International Mathematics Research Notices Advance Access published April 14, 2009

Borisov, A., and M. Sapir. (2009) “Polynomial Maps over $p$-Adics and Residual Properties of Mapping Tori of Group Endomorphisms,”
International Mathematics Research Notices, Article ID rnp040, 14 pages.
doi:10.1093/imrn/rnp040

# Polynomial Maps over $p$-Adics and Residual Properties of Mapping Tori of Group Endomorphisms

**Alexander Borisov[1] and Mark Sapir[2]**

[1]Department of Mathematics, University of Pittsburgh, Pittsburgh, PA 1560, USA and [2]Department of Mathematics, Vanderbilt University, Nashville, TN 37235, USA

*Correspondence to be sent to: borisov@pitt.edu*

We continue our study of residual properties of mapping tori of free group endomorphisms. In this paper, we prove that each of these groups are virtually residually (finite $p$)-groups for all but finitely many primes $p$. The method involves further studies of polynomial maps over finite fields and $p$-adic completions of number fields.

## 1 Introduction

This paper is a continuation of paper [1] where we proved that for every linear finitely generated group $G$ and any injective endomorphism $\phi$ of $G$, the mapping torus of $\phi$ is residually finite. The mapping torus of $\phi$ is the following *ascending* HNN extension of $G$:

$$\mathrm{HNN}_\phi(G) = \langle G, t \mid txt^{-1} = \phi(x)\rangle \text{ where } x \text{ runs over a (finite) generating set of } G.$$

Probably, the most important mapping tori are mapping tori of endomorphisms of free groups $F_k$. These groups appear frequently as fundamental groups of hyperbolic 3-manifolds (in fact there is a conjecture that all fundamental groups of hyperbolic 3-manifolds are virtually mapping tori of free group automorphisms). Also it is proved in [8], that with probability tending to 1 as $n \to \infty$, every 1-related group with three or more generators and relator of length $n$ is embeddable into the mapping torus of a free group endomorphism (and so it is residually finite by [1, Theorem 1.6] and coherent by

Received October 9, 2008; Revised October 9, 2008; Accepted March 5, 2009
Communicated by Prof. Marc Burger

[6]). For 1-related groups with two generators, it is not known whether they are almost surely inside mapping tori of free group endomorphisms, but the computer experiments from [1] and [4] show that the probability of that should be at least 0.94.

A fairly comprehensive survey of our knowledge about mapping tori of free group endomorphisms before [1, 3] is in [7]. The paper [7] ends with several open problems. The first problem asks whether $\mathrm{HNN}_\phi(F_k)$ is residually finite or linear [1] answers positively the first part of the question and [3] answers negatively the second part: it turned out that the group $\langle a, b, t \mid tat^{-1} = a^2, tbt^{-1} = b^2\rangle$ is not linear. After [1] and [3], a natural question arises: do groups $\mathrm{HNN}_\phi(F_k)$ possess stronger residual properties than simple residual finiteness? For example, are they residually finite nilpotent groups, etc.? The answer to that question is "no": consider any endomorphism $\phi$ of $F_k$ that maps $F_k$ into the derived subgroup $[F_k, F_k]$. Then every solvable homomorphic image of $H = \mathrm{HNN}_\phi(F_k)$ is cyclic.

Indeed, let $H = \langle x_1, \dots, x_k, t \mid tx_it^{-1} = \phi(x_i), i = 1, \dots, k\rangle$. Then $\phi(x_i)$ is a product of commutators in $F_k$ for every $i = 1, \dots, k$. Let $H'$ be a noncyclic solvable homomorphic image of $H$. Let $\bar{x}_i$ be the image of $x_i$ and $\bar{t}$ be the image of $t$ in $H'$. Then for every $i$, the element $\bar{t}\bar{x}_i\bar{t}^{-1}$ is a product of commutators in the subgroup $X$ of $H'$ generated by $t^n\bar{x}_1t^{-n}, \dots, t^n\bar{x}_kt^{-n}$, $n \in \mathbb{Z}$. Note that $H'$ is an extension of $X$ by a cyclic group $\langle\bar{t}\rangle$. Hence, $\bar{t}^n\bar{x}_i\bar{t}^{-n}$ is in the derived subgroup of $X$ for every $n, i$. Hence, $X$ coincides with $[X, X]$. Since $X$ is solvable, $X$ must be trivial, and $H'$ must be cyclic, which is a contradiction.

Note that many linear groups (for example, $\mathrm{SL}_n(\mathbb{Z})$ for $n > 2$) are also not residually solvable (by Margulis' normal subgroup theorem), but all finitely generated linear groups are *virtually* residually solvable and even virtually residually (finite $p$)-groups for all but finitely many primes $p$ [9]. That means they have finite index subgroups that are residually (finite $p$)-groups. In this paper, we shall prove that all mapping tori of finitely generated free group endomorphisms also enjoy this property.

**Theorem 1.1.** Every mapping torus of a finitely generated free group endomorphism is virtually residually (finite $p$)-group for every sufficiently large $p$.

We shall illustrate the ideas of the proof by the following example (which was the motivating example for our work).

