Michigan Math. J. 62 (2013), 823–841

Sofic Profile and Computability of Cremona Groups

Yves Cornulier

0. Synopsis

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 $K(t_1, \dots, t_d)$.

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 0, there has been a lot of recent progress including [Be; BeB; B1; B2; B3; Do; DoI1; DoI2]; see notably the survey [Se2] about finite subgroups and [B2; BD1; BD2; Ca1; D] for other subgroups. For $d = 3$ there is much less information currently known; in this direction, see [Pr1; Pr2; PrSh] concerning finite subgroups. For greater d, very little information is known; interesting methods have recently been developed in [Ca2].

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.*

Received November 6, 2012. Revision received May 5, 2013.

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

- $\mathrm{d}^n_{\mathrm{Ham}}(\phi(g)\phi(h), \phi(gh)) \leq \varepsilon$ for all $g, h \in E$ such that $gh \in E$;
- $\phi(1) = 1$;
- $\mathrm{d}^n_{\mathrm{Ham}}(\phi(u), \phi(v)) \geq 1 - \varepsilon$ for all $u \neq v$.

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

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

Note that a group is sofic if and only if all its finitely generated subgroups are sofic. Sofic groups were independently introduced by Weiss [Wei] and Gromov [Gr]. Sofic groups notably include residually finite groups and amenable groups. For more on this topic, see also [ESz2; 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; that is, it satisfies $xy = 1 \Rightarrow yx = 1$. This conjecture is known to hold when G is sofic, by a result of Elek and Szabo [ESz1]. Another conjecture, by Gottschalk, is that if M is a finite set then any G-equivariant continuous injective map $M^G \to M^G$ is surjective (the product M^G is endowed with the product topology, which makes it a compact topological space); Gromov [Gr] proved that this claim 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 $d \geq 0$, 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 Section 5.

This theorem 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

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

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 $n \in I$; that is, $([t^n x t^{-n}, x])_{n \in \mathbf{N}}$ 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. M. Sapir indicated to me that there exist finitely presented groups, constructed in [BirRS], 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 [M] improved the construction of Boone and Novikov by exhibiting nontrivial finitely presented groups all of whose nontrivial quotients have a nonsolvable word problem. We deduce the following corollary.

COROLLARY 1.4. *There exists a nontrivial finitely presented group with no nontrivial 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—for instance, when they fail to satisfy the Tits alternative (which holds in $\mathrm{Cr}_2(\mathbf{C})$ by a result of Cantat [Ca1]). 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 but is much more technical in the general case.

No example is known of a nonsofic 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 nonsofic groups yet with an efficiently solvable word problem. See Section 3, in which the sofic profile is defined and then 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. Section 4 proves Theorem 1.1 in full generality; although the proof uses only basic notions of commutative algebra that are extensively used by algebraic geometers (generic flatness, openness conditions), these notions may not be familiar to readers in geometric group theory, who can stick to Sections 2 and 3. Section 3 can also be read independently (i.e., 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 with the following open questions.

QUESTIONS 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)? Is it 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.)

ACKNOWLEDGMENTS. I thank Jeremy Blanc for pointing out several inaccuracies in an earlier version of the paper. I am grateful to Serge Cantat for stimulating discussions. I thank Julie Deserti and the referee for many useful corrections. I also thank Goulnara Arzhantseva and Pierre-Alain Cherix for letting me know about their work.

2. Soficity of Cremona Groups

We begin with the notion of approximation, which was studied in a much wider context by Mal'cev [Ma2] and is 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 [Gr]) if, for every finite symmetric subset S of G containing 1, there exist a group $H \in \mathcal{C}$ and an abstract injective map $\phi \colon S \to H$ 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 $\mathcal{C}$.

