Polynomial maps over finite fields and residual finiteness of mapping tori of group endomorphisms

Alexander Borisov and Mark Sapir[*]

Abstract

We prove that every mapping torus of any free group endomorphism is residually finite. We show how to use a not yet published result of E. Hrushovski to extend our result to arbitrary linear groups. The proof uses algebraic self-maps of affine spaces over finite fields. In particular, we prove that when such a map is dominant, the set of its fixed closed scheme points is Zariski dense in the affine space.

1 Introduction

This article contains results in group theory and algebraic geometry. We think that both the results and the relationship between them are interesting and will have other applications in the future.

We start with group theory. Let G be a group given by generators $x_1, ..., x_k$ and a set of defining relations R, and let $\phi: x_i \mapsto w_i$, $1 \leq i \leq k$ be an injective endomorphism of G. Then the group

$$\text{HNN}_\phi(G) = \langle x_1, ..., x_k, t \mid R, tx_i t^{-1} = w_i, i = 1, ..., k \rangle$$

is called the *mapping torus* of ϕ (or *ascending HNN extension of G corresponding to ϕ*). This group has an easy geometric interpretation as the fundamental group of the mapping torus of the standard 2-complex of G

---

with bounding maps the identity and ϕ. The simplest and one of the most important cases is when G is the free group F_k of rank k, i.e. when R is empty. These groups appear often in group theory and topology. In particular, many one-relator groups are ascending HNN extensions of free groups (more on that below).

Some essential information about the mapping tori of free group endomorphisms is known. In particular, Feighn and Handel [FH] proved that these groups are coherent, that is, all their finitely generated subgroups are finitely presented. They also characterized all finitely generated subgroups of such groups. We know [GMSW] that these groups are Hopfian, that is every surjective endomorphism of such a group must be injective. On the other hand, ascending HNN extensions of arbitrary residually finite groups are not necessarily Hopfian [SW].

Many of the groups of the form $\text{HNN}_\phi(F_k)$ are hyperbolic (see [BF] and [Kap1]). One of the outstanding problems about hyperbolic groups is whether they are residually finite. Recall that a group is called *residually finite* if the intersection of its subgroups of finite index is trivial. This leads to the following question:

Problem 1.1. *Are all mapping tori of free groups residually finite?*

This question also arises naturally when one tries to characterize residually finite one-related groups. As far as we know Problem 1.1 was explicitly formulated first by Moldavanskii in [Mol] (it is also mentioned in [Wise] and listed as Problem 1 in the list of ten interesting open problems about ascending HNN extensions of free groups in [Kap1]).

Notice that ascending HNN extensions of residually finite groups may be not residually finite. They can even have very few finite homomorphic images as is the case for Grigorchuk's group [SW]. However if ϕ is an automorphism and G is residually finite then $\text{HNN}_\phi(G)$ is also residually finite [Mal2]. Thus the interesting case in Problem 1.1 is when ϕ is not surjective. Some special cases of Problem 1.1 have been solved in [Wise] (these cases proved to be useful in Wise's residually finite version of Rips' construction), and in [HW] (where it is proved that the mapping tori of polycyclic groups are residually finite).

Notice also that the groups $\text{HNN}_\phi(F_k)$ do not necessarily satisfy properties that are known to be somewhat stronger than the residual finiteness. For example, the group $\langle a, t \mid tat^{-1} = a^2 \rangle$ is not a LERF group (a cannot

be separated from the cyclic group $\langle a^2 \rangle$ by a homomorphism onto a finite group).

It is worth noting also that groups $\text{HNN}_\phi(F_k)$ are not necessarily linear (over any field). For example the groups $\langle a, b, t \mid tat^{-1} = a^k, tbt^{-1} = b^l \rangle$, where $|k|, |l| \notin \{1, -1\}$, and $\langle a, b, t \mid tat^{-1} = b, tbt^{-1} = a^2 \rangle$ are not linear [Wer], [DS]. A conjecture from [DS] states that "most" groups of the form $\text{HNN}_\phi(F_k)$ are not linear provided ϕ is not an automorphism.

One of the main goals of this paper is to solve Problem 1.1.

Theorem 1.2. *The mapping torus of any injective endomorphism of a free group is residually finite.*

Computer experiments conducted by Ilya Kapovich, Paul Schupp, and the second author of this paper seem to show that most 1-related groups are subgroups of ascending HNN extensions of a free group[1]. Thus it could well be true that groups with one defining relation are generically inside ascending HNN extensions of free groups. If this conjecture turns out to be true then Theorem 1.2 would imply that one-related groups are generically residually finite. (Recall that there exist non-residually finite one-related groups, for example the Baumslag-Solitar group $BS(2,3) = \langle a, t \mid ta^2t^{-1} = a^3 \rangle$.) Anyway, it is clear that Theorem 1.2 applies to very many one-related groups.

The proof of Theorem 1.2 was obtained in a rather unexpected way. The proofs of the previous major results about mapping tori of groups (see for example [FH], [GMSW], [Kap1]) were of topological nature. We know of several attempts (see [HW], [Wise]) to apply similar methods to Problem 1.1: residual finiteness of the fundamental group of a CW-complex is equivalent to the existence of enough finite covers of that complex to separate all elements of the fundamental groups. But these approaches produced only partial results. Even simple examples like the group $\langle a, b, t \mid tat^{-1} = ab, tbt^{-1} = ba \rangle$ have been untreatable so far by the topological methods.

Our approach is based on a reduction of Problem 1.1 to some questions about periodic orbits of algebraic maps over finite fields (see Section 2). More precisely, we study the orbits consisting of points conjugate over the

---

[1] A simple Maple program written by the second author of this paper checked 30,000 random two-letter group words of length 300,000 Schupp's program checked 50,000 two-letter random words of length between 100,000 and 110,000. Both programs found that at least 99.6% of the corresponding 1-related groups are subgroups of ascending HNN extensions of finitely generated free groups.

base field. In the language of schemes these orbits correspond to the fixed closed scheme points. Such points appeared in the Deligne Conjecture, and were extensively studied before (see, e.g., [Fu], [Pink]). However, these investigations were limited to the quasi-finite maps (that is such maps that the preimage of every geometric point is finite). Most of our maps are not quasi-finite.