Let $H = \langle a, b, t \mid tat^{-1} = ab, tbt^{-1} = ba\rangle$. It is not difficult to prove (almost as above) that this group is not residually nilpotent. We shall prove that it has a subgroup of finite index which is residually (finite 5)-group. Consider two matrices $A = \binom{5\ 2}{2\ 1}$, $B = \binom{1\ 2}{2\ 5}$. These two matrices generate a free subgroup of $\mathrm{SL}_2(\mathbb{Z})$ (which can be easily proved either by noticing that it is a subgroup of Sanov's free subgroup of $PSL_2(\mathbb{Z})$, or by just looking at the subgroup generated by the corresponding Frobenius transformations and using the ping-pong argument). For every group $G$, consider the map $\phi_G\colon G \times G \to G \times G$ given by $\phi(U, V) = (UV, VU)$. It is easy to check that if $G_1 = \mathrm{SL}_2(\mathbb{Z}/5\mathbb{Z})$, then the pair $(A \bmod 5, B \bmod 5)$ is a periodic point for $\phi_{G_1}$ with period 6. Replacing 5 by $5^2 = 25$, and considering the group $G_2 = \mathrm{SL}_2(\mathbb{Z}/25\mathbb{Z})$, one can compute that $(A \bmod 25, B \bmod 25)$ is a periodic point of $\phi_{G_2}$ with period $5 \times 6 = 30$. By induction or by using Theorem 2.12 below, one can prove that for $G_n = \mathrm{SL}_2(Z/5^n\mathbb{Z})$, the pair $(A \bmod 5^n, B \bmod 5^n)$ is a periodic point for $\phi_{G_n}$ with period $q_n = 6 \times 5^{n-1}$. It is observed in [1, Lemma 2.2], that $\mathrm{HNN}_\phi(F_k)$ has homomorphisms $\nu_n$ into the wreath product $G_n \wr \mathbb{Z}/q_n\mathbb{Z}$ which is the semidirect product of $G_n^{q_n}$ and the cyclic group $\mathbb{Z}/q_n\mathbb{Z}$ where the cyclic group acts on the direct power by the cyclic shift. The homomorphism $\nu_m$ takes $t$ to the generator $t_n$ of $\mathbb{Z}/q_n\mathbb{Z}$, $a$ maps to $a_n = (A \bmod 5^n, \phi_{\mathrm{G_n}}(\mathrm{A} \bmod 5^n), \dots, \phi_{G_n}^{q_n-1}(\mathrm{A} \bmod 5^n))$, and $b$ maps to $b_n = (B \bmod 5^n, \phi_{G_n}(\mathrm{B} \bmod 5^n), \dots, \phi_{\mathrm{G_n}}^{q_{n-1}}(B \bmod 5^n))$. There exists a natural homomorphism $\mu_n\colon G_n \to G_1$. The image $\langle a_n, b_n\rangle$ of $F_2 = \langle a, b\rangle$ under $\nu_n\mu_n$ is inside the direct power $G_1^{q_n}$; hence, $\nu_n\mu_n(F_2)$ is a 2-generated group in the variety of groups generated by the finite group $G_1$. (The creators of the theory of varieties of groups (G. Birkhoff mostly) did not anticipate in the 1930s the situation when the word "variety" would be used in the same paper in two different senses: as an algebraic variety and as a variety of algebraic systems, i.e., a class of algebraic systems closed undertaking cartesian products, subsystems, and homomorphic images. This is one of the very few papers (if not the only paper) where the term is used in both senses.) It is well known that $\nu_n\mu_n(F_2)$ has order bounded by some constant $M$. Then the centralizer of $\mu_n\nu_n(F_k)$ in $\mu_n\nu_n(H)$ has index at most $M_1 = M^M$ in $\mu_n\nu_n(H)$. Since $\mathbb{Z}/q_n\mathbb{Z}$ has a 5-subgroup of index 6, $\mu_n\nu_n(H)$ has a 5-subgroup of index at most some constant $M_2$ (independent of $n$). Since by [1, Lemma 2.2], all elements of the group $H$ are separated by homomorphisms $\nu_n$, $H$ has a subgroup of index at most $M_2$ which is residually (finite 5)-group.

One can follow the proof of Theorem 1.1 below (see Section 3) in order to show that $H$ is virtually residually (finite $p$)-group for almost all $p \neq 5$. The differences with the proof above are the following:

- a pair of matrices $(A, B)$ such that $(A \bmod p, B \bmod p)$ is periodic for $\phi_{G_1}$ is found not in $G_1 = \mathrm{SL}_2(\mathbb{Z}/5\mathbb{Z})$, but in $G_1 = \mathrm{SL}_2(\mathcal{O}/p\mathcal{O})$ where $\mathcal{O}$ is the ring of integers of some finite extension of $\mathbb{Q}$ unramified at $p$ (we use the main algebro-geometric result [1, Theorem 3.2] for this); and
- in order to find such a pair of matrices with the additional property that $(A, B)$ generate a free subgroup, we use a strong result of Breuillard and

Gelander [2] about dense free subgroups of Lie groups; the matrices $A, B$ are found not in $\mathrm{SL}_2(\mathcal{O})$ but in the $p$-adic completion of that group. Here we use a new result about polynomial maps over $p$-adics proved in Section 2 (see Theorem 2.12).

## 2 Polynomial Maps over $p$-Adics

For a prime power $q = p^k$, denote by $\mathbb{F}_q$ the field of $q$ elements. Denote by $\mathbb{F}_q^{\mathrm{alg}}$ its algebraic closure ($\mathbb{F}_q^{\mathrm{alg}} = \mathbb{F}_p^{\mathrm{alg}}$).

An affine algebraic variety over $\mathbb{F}_q^{\mathrm{alg}}$ is a subset of $(\mathbb{F}_q^{\mathrm{alg}})^n$ consisting of all common roots of some ideal $I \subset \mathbb{F}_q^{\mathrm{alg}}[x_1, \dots, x_n]$. By Hilbert's Nullstellensatz, we can assume that $I$ is radical: for every $f \in \mathbb{F}_q^{\mathrm{alg}}[x_1, \dots, x_n]$ and $N \in \mathbb{N}$, if $f^N \in I$ then $f \in I$.

If $X$ is an affine algebraic variety over $\mathbb{F}_q^{\mathrm{alg}}$, its field of definition is the smallest subfield of $\mathbb{F}_q^{\mathrm{alg}}$ containing all coefficients of some set of generators of $I$. An affine algebraic variety over $\mathbb{F}_q$ is a variety with the field of definition $\mathbb{F}_q$ or its proper subfield. Equivalently, $X$ is defined over $\mathbb{F}_{p^k}$ if and only if $\mathrm{Fr}^k(X) = X$, where Fr is the geometric Frobenius self-map of the affine space: $\mathrm{Fr}(x_1, x_2, \dots, x_n) = (x_1^p, x_2^p, \dots, x_n^p)$.