Clearly, 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*

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

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 $\mathbf{F}$ a 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 with some basic material about birational transformations of affine spaces. Consider $f = (f_1, \dots, f_d)$, where $f_i \in K(t_1, \dots, t_d)$. Its (affine) *indeterminacy set* X_f is by definition the union of the zero sets of the denominators of the f_i written in irreducible form. (The notion of indeterminacy set is sensitive to our choice to work in affine coordinates; here the indeterminacy set usually has codimension 1, whereas in projective coordinates the indeterminacy set has codimension at least 2.) Such a d-tuple corresponds to the regular map defined outside its singular set mapping, for any extension L of K,

$$(x_1, \dots, x_d) \in L^d \setminus X_f(L) \mapsto (f_1(x_1, \dots, x_d), \dots, f_d(x_1, \dots, x_d)).$$

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

$$\big(g_1(f_1(t_1, \dots, t_d), \dots, f_d(t_1, \dots, t_d)), \dots, g_d(\dots)\big) \in K(t_1, \dots, t_d).$$

The nondegenerate 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,

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

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 $u - v$, where (u, v) ranges over pairs of distinct elements of W. Let A be the domain generated by all coefficients of elements of W, so that $c = c_1c_2 \in A - \{0\}$. 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 $u \in \mathbf{F}$, then we can view u as an element of $\mathbf{F}(t_1, \dots, t_d)^d$ as before (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 $\bar{u} \neq \bar{v}$. $\square$

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 then it is enough to restrict to finite fields of characteristic p; and if K has characteristic 0 then it is enough to restrict to the class of finite fields of characteristic $p \geq p_0$ for any fixed p_0. Also, if $K = \mathbf{Q}$ then 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 $\#Z_u(\mathbf{F}_{q^m}) \leq Cq^{m(d-1)}$ (this is a standard consequence, for instance, of the Lang–Weil estimates [LaW] 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 less than or equal to $2Cq^{-m}$, which tends to 0 as m tends to $+\infty$.

Also, by considering the zero set D_{uv} of the numerator of $u - v$, we obtain that if $u \neq v$ then the Hamming distance from $\hat{u}$ and $\hat{v}$ is no less than $1 - 2C'q^{-m}$ for some fixed constant C' and for all m. We have thus proved that $\mathrm{Cr}_d(K)$ is sofic. $\square$

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 exist a $k \leq n$ and a map $S \to \mathrm{Sym}_k$ satisfying:

- $\mathrm{d}^k_{\mathrm{Ham}}(\phi(g)\phi(h), \phi(gh)) \leq c_S n^{-1/d}$ for all $g, h \in S$ such that $gh \in S$;
- $\phi(1) = 1$ and $\phi(g) = \phi(g^{-1})$ for all $g \in S$;
- $\mathrm{d}^k_{\mathrm{Ham}}(\phi(u), \phi(v)) \geq 1 - c_S n^{-1/d}$ for all $u \neq v$.

Here $\mathrm{d}^k_{\mathrm{Ham}}$ 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 $\mathrm{Cr}_d(K)$ is in $O(n^d)$.) Note that for every integer $m \geq 1$ there exists a distance-preserving homomorphism $(\mathrm{Sym}_k, \mathrm{d}^k_{\mathrm{Ham}}) \to (\mathrm{Sym}_{mk}, \mathrm{d}^{mk}_{\mathrm{Ham}})$; 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 [PiSa] for a more detailed survey). If S and 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

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

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 [vN] is due to Følner [F].

Note that the isoperimetric profile of (G, S) is bounded for every finite subset S (i.e., for all 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.

When $u, v\colon]1,\infty[\to [0,\infty]$ 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 $\alpha_{G,S} \simeq \alpha_{G,T}$. So if G is finitely generated, the $\simeq$-class of the function $\alpha_{G,S}$ does not depend on the finite symmetric generating subset S. This class is usually called the *isoperimetric profile* of G (and it is $\simeq \infty$ if and only if G is nonamenable).

By a result of Coulhon and Saloff-Coste [CoSa], the isoperimetric profile grows at least as fast as the volume growth. If $G = \mathbf{Z}^d$, the isoperimetric profile $\simeq r^d$ 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 $\succeq \exp(r)$ and this is optimal for polycyclic groups [Pi].

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

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

We check immediately that for all reals $r \geq 1$ and integers $n \geq 1$ we have $\alpha_{G,S}(r) \leq n$ if and only if $r < I_{G,S}(n)^{-1}$. 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* that is intuitively associated to a group but more formally associated to its finite pieces or "chunks". A similar but different notion of the "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. We call a *chunk* a finite set E endowed with a basepoint 1_E and a subset D of $E \times E \times E$ satisfying the condition that $(x, y, z), (x, y, z') \in D$ implies $z = z'$. So we can view a chunk 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 a *representation* of E into G a mapping $f\colon E \to G$ such that $f(1_E) = 1_G$ and $f(x)f(y) = f(z)$ whenever $xy = z$.