Let $\Phi: A^n(\mathbb{F}_q) \to A^n(\mathbb{F}_q)$ be a polynomial map, defined over the finite field $\mathbb{F}_q$. It is given in coordinates by the polynomials $\phi_1, ..., \phi_n$ from $\mathbb{F}_q[x_1, ..., x_n]$. Suppose a point $a = (a_1, a_2, ..., a_n) \in A^n$ is defined over the algebraic closure $\overline{\mathbb{F}_q}$ of $\mathbb{F}_q$. We will call this point a *quasi-fixed point of Φ* if for some $Q = q^m$ for all i

$$\phi_i(a_1, a_2, ..., a_n) = a_i^Q.$$

More generally, for any algebraic variety X, we have the following

Definition 1.3. *Suppose $\Phi: X \to X$ is a self-map of a variety over a finite field $\mathbb{F}_q$. A geometric point x of X over some finite extension of $\mathbb{F}_q$ is called quasi-fixed with respect to Φ if $\Phi(x) = Fr^m(x)$. Here Fr^m is the m-th composition power of the geometric Frobenius morphism.*

Here is our main theorem regarding such maps.

Theorem 1.4. *Let $\Phi^n: A^n(\mathbb{F}_q) \to A^n(\mathbb{F}_q)$ be the n-th iteration of Φ. Let V be the Zariski closure of $\Phi^n(A^n)$. It is defined over $\mathbb{F}_q$. The set of its geometric points is $V(\overline{\mathbb{F}_q})$, where $\overline{\mathbb{F}_q}$ is the algebraic closure of $\mathbb{F}_q$. Then the following holds.*

1. *All quasi-fixed points of Φ belong to $V(\overline{\mathbb{F}_q})$.*

2. *Quasi-fixed points of Φ are Zariski dense in V. In other words, suppose $W \subset V$ is a proper Zariski closed subvariety of V. Then for some $Q = q^m$ there is a point $(a_1, ..., a_n) \in V(\overline{\mathbb{F}_q}) \setminus W(\overline{\mathbb{F}_q})$ such that for all i $f_i(a_1, ...a_n) = a_i^Q$.*

After we obtained the proof of Theorem 1.4, we received a preprint [Hr] of E. Hrushovski where he proves a more general result. In particular, his results imply the following statement. Recall that a rational map $\Phi: X \to Y$ is called *dominant* if $\Phi(X)$ is Zariski dense in Y.

Theorem 1.5. *(Hrushovski, [Hr, Corollary 1.2]) Let $\Phi: X \to X$ be a dominant self-map of an absolutely irreducible variety over a finite field. Then the set of the quasi-fixed points of Φ is Zariski dense in X.*

Our Theorem 1.4 is a partial case of Theorem 1.5 where X is the Zariski closure of $\Phi^n(A^n)$. In particular, our theorem captures the (non-trivial) case when $\Phi\colon A^n \to A^n$ is dominant.

Theorem 1.5 allowed us to prove the following statement that is much stronger than Theorem 1.2.

Theorem 1.6. *The mapping torus of any injective endomorphism of a finitely generated linear group[2] is residually finite.*

As we mentioned before, for non-linear residually finite groups this statement is not true [SW]. In fact Theorem 1.2 can serve as a tool to show that a group is *not* linear. For example, the non-Hopfian example from [SW] is an ascending HNN extension of a residually finite finitely generated group that is an amalgam of two free groups. By Theorem 1.6 that amalgam of free groups is not linear.

It is well known that free groups, polycyclic groups, etc. are linear. Thus Theorem 1.2 immediately implies all known positive results about residual finiteness of mapping tori of non-surjective endomorphisms [HW], [GMSW], [Mol], [Wise].

The proof of Theorem 1.5 is complicated and uses some heavy machinery from algebraic geometry and Hrushovski's theory of difference schemes. In comparison, our proof of Theorem 1.4 is basically elementary.

Remark 1.7. Theorems 1.2 and 1.6 will remain true if we drop the requirement that the endomorphism ϕ is injective. Indeed, it is easy to see that for every endomorphism ϕ of a linear group G, the sequence $\mathrm{Ker}(\phi) \subseteq \mathrm{Ker}(\phi^2) \subseteq \mathrm{Ker}(\phi^3) \subseteq \ldots$ eventually stabilizes (see [Mal1, Theorem 11]). Then, for some n, ϕ is injective on $\phi^n(G)$, and the group $HNN_\phi(G)$ is isomorphic to the ascending HNN extension of $\phi^n(G)$. Since $\phi^n(G)$ is again a linear group, we can apply Theorem 1.6 (see details in [Kap2]).

The paper is organized as follows. In Section 2, we reduce Theorems 1.2 and 1.6 to Theorems 1.4 and 1.5. In Section 3, we give a proof of Theorem 1.4. In Section 4 we apply Theorem 1.6 to a question about extendability of endomorphisms of linear groups to automorphisms of their profinite completions. We also present some open problems.

---

[2]That is a group representable by matrices of any size over any field.

2 HNN extensions and dynamical systems

Let $T = \text{HNN}_\phi(G)$ be the ascending HNN extension of a group

$$G = \langle x_1, ..., x_k \mid R \rangle$$

corresponding to an injective endomorphism ϕ. Let t be the free letter of this HNN extension, so that $t x_i t^{-1} = \phi(x_i)$ for every $i = 1, ..., k$.

It is easy to see that every element g of T can be written as a product $t^a w t^b$ for some integers $a \leq 0$ and $b \geq 0$, $w \in G$. The map $z : T \to \mathbb{Z}$ that sends $t^a w t^b$ to $a + b$ is a homomorphism, so if $a + b \neq 0$ then g can be separated from 1 by a homomorphism onto a finite group. If $a = -b$ then g and w are conjugate, so for every homomorphism ψ, $\psi(g) \neq 1$ if and only if $\psi(w) \neq 1$. Therefore the following fact is true.