Note that in algebraic geometry one usually wants to understand the structure of $X$ independent of its embedding into the affine space, as the affine scheme associated to the ring $\mathbb{F}_q[x_1, \dots, x_n]/I$. However, all varieties in this paper naturally appear as subvarieties of the fixed affine space. We will not be dealing with scheme points of $X$, but rather with its geometric points, which are just the points $(x_1, x_2, \dots, x_n)$ of the affine $n$-space over $\mathbb{F}_q^{\mathrm{alg}}$, contained in $X$ (or, more precisely, its base change to $\mathbb{F}_q^{\mathrm{alg}}$.

Let, as usual, $\mathbb{Z}_p, \mathbb{Q}_p$ be the $p$-adic completion of the ring of integers and rational numbers, respectively. For $q = p^k$, let $\mathbb{Q}_q$ be the unrafimied extension of $Q_p$ such that the residue field $Z_q/pZ_q$ of its ring of integers $Z_q$ is isomorphic to $\mathbb{F}_q$ (see, e.g. [10, p. 143, Example 4.18]). Let $\mathrm{A}^n$ be the affine space over $\mathbb{Z}$ of dimension $n$, that is $\mathrm{Spec}\mathbb{Z}[x_1, \dots, x_n]$.

**Definition 2.1.** The following are standard terms in algebraic geometry, adapted for our purposes:

- An algebraic variety is called *geometrically irreducible* if its base change to the variety over the algebraic closure of the ground field is irreducible. This means that the ring $\mathbb{F}_q^{\mathrm{alg}}[x_1, \dots, x_n]/I$ is a domain.
- For a variety $X$ as above, a polynomial self-map $\Phi$ of $X$ is a polynomial self-map of an ambient affine space that preserves $X$. In coordinates, $\Phi$ is given

by polynomials

$$\Phi(x_1, x_2, \dots, x_n) = (f_1(x_1, \dots, x_n), f_2(x_1, \dots, x_n), \dots, f_n(x_1, \dots, x_n)).$$

The field of definition of $\Phi$ is the subfield of $\mathbb{F}_q^{\mathrm{alg}}$, generated by the coefficients of $f_i$. $\Phi$ preserves $X$ when for every $g \in \mathbb{F}_q^{\mathrm{alg}}[x_1, \dots, x_n]$ that belongs to $I$, the formal composition $g \circ \Phi$ also belongs to $I$ (I is assumed to be radical). We will only consider the polynomial self-maps.

The self-map $\Phi$ is called *dominant* if its image (over $\mathbb{F}_q^{\mathrm{alg}}$) is Zariski dense in $V$.

- A dominant self-map $\Phi$ is called *separable* if the corresponding extension of the fields of rational function is separable.
- Zariski tangent space at a point $(x_1, x_2, \dots, x_n) \in X$, defined over $\mathbb{F}_Q$, is the $\mathbb{F}_Q$-vector space, dual to the space $m/m^2$, where $m$ is the ideal in $\mathbb{F}_Q[x_1.x_2, \dots, x_n]$, consisting of polynomials that vanish on $(x_1, x_2, \dots, x_n)$.
- A self-map $\Phi\colon V(\mathbb{F}_q) \to V(\mathbb{F}_q)$ is called *unramified* at a point $x \in V$ if the map $\Phi_*$ on Zariski tangent space of $x$ is invertible. (Note that a separable dominant self-map is unramified at all $x$ in some Zariski open subset of $V$.)
- A geometric point $x$ of an algebraic variety $V$ is called *smooth* if the local ring is regular. Alternatively, the point is smooth if the Zariski tangent space at it has the same dimension as the variety.
- The *degree* of $\Phi$ is the number of geometric points in the preimage of a generic point of $V$.

The following statement is proved in [1].

**Lemma 2.2** ([1], p. 349)**.** Suppose that $\Phi\colon \mathrm{A}^n \to \mathrm{A}^n$ is a polynomial map defined over any algebraically closed field. Denote by $V$ the Zariski closure of $\Phi^n(\mathrm{A}^n)$. Then $V$ is geometrically irreducible and the map $\Phi|_V\colon V \to V$ is dominant.

Suppose now that we have a polynomial map $\Phi$ from $\mathrm{A}^n$ to itself, defined over $\mathbb{Z}$. Applying the above lemma to the map over $\mathbb{Q}^{\mathrm{alg}}$, we get some subvariety $V$ of $\mathrm{A}^n$. Even though it is a priori defined only over $\mathbb{Q}^{\mathrm{alg}}$, its field of definition is $\mathbb{Q}$, because it is fixed by the absolute Galois group of $\mathbb{Q}$. Reducing $\Phi$ modulo $p$, we get a polynomial self-map of $\mathrm{A}^n$ over $\mathbb{F}_p$, and thus over $\mathbb{F}_p^{\mathrm{alg}}$, the algebraic closure of $\mathbb{F}_p$. This in turn produces a subvariety $V_p$ of $\mathrm{A}^n(\mathbb{F}_p^{\mathrm{alg}})$. Naturally, we would like to relate $V_p$ to $V$ for large enough $p$. In order to do this, we need to construct a model of $V$, that is a scheme over Spec$\mathbb{Z}$, such that

$V(\mathbb{Q})$ is its generic fiber. Fortunately, a natural model exists in our situation. To describe it, let us consider $V$, and $V_p$, from a commutative algebra perspective.

Suppose $\Phi = (\Phi_1, \Phi_2, \dots, \Phi_n)$ is an ordered set of polynomials in $\mathbb{Z}[x_1, x_2, \dots, x_n]$, and the varieties $V$ and $V_p$ are defined as above. Abusing the notation a little bit, denote by $\Phi^*$ the corresponding ring homomorphism, for $n$-variable polynomials over any ring. Then the prime ideal $I(V)$ of $\mathbb{Q}^{\mathrm{alg}}[x_1, x_2, \dots, x_n]$, defining $V$, consists of polynomials $f \in \mathbb{Q}^{\mathrm{alg}}[x_1, x_2, \dots, x_n]$ such that $f(\Phi^n) = 0$, where $\Phi^n$ is the $n$th composition power of $\Phi$. This is, in other words, the pullback of the prime ideal $\{0\}$ of $\mathbb{Q}^{\mathrm{alg}}[x_1, x_2, \dots, x_n]$ by the homomorphism $(\Phi^n)^* = (\Phi^*)^n$. As a pullback of a prime ideal, it is also prime, in particular radical. Similarly, the ideal $I(V_p)$ of $V_p$ in $\mathbb{F}_p{}^{\mathrm{alg}}[x_1, x_2, \dots, x_n]$ consists of polynomials $f \in \mathbb{F}_p{}^{\mathrm{alg}}[x_1, x_2, \dots, x_n]$ that $f((\Phi_p)^n) = 0$, where $\Phi_p$ is the reduction of $\Phi$ modulo $p$.

