following immediate restatement of the notion of approximability from Definition 2.1.

Fact 3.3. *Let $\mathcal{C}$ be a class of groups. Then a group G is approximable by the class $\mathcal{C}$ if and only if every chunk of G has an injective representation into a group in the class $\mathcal{C}$.* $\qquad\square$

Definition 3.4. Let E be a chunk. If n is an integer and $\varepsilon > 0$, define an ε-*morphism* from E to Sym_n to be a mapping $f : E \to \mathrm{Sym}_n$ such that $f(1_E) = \mathrm{id}$ and $\mathsf{d}^n_{\mathrm{Ham}}(f(xy), f(x)f(y)) \le \varepsilon$ for all $x, y \in E$, where the Hamming distance $\mathsf{d}^n_{\mathrm{Ham}}$ is defined in (1.1). A mapping from E to the symmetric group Sym_n is said to be $(1 - \varepsilon)$-expansive if $\mathsf{d}^n_{\mathrm{Ham}}(x,y) \ge 1 - \varepsilon$ whenever x, y are distinct points of E.

Define the *sofic profile* of the chunk E as the non-decreasing function

$$\sigma_E(r) = \inf\left\{n : \ \exists f : E \to (\mathrm{Sym}_n, \mathsf{d}^n_{\mathrm{Ham}}),\right.$$
$$\left. f \text{ is a } (1 - r^{-1})\text{-expansive } r^{-1}\text{-morphism}\right\} \qquad (r > 1),$$

where $\inf \emptyset = +\infty$. Say that the chunk E is *sofic* if its sofic profile takes finite values: $\sigma_E(r) < \infty$ for all $r \geq 1$.

The following elementary fact shows that the sofic profile of a chunk is either bounded or grows at least linearly.

Fact 3.5. *If E is a chunk, we have the alternative:*

- *either E has an injective representation into a finite group and hence its sofic profile is bounded, i.e. $\sup_r \sigma_E(r) < \infty$;*
- *or its sofic profile satisfies $\sigma_E(r) \geq r$ for all $r > 1$.*

Proof. If E has an injective representation into a finite group H, then this representation is a $(1 - r^{-1})$-expansive r^{-1}-morphism for every $r > 1$. So, picking n such that H embeds into Sym_n, we have $\sigma_E(r) \leq n$ for all $r \geq 1$.

To show the alternative, assume that the second condition fails, namely $\sigma_E(r) < r$ for some $r > 1$. So E has a $(1 - r^{-1})$-expansive r^{-1}-morphism ϕ into Sym_n for some $n < r$; since $r > 1$, necessarily ϕ is injective. Since the Hamming distance $\mathsf{d}_{\mathrm{Ham}}^n$ takes values in $\{0, 1/n, \dots, 1\}$ and $r^{-1} < n^{-1}$, this shows that ϕ is a 0-morphism, i.e. is an injective representation. □

Definition 3.6. A group G is *sofic* if every chunk in G is sofic, i.e. $\sigma_E(r) < \infty$ for every chunk E in G and $r \geq 1$.

This is a restatement of the definition given in the introduction. We wish to attach to G a "sofic profile", namely the family of the function σ_E, when E ranges over finite subsets of G. Let us be more precise.

Definition 3.7. The *sofic profile* of G is the family of $\simeq$-equivalence classes of the functions σ_E when E ranges over finite subsets of G. If this class has greatest element (in the set of classes of nondecreasing functions modulo $\simeq$), namely the class of a (unique up to $\simeq$) function u, we say that the sofic profile of G is $\simeq u$.

We have the following immediate consequence of Fact 3.5:

Fact 3.8. *Let G be a group. We have the alternative:*

- *G has a bounded sofic profile, in the sense that $\sup_r \sigma_E(r) < \infty$ for every chunk E in G; this occurs precisely when G is approximable by finite groups;*
- *or the sofic profile of G grows at least linearly; more precisely there exists a chunk E in G such that $\sigma_E(r) \geq r$ for all $r > 1$.* □

The class of groups approximable by (the class of) finite groups is well-known [St, VG], and they are also called "LEF-groups", which stands for "Locally Embeddable into Finite groups". A residually finite group is always approximable by finite groups, and the converse holds for finitely presented groups, but not for general finitely generated groups (see [St, VG]).

Example 3.9. Most familiar groups are *locally residually finite* (in the sense that every finitely generated subgroup is residually finite). Such groups are approximable by finite groups and hence have a bounded sofic profile. This includes:

- abelian groups, and more generally abelian-by-nilpotent groups (groups with an abelian normal subgroup such that the quotient is nilpotent) [Hal];
- linear groups, i.e. subgroups of $\mathrm{GL}_n(A)$ for any n and commutative ring A (see [Weh]);
- groups of automorphisms of affine varieties over a field [BasL];
- compact groups (i.e., groups that admit a Hausdorff compact group topology), by the Peter-Weyl theorem;

Examples of groups approximable by finite groups are (locally finite)-by-cyclic groups. Indeed, if such a group is finitely generated, it is, by [BiS, Theorem A], an inductive limit of a sequence of finitely generated virtually free groups. Such groups are not necessarily locally residually finite [St, VG].

For examples of groups not approximable by finite groups, see Examples 3.17 and 3.19.

To pursue the discussion, we use the following useful terminology, which in a certain sense allows to think of the sofic profile as a function.