Lemma 2.1. *The group T is residually finite if and only if for every $w \in G$, $w \neq 1$, there exists a homomorphism ψ of T onto a finite group such that $\psi(w) \neq 1$.*

Let ϕ be an endomorphism of G defined by a sequence of words $w_1, ..., w_k$ from F_k (that is the images of w_i in G under the natural homomorphism $F_k \to G$ generate a subgroup that is isomorphic to G). Let H be any group (or, more generally, a group scheme). Then we can define a map $\phi_H : H^k \to H^k$ that takes every k-tuple $(h_1, ..., h_k)$ to the k-tuple

$$(w_1(h_1, ..., h_k), w_2(h_1, ..., h_k), \ldots, w_k(h_1, ..., h_k)).$$

Notice that this map is not a homomorphism. Nevertheless it defines a dynamical system on H^k.

The following lemma reformulates residual finiteness in terms of these dynamical systems.

Lemma 2.2. *The group $T = HNN_\phi(G)$ is residually finite if and only if for every $w = w(x_1, ..., x_k) \neq 1$ in G there exists a finite group $H = H_w$ and an element $h = (h_1, ..., h_k)$ in H^k such that*

(i) *$h_1, ..., h_k$ satisfy the relations from R (where h_i is substituted for x_i, $i = 1, ..., k$).*

(ii) *h is a fixed point of some power of ϕ_H, and*

(iii) $w(h_1, ..., h_k) \neq 1$ *in* H.

Proof. $\Rightarrow$ Suppose T is residually finite. Take any word $w \neq 1$ in G. Then there exists a homomorphism γ from G onto a finite group H such that $\gamma(w) \neq 1$. Let t be the free letter in G. Then $\gamma(t)\gamma(G)\gamma(t^{-1}) \subseteq \gamma(G)$. Since H is finite, $\gamma(t)$ acts on $\gamma(G)$ by conjugation. It is clear that for every element $h = (h_1, ..., h_k)$ in $\gamma(G)^k$,

$$\phi_H(h) = (\gamma(t)h_1\gamma(t^{-1}), ..., \gamma(t)h_k\gamma(t^{-1})) \in \gamma(F_k)^k. \tag{2.1}$$

Take $h = (\gamma(x_1), ..., \gamma(x_k))$. Property (i) is obvious. Property (iii) holds because $\gamma(w) \neq 1$. Property (ii) holds also because by (2.1) powers of ϕ_H act on $\gamma(G)^k$ as conjugation by the corresponding powers of $\gamma(t)$, and some power of $\gamma(t)$ is equal to 1 since H is finite.

$\Leftarrow$ Suppose that for every $w \neq 1$ in G there exists a finite group $H = H_w$ and an element $h = (h_1, ..., h_k)$ in H^k such that conditions (i), (ii) and (iii) hold. We need to prove that G is residually finite. By Lemma 2.1, it is enough to show that every such w can be separated from 1 by a homomorphism of G onto a finite group.

Pick a $w \neq 1$ in G. Let a finite group H, $h \in H^k$, be as above. By (ii), there exists an integer $n \geq 1$ such that $\phi_H^n(h) = h$. Let P be the wreath product of H and a cyclic group $C = \langle c \rangle$ of order n. Recall that P is the semidirect product of H^n and C where elements of C act on H^n by cyclically permuting the coordinates.

Consider the ϕ_H-orbit $h^{(0)} = h, h^{(1)} = \phi_H(h), ..., h^{(n-1)} = \phi_H^{n-1}(h)$ of h. Let $h^{(i)} = (h_1^{(i)}, ..., h_k^{(i)})$, $i = 0, ..., n-1$. For every $j = 1, ..., k$ let y_j be the n-tuple $(h_j^{(0)}, h_j^{(1)}, ..., h_j^{(n-1)})$. Notice that since h satisfies relations from R, $\phi_H(h)$, $\phi_H^2(h)$,... also satisfy these relations because ϕ is an endomorphism of G. This and (ii) immediately imply that the map $\phi : t \mapsto c, x_j \mapsto y_j, j = 1, ..., k$, can be extended to a homomorphism of T onto a subgroup of P generated by $c, y_1, ..., y_k$. Notice that the image of w under this homomorphism is an n-tuple $w(y_1, ..., y_k)$ from H^n whose first coordinate is $w(h_1, ..., h_k) \neq 1$ in H by property (iii). Thus w can be separated from 1 by a homomorphism of T onto a finite group. $\square$

Now we are going to show how to apply Lemma 2.2 to free groups and other linear groups. First we need to fix some notation.

Let us identify the scheme M_r of all r by r matrices with the scheme $\mathrm{Spec}\,\mathbb{Z}[a_{i,j}]$, $1 \leq i, j \leq r$. The scheme GL_r is its open subscheme obtained by

localization by the determinant polynomial det. This is a group scheme (see [Wat]). The group scheme $SL_r = Spec\mathbb{Z}[a_{i,j}]/(\det -1)$ is a closed subscheme of M_r. For every field K the group schemes $GL_r(K)$ and $SL_r(K)$ are obtained from GL_r and SL_r by the base change. Then the groups $GL_r(K)$ and $SL_r(K)$ are the groups of the $K-$rational geometric points of the corresponding group schemes.

The multiplicative abelian group scheme T_m acts on M_r by scalar multiplication. The scheme GL_r is invariant under this action. This induces the action of the multiplicative group K^* on the group $GL_r(K)$. The quotient of $GL_r(K)$ by this action is the group $PGL_r(K)$.

For every group word w we consider the formal expression $\bar{w}$ which is obtained from w by replacing every letter x^{-1} by the symbol $adj(x)$. Thus to every word w in k letters, we can associate a polynomial map $\pi_w \colon M_r^k \to M_r$ which takes every k-tuple of matrices $(A_1, ..., A_k)$ to $\bar{w}(A_1, ..., A_k)$ where $adj(A_i)$ is interpreted as the adjoint of A_i. This map coincides with w on SL_r since for the matrices in SL_r, the adjoint coincides with the inverse.

Similarly, for every endomorphism ϕ of the free group F_k, we can extend the map $\phi_{SL_r} \colon SL_r^k \to SL_r^k$ to a self-map of M_r^k which we shall denote by Φ.

The map Φ is a self-map of the scheme $Spec\mathbb{Z}[a_{i,j}^m]$, $1 \leq i,j \leq r, 1 \leq m \leq k$. By base change it induces a self-map of the scheme $SpecK[a_{i,j}^m]$. $1 \leq i,j \leq r, 1 \leq m \leq k$ for every field K. This map can be restricted to the self-map of $GL_r^k(K)$. The induced map on the $K-$rational points is $\phi_{GL_r(K)}$. It descends to the self-map of $PGL_r^k(K)$ which coincides with the map $\phi_{PGL_r(K)}$ defined above.