Now we define a model of $V$ as an affine scheme over $\mathbb{Z}$, which is a subscheme of $\mathrm{Spec}\mathbb{Z}^n$ defined by the ideal $I(V(\mathbb{Z})) \in \mathbb{Z}[x_1, x_2, \dots, x_n]$, consisting of all $f$ that $f(\Phi^n) = 0$ in $I \in \mathbb{Z}[x_1, x_2, \dots, x_n]$.

**Lemma 2.3.** The ideal $I(V(\mathbb{Z}))$ is prime. It is finitely generated and its generators when considered over $\mathbb{Q}^{\mathrm{alg}}$ generate the ideal $I(V)$.

**Proof.** The ideal $I(V(\mathbb{Z}))$ is prime because it is a pullback of the prime ideal $\{0\}$, like in the argument above. It is finitely generated because the ring $\mathbb{Z}[x_1, x_2, \dots, x_n]$ is Noetherian. For the last statement, it is obvious that all elements of $I(V(\mathbb{Z}))$ belong to $I(V)$. Suppose $f$ is any element of $I(V) \subset \mathbb{Q}^{\mathrm{alg}}[x_1, \dots, x_n]$. Because all coefficients of $\Phi$ are integers, all conjugates of $f$ also belong to $I(V) \subset \mathbb{Q}^{\mathrm{alg}}[x_1, \dots, x_n]$. Consider a $\mathbb{Q}^{\mathrm{alg}}$-vector subspace of a space of $n$-variable polynomials of large enough degree, generated by all these conjugates of $f$. This subspace is invariant under the natural action of the absolute Galois group of $\mathbb{Q}$, thus it has a basis consisting of polynomials with rational coefficients. For every element in this basis, some nonzero integer multiple of it belongs to $\mathbb{Z}^{\mathrm{alg}}[x_1, x_2, \dots, x_n]$. It is obvious that it must belong to $I(V(\mathbb{Z}))$, which implies that $f$ is a linear combination with algebraic coefficients of elements from $I(V(\mathbb{Z}))$.

We would like to say that for all $p$ the reductions of the generators of $I(V(\mathbb{Z}))$ modulo $p$ generate the ideal $I(V(\mathbb{Z}/p\mathbb{Z}))$, but this is in general not true, as the following example shows.

**Example.** Suppose $n = 2$, denote the coordinates by $x$ and $y$. Suppose $\Phi(x, y) = (x, 5y)$. Then $\Phi^2(x, y) = (x, 25y)$. In characteristic zero this is an invertible linear map, so the ideal $I(V(\mathbb{Z}))$ is zero. However, as modulo $p = 5$, this map is not invertible and $I(V(\mathbb{Z}/p\mathbb{Z}))$ is the principal ideal, generated by the polynomial $x$.

The following theorem is very important. It shows that for all sufficiently large primes $p$ the reductions of the generators of $I(V(\mathbb{Z}))$ modulo $p$ generate the ideal $I(V(\mathbb{Z}/p\mathbb{Z}))$.

**Theorem 2.4.** Suppose $\Phi \in (\mathbb{Z}[x_1, \dots, x_n])^n$ is a polynomial automorphism in $n$ variable with integer coefficients. Define $I(V(\mathbb{Z}))$ and $I(V(\mathbb{Z}/p\mathbb{Z}))$ are as above. Then there exists some natural number $B$, such that for all $p > B$ the reductions of the generators of $I(V(\mathbb{Z}))$ modulo $p$ do generate the ideal $I(V(\mathbb{Z}/p\mathbb{Z}))$.

**Proof.** For every $p$ we have the inclusion of the ideals in $\mathbb{F}_p[x_1, x_2, \dots, x_n]$: $I(V(\mathbb{F}_p))$ contains the reduction modulo $p$ of the ideal $I(V(\mathbb{Z}))$, to be denoted by $I_p$. By a very general result on fibers of algebraic morphisms of schemes (see [5], Theorem 14.8), all irreducible components of Spec$(\mathbb{F}_p[x_1, \dots, x_n]/I_p)$ have the dimension equal to the dimension of $\mathbb{Q}[x_1, \dots, x_n]/I(V(Q))$. Because $I(V(\mathbb{F}_p))$ is prime, it is enough to show that the dimension of Spec$\mathbb{F}_p[x_1, \dots, x_n]/I(V(\mathbb{F}_p))$ is also the same for all sufficiently large $p$. The key idea of this argument is the following construction.

Suppose $\mathbb{F}$ is any field, and $M$ is a polynomial self-map of the affine space Spec$\mathbb{F}[x_1, x_2, \dots, x_n]$. The map $M$ is given in coordinates by its components $M_i$, which are polynomials in $\mathbb{F}[x_1, x_2, \dots, x_n]$. Consider its formal Jacobian matrix. $J = (\frac{\partial M_i}{\partial x_j})_{i,j=1,\dots n}$. The entries are in $\mathbb{F}[x_1, x_2, \dots, x_n]$, so the matrix is well defined as an $n \times n$ matrix $T$ over the field $\mathbb{F}(x_1, \dots, x_n)$. We define the ideal $I$ in $\mathbb{F}[x_1, \dots, x_n]$ as a pullback of the zero ideal by $M$.

**Lemma 2.5.** In the above notation, if the map $M$ is separable, then the dimension of Spec$\mathbb{F}[x_1, \dots, x_n]/I$ equals the rank of the matrix $T$.

