Polynomial maps over fields and residually finite groups

Mark Sapir

August, 2009, Bath, UK

Lecture 3. Polynomial maps over finite fields.

The main result

Theorem.

The main result

Theorem. Almost surely as $n \to \infty$, every 1-related group with 3 or more generators and relator of length n, is embedded into a 2-generated 1-related group which is an ascending HNN extension of a free group, so it is

The main result

Theorem. Almost surely as $n \to \infty$, every 1-related group with 3 or more generators and relator of length n, is embedded into a 2-generated 1-related group which is an ascending HNN extension of a free group, so it is

- Residually finite,

The main result

Theorem. Almost surely as $n \to \infty$, every 1-related group with 3 or more generators and relator of length n, is embedded into a 2-generated 1-related group which is an ascending HNN extension of a free group, so it is

- Residually finite,
- Virtually residually (finite p-)group for all but finitely many primes p,

The main result

Theorem. Almost surely as $n \to \infty$, every 1-related group with 3 or more generators and relator of length n, is embedded into a 2-generated 1-related group which is an ascending HNN extension of a free group, so it is

- Residually finite,
- Virtually residually (finite p-)group for all but finitely many primes p,
- Coherent (that is all finitely generated subgroups are finitely presented).

Homework

HW 1. We know that the group $\langle x, y, t \mid txt^{-1} = xy, tyt^{-1} = yx \rangle$ is hyperbolic (A. Minasyan). By Olshanskii, it must have infinitely many non-abelian finite simple homomorphic images. Find one. The group has the one-relation presentation $\langle x, t \mid [x, t, t] = x \rangle$.

Periodic points of a word map

Consider the group

$$G = \langle x_1, ..., x_k, t \mid x_1^t = \phi(x_1), ..., x_k^t = \phi(x_k) \rangle$$

for some injective endomorphism ϕ of F_k.

Periodic points of a word map

Consider the group

$$G = \langle x_1, ..., x_k, t \mid x_1^t = \phi(x_1), ..., x_k^t = \phi(x_k) \rangle$$

for some injective endomorphism ϕ of F_k.
For example,

$$G = \langle x, y, t \mid txt^{-1} = xy, tyt^{-1} = yx \rangle.$$

Periodic points of a word map

Consider the group

$$G = \langle x_1, \ldots, x_k, t \mid x_1^t = \phi(x_1), \ldots, x_k^t = \phi(x_k) \rangle$$

for some injective endomorphism ϕ of F_k.
For example,

$$G = \langle x, y, t \mid txt^{-1} = xy, tyt^{-1} = yx \rangle.$$

So the endomorphism

$$\phi \colon x \mapsto xy, y \mapsto yx.$$

Periodic points of a word map

Consider the group

$$G = \langle x_1, \ldots, x_k, t \mid x_1^t = \phi(x_1), \ldots, x_k^t = \phi(x_k) \rangle$$

for some injective endomorphism ϕ of F_k.
For example,

$$G = \langle x, y, t \mid txt^{-1} = xy, tyt^{-1} = yx \rangle.$$

So the endomorphism

$$\phi \colon x \mapsto xy, y \mapsto yx.$$

Consider any $w = w(x, y) \neq 1$.

Periodic points of a word map

Consider the group

$$G = \langle x_1, ..., x_k, t \mid x_1^t = \phi(x_1), ..., x_k^t = \phi(x_k) \rangle$$

for some injective endomorphism ϕ of F_k.
For example,

$$G = \langle x, y, t \mid txt^{-1} = xy, tyt^{-1} = yx \rangle.$$

So the endomorphism

$$\phi \colon x \mapsto xy, y \mapsto yx.$$

Consider any $w = w(x, y) \neq 1$. We want to find $\psi \colon G \to V$ with $\psi(w) \neq 1$, $|V| < \infty$.

Periodic points of a word map

Consider the group

$$G = \langle x_1, ..., x_k, t \mid x_1^t = \phi(x_1), ..., x_k^t = \phi(x_k)\rangle$$

for some injective endomorphism ϕ of F_k.
For example,

$$G = \langle x, y, t \mid txt^{-1} = xy, tyt^{-1} = yx\rangle.$$

So the endomorphism

$$\phi\colon x \mapsto xy, y \mapsto yx.$$

Consider any $w = w(x, y) \neq 1$. We want to find $\psi\colon G \to V$ with $\psi(w) \neq 1$, $|V| < \infty$. Suppose that ψ exists.