Definition 3.10. Given fixed functions u, v, we say that the sofic profile of G is $\preceq u$ if $\sigma_E \preceq u$ for *every* chunk E in G and is $\succeq v$ if $\sigma_E \succeq v$ for *some* chunk E in G. Similarly we say that the sofic profile of G is *polynomial* (resp. *at most polynomial of degree k*) if for every chunk E of G, there is a polynomial (resp. polynomial of degree k) f such that $\sigma_E \preceq f$.

Note that to say that the sofic profile is at most polynomial of degree 0 just means that it is bounded.

Remark 3.11. An advantage of this definition is that for a group it depends only on its chunks, and therefore, tautologically, if any group in $\mathcal{C}$ has the property that its sofic profile is $\preceq u(r)$, then it still holds for any group approximable by the class $\mathcal{C}$. In particular, for any u, to have sofic profile $\preceq u(r)$ is a closed property in the space of marked groups (see e.g. [CoGP, Sec. 1] for basics about this space).

Remark 3.12. In contrast to the isoperimetric profile, it is not true that the sofic profile of a finitely generated group G is the sofic profile of any chunk attached to a symmetric generating subset (with unit). A natural assumption is to require that the corresponding subset S contains enough relations, namely that G has a presentation with S as set of generators and relators of length ≤ 3. However, I do not know if for such an S, denoting by E the corresponding chunk, σ_E is the sofic profile of G in the sense of Definition 3.7, nor if an arbitrary presented group has a sofic profile $\simeq$-equivalent to some function as in Definition 3.7.

Remark 3.13. The notion of sofic dimension growth due to Arzhantseva and Cherix (work in progress) is the following. Let G be generated by a finite symmetric subset S. The *sofic dimension growth* $\phi(n)$ is, in the language introduced here, $\phi_S(n) = \sigma_{S^n}(n)$. Arzhantseva and Cherix show that its asymptotics only depend on G and not on the choice of S, and related it to the isoperimetric profile. However, it is quite different in spirit to the sofic profile, because it takes into account the shape of balls. In particular, the sofic dimension growth is bounded only for finite groups.

I am not able to adapt the specification process used to estimate the sofic profile of Cremona groups (Proposition 2.2) to give any upper bound on the sofic dimension growth of their finitely generated subgroups. This is probably doable, but at the cost of some tedious estimates on the degrees of singular subvarieties arising in the proof, which would not give better than an exponential upper bound for the sofic dimension growth.

Note that the knowledge of the function of two variables $\Phi(m,n) = \sigma_{S^m}(n)$ encompasses both the sofic dimension growth $\phi_S(n) = \Phi(n,n)$ and the sofic profile (asymptotic behavior of $\Phi(m,n)$ when m is fixed).

3.3. **Sofic vs isoperimetric profile.** Informally, soficity of G means that points in G are well separated by "quasi-actions" of G on finite sets, and amenability is the additional requirement that these finite sets lie inside G with the action by the left multiplication. With this in mind, it is elementary to check that the sofic profile is asymptotically bounded above by the isoperimetric profile; precisely we have the following result.

Proposition 3.14. *For any finite subset S of G, we have the following comparison between the sofic profile and the isoperimetric profile*

$$\sigma_S(r/3) \leq \alpha_{G,S}(r), \quad \forall r \geq 3.$$

Proof. Suppose that $\alpha_{G,S}(r) \leq n$ and let us show that $\sigma_S(r/3) \leq n$. By assumption there exists $E \subset G$ with $0 < \#(E) \leq n$ and $\#(SE - E)/\#(E) < r^{-1}$. For $s \in S$, define $\phi(s) : E \to E$ to map $x \mapsto sx$ if $sx \in E$, and extend it arbitrarily to a bijection. By assumption, for each s, the proportion of $x \in E$ such that $\phi(s)(x) = sx$ is $> 1 - r^{-1}$. It follows that the Hamming distance of $\phi(s)$ and $\phi(s')$ is $> 1 - 2r^{-1}$ whenever $s, s' \in S$ and $s \neq s'$, and the Hamming distance between $\phi(st)$ and $\phi(s)\phi(t)$ is $< 3r^{-1}$ whenever $s, t, st \in S$. So $\sigma_S(r/3) \leq n$. $\square$

It is known [ES2] that any sofic-by-amenable group (i.e. lying in an extension with sofic kernel and amenable quotient) is still sofic. The proof given there is an explicit construction, yielding without any change the following.

Theorem 3.15. *Let G be a group in a short exact sequence $1 \to N \to G \to Q \to 1$. Then for every symmetric chunk E in G there exists a symmetric chunk E' in N and a finite symmetric subset S in Q such that $\sigma_E(r) \leq \sigma_{E'}(r)\alpha_{Q,S}(r)$ for all $r > 1$.*

In particular, given nondecreasing functions $u, v :]1, \infty[\to [1, \infty]$, if the sofic profile of N is $\preceq u(r)$ and the isoperimetric profile of Q is $\preceq v(r)$, then the sofic profile of G is $\preceq u(r)v(r)$.

Example 3.16. It follows from Theorem 3.15 that the class of groups with polynomial sofic profile (see Definition 3.10) is stable under extension with virtually abelian quotients. Since it is also stable under taking filtering inductive limits, it follows that every elementary amenable group has a polynomial sofic profile. (Recall that the class of elementary amenable groups is the smallest class containing the trivial group and stable under direct limits and extensions with finitely generated virtually abelian quotients.) In particular, any solvable group has a polynomial sofic profile. Note that this does not prove that it has a sofic profile $\preceq r^d$ for some d, as the degree d may depend on the chunk.