**Proof.** This is (the algebraic version of) the classical inverse function theorem, see e.g. [5], Chapter 16 for the reference. ■

We now apply the above lemma to $M = \Phi^n$ for various fields $\mathbb{F}$. For $\mathbb{F} = \mathbb{Q}$ the rank of $T$ is the dimension of $V(\mathbb{Q})$, let us denote it by $r$. The entries of $T$ over $\mathbb{Q}$ are actually polynomials with integer coefficients. For some $r \times r$ minor of $T$ the determinant is a nonzero polynomial with integer coefficients. For all sufficiently large primes $p$, its reduction modulo $p$ is also nonzero. So for these $p$, the rank of the Jacobian matrix for $\mathbb{F} = \mathbb{F}_p$ is at least $r$. Thus, the dimension of Spec$\mathbb{F}_p[x_1, \dots, x_n]/I(V(\mathbb{F}_p))$ is at least $r$. On the other hand, any $(r+1)$ rows of $T$ over $\mathbb{Q}$ are linearly dependent over $\mathbb{Q}(x_1, \dots, x_n)$. Multiplying by a suitable polynomial in $\mathbb{Z}[x_1, \dots, x_n]$, we get nontrivial linear combination of rows of $T$ with coefficients in $\mathbb{Z}[x_1,\dots,x_n]$ that equals to zero. Since $T$ for $\mathbb{F}=\mathbb{F}_p$ is just the reduction of $T$ for $\mathbb{Z}$ modulo $p$, for all sufficiently large $p$ all of these linear combinations are still nontrivial. So the rank of $T$ is exactly $r$ for all sufficiently large $p$. For such $p$, we have Spec$I_p$, a possibly reducible subvariety of an irreducible variety $V(\mathbb{F}_p)$, and every component of Spec$I_p$ has the same dimension $r$ as $V(\mathbb{F}_p)$. This implies that the varieties are the same, so the ideals $I(V(p))$ and $I_p$ are equal, for any sufficiently large $p$. ■

From now on, the prime $p$ will always be sufficiently large so that the conclusion of Theorem 2.4 holds. Let us denote by $\pi_p$ (or just $\pi$,) when $p$ is the reduction map from $\mathbb{Z}$ to $\mathbb{Z}/p\mathbb{Z}$ and, abusing the notation a bit, all other reduction modulo $p$ maps. Recall, that for any $q=p^k$ we denoted by $\mathbb{Z}_q$ the unramified extension of the $p$-adic integers $\mathbb{Z}_p$ with the residue field $\mathbb{F}_q$. With the above convention, we will denote by $\pi_p$ the reduction map from $\mathbb{Z}_q$ to $\mathbb{F}_q$, as well as the reduction map from $\mathbb{Z}_q[x_1,\dots,x_n]$ to $\mathbb{F}_q[x_1,\dots,x_n]$.

In what follows, unless otherwise specified, we will denote by upper case letters objects in characteristic zero, and by corresponding lower case letters the objects in characteristic $p$. For example, if $T\in\mathbb{Z}_q[x_1,\dots,x_n]$, then $t\in\mathbb{F}_q[x_1,\dots,x_n]$ is its reduction modulo $p: t=\pi_p(T)$.

**Lemma 2.6.** For $p$ as above, for any $q=p^k$ define $I(V(\mathbb{Z}_q))\subset\mathbb{Z}_q[x_1,\dots,x_n]$ and $I(V(\mathbb{F}_q))\subset\mathbb{F}_q[x_1,\dots,x_n]$ as before. Then

$$I(V(\mathbb{F}_q))=\pi_p(I(V(\mathbb{Z}_q))).$$

**Proof.** We need to prove two inclusions, one of which is easy. Indeed, if $g=\pi_p(G)$, $G\in I(V(\mathbb{Z}_q))$, then $G(\Phi^n)=0$, so $G(\Phi^n)=0 \bmod p$, so $g\in I(V(\mathbb{F}_q))$.

Now we would like to prove that if $g\in I(V(\mathbb{F}_q))$, there exists $G\in I(V(\mathbb{Z}_q))$ such that $g=\pi_p(G)$. Choose a set of generators $\{G_1,G_2,\dots,G_m\}$ of the ideal $I(V(\mathbb{Z}))$, as the ideal in $\mathbb{Z}[x_1,\dots,x_n]$. By assumption, $g_i=\pi_p(G_i)$ generate $I(V(\mathbb{F}_p))$ as the ideal in $\mathbb{F}_p[x_1,\dots,x_n]$. By the same argument as in the Lemma 2.3, this implies that they generate $I(V(\mathbb{F}_q))$ in $\mathbb{F}_q[x_1,\dots,x_n]$.

So, modulo $p$, $\pi_p(G)=\sum\limits_{(\alpha,\beta)} c_{(\alpha,\beta)}g_1^{\alpha_1}\cdot\dots\cdot g_m^{\alpha_m}\cdot x_1^{\beta_1}\cdot\dots\cdot x_n^{\beta_n}$, where $\alpha$ and $\beta$ are multi-indices. Lifting $c_{(\alpha,\beta)}$ to $C_{(\alpha,\beta)}$, we get

$$G=\sum_{(\alpha,\beta)} C_{(\alpha,\beta)}G_1^{\alpha_1}\cdot\dots\cdot G_m^{\alpha_m}\cdot x_1^{\beta_1}\cdot\dots\cdot x_n^{\beta_n}+p\cdot G_1,$$

for some $G_1\in\mathbb{Z}_q[x_1,\dots,x_n]$.