Let us denote $\psi(x), \psi(y), \psi(t)$ by $\bar{x}, \bar{y}, \bar{t}$.

Let us denote $\psi(x), \psi(y), \psi(t)$ by $\bar{x}, \bar{y}, \bar{t}$. So we want

$$w(\bar{x}, \bar{y}) \neq 1.$$

Let us denote $\psi(x), \psi(y), \psi(t)$ by $\bar{x}, \bar{y}, \bar{t}$. So we want

$$w(\bar{x}, \bar{y}) \neq 1.$$

Note:

$$\bar{t}(\bar{x}, \bar{y})\bar{t}^{-1} = (\bar{x}\bar{y}, \bar{y}\bar{x}) = (\phi(x), \phi(y))$$

Let us denote $\psi(x), \psi(y), \psi(t)$ by $\bar{x}, \bar{y}, \bar{t}$. So we want

$$w(\bar{x}, \bar{y}) \neq 1.$$

Note:

$$\bar{t}(\bar{x}, \bar{y})\bar{t}^{-1} = (\bar{x}\bar{y}, \bar{y}\bar{x}) = (\phi(x), \phi(y))$$

We can continue:

$$\bar{t}^2(\bar{x}, \bar{y})\bar{t}^{-2} = (\bar{x}\bar{y}\bar{y}\bar{x}, \bar{y}\bar{x}\bar{x}\bar{y}) = (\phi^2(\bar{x}), \phi^2(\bar{y})).$$

Let us denote $\psi(x), \psi(y), \psi(t)$ by $\bar{x}, \bar{y}, \bar{t}$. So we want

$$w(\bar{x}, \bar{y}) \neq 1.$$

Note:

$$\bar{t}(\bar{x}, \bar{y})\bar{t}^{-1} = (\bar{x}\bar{y}, \bar{y}\bar{x}) = (\phi(x), \phi(y))$$

We can continue:

$$\bar{t}^2(\bar{x}, \bar{y})\bar{t}^{-2} = (\bar{x}\bar{y}\bar{y}\bar{x}, \bar{y}\bar{x}\bar{x}\bar{y}) = (\phi^2(\bar{x}), \phi^2(\bar{y})).$$

$$\ldots$$

$$\bar{t}^k(\bar{x}, \bar{y})\bar{t}^{-k} = (\phi^k(\bar{x}), \phi^k(\bar{y})).$$

Let us denote $\psi(x), \psi(y), \psi(t)$ by $\bar{x}, \bar{y}, \bar{t}$. So we want

$$w(\bar{x}, \bar{y}) \neq 1.$$

Note:

$$\bar{t}(\bar{x}, \bar{y})\bar{t}^{-1} = (\bar{x}\bar{y}, \bar{y}\bar{x}) = (\phi(x), \phi(y))$$

We can continue:

$$\bar{t}^2(\bar{x}, \bar{y})\bar{t}^{-2} = (\bar{x}\bar{y}\bar{y}\bar{x}, \bar{y}\bar{x}\bar{x}\bar{y}) = (\phi^2(\bar{x}), \phi^2(\bar{y})).$$

$$\ldots$$

$$\bar{t}^k(\bar{x}, \bar{y})\bar{t}^{-k} = (\phi^k(\bar{x}), \phi^k(\bar{y})).$$

Since $\bar{t}$ has finite order in V, for some k, we must have

$$(\phi^k(\bar{x}), \phi^k(\bar{y})) = (\bar{x}, \bar{y}).$$

Let us denote $\psi(x), \psi(y), \psi(t)$ by $\bar{x}, \bar{y}, \bar{t}$. So we want

$$w(\bar{x}, \bar{y}) \neq 1.$$

Note:

$$\bar{t}(\bar{x}, \bar{y})\bar{t}^{-1} = (\bar{x}\bar{y}, \bar{y}\bar{x}) = (\phi(x), \phi(y))$$

We can continue:

$$\bar{t}^2(\bar{x}, \bar{y})\bar{t}^{-2} = (\bar{x}\bar{y}\bar{y}\bar{x}, \bar{y}\bar{x}\bar{x}\bar{y}) = (\phi^2(\bar{x}), \phi^2(\bar{y})).$$

$$\dots$$

$$\bar{t}^k(\bar{x}, \bar{y})\bar{t}^{-k} = (\phi^k(\bar{x}), \phi^k(\bar{y})).$$

Since $\bar{t}$ has finite order in V, for some k, we must have

$$(\phi^k(\bar{x}), \phi^k(\bar{y})) = (\bar{x}, \bar{y}).$$

So $(\bar{x}, \bar{y})$ is a periodic point of the map

$$\tilde{\phi} \colon (a, b) \mapsto (ab, ba).$$

on the "space" $V \times V$.