Example 3.17. For $k, \ell \in \mathbf{Z} \smallsetminus \{0\}$, the sofic profile of the Baumslag-Solitar group

$$\Gamma = \mathrm{BS}(k, \ell) = \langle t, x | tx^k t^{-1} \rangle$$

is at most linear (i.e. is $\preceq r$); more precisely it is linear (i.e. is $\simeq r$), unless $|k| = 1$, $|\ell| = 1$, or $|k| = |\ell|$, in which case it is bounded.

Proof. Let N be the kernel of the homomorphism of Γ onto $Q = \mathbf{Z}$ mapping (t, x) to $(1, 0)$. The assertion follows from Theorem 3.15 the fact that the isoperimetric profile of $\mathbf{Z}$ is linear, and that N is approximable by finite groups (so its sofic profile is bounded). Let us check the latter fact: using that Γ is the HNN-extension of $\mathbf{Z}$ by the two embeddings of $\mathbf{Z}$ into itself by multiplication by k and ℓ respectively, the group N is an iterated free product with amalgamation $\cdots \mathbf{Z} *_{\mathbf{Z}} \mathbf{Z} *_{\mathbf{Z}} \mathbf{Z} *_{\mathbf{Z}} \cdots$, where each embedding of $\mathbf{Z}$ to the left, resp. to the right, is given by multiplication by k, resp. by ℓ [Se1, I.1.4, Prop. 6]. This group is locally residually finite, i.e. every such finite iteration $\mathbf{Z} *_{\mathbf{Z}} \mathbf{Z} *_{\mathbf{Z}} \cdots *_{\mathbf{Z}} \mathbf{Z}$ is residually finite; this follows, for instance, from [Ev]. (In case k, ℓ are coprime, R. Campbell [Cam] checked that N itself is not residually finite, and even that all its finite quotients are abelian.)

By Fact 3.8, the sofic profile is $\simeq r$ unless Γ is approximable by finite groups. Since Γ is finitely presented, this occurs if and only if Γ is residually finite, which precisely holds in the given cases, by a result of Meskin [Me] (correcting an error in [BauS]).   □

Note that the fact that $\mathrm{BS}(k, \ell)$ is residually solvable (indeed, free-by-metabelian) immediately implies its soficity, but yields a much worse upper bound on its sofic profile.

Problem 3.18. Develop methods to compute lower bounds for the sofic profile of explicit groups. Is there any group for which the sofic profile is unbounded and not $\simeq r$? Can such a group be sofic?

This problem only concerns groups not approximable by finite groups, since otherwise the sofic profile is bounded. Otherwise the sofic profile grows at least linearly as we observed above, but we have no example with a better lower bound.

Example 3.19. Here are some examples of finitely generated groups not approximable by finite groups, whose sofic profile could be looked over.

- Infinite isolated groups. A group G is by definition *isolated* if it has a chunk S such that any injective representation of S into a group H extends to an injective homomorphism $G \to H$. (This clearly implies that G is generated by S and actually is presented with the set of conditions $st = u$, $s, t, u \in S$ as a set of relators.) These include finitely presented simple groups. Many more examples are given in [CoGP], e.g. Thompson's group F of the interval. It includes several examples that are amenable (solvable or not) and therefore sofic. We can also find in [CoGP] examples of non-amenable isolated groups but whether they are sofic is not known; however an example of a non-amenable isolated group that is known to be sofic, is given in [Co].
- Other finitely presented non-residually finite groups. This includes most Baumslag-Solitar groups as mentioned in Example 3.17, as well as various other one-relator groups [Bau2, BMT]. Another example is Higman's group [Se1, I.1.4, Prop. 5]

$$\langle x_1, x_2, x_3, x_4 |\ x_{i-1} x_i x_{i-1}^{-1} = x_i^2\ (i = 1, 2, 3, 4 \mod 4) \rangle,$$

which has no proper subgroup of finite index. Whether it is sofic is not known.
- Direct products of the above groups. For instance, $\mathrm{BS}(2,3)^d$ has sofic profile $\preceq n^d$.

4. General varieties

The purpose of this section is to prove Theorem 1.1 in its general formulation (for an arbitrary absolutely irreducible variety). Since the group of birational transformations of an absolutely irreducible variety can be canonically identified with that of an open affine subset, we can, in the sequel, stick to affine varieties.

If X is an affine variety over the field K, we define a *specification* of X over a finite field $\mathbf{F}$ as an affine variety X'' over $\mathbf{F}$ satisfying the following condition. Denoting by B and B'' the K-algebras of functions of X and the $\mathbf{F}$-algebra of functions on X'', there exists a finitely generated subdomain A of K, a finitely generated A-subalgebra B' of B, a surjective homomorphism $A \to \mathbf{F}$, so that $B' \otimes_A \mathbf{F} \simeq B''$ as A-algebras, and the natural K-algebra homomorphism $B' \otimes_A K \to B$ is an isomorphism. Note that $\dim(X'') \leq \dim(X)$.

Proposition 4.1. *Let X be an affine d-dimensional absolutely irreducible variety over a field K. Then the group $\mathrm{Bir}_K(X)$ is approximable (in the sense of Definition 2.1) by the family of groups $\{\mathrm{Bir}_{\mathbf{F}}(X')\}$, where $\mathbf{F}$ ranges over finite fields*

and X' ranges over d-dimensional specifications of X over $\mathbf{F}$ that are absolutely irreducible over $\mathbf{F}$.