Clearly, $G_1(\Phi^n) = 0$, so $G_1 \in Z_q[x_1, \dots, x_n]$. Repeating the above procedure, we get $G_1$ as a linear combination of $g_1^\alpha x^\beta$ plus $pG_2$, and so on. Combining all these together and using the completeness of $\mathbb{Z}_q$ in $p$-adic topology, we prove the lemma. ■

From [1, Theorem 3.2], for some $q = p^\tau$ there is a point $x = (x_1, \dots, x_n) \in V(\mathbb{F}_q^n)$ such that $\Phi(x) = x^Q$ for some $Q = p^l$. Additionally, we can choose $x$ to lie outside of any fixed Zariski closed subset. So we choose $x$ to be a smooth point of $V$, where the restriction of the tangent map $\Phi_*$ to the Zariski tangent space $T_xV$ is injective. This implies that $\Phi_*|_{T_{x^Q}(V)}, \Phi_*|_{T_{x^{Q^2}}(V)}, \dots$ are all injective. Suppose $N \in \mathbb{N}$ is such that $\Phi^N(x) = x$. Then $\Phi_*^N|_{T_x(V)}$ is injective as a composition of injective linear operators. So it is invertible.

By our choice of notation, $T_x(V)$ is a vector space over $\mathbb{F}_p^{\mathrm{alg}}$. But it has an $\mathbb{F}_q$-basis, because $x$ is defined over $\mathbb{F}_q$ and $V$ is defined over $\mathbb{F}_p$. In this basis, the matrix of $\Phi^N$ has coefficients in the finite field $\mathbb{F}_q$. It is invertible, so some power of it, $\Phi_*^M$ is identity.

By Theorem 2.4, there exists a point $X \in V(\mathbb{Z}_q)$ such that $\pi(X) = x$. By definition of $M$, $\Phi^M(X) \equiv X \bmod p$.

The following general observation is very important.

**Lemma 2.7.** Suppose $P = P(x_1, x_2, \dots, x_n) \in \mathbb{Z}_q[x_1, \dots, x_n]$. Suppose $A = (A_1, \dots, A_n) \in \mathbb{Z}_q^n$. Suppose $l \in \mathbb{N}$. Denote by $\nabla P(A)$ the formal gradient of $P$, evaluated at $A$. Then for every $Y = (Y_1, \dots, Y_n) \in \mathbb{Z}_q^n$, we have the following:

$$P(A + Y \cdot p^l) \equiv P(A) + (\nabla P(A) \cdot Y)p^l \bmod p^{l+1}.$$

**Proof.** We rewrite the polynomial $P$ as a linear combination of products of powers of $(x_i - A_i)$. When evaluated at $A + Y \cdot p^l$, the terms of degree at least two are zero modulo $p^{2l}$, so are zero modulo $p^{l+1}$. The linear term is exactly the dot product of the gradient and $Y \cdot p^l$. ■

An immediate corollary is the following.

**Lemma 2.8.** Suppose $\Omega$ is an $n$-variable polynomial automorphism, with coefficients from $\mathbb{Z}_q$, and $X \in \mathbb{Z}_q^n$ is a point such that $\omega(x) = x$, where $x = \pi(X)$ and $\omega$ is a reduction of $\Omega$ modulo $p$. Denote the induced map on the tangent space at $x$ by $\omega_*$. Then for any $Y \in Z_q^n$ with $y = \pi(Y)$, we have

$$\Omega(X + p^l Y) = \Omega + p^l \cdot \omega_*(y) \bmod p^{l+1}.$$

(Note that $\omega_*(y)$ is only defined modulo $p$, but its product with $p^l$ makes sense modulo $p^{l+1}$.)

**Proof.** Apply the previous lemma to each component of $\Omega$, with $A = X$. ■

Now we go back to our map $\Phi$ that fixes the subvariety $V$. By the choice of $M$ and $X$, $\Phi^M(X) \equiv X \bmod p$. Also, $\phi_*^M$ restricted to the tangent space of $V(\mathbb{F}_q)$ at $x$ is the identity. Denote by $\alpha^{(1)} \in \mathbb{F}_q^n$ the divided difference $\frac{\Phi^M(X)-X}{p} (\bmod p)$.

**Lemma 2.9.** For any $X' \equiv X \bmod p$ with $X' \in V(\mathbb{Z}_q)$,

$$\Phi^M(X') \equiv X' + \alpha^{(1)} \cdot p \bmod p^2.$$

**Proof.** First of all, $X' = X + pY$ for some $Y$. We are going to show that $\pi(Y) \in T_*(V)(x)$. This is equivalent to showing that any polynomial in $\mathbb{F}_q[x_1, \dots, x_n]$ that vanishes on $V$ has its gradient, evaluated at $x$, vanishing at $\pi(y)$. Suppose $g$ is such a polynomial. By Lemma 2.6 there exists $G \in I(V(\mathbb{Z}_q))$ such that $g = \pi(G)$. By Lemma 2.7,

$$G(X') = G(X + pY) \equiv G(X) + p(\nabla G)(X) \cdot Y \bmod p^2.$$

Since $G(X') = G(X) = 0$, this implies that $\nabla G(X) \cdot Y \equiv 0 \bmod p$, so $\nabla g(x) \cdot y = 0$ in $\mathbb{F}_q$.

Now we apply Lemma 2.8. to the map $\Omega = \Phi^M$.

$$\Phi^M(X') \equiv \Phi^M(X) + p\Phi_*^M(X)(Y) \equiv (X + p\alpha^{(1)}) + pY \equiv X' + \alpha^{(1)} \cdot p \bmod p^2.$$ ■

As an immediate corollary, we have the following.

**Lemma 2.10.** For any $X' \equiv X$ mod p with $X' \in V(\mathbb{Z}_q)$,

$$\Phi^{pM}(X') \equiv X' \bmod p^2.$$

**Proof.** We know that $\Phi^M$ fixes $V$. So, by induction, for all natural $j$

$$\Phi^{jM}(X') \equiv X' + \alpha^{(1)} \cdot p \cdot j \bmod p^2.$$ ■

Now we denote by $\alpha^{(2)} \in \mathbb{F}_q^n$ the divided difference $\frac{\Phi^{pM}(X)-X}{p^2}(\bmod\ p)$. We have the following lemma.

**Lemma 2.11.** For any $X' \equiv X \ mod\ p^2$ with $X' \in V(\mathbb{Z}_q)$,

$$\Phi^{pM}(X') \equiv X' + \alpha^{(2)} \cdot p^2 \bmod p^3.$$

**Proof.** The proof is analogous to that of Lemma 9, using Lemmas 2.7 and 2.8. The details are left to the reader. ■

As a corollary of Lemma 2.11, we get that $\Phi^{p^2M}(X') \equiv X' \bmod p^3$, and so on. Putting it all together, we get the following theorem.