Now we are ready to derive Theorems 1.2 and 1.6 from Theorems 1.4 and 1.5, respectively.

Proof of Theorem 1.2. Let ϕ be an injective endomorphism of the free group $F_k = <x_1, ..., x_k>$ and $1 \neq w \in F_k$. Consider the self-map Φ of the scheme M_2^k as above. Denote $n = 4k$. Similarly to Theorem 1.4, we denote by V the Zariski closure of $\Phi^n(M_2^k)$. This is a scheme over $Spec\mathbb{Z}$. Consider the map $\pi_w \colon V \to M_2$ as above. We have the following lemma.

Lemma 2.3. *In the above notation, $\pi_w(V)$ is not contained in the scheme of the scalar matrices.*

Proof. It is enough to find a point of V over $\mathbb{C}$ which is not mapped to a scalar matrix by π_w. By the result of Sanov [San] there is an embedding $\gamma \colon F_k \to SL_2(\mathbb{Z})$. Obviously, $\gamma(F_k)$ does not contain the matrix $-Id$, so all

8

nontrivial elements of F_k are mapped to non-scalar matrices. Consider the point $u \in V(\mathbb{C})$ defined as $u = \Phi^n(\gamma(x_1), ..., \gamma(x_k))$. By the definitions of π_w and Φ we get $\pi_w(u) = \gamma(\phi^n(w))$. Since ϕ is injective, $\phi^n(w) \neq 1$. Therefore $\pi_w(u)$ is not a scalar matrix.

$\square$

Now we fix a big enough prime p and make a base change from $\mathbb{Z}$ to the finite field $\mathbb{F}_p$. Slightly abusing the notation, we will from now on denote by Φ and π_w the maps of the corresponding schemes over $\mathbb{F}_p$. And V will also denote the corresponding scheme over $\mathbb{F}_p$. From Lemma 2.3, for big enough p, $\pi_w V$ is not contained in the scheme of scalar matrices. Consider the subscheme Z_w of V which is the union of the π_w-pullback of scalar matrices and the subscheme of V consisting of k-tuples where one of the coordinates is singular. We have that Z_w is a proper subscheme of of V. By Theorem 1.4 there exists a point $h = (a_1, ..., a_k) \in V \setminus Z_w$ such that $\Phi(h) = (a_1^Q, ..., a_k^Q)$ for some $Q = p^s$. Then the powers of Φ take the point h to $(a_1^{Q^l}, ..., a_k^{Q^l})$, $l \geq 1$ (we use the fact that, in characteristic p, the Frobenius commutes with every polynomial map defined over $\mathbb{F}_p$). Therefore some power of Φ fixes h. In addition $\pi_w(h)$ is not a scalar matrix and each a_i is not a singular matrix because $h \notin Z_w$. Taking the factor over the torus action, we get a point h' in $\mathrm{PGL}_2^k(\mathbb{F}_{p^i})$ that is fixed by some power of the map Φ and such that $w(h') \neq 1$ in $\mathrm{PGL}_2(\mathbb{F}_{p^i})$. Thus the group $\mathrm{PGL}_2(\mathbb{F}_{p^i})$ and the point h' satisfy all three conditions of Lemma 2.2. Since $w \in F_k$ was chosen arbitrarily, the group $\mathrm{HNN}_\phi(F_k)$ is residually finite. This completes the proof of Theorem 1.2.

Proof of Theorem 1.6. Suppose $G \subseteq \mathrm{SL}_r(K)$. Here K is some field and $G = <x_1, ..., x_k \mid R>$. Let U_G be the representation scheme of the group G in SL_r, i.e. the reduced scheme of k-tuples of matrices from SL_r satisfying the relations from R. This is a scheme over $\mathrm{Spec} K$. Suppose ϕ is an injective endomorphism of G and $1 \neq w \in G$. We choose a representation of ϕ and w using the words on $x_1, ..., x_k$ and consider the maps Φ and π_w. Since ϕ is an endomorphism of G, the representation subscheme U_G is invariant under Φ. Obviously, for big enough m the map Φ is dominant on the subscheme V, which is the Zariski closure of $\Phi^m(U_G)$. Note that V may be reducible because U_G may be reducible. Since ϕ is injective, $\phi^m(w) \neq 1$. Therefore $\pi_w(V) \neq \{Id\}$. By the usual specialization argument (as in [Mal1]) there exists a finite field $\mathbb{F}_q$ such that for the corresponding schemes and maps over $\mathbb{F}_q$ the same properties are satisfied. That is, Φ is dominant on V, where V is the Zariski closure of $\Phi^m(U_G)$, everything over $\mathbb{F}_q$. In addition,

$\pi_w(V) \neq \{Id\}$. Consider the subscheme Z_w of V which is the π_w-pullback of the identity. We have that Z_w is a proper subscheme of V. We enlarge the finite field to make all irreducible components of V defined over $\mathbb{F}_q$. Some power of Φ maps each of these components into itself, dominantly. We now apply Theorem 1.5 to this power of Φ, the scheme $V \subseteq \mathrm{SL}_r^k$ and its subscheme Z_w. As in the proof of Theorem 1.2, we find a point $h \in V(\mathbb{F}_{q^i}) \setminus Z_w(\mathbb{F}_{q^i})$ that is fixed by some power of Φ. Since h belongs to the representation variety U_G, its coordinates satisfy all the relations from R, so the condition (i) of Lemma 2.2 is satisfied. Other conditions of the lemma hold as before. Thus we can take the group $\mathrm{SL}_r(\mathbb{F}_{q^i})$ as H_w, and h as the point required by Lemma 2.2. This completes the proof of Theorem 1.6.

3 Polynomial maps over finite fields

In this section, we shall give a self-contained proof of Theorem 1.4. It is of independent interest from an algebraic geometry perspective. So while writing it we tried to strike a balance between using a formal algebraic geometry language best suitable for generalizations and keeping the algebraic geometry to the minimum for the benefit of the group theorists. Except for the reference to the Fulton's book at the end (in one of the two versions of the proof) all algebraic geometry used here is very basic. It is certainly covered by the Atiyah-Macdonald's commutative algebra textbook [AM] together with the first few chapters of most algebraic geometry textbooks (for example, [Bump]).