Suppose E is a subset of a group G with $1_G \in E$. Then E is naturally a chunk with basepoint 1_G by setting $xy = z$ whenever this holds in the group G; we call E a chunk of G (a 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 $\mathcal{C}$.*

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 as a mapping $f\colon E \to \mathrm{Sym}_n$ such that $f(1_E) = \mathrm{id}$ and $\mathrm{d}^n_{\mathrm{Ham}}(f(xy), f(x)f(y)) \leq \varepsilon$ for all $x, y \in E$, where the Hamming distance $\mathrm{d}^n_{\mathrm{Ham}}$ is defined in (1.1). A mapping from E to the symmetric group Sym_n is said to be $(1-\varepsilon)$-*expansive* if $\mathrm{d}^n_{\mathrm{Ham}}(x, y) \geq 1 - \varepsilon$ whenever x, y are distinct points of E.

Define the *sofic profile* of the chunk E as the nondecreasing function

$$\begin{aligned}\sigma_E(r) = \inf\{n \mid \exists f\colon E \to (\mathrm{Sym}_n, \mathrm{d}^n_{\mathrm{Ham}}),\\ f \text{ is a } (1 - r^{-1})\text{-expansive } r^{-1}\text{-morphism}\} \quad (r > 1),\end{aligned}$$

where $\inf\{\emptyset\} = +\infty$. We 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, then one of the following statements holds.*

- *E has an injective representation into a finite group and hence its sofic profile is bounded*; *that is,* $\sup_r \sigma_E(r) < \infty$.
- *The sofic profile of E 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 $r > 1$. Hence, 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; that is, suppose $\sigma_E(r) < r$ for some $r > 1$. Then 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 $\mathrm{d}^n_{\mathrm{Ham}}$ takes values in $\{0, 1/n, \ldots, 1\}$ and since $r^{-1} < n^{-1}$, this shows that ϕ is a 0-morphism; in other words, ϕ is an injective representation. □

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

This definition is a restatement of the one 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—then 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. Then one of the following statements holds.*

- *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.*
- *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 [Ste; VGo]; 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 [Ste; VGo]).

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. They include:

- abelian groups and, more generally, abelian-by-nilpotent groups (groups with an abelian normal subgroup such that the quotient is nilpotent) [H];
- linear groups—that is, subgroups of $\mathrm{GL}_n(A)$ for any n and commutative ring A (see [We]);
- groups of automorphisms of affine varieties over a field [BaL]; and
- 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 then it is, by [BiSt, Thm. A], an inductive limit of a sequence of finitely generated virtually free groups. Such groups are not necessarily locally residually finite [Ste; VGo]. For examples of groups not approximable by finite groups, see Proposition 3.17 and Example 3.19.

To pursue the discussion, we use the following useful terminology, which in a certain sense allows one 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 this property 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. [CGP, 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 contain 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 and corresponding chunk E, 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 showed that its asymptotics depend only on G and not on the choice of S, and they related the sofic dimension growth to the isoperimetric profile. However, the sofic dimension growth is quite different in spirit from the sofic profile because the former takes into account the shape of balls. In particular, it is bounded only for finite groups.

I have so far been unable 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 could probably be done—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 versus 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 endowed with the action of left multiplication. With this in mind, it is elementary to check that the sofic profile is asymptotically bounded above by the isoperimetric profile; more 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 $\alpha_{G,S}(r) \le n$ and let us show that $\sigma_S(r/3) \le n$. By assumption, there exists an $E \subset G$ with $0 < \#(E) \le n$ and $\#(SE - E)/\#(E) < r^{-1}$. For $s \in S$, define $\phi(s)\colon E \to E$ to map $x \mapsto sx$ if $sx \in E$, and extend this mapping arbitrarily to a bijection. By assumption, for each s, the proportion of $x \in E$ such that $\phi(s)(x) = sx$ is greater than $1 - r^{-1}$. It follows that the Hamming distance between $\phi(s)$ and $\phi(s')$ is greater than $1-2r^{-1}$ whenever $s, s' \in S$ and $s \neq s'$ and that the Hamming distance between $\phi(st)$ and $\phi(s)\phi(t)$ is less than $3r^{-1}$ whenever $s, t, st \in S$. Therefore, $\sigma_S(r/3) \le n$. □

It is known [ESz2] that any sofic-by-amenable group (i.e., a group lying in an extension with sofic kernel and amenable quotient) is still sofic. The proof given there is an explicit construction that yields, without any change, the following theorem.