**Theorem 2.12.** Suppose $\Phi$ is an $n$-variable polynomial map with integer coefficients, and $V$ is the Zariski closure of the image of $\Phi^n$ (over $\mathbb{Z}$). Suppose $W$ is a proper subscheme of $V$. Then for every sufficiently large prime $p$ there exist $q = p^l$ and a point $x \in V(\mathbb{F}_q) \setminus W(\mathbb{F}_q)$ such that for every $X \in V(\mathbb{Z}_q)$ with $\pi(X) = x$ we have

$$\Phi^{ap^{(k-1)}} - 1 \equiv X(\bmod p^k),$$

where $a$ is fixed and $k$ is arbitrary.

In particular, the point $X$ is uniformly recurrent for $\Phi$ in the $p$-adic topology on $V(\mathbb{Z}_q)$.

## 3 Residually Finite Groups

In this section, we shall prove the following theorem.

**Theorem 3.1.** Let $\phi$ be any injective endomorphism of a free group $F_k$. Then for every sufficiently large prime $p$, the HNN extension $\mathrm{HNN}_\phi(F_k)$ has a subgroup of finite index that is residually (finite $p$-group) and also is an ascending HNN-extension of a free group.

**Proof.** Let $F_k = \langle x_1, \ldots, x_k \rangle$. The endomorphism $\phi$ is defined by $k$ words

$$w_1(x_1, \ldots, x_k), \ldots, w_k(x_1, \ldots, x_k),$$

the images of $x_1, \ldots, x_k$. For every finite group $G$, consider the map $\phi_G \colon G^k \to G^k$ defined as follows:

$$(g_1, \ldots, g_k) \to (w_1(g_1, \ldots, g_k), \ldots, w_k(g_1, \ldots, g_k)).$$

Let $H = \mathrm{HNN}_\phi(F_k)$.

Suppose that a point $(g_1, \ldots, g_k) \in G^k$ is periodic with respect to the map $\phi_G$ and $l$ is the length of the period. Consider the wreath product $P$ of $G$ and the cyclic group $C_l = \langle c \rangle$ of order $l$, i.e. $P$ is the semidirect product of $G^l$ and $C_l$ where the elements of $C_l$ cyclically permute the factors of $G^l$. Let $t$ be the free letter of $\mathrm{HNN}_\phi(F_k)$. It was observed in [1, p. 346] that the map

$$t \to c, \quad x_i \to \left(g_i, \phi_G(g_i), \phi_G^2(g_i), \ldots, \phi_G^{l-1}(g_i)\right) \tag{3.1}$$

extends to a homomorphism from $H$ into $P$.

Consider the ring of $2 \times 2$-matrices $M = M(2, \bar{\mathbb{F}}_p)$ over the algebraic closure of $\mathbb{F}_p$ as a copy of the affine space of dimension 4. Replacing the inverses $x^{-1}$ in the words $w_i$ by symbols $\mathrm{adj}(x)$ interpreted as the adjoint matrix, we turn $\phi_M$ into a polynomial map $\bar{\phi} \colon M^k \to M^k$. Assume that $p$ is large enough (as in Theorem 2.12). Choose a point $x = (x_1, \ldots, x_k)$ as in Theorem 2.12 (here $x_k$ are $2 \times 2$ matrices). It belongs to the Zariski closure of $\phi^{4k}(M^k)$, over some extension $\mathbb{F}_q$ of $\mathbb{F}_p$, and all matrices $x_i$ are invertible. Adjoining to $F_q$ the square roots of the determinants of $x_i$, we can write each $x_i$ as $a_i \cdot u_i$, where $a_i \in F_q$ and $u_i \in \mathrm{SL}(2, F_q)$. Clearly, the point $u = (u_1, \ldots, u_k)$ satisfies the same properties with respect to the map $\bar{\phi}$ as the point $x$. Note that on the orbit of $u$, the map $\bar{\phi}$ coincides with the map $\phi_{\mathrm{SL}(2,F_q)}$.

Consider an unramified at $p$ finite extension $K$ of $\mathbb{Q}$ with the ring of integers $\mathcal{O}$ and a maximal ideal $(p)$ of $\mathcal{O}$ with the quotient field $\mathbb{F}_q$. Let, as before, $\mathbb{Z}_q$ be the $p$-adic completion of $\mathcal{O}$. Then the group $\mathrm{SL}(2, \mathcal{O})$ naturally embeds into $\mathrm{SL}(2, \mathbb{Z}_q)$. By [2, Theorem 4.3], there exists a free nonabelian subgroup $\Gamma$ in $\mathrm{SL}(2, \mathcal{O})$ that is dense in the profinite topology induced by the congruence subgroups of $\mathrm{SL}(2, \mathcal{O})$ modulo $p^k$, $k \geq 0$. Hence, the homomorphism $\mu \colon \mathrm{SL}(2, \mathcal{O}) \to \mathrm{SL}(2, \mathcal{O}/(p))$ is surjective on $\Gamma$. Again by [2, Theorem 4.3] (see also [2, Corollary 4.4]), there exist preimages $\bar{u}_1, \ldots, \bar{u}_k$ of $u_1, \ldots, u_k$ that freely generate a free subgroup $F$ of $\mathrm{SL}(2, \mathcal{O})$ which we shall identify with $F_k$. Consider the $p$-adic variety $V(\mathbb{Z}_q)$. It contains the subset $\phi_F^m(F)$ for all $m \geq 4k$. Since the point $(u_1, \ldots, u_k)$ is periodic, the point $u = \phi_H^m(\bar{u}_1, \ldots, \bar{u}_k)$ for a divisible enough $m$ also is a preimage of $(u_1, \ldots, u_k)$ under $\mu$. The coordinates of $u$ also freely generate a free subgroup since $\phi$ is injective. Hence, we can assume that $(\bar{u}_1, \ldots, \bar{u}_k)$ belongs to $V(\mathbb{Z}_q)$.