Let A^n be the affine space. Consider a map $\Phi : A^n \to A^n$ given in coordinates by polynomials

$$f_1(x_1, ..., x_n), f_2(x_1, ..., x_n), ... f_n(x_1, ..., x_n).$$

The coordinate functions of the composition power Φ^k will be denoted by $f_i^{(k)}(x_1, ..., x_n)$, for $1 \leq i \leq n$. In what follows, Φ will be defined over the finite field $\mathbb{F}_q$ of q elements (this just means that all coefficients of f_i belong to $\mathbb{F}_q$). The number Q will always mean some (big enough) power of q.

We define by induction a chain of irreducible closed subvarieties of A^n. Let $V_0 = A^n$, and for every $i \geq 1$ let V_i be the Zariski closure in A^n of $\Phi(V_{i-1})$. Alternatively, V_i is the Zariski closure of $\Phi^i(A^n)$.

The varieties V_i are irreducible (as polynomial images of an irreducible variety) and $V_{i+1} \subseteq V_i$ for all i. Because the dimension could only drop n

times, $V_n = V_{n+1} = ...$ We will denote this variety V_n by V. Note that $V = A^n$ if and only if Φ is a dominant map.

Suppose a point $a = (a_1, a_2, ..., a_n) \in A^n$ is defined over the algebraic closure $\overline{\mathbb{F}_q}$ of $\mathbb{F}_q$. Recall that a is called quasi-fixed (with respect to Φ) if there exists $Q = q^m$ such that $f_i(a_1, a_2, ..., a_n) = a_i^Q, i = 1, ..., n$.

In other words, the quasi-fixed points are those that are mapped by Φ to their conjugates. They correspond to the closed scheme points of A^n, which are fixed by Φ.

The following lemma is the first part of Theorem 1.4.

Lemma 3.1. *All quasi-fixed points belong to the variety V.*

Proof. Since Φ is defined over $\mathbb{F}_q$, all varieties V_i, $i = 1, 2, ..., n$ are defined over $\mathbb{F}_q$. For a point $a = (a_1, ..., a_n) \in A^n$ we denote by a^Q the point $\mathrm{Fr}_q^m(a) = (a_1^Q, ..., a_n^Q)$. Then suppose $\Phi(a) = a^Q$, for $Q = q^m$. This implies that $a^Q \in V_1$. Since the Frobenius Fr_q commutes with Φ, all varieties V_i are invariant with respect to Fr_q. Therefore $a \in V_1$. Hence $a^Q = \Phi(a) \in V_2$ and $a \in V_2$. By induction, we get $a \in V$. $\square$

In the above notation, our main goal is to prove the following (this is the second part of Theorem 1.4).

Theorem 3.2. *Let V be the Zariski closure of $\Phi^n(A^n)$. Then quasi-fixed points of Φ are Zariski dense in V. In other words, suppose $W \subset V$ is a proper Zariski closed subvariety. Then for some Q there is a point $(a_1, ..., a_n) \in V(\overline{\mathbb{F}_q}) \setminus W(\overline{\mathbb{F}_q})$ such that $f_i(a_1, ...a_n) = a_i^Q, i = 1, ..., n$.*

We denote by I_Q the ideal in $\overline{\mathbb{F}_q}[x_1, ..., x_n]$ generated by the polynomials $f_i(x_1, ..., x_n) - x_i^Q$, for $i = 1, 2, ..., n$.

Lemma 3.3. *For a big enough Q the ideal I_Q has finite codimension in the ring $\overline{\mathbb{F}_q}[x_1, ..x_n]$.*

Proof. We compactify A_n to the projective space P^n in the usual way. We also projectivize the polynomials $f_i - x_i^Q$. If there is a curve in P^n on which all of these projective polynomials vanish, then it must have some points on the infinite hyperplane of P^n. But this is impossible if Q is bigger than the degrees of f_i. Thus the scheme of common zeroes is zero-dimensional, which is equivalent to the ideal I_Q having finite codimension (cf. [AM], Theorem 8.5 and Exercise 8.3). $\square$

One can also prove the above Lemma directly, in the spirit of the Proof #2 below.

Lemma 3.4. *For all $1 \le i \le n$ and $j \ge 1$*

$$f_i^{(j)}(x_1, ..., x_n) - x_i^{Q^j} \in I_Q.$$

Proof. We use induction on j. For $j = 1$ the statement is obvious. Suppose it is true for some $j \ge 1$. Then

$$f_i^{(j+1)}(x_1, ..., x_n) = f_i(f_1^{(j)}, ..., f_n^{(j)}) \equiv f_i(x_1^{Q^j}, ..., x_n^{Q^j}) =$$

$$= f_i(x_1, ..., x_n)^{Q^j} \equiv x_i^{Q^{j+1}} \pmod{I_Q}$$

$\square$

The next lemma is the crucial step in the proof.

Lemma 3.5. *There exists a number k such that for every quasi-fixed point $(a_1, ..., a_n)$ with big enough Q and for every $1 \le i \le n$ the polynomial*

$$(f_i^{(n)}(x_1, ..., x_n) - f_i^{(n)}(a_1, ..., a_n))^k$$

is contained in the localization of I_Q at $(a_1, ..., a_n)$.

Proof. Let us fix i from 1 to n. The polynomials $x_i, f_i, f_i^{(2)}, ..., f_i^{(n)}$ are algebraically dependent over $\mathbb{F}_q$. This means that

$$\sum_s a_s \cdot (x_i)^{\alpha_{0,s}} \cdot (f_i)^{\alpha_{1,s}} \cdot ... \cdot (f_i^{(n)})^{\alpha_{n,s}} = 0 \tag{3.2}$$

with some non-zero $a_s \in \mathbb{F}_q$. By Lemma 3.4 the polynomial in the left hand side of (3.2) is congruent modulo I_Q to

$$P_Q(x_i) = \sum_s a_s \cdot x_i^{\alpha_s},$$

where $\alpha_s = \sum_{j=0}^{n} \alpha_{j,s} Q^j$. For big enough Q, the polynomial P_Q is non-zero. For any $(a_1, ...a_n)$ we rewrite $P_Q(x_i)$ as $\sum_t b_t \cdot (x_i - a_i)^{\beta_t}$.