The first reduction

So if G is residually finite then

The first reduction

So if G is residually finite then for every $w(x, y) \neq 1$,

The first reduction

So if G is residually finite then for every $w(x, y) \neq 1$, we found a finite group V

The first reduction

So if G is residually finite then for every $w(x, y) \neq 1$, we found a finite group V and a periodic point $(\bar{x}, \bar{y})$ of the map

$$\tilde{\phi}\colon (a, b) \mapsto (\phi(a), \phi(b))$$

on $V \times V$

The first reduction

So if G is residually finite then for every $w(x, y) \neq 1$, we found a finite group V and a periodic point $(\bar{x}, \bar{y})$ of the map

$$\tilde{\phi}\colon (a, b) \mapsto (\phi(a), \phi(b))$$

on $V \times V$ such that

$$w(\bar{x}, \bar{y}) \neq 1.$$

The first reduction

So if G is residually finite then for every $w(x, y) \neq 1$, we found a finite group V and a periodic point $(\bar{x}, \bar{y})$ of the map

$$\tilde{\phi}\colon (a, b) \mapsto (\phi(a), \phi(b))$$

on $V \times V$ such that

$$w(\bar{x}, \bar{y}) \neq 1.$$

So the periodic point should be outside the "subvariety" given by $w = 1$.

A key observation

Key observation. If $(\bar{x}, \bar{y})$ is periodic with period of length ℓ,

A key observation

Key observation. If $(\bar{x}, \bar{y})$ is periodic with period of length ℓ, then there exists a homomorphism from G into the wreath product $V' = V \wr \mathbb{Z}/\ell\mathbb{Z} = (V \times V \times ... \times V) \rtimes \mathbb{Z}/\ell\mathbb{Z}$ which separates w from 1.

A key observation

Key observation. If $(\bar{x}, \bar{y})$ is periodic with period of length ℓ, then there exists a homomorphism from G into the wreath product $V' = V \wr \mathbb{Z}/\ell\mathbb{Z} = (V \times V \times ... \times V) \rtimes \mathbb{Z}/\ell\mathbb{Z}$ which separates w from 1.

Indeed, the map

$$x \mapsto ((\bar{x}, \phi(\bar{x}), \phi^2(\bar{x}), ..., \phi^{l-1}(\bar{x})), 0),$$

$$y \mapsto ((\bar{y}, \phi(\bar{y}), \phi^2(\bar{y}), ..., \phi^{\ell-1}(\bar{y})), 0),$$

$$t \mapsto ((1, 1, ..., 1), \mathbf{1})$$

A key observation

Key observation. If $(\bar{x}, \bar{y})$ is periodic with period of length ℓ, then there exists a homomorphism from G into the wreath product $V' = V \wr \mathbb{Z}/\ell\mathbb{Z} = (V \times V \times ... \times V) \rtimes \mathbb{Z}/\ell\mathbb{Z}$ which separates w from 1.

Indeed, the map

$$x \mapsto ((\bar{x}, \phi(\bar{x}), \phi^2(\bar{x}), ..., \phi^{l-1}(\bar{x})), 0),$$

$$y \mapsto ((\bar{y}, \phi(\bar{y}), \phi^2(\bar{y}), ..., \phi^{\ell-1}(\bar{y})), 0),$$

$$t \mapsto ((1, 1, ..., 1), \mathbf{1})$$

extends to a homomorphism $\gamma : G \to V'$

A key observation

Key observation. If $(\bar{x}, \bar{y})$ is periodic with period of length ℓ, then there exists a homomorphism from G into the wreath product $V' = V \wr \mathbb{Z}/\ell\mathbb{Z} = (V \times V \times ... \times V) \rtimes \mathbb{Z}/\ell\mathbb{Z}$ which separates w from 1.
Indeed, the map