Proof. Let B be the K-algebra of functions on X and L be its field of fractions, so that $\mathrm{Bir}_K(X) = \mathrm{Aut}_K(L)$.

Suppose that a finite symmetric subset W containing the identity is given in $\mathrm{Aut}_K(L)$. It consists of a finite family (v_i) of pairwise distinct elements of $\mathrm{Aut}_K(L)$. There exists $f \in B - \{0\}$ such that $v_i(B) \subset B[f^{-1}]$ for all i. Denote by $u_i : B \to B[f^{-1}]$ the K-algebra homomorphism which is the restriction of v_i.

Fix generators $t_1, \ldots, t_m$ of B as a K-algebra, so that $B[f^{-1}]$ is generated by $t_1, \ldots, t_m, f^{-1}$ as a K-algebra. For each (i, j), we can write $u_i(t_j)$ as a certain polynomial with coefficients in K and $m + 1$ indeterminates, evaluated at $(t_1, \ldots, t_m, f^{-1})$. Let C_1 be the (finite) subset of K consisting of the coefficients of these polynomials (i, j varying). Also, under the mapping $X_j \mapsto t_j$, the K-algebra B is the quotient of $K[X_1, \ldots, X_m]$ by some ideal; we can consider a certain finite set of polynomials with coefficients in K generating this ideal. Let C_2 be the finite subset of K consisting of the coefficients of those polynomials. Also, f can be written as a polynomial in $t_1, \ldots, t_m$; let $C_3 \subset K$ consist of the coefficients of this polynomial. Let A_0 be the subring of K generated by $C_1 \cup C_2 \cup C_3$.

Let B'_0 be the A_0-subalgebra of B generated by the t_j. By generic flatness [SGA, Lem. 6.7], there exists $s \in A_0 - \{0\}$ such that $B' = B'_0[s^{-1}]$ is flat over $A = A_0[s^{-1}]$. Since A contains coefficients of the polynomials defining B, we have, in a natural way, $B = B' \otimes_A K$. Moreover, $f \in B'$ and the homomorphisms u_i actually map B' to $B'[f^{-1}]$; if u'_i denotes the corresponding restriction map $B' \to B'[f^{-1}]$, then $u'_i \otimes_A K = u_i$ (here we view $- \otimes_A K$ as a functor). In particular, since the u_i are pairwise distinct by definition, the u'_i are pairwise distinct as well. This means that for all $i \neq i'$ there exists an element $x_{ii'} \in B'$ such that $u_i(x_{ii'}) \neq u_{i'}(x_{ii'})$. Let $x \in B' - \{0\}$ be the product of all $u_i(x_{ii'}) - u_{i'}(x_{ii'})$, where $\{i, i'\}$ ranges over pairs of distinct indices. Also, fix k large enough so that the element $g = f^k \prod_i u_i(f) \in B'[f^{-1}] - \{0\}$ belongs to $B' - \{0\}$.

There is a natural map $\phi : \mathrm{Spec}(B') \to \mathrm{Spec}(A)$ consisting in taking the intersection with A. This map is continuous for the Zariski topology. Consider the open subset of $\mathrm{Spec}(B')$ consisting of those primes not containing gx; this is an open subset of $\mathrm{Spec}(B')$ containing $\{0\}$. Since B' is A-flat, the map ϕ is open [SGA, Th. 6.6]. Therefore there exists $a \in A - \{0\}$ such that every prime of A not containing a is of the form $\mathfrak{P} \cap A$ for some prime $\mathfrak{P}$ of B' not containing gx.

Now since B' is A-flat and absolutely integral, by [EGA, 12.1.1] there exists $a' \in A - \{0\}$ such that for every prime $\mathcal{Q}$ of A not containing a', the quotient ring $B' \otimes_A (A/\mathcal{Q}) = B'/\mathcal{Q}B'$ is an absolutely integral $(A/\mathcal{Q})$-algebra.

It follows that if $\mathfrak{m}$ is a maximal ideal of A not containing aa', then $B'/\mathfrak{m}B'$ is an absolutely integral $(A/\mathfrak{m})$-algebra and $\mathfrak{m}B'$ does not contain gx. Let us fix such a maximal ideal $\mathfrak{m} \subset A$ (it exists because in a finitely generated domain, the intersection of maximal ideals is trivial, see for instance [Eis, Th. 4.19]). Since u'_i

is a A-algebra homomorphism, it sends $\mathfrak{m}B'$ to $\mathfrak{m}B'[f^{-1}]$, and therefore induces a $(A/\mathfrak{m})$-algebra homomorphism $u_i'' : B'/\mathfrak{m}B' \to B'[f^{-1}]/\mathfrak{m}B'[f^{-1}]$. Since $x \neq 0$ in $B'/\mathfrak{m}B'$, the u_i'' are pairwise distinct.

We need to check that $\dim(B'/\mathfrak{m}B') \leq d$. First, by [Eis, Th. 13.8], $\dim(B') \leq \dim(A) + d$. Now since B' is A-flat, by [Eis, Th. 10.10] we have $\dim(B'/\mathfrak{m}B') \leq \dim(B') - \dim(A_{\mathfrak{m}})$. Since A is a finitely generated domain, and $\mathfrak{m}$ is a maximal ideal, we have $\dim(A_{\mathfrak{m}}) = \dim(A)$ (see Lemma 4.3), and from the two inequalities above we deduce $\dim(B'/\mathfrak{m}B') \leq d$. (Actually both inequalities are equalities (same references): for the first one, [Eis, Th. 13.8] uses the fact that A is universally catenary, which follows in turn from the fact that $\mathbf{Z}$ is universally catenary, which is part of [Eis, Cor. 18.10].)