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 exist a symmetric chunk E' in N and a finite symmetric subset S in Q such that $\sigma_E(r) \le \sigma_{E'}(r)\alpha_{Q,S}(r)$ for all $r > 1$.*

In particular, given nondecreasing functions $u, v\colon]1,\infty[\to [1,\infty]$, 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 this class 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 that contains the trivial group and is 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, since the degree d may depend on the chunk.

PROPOSITION 3.17. *For $k, \ell \in \mathbf{Z} \setminus \{0\}$, the sofic profile of the Baumslag–Solitar group*

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

is at most linear (i.e., $\preceq r$); more precisely, it is linear (i.e., $\simeq r$) 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 linearity of $\mathbf{Z}$'s isoperimetric profile, and because 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 via multiplication by k and ℓ, respectively, the group N is an iterated free product with amalgamation $\cdots \mathbf{Z} *_{\mathbf{Z}} \mathbf{Z} *_{\mathbf{Z}} \mathbf{Z} *_{\mathbf{Z}} \cdots$; here each embedding of $\mathbf{Z}$ to the left (resp., right) is given by multiplication by k (resp., by ℓ) [Se1, I.1.4, Prop. 6]. This group is locally residually finite; in other words, every such finite iteration $\mathbf{Z} *_{\mathbf{Z}} \mathbf{Z} *_{\mathbf{Z}} \cdots *_{\mathbf{Z}} \mathbf{Z}$ is residually finite—as follows, for instance, from [Ev]. (In case k, ℓ are coprime, Campbell [Cam] showed that N itself is not residually finite and even that all of its finite quotients are abelian.)

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

Note that $\mathrm{BS}(k, \ell)$ being 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. Then the sofic profile grows at least linearly, as we observed previously, but we have no example with a better lower bound.

EXAMPLE 3.19. Here are some examples of finitely generated groups that are not approximable by finite groups but whose sofic profiles could be overlooked.

- *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 groups include finitely presented simple groups. Many more examples—including Thompson's group F of the interval—are given in [CGP], which also gives several examples that are amenable (solvable or not) and therefore sofic. In addition, we can find in [CGP] examples of nonamenable isolated groups, but whether they are sofic is not known; however, an example of a nonamenable isolated group that is known to be sofic is given in [C].
- *Other finitely presented nonresidually finite groups.* This category includes most Baumslag–Solitar groups (as established in Proposition 3.17) as well as various other one-relator groups [Bau2; BauMT]. Another example is Higman's group
$$\langle x_1, x_2, x_3, x_4 \mid x_{i-1} x_i x_{i-1}^{-1} = x_i^2 \ (i = 1, 2, 3, 4 \bmod 4)\rangle$$
[Se1, I.1.4, Prop. 5], which has no proper subgroup of finite index. Whether it is sofic is not known.
- *Direct products of the preceding 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 $\mathbf{F}$ that satisfies the following condition. If we denote by B and B'' the K-algebras of functions of X and the $\mathbf{F}$-algebra of functions on X'' (respectively), then there exist a finitely generated subdomain A of K, a finitely generated A-subalgebra B' of B, and a surjective homomorphism $A \to \mathbf{F}$ such 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 let 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 $\mathrm{Aut}_K(L)$; this subset consists of a finite family (v_i) of pairwise distinct elements of $\mathrm{Aut}_K(L)$. Then there exists an $f \in B - \{0\}$ such that $v_i(B) \subset B[f^{-1}]$ for all i. Denote by $u_i \colon B \to B[f^{-1}]$ the K-algebra homomorphism that is the restriction of v_i.