So in the local ring of $(a_1, ..., a_n)$, the polynomial $P_Q(x_i)$ is equal to

$$(x_i - a_i)^{\beta} \cdot u,$$

where u is invertible and $\beta \leq \max \beta_t$. Clearly, $\max \beta_t$ is bounded by kQ^n for some k that does not depend on $Q, a_1, ..., a_n$. Denote by $I_Q^{(a_1,...,a_n)}$ the localization of I_Q in the local ring of $(a_1, ..., a_n)$. Then by (3.2) $(x_i - a_i)^{kQ^n} \equiv 0 \pmod{I_Q^{(a_1,...,a_n)}}$. Now we note that

$$f_i^{(n)}(x_1, ..., x_n) - f_i^{(n)}(a_1, ..., a_n) =$$

$$= f_i^{(n)}(x_1, ..., x_n) - a_i^{Q^n} \equiv x_i^{Q^n} - a_i^{Q^n} = (x_i - a_i)^{Q^n} (\mathrm{mod}\ I_Q^{(a_1,...,a_n)}).$$

$\square$

Let us fix some polynomial D with the coefficients in a finite extension of $\mathbb{F}_q$ such that it vanishes on W but not on V. By base change we will assume that all coefficients of D are in $\mathbb{F}_q$.

Lemma 3.6. *There exists a positive integer K such that for all quasi-fixed points $(a_1, ..., a_n) \in W$ with big enough Q we get*

$$(D(f_1^{(n)}(x_1, ..., x_n), ..., f_n^{(n)}(x_1, ..., x_n)))^K \equiv 0 (mod\ I_Q^{(a_1,...,a_n)})$$

Proof. For every $(a_1, ..., a_n) \in W$ we can rewrite $D(x_1, ..., x_n)$ as a polynomial in $x_i - a_i^{Q^n}$. This polynomial has no free term because D vanishes on W and $(a_1, ..., a_n) \in W$ by the assumption. The number of non-zero terms of D is bounded independently of a_i and Q by some number N. Then by the binomial formula and Lemma 3.5 we can take $K = N(k-1) + 1$ where k is the constant from Lemma 3.5. $\square$

The polynomial $P = (D(f_1^{(n)}(x_1, ..., x_n), ..., f_n^{(n)}(x_1, ..., x_n)))^K$ is non-zero because D does not vanish on the whole U and the map Φ is dominant on U. We now complete the proof of Theorem 3.2.

In fact we give two proofs. The first one uses the Bezout theorem, while the second one is elementary and self-contained.

Proof # 1. We denote by Z the subscheme of A^n that corresponds to P. Note that Z does not depend on Q. Now for every Q consider the $\mathbb{F}_q-$linear subspace of polynomials spanned by $f_i - x_i^Q$, $1 \leq i \leq n$. By Lemma 3.3 its base locus is zero-dimensional, i.e. these polynomials do not vanish simultaneously at any curve. The scheme Z is of pure dimension $(n-1)$. A general element τ_1 of the above linear subspace does not vanish at any of the irreducible components of Z, or their positive-dimensional intersections. So its scheme of zeroes intersects Z properly, the intersection Z_1 has pure dimension $(n-2)$.

13

Then we choose τ_2 that intersects Z_1 properly to get Z_2, and so on. After choosing $(n-1)$ elements $\tau_1, \tau_2, ..., \tau_{n-1}$ we get an ideal $I'_Q \langle D^k, \tau_1, \tau_2, ..., \tau_{n-1} \rangle$ of finite codimension. After localization at any $(a_1, ...a_n) \in W$ this ideal is contained in I_Q. By Bezout theorem (cf., e.g. [Ful])) the codimension of I'_Q is equal to $const \cdot Q^{n-1}$. But the codimension of I_Q is equal to Q^n, which is bigger for big enough Q. This implies the existence of quasi-fixed points in $V \setminus W$.

Proof # 2. This proof is elementary. Though it may appear to be longer than Proof # 1, it bypasses a lot of the intersection theory that is hidden there in the reference to the Bezout theorem. Our main object will be the ring $\mathcal{R} = \overline{\mathbb{F}_q}[x_1, ...x_n]$, where $\overline{\mathbb{F}_q}$ is the algebraic closure of $\mathbb{F}_q$. Fix $Q = q^i$ such that it is bigger than the degrees of f_i and P. By Lemma 3.1 all points with $\Phi(x) = x^Q$ belong to V. We want to prove that some of them do not belong to W.

We suppose that they all do, and we are going to derive a contradiction. First of all, we claim that in this case P lies in the localizations of I_Q with respect to all maximal ideals of $\mathcal{R}$. Indeed, the localization of I_Q with respect to the maximal ideal of a point not satisfying $\Phi(x) = x^Q$ is the whole ring. And all the localizations at the points satisfying $\Phi(x) = x^Q$ are handled by Lemma 3.6.

This implies that $P \in I_Q$. This is essentially contained in [AM], Proposition 3.8, but here is a direct argument. For every maximal ideal M of $\mathcal{R}$ there is an element u not in M such that $u \cdot P \in I_Q$. Consider the ideal $I_Q : P$. It consists of all elements $u \in \mathcal{R}$ such that $u \cdot P \in I_Q$. Since it is not contained in any maximal ideal of $\mathcal{R}$, it must be the whole $\mathcal{R}$. In particular, it contains the identity, which means that $P \in I_Q$.

This means that there exist polynomials $u_1, ...u_n$ in $\mathcal{R}$ such that

$$P = \sum_{i=1}^{n} u_i \cdot (f_i - x_i^Q) \tag{3.3}$$

The system of polynomials $u_1, ..., u_n$ as above is not unique. In fact, we can always modify it as follows. For every $i < j$ and every polynomial A, we can add $A(f_j - x_j^Q)$ to u_i and subtract $A(f_i - x_i^Q)$ from u_j. We are going to use this to get a system with the following property:

(*) For every $i < j$ the degree of x_i in every monomial in u_j is smaller than Q.