To conclude it is enough to prove the following claim

Claim 4.2. *The homomorphisms u_i'' uniquely extend to pairwise distinct $(A/\mathfrak{m})$-automorphisms v_i'' of the field of fractions of $B'/\mathfrak{m}B'$ and whenever $v_i v_j = v_k$ we have $v_i'' v_j'' = v_k''$.*

To check the claim, begin with the following general remark. If R is a domain, s a nonzero element of R, and we have two homomorphisms $\alpha, \beta : R \to R[s^{-1}]$, such that $\alpha(s)$ is nonzero, then α uniquely extends to a homomorphism $R[s^{-1}] \to R[(s\alpha(s))^{-1}]$ and we can define the composite map $\alpha\beta : R \to R[(s\alpha(s))^{-1}]$.

Since $g \neq 0$ in B, this can be applied to the K-algebra homomorphisms $u_i : B \to B[f^{-1}]$, which are given by

$$t_\ell \mapsto u_i(t_\ell) = v_i(t_\ell) = U_{\ell i}(t_1, \ldots, t_m)/f^d,$$

where $U_{\ell i} \in A[X_1, \ldots, X_m]$. We thus have, for all ℓ

$$
\begin{aligned}
v_i(v_j(t_\ell)) &= v_i(U_{\ell j}(t_1, \ldots, t_m)/f^d) \\
&= U_{\ell j}(u_i(t_1), \ldots, u_i(t_m))/u_i(f)^d \\
&= U_{\ell j}(U_{1i}(t_1, \ldots, t_m)/f^d, \ldots U_{mi}(t_1, \ldots, t_m)/f^d)/u_i(f)^d.
\end{aligned}
$$

For all ℓ, j can write the formal identity

$$U_{\ell j}(X_1/Y, \ldots, X_m/Y)Y^\delta = V_{\ell j}(T_1, \ldots, T_m, Y)$$

for some $V_{\ell j} \in B[X_1, \ldots, X_m, Y]$ and some positive integer δ. Thus $v_i v_j = v_k$ (or equivalently $u_i u_j = u_k$) means that for all ℓ we have the equality in L

$$U_{\ell j}(U_{1i}(t_1, \ldots, t_m)/f^d, \ldots U_{mi}(t_1, \ldots, t_m)/f^d)/u_i(f)^d = U_{\ell k}(t_1, \ldots, t_m)/f^d,$$

that is

$$V_{\ell j}(U_{1i}(t_1, \ldots, t_m), \ldots U_{mi}(t_1, \ldots, t_m)) = U_{\ell k}(t_1, \ldots, t_m)u_i(f)^d f^{d\delta - d},$$

which actually holds in $B' \subset L$. This equality still holds modulo the ideal $\mathfrak{m}B'$. Since $g \neq 0$ in $B'/\mathfrak{m}B'$ (i.e., f and $u_j(f)$ are nonzero elements of the domain $B'/\mathfrak{m}B'$), this equality exactly means that $u_i'' u_j'' = u_k''$ in the sense above.

Since in particular for every i there exists ι such that $v_i v_\iota$ and $v_\iota v_i$ are the identity, $u_i'' u_\iota''$ and $u_\iota'' u_i''$ are the identity; in particular u_i'' extends to an automorphism v_i'' of the fraction field of $B'/\mathfrak{m}B'$. Since the u_i'' are pairwise distinct, so are the v_i''. Moreover, whenever $u_i u_j = u_k$, we have $u_i'' u_j'' = u_k''$ which in turn implies $v_i'' v_j'' = v_k''$. So the claim is proved, and hence Proposition 4.1 as well. $\square$

We used the following standard lemma.

Lemma 4.3. *Let A be a finitely generated domain. Then for any maximal ideal $\mathfrak{m}$, we have $\dim(A) = \dim(A_{\mathfrak{m}})$.*

Proof. If the characteristic p is positive, A is a finitely generated algebra over the field on p elements, and [Eis, Cor. 13.4] (based on Noether normalization) applies, giving $\dim(A) = \dim(A_{\mathfrak{m}}) + \dim(A/\mathfrak{m}) = \dim(A_{\mathfrak{m}})$.

If the characteristic is zero, we use the fact that the ring $\mathbf{Z}$ is universally catenary [Eis, Cor. 18.10], to apply [Eis, Th. 13.8], which yields $\dim(A_{\mathfrak{m}}) = \dim(\mathbf{Z}_{\mathfrak{m}\cap\mathbf{Z}}) + \dim(A \otimes_{\mathbf{Z}} \mathbf{Q})$. Since $\mathfrak{m}$ has finite index, $\mathfrak{m} \cap \mathbf{Z} = p\mathbf{Z}$ for some prime p and $\dim(\mathbf{Z}_{\mathfrak{m}\cap\mathbf{Z}}) = 1$. So $\dim(A_{\mathfrak{m}}) = 1 + \dim(A \otimes_{\mathbf{Z}} \mathbf{Q})$. Since this value does not depend on $\mathfrak{m}$, we deduce that $\dim(A_{\mathfrak{m}}) = \dim(A)$. $\square$

Proposition 4.4. *For every absolutely irreducible affine variety X over a finite field $\mathbf{F}$, the group $\mathrm{Bir}_{\mathbf{F}}(X)$ is sofic. Actually, its sofic profile is $\preceq n^d$, where $d = \dim(X)$.*

The proof is similar to the one of Proposition 2.3 and left to the reader. The only additional feature is the fact, which follows from the Lang-Weil estimates (making use of the assumption that X is absolutely irreducible), that for some constants $c > 0$ and $c' \in \mathbf{R}$ and every finite extension $\mathbf{F}'$ of $\mathbf{F}$ with q elements, the number of points in $X(\mathbf{F}')$ is $\geq cq^d - c'$.