Fix generators $t_1, \dots, t_m$ of B as a K-algebra, so that $B[f^{-1}]$ is generated by $t_1, \dots, t_m, f^{-1}$ 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 $(t_1, \dots, t_m, f^{-1})$. 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 $K[X_1, \dots, X_m]$ 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 $t_1, \dots, t_m$; 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, Lemma 6.7], there exists an $s \in A_0 - \{0\}$ such that $B' = B'_0[s^{-1}]$ is flat over $A = A_0[s^{-1}]$. Because 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 "$\cdot \otimes_A K$" 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 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 $\phi \colon \mathrm{Spec}(B') \to \mathrm{Spec}(A)$ that consists of 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 Spec(B') containing $\{0\}$. Since B' is A-flat, the map ϕ is open [SGA, Thm. 6.6]. Hence there exists an $a \in A - \{0\}$ 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 an $a' \in A - \{0\}$ 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 e.g. [Ei, Thm. 4.19]). Since u_i' is an A-algebra homomorphism, it sends $\mathfrak{m}B'$ to $\mathfrak{m}B'[f^{-1}]$ and therefore induces an $(A/\mathfrak{m})$-algebra homomorphism $u_i''\colon B'/\mathfrak{m}B' \to B'[f^{-1}]/\mathfrak{m}B'[f^{-1}]$. Since $x \neq 0$ in $B'/\mathfrak{m}B'$, the u_i'' are pairwise distinct.

We need to check that $\dim(B'/\mathfrak{m}B') \le d$. First, by [Ei, Thm. 13.8], $\dim(B') \le \dim(A)+d$. Now, since B' is A-flat, by [Ei, Thm. 10.10] we have $\dim(B'/\mathfrak{m}B') \le \dim(B') - \dim(A_\mathfrak{m})$. Since A is a finitely generated domain and since $\mathfrak{m}$ is a maximal ideal, it follows that $\dim(A_\mathfrak{m}) = \dim(A)$ (see Lemma 4.3); then the two preceding inequalities allow us to deduce that $\dim(B'/\mathfrak{m}B') \le d$. (Actually, both inequalities are equalities (same references): for the first one, [Ei, Thm. 13.8] uses that A is universally catenary, which follows because $\mathbf{Z}$ is universally catenary according to [Ei, 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 there exist two homomorphisms $\alpha, \beta\colon R \to R[s^{-1}]$ 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 $\alpha\beta\colon R \to R[(s\alpha(s))^{-1}]$.

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

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

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

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

For all ℓ, j, we can write the formal identity

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

for some $V_{\ell j} \in B[X_1, \dots, X_m, Y]$ 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 following equality in L:

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

that is,

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

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 just described.

Since in particular for every i there exists an ι such that $v_i v_\iota$ and $v_\iota v_i$ are the identity, it follows that $u_i''u_\iota''$ 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, if $u_i u_j = u_k$ then $u_i''u_j'' = u_k''$, which implies that $v_i''v_j'' = v_k''$. Thus the claim is proved and hence Proposition 4.1 as well. □

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, then A is a finitely generated algebra over the field on p elements and so [Ei, Cor. 13.4] (based on Noether normalization) applies; therefore, $\dim(A) = \dim(A_{\mathfrak{m}}) + \dim(A/\mathfrak{m}) = \dim(A_{\mathfrak{m}})$.

If the characteristic is 0 then we use that the ring $\mathbf{Z}$ is universally catenary [Ei, Cor. 18.10] to apply [Ei, Thm. 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 $\dim(\mathbf{Z}_{\mathfrak{m}\cap\mathbf{Z}}) = 1$; hence $\dim(A_{\mathfrak{m}}) = 1 + \dim(A \otimes_{\mathbf{Z}} \mathbf{Q})$. Because this value does not depend on $\mathfrak{m}$, we can deduce that $\dim(A_{\mathfrak{m}}) = \dim(A)$. □

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 $\preceq n^d$, where $d = \dim(X)$.*

The proof is similar to that for Proposition 2.3 and is 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 no less than $cq^d - c'$.

From Propositions 4.1 and 4.4 we deduce the following result.

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 $\preceq n^d$, 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—that is, 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 $p\colon \mathbb{F} \to \Gamma$ 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 depends neither on the choice of $\mathbb{F}$ nor on 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 $\mathbb{F} = \mathbb{F}_k = \langle t_1, \dots, t_k \rangle$ and set $u_i = p(t_i)$. If we input any word $w \in \mathbb{F}$, then we can compute $w(u_1, \dots, u_k)$ (computed according to the given law on $\mathbf{N}$) and answer Yes or No according as whether or not $w(u_1, \dots, u_k) = e$.