$$x \mapsto ((\bar{x}, \phi(\bar{x}), \phi^2(\bar{x}), ..., \phi^{l-1}(\bar{x})), 0),$$

$$y \mapsto ((\bar{y}, \phi(\bar{y}), \phi^2(\bar{y}), ..., \phi^{\ell-1}(\bar{y})), 0),$$

$$t \mapsto ((1, 1, ..., 1), \mathbf{1})$$

extends to a homomorphism $\gamma : G \to V'$ and

$$\gamma(w) = ((w(\bar{x}, \bar{y}), ...), 0) \neq 1.$$

The idea

Thus in order to prove that the group $\mathrm{HNN}_\phi(F_k)$ is residually finite,

The idea

Thus in order to prove that the group $\mathrm{HNN}_{\phi}(F_k)$ is residually finite, we need,

The idea

Thus in order to prove that the group $\mathrm{HNN}_{\phi}(F_k)$ is residually finite, we need, for every word $w \neq 1$ in F_k,

The idea

Thus in order to prove that the group $\mathrm{HNN}_\phi(F_k)$ is residually finite, we need, for every word $w \neq 1$ in F_k, find a finite group G

The idea

Thus in order to prove that the group $\mathrm{HNN}_\phi(F_k)$ is residually finite, we need, for every word $w \neq 1$ in F_k,find a finite group G and a periodic point of the map $\tilde{\phi}\colon G^k \to G^k$

The idea

Thus in order to prove that the group $\mathrm{HNN}_\phi(F_k)$ is residually finite, we need, for every word $w \neq 1$ in F_k,find a finite group G and a periodic point of the map $\tilde{\phi}\colon G^k \to G^k$outside the "subvariety" given by the equation $w = 1$.

Example

Consider again the group $\langle a, b, t \mid tat^{-1} = ab, tbt^{-1} = ba \rangle$.

Example

Consider again the group $\langle a, b, t \mid tat^{-1} = ab, tbt^{-1} = ba \rangle$.
Consider two matrices

$$U = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}, V = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}.$$

Example

Consider again the group $\langle a, b, t \mid tat^{-1} = ab, tbt^{-1} = ba \rangle$.
Consider two matrices

$$U = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}, V = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}.$$

They generate a free subgroup in $\mathrm{SL}_2(\mathbb{Z})$ (Sanov, '48).

Example

Consider again the group $\langle a, b, t \mid tat^{-1} = ab, tbt^{-1} = ba \rangle$. Consider two matrices

$$U = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}, V = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}.$$

They generate a free subgroup in $\mathrm{SL}_2(\mathbb{Z})$ (Sanov, '48). Then the matrices

$$A = UV = \begin{bmatrix} 5 & 2 \\ 2 & 1 \end{bmatrix}, B = VU = \begin{bmatrix} 1 & 2 \\ 2 & 5 \end{bmatrix}$$

also generate a free subgroup.

Example

Consider again the group $\langle a, b, t \mid tat^{-1} = ab, tbt^{-1} = ba \rangle$. Consider two matrices

$$U = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}, V = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}.$$

They generate a free subgroup in $SL_2(\mathbb{Z})$ (Sanov, '48). Then the matrices

$$A = UV = \begin{bmatrix} 5 & 2 \\ 2 & 1 \end{bmatrix}, B = VU = \begin{bmatrix} 1 & 2 \\ 2 & 5 \end{bmatrix}$$

also generate a free subgroup. Now let us iterate the map $\psi\colon (x, y) \to (xy, yx)$ starting with (A, B) mod 5.

Example

Consider again the group $\langle a, b, t \mid tat^{-1} = ab, tbt^{-1} = ba \rangle$. Consider two matrices

$$U = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}, V = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}.$$

They generate a free subgroup in $SL_2(\mathbb{Z})$ (Sanov, '48). Then the matrices

$$A = UV = \begin{bmatrix} 5 & 2 \\ 2 & 1 \end{bmatrix}, B = VU = \begin{bmatrix} 1 & 2 \\ 2 & 5 \end{bmatrix}$$

also generate a free subgroup. Now let us iterate the map $\psi\colon (x, y) \to (xy, yx)$ starting with (A, B) mod 5. That is we are considering the finite group $SL_2(\mathbb{Z}/5\mathbb{Z})$.