From Propositions 4.1 and 4.4 we deduce

Corollary 4.5. *For every absolutely irreducible affine variety X over a field K, the group $\mathrm{Bir}_K(X)$ is sofic. Actually, its sofic profile is $\preceq n^d$, where $d = \dim(X)$.*

5. Solvability of the word problem

Definition 5.1. A countable group has a *solvable word problem* if it is finite or isomorphic to $\mathbf{N}$ endowed with a recursive group law, i.e. recursive as a map $\mathbf{N} \times \mathbf{N} \to \mathbf{N}$.

The terminology is motivated by the following elementary characterization in the case of finitely generated groups:

Proposition 5.2. *A finitely generated group Γ, given with a surjective homomorphism $p : \mathbb{F} \to \Gamma$ with $\mathbb{F}$ a free group of finite rank, has a solvable word problem if and only if the kernel N of p is a recursive subset of $\mathbb{F}$. (In particular, this does not depend on the choice of $\mathbb{F}$ and the surjective homomorphism p.)*

Proof. Suppose that Γ has solvable word problem in the sense of Definition 5.1. We can suppose that $\Gamma = \mathbf{N}$ (or a finite segment therein) with a recursive group law, whose unit is a fixed number e. Write $\mathbb{F} = \mathbb{F}_k = \langle t_1, \ldots, t_k \rangle$ and set $u_i = p(t_i)$. If we input any word $w \in \mathbb{F}$, we can compute $w(u_1, \ldots, u_k)$ (computed according to the given law on $\mathbf{N}$) and answer yes or no according to whether $w(u_1, \ldots, u_k) = e$.

Conversely, suppose that the condition is satisfied. Start from a recursive enumeration $u : \mathbf{N} \to \mathbb{F}$. Given n, we define $\kappa(n) = \inf\{k \le n : u(k)u(n)^{-1} \in N\}$. Since N is recursive, κ is computable. Note that $\kappa \circ \kappa = \kappa$. Define

$$J = \{n \in \mathbf{N} : \kappa(n) = n\};$$

this is a recursive subset of $\mathbf{N}$. By construction, the composite map $J \xrightarrow{u} \mathbb{F} \to \mathbb{F}/N = \Gamma$ is a bijection. If J is finite, we are done. So suppose J is infinite; then there is a recursive enumeration $q : \mathbf{N} \to J$, defined by an obvious induction. Finally define $n * m = q^{-1}(\kappa(u^{-1}(u(q(n))u(q(m)))))$. This is a recursive law on $\mathbf{N}$ and by construction the composite map $\mathbf{N} \xrightarrow{q} J \xrightarrow{u} \mathbb{F} \to \mathbb{F}/N$ is a magma isomorphism. Thus Γ is isomorphic to $(\mathbf{N}, *)$. $\square$

Theorem 5.3. *Let K be a field and n a non-negative integer. Then every finitely generated subgroup of $\mathrm{Cr}_d(K)$ has solvable word problem.*

Proof. Since every finitely generated subgroup of $\mathrm{Cr}_d(K)$ is contained in Cr_d of a finitely generated field, we can suppose that K is finitely generated. So K is an extension of degree m of some purely transcendental field $L = F(t_1, \ldots, t_n)$ with F a prime field ($\mathbf{F}_p$ or $\mathbf{Q}$). Observe that there is an inclusion $\mathrm{Cr}_d(K) \subset \mathrm{Cr}_{md}(L)$, so we can suppose that K itself is a purely transcendental field. We can therefore implement formal calculus of K, where in case $F = \mathbf{Q}$, elements of $\mathbf{Q}$ are written as a pair (denominator and numerator) of integers, written in radix 2.

We can also implement formal calculus on $\mathrm{Cr}_d(K)$. Each element can be written as a d-tuple of elements in $K(u_1, \ldots, u_d)$; each given as a pair of polynomials (numerator and nonzero denominator). The product of two elements in $\mathrm{Cr}_d(K)$ can be computed, namely by composition. That these elements belong to $\mathrm{Cr}_d(K)$ ensures that no zero denominator incurs. Therefore any product can be computed and put in irreducible form.

The equality of two fractions P_1/Q_1 and P_2/Q_2 can be checked by computing $P_1Q_2 - P_2Q_1$ and checking whether it is the zero polynomial in $F(t_1, \ldots, t_n, u_1, \ldots, u_d)$. In particular the equality of $(P_1/Q_1, \ldots, P_d/Q_d)$ and $(u_d, \ldots, u_d)$ can be checked. $\square$

Remark 5.4. The composition of elements of the Cremona group is submultiplicative for the length of formulas (i.e., the number of symbols involved). It follows that, given fixed Cremona transformations $g_1, \ldots, g_k$, the above algorithm, whose input is a group word $w \in F_k$ and whose output is yes or no according to whether $w(g_1, \ldots, g_k) = 1$ in $\mathrm{Cr}_d(K)$, has exponential time with respect to the length of w.