Conversely, suppose that the condition is satisfied. Start from a recursive enumeration $u\colon \mathbf{N} \to \mathbb{F}$. Given n, we define $\kappa(n) = \inf\{k \le n : u(k)u(n)^{-1} \in N\}$. Since N is recursive, κ must be 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 $q\colon \mathbf{N} \to J$ defined by an obvious induction. Finally, define $n * m = q^{-1}\big(\kappa(u^{-1}(u(q(n))u(q(m))))\big)$. 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 nonnegative 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. Therefore, K is a degree m extension of some purely transcendental field $L = F(t_1, \dots, t_n)$ with F a prime field ($\mathbf{F}_p$ or $\mathbf{Q}$). Given that there is an inclusion $\mathrm{Cr}_d(K) \subset \mathrm{Cr}_{md}(L)$, we can suppose that K is itself a purely transcendental field. Hence we can implement formal calculus of K, where for $F = \mathbf{Q}$ the 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 $K(u_1, \dots, u_d)$; each is given as a pair of polynomials (numerator and nonzero denominator). The product of two elements in $\mathrm{Cr}_d(K)$ can be computed by way of 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 established by computing $P_1Q_2 - P_2Q_1$ and then checking whether this difference is the zero polynomial in $F(t_1, \dots, t_n, u_1, \dots, u_d)$. In particular, we can check the equality of $(P_1/Q_1, \dots, P_d/Q_d)$ and $(u_d, \dots, u_d)$. $\square$

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 $g_1, \dots, g_k$, the preceding algorithm—whose input is a group word $w \in F_k$ and whose output is Yes or No according as whether or not $w(g_1, \dots, g_k) = 1$ in $\mathrm{Cr}_d(K)$—has exponential time with respect to the length of w.

The proof of Theorem 5.3 is similar to the proof (due to Rabin [Ra]) of the more specific case of finitely generated linear groups. However, in the latter case the elements can be implemented as matrices, from which 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. More generally, the proof of Theorem 5.3 shows 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 $K(t_1,\dots,t_n)$) has a solvable word problem. In other words, given $g_1,\dots,g_k$, there is an algorithm whose input is a pair of words w,w' in k letters and whose output is Yes or No according as whether or not $w(g_1,\dots,g_k) = w'(g_1,\dots,g_k)$. For the same reason as given in Remark 5.4, this algorithm has exponential time.

References

[Ba] H. Bass, *Automorphismes de schémas et de groupes de type fini,* Paul Dubreil and Marie-Paule Malliavin algebra seminar (Paris, 1981), Lecture Notes in Math., 924, pp. 310–321, Springer-Verlag, Berlin, 1982.

[BaL] H. Bass and A. Lubotzky, *Automorphisms of groups and of schemes of finite type,* Israel J. Math. 44 (1983), 1–22.

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

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

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

[BauSo] G. Baumslag and 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), 257–259.

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

[BirRS] J.-C. Birget, E. Rips, and M. Sapir, *Isoperimetric and isodiametric functions of groups,* Ann. of Math. (2) 156 (2002), 345–466.

[B1] J. Blanc, *Finite abelian subgroups of the Cremona group of the plane,* C. R. Math. Acad. Sci. Paris 344 (2007), 21–26.

[B2] ———, *Sous-groupes algébriques du groupe de Cremona,* Transform. Groups 14 (2009), 249–285.

[B3] ———, *Elements and cyclic subgroups of finite order of the Cremona group,* Comment. Math. Helv. 86 (2011), 469–497.

[BD1] J. Blanc and J. Déserti, *Embeddings of* $\mathrm{SL}(2,\mathbb{Z})$ *into the Cremona group* (English summary), Transform. Groups 17 (2012), 21–50.

[BD2] ———, *Degree growth of birational maps of the plane,* preprint, math:ArXiv/1109.6810.

[Cam] R. I. Campbell, *Notes on the Baumslag–Solitar non-residually finite examples,* Proc. Amer. Math. Soc. 109 (1990), 59–62.

[Ca1] S. Cantat, *Sur les groupes de transformations birationnelles des surfaces,* Ann. of Math. (2) 174 (2011), 299–340.