14

Here is how we can do it. Suppose that for some $i < j$ there is a monomial in u_j with the degree of x_i being at least Q. That is, $u_j = \ldots + c \cdot x_1^{a_1} \cdot \ldots \cdot x_i^{a_i+Q} \cdot \ldots \cdot x_n^{a_n} + \ldots$, where $a_l \geq 0$ for all l. Then we can replace the system $(u_1, \ldots, u_i, \ldots, u_j, \ldots, u_n)$ by the following system

$$(u_1, \ldots, u_i - c \cdot x_1^{a_1} \cdot \ldots \cdot x_i^{a_i} \cdot \ldots \cdot x_n^{a_n}(f_j - x_j^Q), \ldots, u_j + c \cdot x_1^{a_1} \cdot \ldots \cdot x_i^{a_i} \cdot \ldots \cdot x_n^{a_n}(f_i - x_i^Q), \ldots, x_n)$$

Because $Q > \deg f_l$ for all l, by repeating this procedure a finite number of times for $j = n$ we get a system $(u_1, \ldots, u_n)$ such that for all $i \leq (n-1)$ the degree of u_n with respect to x_i is less than Q. Then we do the same for $j = (n-1), (n-2)$, and so on. As a result we get a system satisfying property (*). From now on, this is going to be our system. We look at a monomial of the highest total degree among all the monomials in all the u_i, $i = 1, \ldots, n$. Suppose it belongs to u_j and equals $cx_1^{a_1} \ldots x_n^{a_n}$. Then the right hand side of the equation (3.3) contains (after multiplying out) the monomial $M = -cx_1^{a_1} \ldots x_j^{a_j+Q} \ldots x_n^{a_n}$. All monomials of the left hand side have smaller total degree because $Q > \deg P$. So there must be another monomial, M', on the right hand side with the same degrees for all variables. Because we chose the monomial of the highest total degree, and $Q > \deg f_l$ for all l, the monomial M' must also be of the form $c'x_1^{a_1'} \ldots x_n^{a_n'} \cdot x_i^Q$, for some $i \neq j$.

If $i < j$ then the degree of x_i on M' is at least Q, while the degree of x_i in M is less than Q by the property (*) of the system $(u_1, \ldots u_n)$. If $j < i$ then the degree of x_j in M is at least Q while the degree of x_j in M' is less than Q. So in both cases we have a contradiction which completes the proof.

4 Extendable endomorphisms of linear groups, and some open problems

Recall that a profinite group is, by definition, a projective limit of finite groups.

Definition 4.1. Let G be a residually finite group, ϕ be an endomorphism of G. We say that ϕ is *extendable* if there exists a profinite group $\bar{G}$ containing G as a dense subgroup, and a (continuous) automorphism $\bar{\phi}$ of $\bar{G}$ such that ϕ is the restriction of $\bar{\phi}$ on G.

Notice that even if ϕ is injective and continuous in a profinite topology of G, its (unique) extension to the corresponding completion of G may not

be injective. Injective endomorphisms of free groups that have injective extensions in p-adic (resp. pro-solvable, and many other profinite) topologies of a free group are completely described in [CSW].

There is a close connection between extendable endomorphisms and residually finite HNN extensions.

Theorem 4.2. *An injective endomorphism ϕ of a residually finite group G is extendable if and only if $HNN_\phi(G)$ is residually finite.*

Proof. Suppose that $P = \text{HNN}_\phi(G)$ is residually finite. Let Ψ be the set of all homomorphisms of P onto finite groups, Ψ' be the set of all restrictions of homomorphisms from Ψ to G. Let $\mathcal{T}$ be the smallest profinite topology on G for which all the homomorphisms from Ψ' are continuous. The base of neighborhoods of 1 for $\mathcal{T}$ is formed by the kernels of all the homomorphisms from Ψ'.

It is easy to see that for every $\psi \in \Psi'$, the homomorphism $\phi\psi$ (ϕ acts first) is also in Ψ'. Therefore the endomorphism ϕ is continuous in the topology $\mathcal{T}$. Let $\bar{G}$ be the profinite completion of G with respect to $\mathcal{T}$, and let $\bar{\phi}$ be the (unique) continuous extension of ϕ onto $\bar{G}$. Let us prove that $\bar{\phi}$ is an automorphism of $\bar{G}$.

Suppose that $\bar{\phi}$ is not injective. This means that there is a sequence of elements w_i, $i \geq 1$, in G such that w_i do not converge to 1 in $\bar{G}$ but $\phi(w_i)$ converge to 1. The latter means that there exists a sequence of subgroups $N_i = \text{Ker}(\psi_i) \subset P$, $\psi_i \in \Psi$, such that $\cap N_i = \{1\}$, $\phi(w_i) \in N_i$, $i \geq 1$.

Notice that by definition of $P = \text{HNN}_\phi(G)$, $\phi(w_i)N_i$ is a conjugate of $w_i N_i$ in P/N_i (the conjugating element is tN_i where t is the free letter of the HNN extension). Thus we can conclude that $w_i \in N_i$, $i \geq 1$. Hence $w_i \to 1$ in $\mathcal{T}$, a contradiction. Therefore $\bar{\phi}$ is injective.

Let us prove that $\bar{\phi}$ is surjective. Consider a Cauchy sequence $w = \{w_i, i \geq 1\}$ in G, that is suppose there exist $N_i = \text{Ker}(\psi_i)$, $\psi_i \in \Psi$, $i \geq 1$, such that $\cap N_i = \{1\}$ and $w_i^{-1}w_j \in N_i$ for every $j > i$.

For every $x \in G$ we have $\phi(x)N_i = txt^{-1}N_i$, and P/N_i is finite. So ϕ induces an automorphism in $G/(N_i \cap G)$. Hence for every $i \geq 1$, we can find an element u_i in G such that $\phi(u_i)N_i = w_i N_i$. Moreover since $w_i^{-1}w_j \in N_i$ for all $j > i$, $u_i^{-1}u_j \in N_i$ as well. Therefore $\{u_i, i \geq i\}$ is a Cauchy sequence and $\bar{\phi}(u) = w$. Thus $\bar{\phi}$ is an automorphism of $\bar{G}$. Notice that since $\bar{G}$ is compact, ϕ^{-1} is also continuous.