Example continued

$$\left(\begin{bmatrix} 5 & 2 \\ 2 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 2 & 5 \end{bmatrix} \right) \to \left(\begin{bmatrix} 4 & 0 \\ 4 & 4 \end{bmatrix}, \begin{bmatrix} 4 & 4 \\ 0 & 4 \end{bmatrix} \right) \to$$

Example continued

$$\left(\begin{bmatrix} 5 & 2 \\ 2 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 2 & 5 \end{bmatrix}\right) \to \left(\begin{bmatrix} 4 & 0 \\ 4 & 4 \end{bmatrix}, \begin{bmatrix} 4 & 4 \\ 0 & 4 \end{bmatrix}\right) \to$$

$$\left(\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}, \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}\right) \to \left(\begin{bmatrix} 3 & 2 \\ 4 & 3 \end{bmatrix}, \begin{bmatrix} 3 & 4 \\ 2 & 3 \end{bmatrix}\right) \to$$

Example continued

$$\left(\begin{bmatrix} 5 & 2 \\ 2 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 2 & 5 \end{bmatrix}\right) \rightarrow \left(\begin{bmatrix} 4 & 0 \\ 4 & 4 \end{bmatrix}, \begin{bmatrix} 4 & 4 \\ 0 & 4 \end{bmatrix}\right) \rightarrow$$

$$\left(\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}, \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}\right) \rightarrow \left(\begin{bmatrix} 3 & 2 \\ 4 & 3 \end{bmatrix}, \begin{bmatrix} 3 & 4 \\ 2 & 3 \end{bmatrix}\right) \rightarrow$$

$$\left(\begin{bmatrix} 3 & 3 \\ 3 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 3 \\ 3 & 3 \end{bmatrix}\right) \rightarrow \left(\begin{bmatrix} 4 & 3 \\ 0 & 4 \end{bmatrix}, \begin{bmatrix} 4 & 0 \\ 3 & 4 \end{bmatrix}\right) \rightarrow$$

Example continued

$$\left(\begin{bmatrix} 5 & 2 \\ 2 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 2 & 5 \end{bmatrix}\right) \to \left(\begin{bmatrix} 4 & 0 \\ 4 & 4 \end{bmatrix}, \begin{bmatrix} 4 & 4 \\ 0 & 4 \end{bmatrix}\right) \to$$

$$\left(\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}, \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}\right) \to \left(\begin{bmatrix} 3 & 2 \\ 4 & 3 \end{bmatrix}, \begin{bmatrix} 3 & 4 \\ 2 & 3 \end{bmatrix}\right) \to$$

$$\left(\begin{bmatrix} 3 & 3 \\ 3 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 3 \\ 3 & 3 \end{bmatrix}\right) \to \left(\begin{bmatrix} 4 & 3 \\ 0 & 4 \end{bmatrix}, \begin{bmatrix} 4 & 0 \\ 3 & 4 \end{bmatrix}\right) \to$$

$$\left(\begin{bmatrix} 5 & 2 \\ 2 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 2 & 5 \end{bmatrix}\right).$$

Example continued

$$\left(\begin{bmatrix} 5 & 2 \\ 2 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 2 & 5 \end{bmatrix}\right) \to \left(\begin{bmatrix} 4 & 0 \\ 4 & 4 \end{bmatrix}, \begin{bmatrix} 4 & 4 \\ 0 & 4 \end{bmatrix}\right) \to$$

$$\left(\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}, \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}\right) \to \left(\begin{bmatrix} 3 & 2 \\ 4 & 3 \end{bmatrix}, \begin{bmatrix} 3 & 4 \\ 2 & 3 \end{bmatrix}\right) \to$$

$$\left(\begin{bmatrix} 3 & 3 \\ 3 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 3 \\ 3 & 3 \end{bmatrix}\right) \to \left(\begin{bmatrix} 4 & 3 \\ 0 & 4 \end{bmatrix}, \begin{bmatrix} 4 & 0 \\ 3 & 4 \end{bmatrix}\right) \to$$

$$\left(\begin{bmatrix} 5 & 2 \\ 2 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 2 & 5 \end{bmatrix}\right).$$

Thus the point (A, B) is periodic in $SL_2(\mathbb{Z}/5\mathbb{Z})$ with period 6.