Consider the sequence of congruence subgroups of $F$ corresponding to powers of $p$:

$$F > F^{(1)} > F^{(2)} > \cdots > \cdots .$$

The intersection $\cap F^{(i)}$ is $\{1\}$ and factor-groups $F^{(i)}/F^{(i+1)}$ are $p$-groups for every $i \geq 1$. Let $\gamma_i$ be the natural homomorphisms of $F$ onto $\Gamma_i = F/F_i$. By Theorem 2.12, for every $i \geq 1$, the point $(\gamma_i(\bar{u}_1), \ldots, \gamma_i(\bar{u}_k))$ in $\Gamma_i^k$ is periodic with respect to $\phi_{\Gamma_i}$ with period $l_i = ap^{i-1}$ for some integer constant $a$ (the length of the period of the point $(u_1, \ldots, u_k)$ from $\Gamma_1^k$).

For every $i$ let $C_{l_i}$ be the cyclic group of order $l_i$. Consider the homomorphism $\nu_i$ from $H$ into the wreath product $P_i = \Gamma_i \wr C_{l_i}$ defined as in (3.1). These homomorphisms separate all elements of $\mathrm{HNN}_\phi(F_k)$. Indeed, every nonidentity element in $\mathrm{HNN}_\phi(F_k)$ can be represented as $t^n w t^{n'}$ for some $n, n' \in \mathbb{Z}$ and some word $w \in F_k$ where either $w \neq 1$ or $n + n' \neq 0$. If $w \notin H_i$ for some $i$, then this element is not in the kernel of $\nu_i$. If $w = 1$ and $n + n' \neq 0$, then it is not in the kernel of any $\nu_i$ with $i > |n + n'|$.

For every $i \geq 1$, consider the natural homomorphism $\mu_i$ from $\Gamma_i^{l_i}$ to $\Gamma_1^{l_i}$. Note that $\mu_i \nu_i(F)$ is a $k$-generated subgroup of the direct power of $\Gamma_1$, and that the kernel $K_i$ of $\nu_i$ is a $p$-group. Hence, $\mu_i \nu_i(F)$ belongs to the variety of groups generated by the finite group $\Gamma_1$. Since a variety generated by a finite group is locally finite [11], there exists a constant $M$ such that $|\mu_i \nu_i(F)| \leq M$ for every $i$. The subgroup $K_i$ is normal in $P_i$, so $K_i \cap \nu_i(F)$ is normal in $\nu_i(H)$. The group $\nu_i(H)/(K_i \cap \nu_i(F)$ is an extension of a group $E_i$ of order at most $M$ by a cyclic group of order $l_i = ap^{i-1}$ for some constant $a$. The centralizer of $E$ in $\nu_i(H)/(K_i \cap \nu_i(F))$ has index at most $M^M$; hence, there exists a constant $M_1$ such that the group $\mu_i \nu_i(H)$ contains a $p$-subgroup of index at most $M_1$. Since the kernel $K_i$ is a $p$-group, the group $\mu_i(H)$ has a $p$-subgroup of index $\leq M_1$. Hence, $H$ has a subgroup $N$ of index at most $M_1$ that is residually (finite $p$)-group. We can assume that $N$ is a normal subgroup.

It remains to note that $N$ is generated by the intersection $F_k \cap N$ and $t_1 = t^{ap^s}$ for some $s$. Moreover, $t_1 (F_k \cap N) t_1^{-1} \subseteq F_k \cap N$ since $t_1 F_k t_1^{-1} \subseteq F_k$ and $t_1 \in N$. Hence, $N$ is an ascending HNN-extension of a free group (see, for instance, [3]). ■

## Acknowledgment

The research of the first author was supported in part by the National Security Agency grants H98230-06-1-0034 and H98230-08-1-0129. The work of the second author was supported in part by the National Science Foundation grant Division of Mathematical Sciences 0700811 and by a Israel Binational Science Foundation grant. The second author is grateful to the teams of doctors at Duke University and Vanderbilt University Medical Centers who made this paper possible. He is especially grateful to Dr. Allan Friedman from Duke University. He thanks his friends and colleagues for their support.

## References

[1] Borisov, A., and M. Sapir. "Polynomial maps over finite fields and residual finiteness of mapping tori of group endomorphisms." *Inventiones Mathematicae* 160, no. 2 (2005): 341–56.

[2] Breuillard, E., and T. Gelander. "A topological Tits alternative." *Annals of Mathematics* 166, no. 2 (2007): 427–74.

[3] Druţu, C., and M. Sapir. "Non-linear residually finite groups." *Journal of Algebra* 284, no. 1 (2005): 174–8.

[4] Dunfield, N. M., and D. P. Thurston. "A random tunnel number one 3-manifold does not fiber over the circle." *Geometry & Topology* 10 (2006): 2431–99.

[5] Eisenbud, D. *Commutative Algebra with a View Toward Algebraic Geometry.* Graduate Texts in Mathematics 150. New York: Springer, 1995.

[6] Feighn, M., and M. Handel. "Mapping tori of free group automorphisms are coherent." *Annals of Mathematics* 149, no. 2 (1999): 1061–77.

[7] Kapovich, I. "Mapping tori of endomorphisms of free groups." *Communications in Algebra* 28, no. 6 (2000): 2895–917.

[8] Kozáková, I., and M. Sapir. "Almost all one-relator groups with at least three generators are residually finite." (2008): preprint arXiv math0809.4693.

[9] Malcev, A. I. "On isomorphic matrix representations of infinite groups" [Russian]. *Recreational Mathematics (Matematicheskiĭ Sbornik)* N.S. 8, no. 50 (1940): 405–22.

[10] Manin, Yu. I., and A. A. Panchishkin. *Introduction to Modern Number Theory: Fundamental Problems, Ideas and Theories* [Translated from Russian], 2nd ed. Encyclopaedia of Mathematical Sciences 49. Berlin: Springer, 2005.

[11] Neumann, H. *Varieties of Groups*. New York: Springer, 1967.