The above proof is very similar to that of the more specific case of finitely generated linear groups, due to Rabin [Ra]. However, in the latter case, the elements can be implemented as matrices, and it follows that the algorithm has polynomial time. We do not know whether finitely generated subgroups of the Cremona groups have word problem solvable in polynomial time (however, some of them have no faithful finite-dimensional linear representation).

Remark 5.5. The above proof shows, more generally, that finitely generated sub-semigroups of the Cremona semigroup (the group of dominant self-maps of the affine space, or equivalently the semigroup of K-algebra endomorphisms of the field $K(t_1, \ldots, t_n)$) has a solvable word problem, i.e., given $g_1, \ldots, g_k$, there is an algorithm whose input is a pair of words w, w' in k letters and the output is yes or no according to whether $w(g_1, \ldots, g_k) = w'(g_1, \ldots, g_k)$. For the same reason, it has exponential time.

References

[Bas]   H. Bass. Automorphismes de schémas et de groupes de type fini. Paul Dubreil and Marie-Paule Malliavin Algebra Seminar, 34th Year (Paris, 1981), pp. 310–321, Lecture Notes in Math., 924, Springer, Berlin-New York, 1982.

[BasL]   H. Bass, A. Lubotzky. Automorphisms of groups and of schemes of finite type. Israel J. Math. 44 (1983), no. 1, 1–22.

[Bau1]   G. Baumslag. Wreath products and finitely presented groups. Math. Z.75 (1961) 22–28.

[Bau2]   G. Baumslag. A non-cyclic one-relator group all of whose finite factor groups are cyclic, J. Australian Math. Soc. 10 (1969) 497–498.

[BauS]   G. Baumslag, D. Solitar. Some two-generator one-relator non-Hopfian groups. Bull. Amer. Math. Soc 68 (1962) 199–201.

[Be]   A. Beauville. p-elementary subgroups of the Cremona group, J. Algebra 314 (2007), 553-564.

[BeB]   A. Beauville and J. Blanc. On Cremona transformations of prime order. C. R. Math. Acad. Sci. Paris 339 (2004), no. 4, 257–259.

[BiS]   R. Bieri, R. Strebel. Almost finitely presented soluble groups. Comment. Math. Helv. 53(2) 258–278, 1978.

[Bl1]   J. Blanc. Finite abelian subgroups of the Cremona group of the plane. C. R. Math. Acad. Sci. Paris 344 (2007), no. 1, 21–26.

[Bl2]   J. Blanc. Sous-groupes algébriques du groupe de Cremona. (French) [Algebraic subgroups of the Cremona group] Transform. Groups 14 (2009), no. 2, 249–285.

[Bl3]   J. Blanc. Elements and cyclic subgroups of finite order of the Cremona group. Comment. Math. Helv. 86 (2011), no. 2, 469–497.

[BlD1]   J. Blanc and J. Déserti. Embeddings of $SL(2, \mathbb{Z})$ into the Cremona group. (English summary) Transform. Groups 17 (2012), no. 1, 21?50.

[BlD2]   J. Blanc and J. Déserti. Degree growth of birational maps of the plane. Preprint, math:ArXiv/1109.6810.

[BMT]   G. Baumslag, C. Miller, and D. Troeger. Reflections on the residual finiteness of one-relator groups, Groups Geom. Dyn. 1 (2007), pp. 209–219.

[BRS]   J-C. Birget, E. Rips, M. Sapir. Isoperimetric and isodiametric functions of groups. Ann. of Math. (2) 156 (2002), no. 2, 345–466.

[Cam]   R.I. Campbell. Notes on the Baumslag-Solitar non-residually finite examples. Proc. Amer. Math. Soc. 109 (1990), no. 1, 59–62.

[Can1]   S. Cantat. Sur les groupes de transformations birationnelles des surfaces. (French) [On groups of birational transformations of surfaces] Ann. of Math. (2) 174 (2011), no. 1, 299–340.

[Can2]   S. Cantat. Morphisms between Cremona groups and a characterization of rational varieties. Preprint, 2013.

[CeD]   D. Cerveau, J. Déserti. Transformations birationnelles de petit degré. To appear in Cours Spécialisés, Soc. Math. France.

[Co]   Y. Cornulier. A sofic group away from amenable groups. Math. Ann. 350(2) (2011) 269–275.

[CoGP]   Y. de Cornulier, L. Guyot, and W. Pitsch. On the isolated points in the space of groups. J. Algebra 307 (2007), no. 1, 254–277.

[CouS]   T. Coulhon, L. Saloff-Coste, Isopérimétrie pour les groupes et variétés. Rev. Math. Iberoamericana 9 (1993), 293–314.

[De]   J. Déserti. Sur les sous-groupes nilpotents du groupe de Cremona. (French) [The nilpotent subgroups of the Cremona group] Bull. Braz. Math. Soc. (N.S.) 38 (2007), no. 3, 377–388.

[Do]   I.V. Dolgachev. On elements of order p^s in the plane Cremona group over a field of characteristic p. Tr. Mat. Inst. Steklova 264 (2009), Mnogomernaya Algebraicheskaya Geometriya, 55–62; translation in Proc. Steklov Inst. Math. 264 (2009), no. 1, 48–55

[DoI1]   I.V. Dolgachev and V. A. Iskovskikh. Finite subgroups of the plane Cremona group. Algebra, arithmetic, and geometry: in honor of Yu. I. Manin. Vol. I, 443–548, Progr. Math., 269, Birkhäuser Boston, Inc., Boston, MA, 2009.