Example continued. Dynamics of polynomial maps over local fields

Replace 5 by 25, 125, etc. It turned out that (A, B) is periodic in $SL_2(\mathbb{Z}/25\mathbb{Z})$ with period 30, in $\mathrm{SL}_2(\mathbb{Z}/125\mathbb{Z})$ with period 150, etc.

Example continued. Dynamics of polynomial maps over local fields

Replace 5 by 25, 125, etc. It turned out that (A, B) is periodic in $SL_2(\mathbb{Z}/25\mathbb{Z})$ with period 30, in $\mathrm{SL}_2(\mathbb{Z}/125\mathbb{Z})$ with period 150, etc. Moreover there exists the following general Hensel-like statement

Example continued. Dynamics of polynomial maps over local fields

Replace 5 by 25, 125, etc. It turned out that (A, B) is periodic in $SL_2(\mathbb{Z}/25\mathbb{Z})$ with period 30, in $\mathrm{SL}_2(\mathbb{Z}/125\mathbb{Z})$ with period 150, etc. Moreover there exists the following general Hensel-like statement

Theorem. Let $P\colon \mathbb{Z}^n \to \mathbb{Z}^n$ be a polynomial map with integer coefficients.

Example continued. Dynamics of polynomial maps over local fields

Replace 5 by 25, 125, etc. It turned out that (A, B) is periodic in $SL_2(\mathbb{Z}/25\mathbb{Z})$ with period 30, in $\mathrm{SL}_2(\mathbb{Z}/125\mathbb{Z})$ with period 150, etc. Moreover there exists the following general Hensel-like statement

Theorem. Let $P\colon \mathbb{Z}^n \to \mathbb{Z}^n$ be a polynomial map with integer coefficients.Suppose that a point $\vec{x}$ is periodic with period d modulo some prime p, and the Jacobian $J_P(x)$ is not zero.

Example continued. Dynamics of polynomial maps over local fields

Replace 5 by 25, 125, etc. It turned out that (A, B) is periodic in $SL_2(\mathbb{Z}/25\mathbb{Z})$ with period 30, in $\mathrm{SL}_2(\mathbb{Z}/125\mathbb{Z})$ with period 150, etc. Moreover there exists the following general Hensel-like statement

Theorem. Let $P\colon \mathbb{Z}^n \to \mathbb{Z}^n$ be a polynomial map with integer coefficients.Suppose that a point $\vec{x}$ is periodic with period d modulo some prime p, and the Jacobian $J_P(x)$ is not zero. Then $\vec{x}$ is periodic modulo p^k with period $p^{k-1}d$ for every k.

Example continued. Dynamics of polynomial maps over local fields

Replace 5 by 25, 125, etc. It turned out that (A, B) is periodic in $SL_2(\mathbb{Z}/25\mathbb{Z})$ with period 30, in $\mathrm{SL}_2(\mathbb{Z}/125\mathbb{Z})$ with period 150, etc. Moreover there exists the following general Hensel-like statement

Theorem. Let $P\colon \mathbb{Z}^n \to \mathbb{Z}^n$ be a polynomial map with integer coefficients.Suppose that a point $\vec{x}$ is periodic with period d modulo some prime p, and the Jacobian $J_P(x)$ is not zero. Then $\vec{x}$ is periodic modulo p^k with period $p^{k-1}d$ for every k.

Now take any word $w \neq 1$ in x, y.

Example continued. Dynamics of polynomial maps over local fields

Replace 5 by 25, 125, etc. It turned out that (A, B) is periodic in $SL_2(\mathbb{Z}/25\mathbb{Z})$ with period 30, in $\mathrm{SL}_2(\mathbb{Z}/125\mathbb{Z})$ with period 150, etc. Moreover there exists the following general Hensel-like statement

Theorem. Let $P\colon \mathbb{Z}^n \to \mathbb{Z}^n$ be a polynomial map with integer coefficients.Suppose that a point $\vec{x}$ is periodic with period d modulo some prime p, and the Jacobian $J_P(x)$ is not zero. Then $\vec{x}$ is periodic modulo p^k with period $p^{k-1}d$ for every k.