Suppose now that ϕ can be extended to a continuous automorphism $\bar{\phi}$ of a profinite group $\bar{G} \geq G$. Let $w \neq 1 \in G$. Notice that for every $w \in G$,

16

$\bar{\phi}(w) = \phi(w)$. Therefore there exists a homomorphism θ from P to the semidirect product $\bar{G} \rtimes \langle\bar{\phi}\rangle$ which is identity on G and sends t to $\bar{\phi}$. This homomorphism is clearly injective: it is easy to check that no non-trivial element $t^k w t^l$ can lie in the kernel of θ. It remains to prove that $\bar{G} \rtimes \langle\bar{\phi}\rangle$ is residually finite. But that can be done exactly as in the case of split extensions of finitely generated residually finite groups [Mal2]. Indeed, since $\bar{G}$ is finitely generated as a profinite group, it has only finitely many open subgroups of any given (finite) index, and the automorphism $\bar{\phi}$ permutes these subgroups. Hence $\bar{\phi}$ leaves invariant their intersection which also is of finite index. Therefore $\bar{G} \rtimes \langle\phi\rangle$ is residually finite-by-cyclic, so $G \rtimes \langle\phi\rangle$ is residually finite. $\qquad\square$

Theorems 1.6 and 4.2 immediately imply:

Corollary 4.3. *Every injective endomorphism of a finitely generated linear group is extendable.*

Finally let us mention two open problems.

Problem 4.4. Let ϕ and ψ be two injective endomorphisms of the free group $F_k = \langle x_1, ..., x_k \rangle$. Consider the corresponding HNN extension of F_k with two free letters t, u:

$$\text{HNN}_{\phi,\psi}(F_k) = \langle x_1, ..., x_k, t, u \mid t x_i t^{-1} = \phi(x_i), u x_i u^{-1} = \psi(x_i), 1 \le i \le k \rangle.$$

Is $\text{HNN}_{\phi,\psi}(F_k)$ always residually finite?

We believe that the answer is negative in a very strong sense: the groups $\text{HNN}_{\phi,\psi}$ should be generically non-residually finite. Since many of these groups are hyperbolic, this may provide a way to construct hyperbolic non-residually finite groups.

The next question is natural to ask for any residually finite groups.

Problem 4.5. Are mapping tori of free group endomorphisms linear?

Notice that although we use linear groups in our proof of Theorems 1.2 and 1.6, our proof does not prove linearity of the mapping tori. It is easy to extract from our proof that the mapping torus of a linear group endomorphism is embeddable into the wreath product of a linear group and the infinite cyclic group. Notice that this wreath product is not even residually finite.

References

[AM] M.F. Atiyah, I.G. Macdonald. Introduction to commutative algebra. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont. 1969.

[BF] M. Bestvina, M. Feighn. A combination theorem for negatively curved groups. J. Differential Geom. 35 (1992), no. 1, 85–101.

[Bump] Daniel Bump. Algebraic geometry. World Scientific Publishing Co., Inc., River Edge, NJ, 1998.

[CSW] Thierry Coulbois, Mark Sapir, Pascal Weil. A note on the continuous extensions of injective morphisms between free groups to relatively free profinite groups. Publicacions Matematiques, to appear (2003).

[DS] Cornelia Druţu, Mark Sapir. Non-linear 1-related residually finite groups. arXive math.GR/0405470.

[FH] Mark Feighn, Michael Handel, Mapping tori of free group automorphisms are coherent. Ann. of Math. (2) 149 (1999), no. 3, 1061–1077.

[Fu] Kazuhiro Fujiwara. Rigid geometry, Lefschetz-Verdier trace formula and Deligne's conjecture. Invent. Math. 127 (1997), no. 3, 489–533.

[Ful] William Fulton, Intersection theory. Second edition. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], 2. Springer-Verlag, Berlin, 1998.

[GMSW] Ross Geoghegan, Michael L. Mihalik, Mark Sapir, Daniel T. Wise. Ascending HNN extensions of finitely generated free groups are Hopfian. Bull. London Math. Soc. 33 (2001), no. 3, 292–298.

[Hr] E. Hrushovski. The Elementary Theory of the Frobenius Automorphisms, arXive math.LO/0406514.

[HW] Tim Hsu, Daniel T. Wise. Ascending HNN extensions of polycyclic groups are residually finite. J. Pure Appl. Algebra 182 (2003), no. 1, 65–78.

[Kap1] Ilya Kapovich. Mapping tori of endomorphisms of free groups. Comm. Algebra 28 (2000), no. 6, 2895–2917.

[Kap2] Ilya Kapovich. A remark on mapping tori of free group endomorphisms. Preprint, arXive math.GR/0208189.

[Mal1] A.I. Malcev. On isomorphic matrix representations of infinite groups. Mat. Sbornik, N.S. 8 (50), (1940). 405–422.

[Mal2] A.I. Malcev. On homomorphisms onto finite groups. Uchen. Zapiski Ivanovsk. ped. instituta. 1958, 18, 5, 49-60 (also in "Selected papers", Vol. 1, Algebra, (1976), 450-461).

[Mol] D.I. Moldavanskij. Residual finiteness of descending HNN-extensions of groups. Ukr. Math. J. 44, No.6, 758-760 (1992); translation from Ukr. Mat. Zh. 44, No.6, 842-845 (1992).

[Pink] Richard Pink. On the calculation of local terms in the Lefschetz-Verdier trace formula and its application to a conjecture of Deligne. Ann. of Math. (2) 135 (1992), no. 3, 483–525.

[San] I. N. Sanov. A property of a representation of a free group. Doklady Akad. Nauk SSSR (N. S.) 57, (1947). 657–659.

[SW] Mark Sapir, Daniel T. Wise. Ascending HNN extensions of residually finite groups can be non-Hopfian and can have very few finite quotients. J. Pure Appl. Algebra 166 (2002), no. 1-2, 191–202.

[Wat] William C. Waterhouse. Introduction to affine group schemes. Graduate Texts in Mathematics, 66. Springer-Verlag, New York-Berlin, 1979.

[Wer] B.A.F. Wehrfritz. Generalized free products of linear groups. Proc. London Math. Soc. (3) 27 (1973), 402–424.

[Wise] Daniel T. Wise. A residually finite version of Rips's construction. Bull. London Math. Soc. 35 (2003), no. 1, 23–29.

Alexander Borisov   Mark V. Sapir
Department of Mathematics   Department of Mathematics
Penn State University   Vanderbilt University
borisov@math.psu.edu   m.sapir@vanderbilt.edu