[DoI2]   I.V. Dolgachev and V. A. Iskovskikh. On elements of prime order in the plane Cremona group over a perfect field. Int. Math. Res. Not. IMRN 2009, no. 18, 3467–3485

[EGA]   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.

[Eis]   D. Eisenbud. "Commutative Algebra with a View Toward Algebraic Geometry". Grad. Texts in Math. 150, Springer-Verlag, 1994.

[ES1]   G. Elek, E. Szabó. Sofic groups and direct finiteness. J. Algebra 280 (2004) 426–434.

[ES2]   G. Elek, E. Szabó. On sofic groups. J. Group Theory 9(2) (2006) 161–171.

[Ev]   B. Evans. Cyclic amalgamations of residually finite groups. Pacific J. Math. Volume 55, Number 2 (1974), 371–379.

[Fol]   E. Følner. On groups with full Banach mean value. Math. Scandinavica 3 (1955) 243–254.

[Gro]   M. Gromov. *Endomorphisms of symbolic algebraic varieties*. J. Eur. Math. Soc. 1(2) (1999) 109–197.

[Hal]   P. Hall. Finiteness conditions for soluble groups. Proc. London Math. Soc. i, No. 16, 419–436 (1954).

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

[Ma1]   A. Malcev. On the faithful representation of infinite groups by matrices, Mat. Sb., 8(50) (1940), pp. 405–422.

[Ma2]   A. Malcev. I. Algebraic systems. Posthumous edition, edited by D. Smirnov and M. Taclin. Translated from the Russian by B. D. Seckler and A. P. Doohovskoy. Die Grundlehren der mathematischen Wissenschaften, Band 192. Springer-Verlag, New York-Heidelberg, 1973.

[Me]   S. Meskin. Nonresidually finite one-relator groups. Trans. Amer. Math. Soc. 164 (1972) 105–114.

[Mi]   C.F. Miller III. The word problem in quotients of a group, in: J.N. Crossley (Ed.), Aspects of Effective Algebra, Proceedings of a Conference at Monash University, August 1979, Upside Down A Book Company, Steel's Creek, 1981, pp. 246?250.

[Pe]   V. Pestov. *Hyperlinear and sofic groups: a brief guide.* Bull. Symbolic Logic 14(4) (2008) 449–480.

[Pi]   C. Pittet, Følner sequences in polycyclic groups, Rev. Mat. Iberoamericana 11 (1995), 675–685.

[PiS]   C. Pittet, L. Saloff-Coste. Random walk and isoperimetry on discrete subgroups of Lie groups. Random walks and discrete potential theory (Cortona, 1997), 306–319, Sympos. Math., XXXIX, Cambridge Univ. Press, Cambridge, 1999.

[Pr1]   Yu. Prokhorov. p-elementary subgroups of the Cremona group of rank 3. Yuri Prokhorov. Classification of algebraic varieties, 327–338, EMS Ser. Congr. Rep., Eur. Math. Soc., Zürich, 2011.

[Pr2]   Yu. Prokhorov. Simple finite subgroups of the Cremona group of rank 3. J. Algebraic Geom. 21 (2012), 563–600.

[PrS]   Yu. Prokhorov, C. Shramov. Jordan property for Cremona groups. ArXiv:math/1211.3563.

[Ra]   M. O. Rabin. Computable algebra, general theory and theory of computable fields. Trans. Amer. Math. Soc., 95:341–360, 1960.

[Sch]   P. Schupp. Small cancellation theory over free products with amalgamation. Math. Annalen 193(4) (1971) 255–264.

[Se1]   J-P. Serre. "Arbres, amalgames, SL$_2$". Astérisque **46**, SMF, 1977.

[Se2]   J-P. Serre. Le groupe de Cremona et ses sous-groupes finis. Séminaire Bourbaki. Volume 2008/2009. Exposés 997–1011. Astérisque No. 332 (2010), Exp. No. 1000, vii, 75–100.

[SGA]   A. Grothendieck et al. "Revêtements Étales et Groupe Fondamental", Lecture Notes in Mathematics, 224, Springer-Verlag, Berlin-Heidelberg- New York, 1971.

[St]   A. M. Stëpin, "Approximability of groups and group actions", Uspekhi Mat. Nauk, 38:6(234) (1983), 123–124. English translation: Russian Math. Surveys, 38 (1983), 131–132.

[V]   A.M. Vershik. Amenability and approximation of infinite groups. Selecta Math. Soviet. 2 (1982), no. 4, 311–330.

[VG]   A. M. Vershik and E. I. Gordon. Groups that are locally embeddable in the class of finite groups. St. Petersburg Math. J. 9 (1998) no. 1, 49–67.

[vNe]   J. von Neumann. Zur allgemeinen Theorie des Maßes", Fund. Math. 13 (1929) 73–111

[Weh]   B. Wehrfritz. Infinite linear groups. Ergebnisse der Math. Band 76, Springer-Verlag 1973.

[Wei]   B. Weiss. Sofic groups and dynamical systems. Sankhyā Ser. A 62 (2000), no. 3, 350–359. Ergodic theory and harmonic analysis (Mumbai, 1999).

Laboratoire de Mathématiques, Bâtiment 425, Université Paris-Sud 11, 91405 Orsay, FRANCE

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