[Ca2] ———, *Morphisms between Cremona groups and a characterization of rational varieties,* Compositio Math. (to appear).

[CeD] D. Cerveau and J. Déserti, *Transformations birationnelles de petit degré,* Cours Spéc., Soc. Math. France, Paris (to appear).

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

[CGP] Y. Cornulier, L. Guyot, and W. Pitsch, *On the isolated points in the space of groups,* J. Algebra 307 (2007), 254–277.

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

[D] J. Déserti, *Sur les sous-groupes nilpotents du groupe de Cremona,* Bull. Braz. Math. Soc. (N.S.) 38 (2007), 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), 55–62 (Russian); English translation in Proc. Steklov Inst. Math. 264 (2009), 48–55.

[DoI1] I. V. Dolgachev and V. A. Iskovskikh, *Finite subgroups of the plane Cremona group,* Algebra, arithmetic, and geometry, Progr. Math., 269, pp. 443–548, Birkhäuser, Boston, 2009.

[DoI2] ———, *On elements of prime order in the plane Cremona group over a perfect field,* Int. Math. Res. Not. 2009 (2009), 3467–3485.

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

[Ei] D. Eisenbud, *Commutative algebra. With a view toward algebraic geometry,* Grad. Texts in Math., 150, Springer-Verlag, Berlin, 1994.

[ESz1] G. Elek and E. Szabó, *Sofic groups and direct finiteness,* J. Algebra 280 (2004), 426–434.

[ESz2] ———, *On sofic groups,* J. Group Theory 9 (2006), 161–171.

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

[F] E. Følner, *On groups with full Banach mean value,* Math. Scand. 3 (1955), 243–254.

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

[H] P. Hall, *Finiteness conditions for soluble groups,* Proc. London Math. Soc. (3) 16 (1954), 419–436.

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

[Ma1] A. Mal'cev, *On the faithful representation of infinite groups by matrices,* Mat. Sb. 8 (1940), 405–422 (Russian); English translation in Amer. Math. Soc. Transl. (2) 45 (1965), 1–18.

[Ma2] ———, *Algebraic systems* (D. Smirnov, M. Taclin, eds.; B. D. Seckler, A. P. Doohovskoy, transls.), Grundlehren Math. Wiss., 192, Springer-Verlag, New York, 1973.

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

[M] C. F. Miller III, *The word problem in quotients of a group,* Aspects of effective algebra (Clayton, 1979), pp. 246–250, Upside Down, Yarra Glen, Victoria, 1981.

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

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

[PiSa] C. Pittet and L. Saloff-Coste, *Random walk and isoperimetry on discrete subgroups of Lie groups,* Random walks and discrete potential theory (Cortona, 1997), Sympos. Math., 39, pp. 306–319, Cambridge Univ. Press, Cambridge, 1999.

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

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

[PrSh] Yu. Prokhorov and C. Shramov, *Jordan property for Cremona groups,* preprint, arXiv:math/1211.3563.

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

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

[Se1] J-P. Serre, *Arbres, amalgames,* SL_2, Astérisque 46 (1977).

[Se2] ———, *Le groupe de Cremona et ses sous-groupes finis,* Astérisque 332 (2010), 75–100.

[SGA] A. Grothendieck et al., *Revêtements Étales et Groupe Fondamental,* Lecture Notes in Math., 224, Springer-Verlag, Berlin, 1971.

[Ste] A. M. Stëpin, *Approximability of groups and group actions,* Uspekhi Mat. Nauk 38 (1983), 123–124.

[V] A. M. Vershik, *Amenability and approximation of infinite groups,* Selecta Math. Soviet. 2 (1982), 311–330.

[VGo] A. M. Vershik and E. I. Gordon, *Groups that are locally embeddable in the class of finite groups,* St. Petersburg Math. J. 9 (1998), 49–67.

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

[We] B. Wehrfritz, *Infinite linear groups,* Ergeb. Math. Grenzgeb. (3), 76, Springer-Verlag, New York, 1973.

[Wei] B. Weiss, *Sofic groups and dynamical systems,* Ergodic theory and harmonic analysis (Mumbai, 1999), Sankhyā Ser. A 62 (2000), 350–359.

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

yves.cornulier@math.u-psud.fr