Now take any word $w \neq 1$ in x, y. Since $\langle A, B\rangle$ is free in $\mathrm{SL}_2(\mathbb{Z})$, the matrix $w(A, B)$ is not 1,

Example continued. Dynamics of polynomial maps over local fields

Replace 5 by 25, 125, etc. It turned out that (A, B) is periodic in $SL_2(\mathbb{Z}/25\mathbb{Z})$ with period 30, in $\mathrm{SL}_2(\mathbb{Z}/125\mathbb{Z})$ with period 150, etc. Moreover there exists the following general Hensel-like statement

Theorem. Let $P\colon \mathbb{Z}^n \to \mathbb{Z}^n$ be a polynomial map with integer coefficients.Suppose that a point $\vec{x}$ is periodic with period d modulo some prime p, and the Jacobian $J_P(x)$ is not zero. Then $\vec{x}$ is periodic modulo p^k with period $p^{k-1}d$ for every k.

Now take any word $w \neq 1$ in x, y. Since $\langle A, B\rangle$ is free in $\mathrm{SL}_2(\mathbb{Z})$, the matrix $w(A, B)$ is not 1, and there exists $k \geq 1$ such that $w(A, B) \neq 1 \mod 5^k$.

Example continued. Dynamics of polynomial maps over local fields

Replace 5 by 25, 125, etc. It turned out that (A, B) is periodic in $SL_2(\mathbb{Z}/25\mathbb{Z})$ with period 30, in $\mathrm{SL}_2(\mathbb{Z}/125\mathbb{Z})$ with period 150, etc. Moreover there exists the following general Hensel-like statement

Theorem. Let $P\colon \mathbb{Z}^n \to \mathbb{Z}^n$ be a polynomial map with integer coefficients.Suppose that a point $\vec{x}$ is periodic with period d modulo some prime p, and the Jacobian $J_P(x)$ is not zero. Then $\vec{x}$ is periodic modulo p^k with period $p^{k-1}d$ for every k.

Now take any word $w \neq 1$ in x, y. Since $\langle A, B\rangle$ is free in $\mathrm{SL}_2(\mathbb{Z})$, the matrix $w(A, B)$ is not 1, and there exists $k \geq 1$ such that $w(A, B) \neq 1 \mod 5^k$.

Therefore our group $\langle a, b, t \mid tat^{-1} = ab, tbt^{-1} = ba\rangle$ is residually finite.

Polynomial maps over finite fields

Let $G = \langle a_1, ..., a_k, t \mid t a_i t^{-1} = w_i, i = 1, ..., k \rangle$.

Polynomial maps over finite fields

Let $G = \langle a_1, ..., a_k, t \mid t a_i t^{-1} = w_i, i = 1, ..., k \rangle$. Consider the ring of matrices $M_2(\mathbb{Z})$.

Polynomial maps over finite fields

Let $G = \langle a_1, \ldots, a_k, t \mid t a_i t^{-1} = w_i, i = 1, \ldots, k \rangle$.Consider the ring of matrices $M_2(\mathbb{Z})$.

The map $\psi \colon M_2(\mathbb{Z})^k \to M_2(\mathbb{Z})^k$ is given by

$$\vec{x} \mapsto (w_1(\vec{x}), \ldots, w_k(\vec{x})).$$

Polynomial maps over finite fields

Let $G = \langle a_1, ..., a_k, t \mid t a_i t^{-1} = w_i, i = 1, ..., k \rangle$.Consider the ring of matrices $M_2(\mathbb{Z})$.

The map $\psi\colon M_2(\mathbb{Z})^k \to M_2(\mathbb{Z})^k$ is given by

$$\vec{x} \mapsto (w_1(\vec{x}), ..., w_k(\vec{x})).$$

It can be considered as a polynomial map $A^{4k} \to A^{4k}$.

Polynomial maps over finite fields

Let $G = \langle a_1, ..., a_k, t \mid ta_i t^{-1} = w_i, i = 1, ..., k\rangle$.Consider the ring of matrices $M_2(\mathbb{Z})$.

The map $\psi \colon M_2(\mathbb{Z})^k \to M_2(\mathbb{Z})^k$ is given by

$$\vec{x} \mapsto (w_1(\vec{x}), ..., w_k(\vec{x})).$$

It can be considered as a polynomial map $A^{4k} \to A^{4k}$. The group we consider will be $\mathrm{PGL}_2(.)$.

Polynomial maps over finite fields

Let $G = \langle a_1, ..., a_k, t \mid ta_it^{-1} = w_i, i = 1, ..., k\rangle$.Consider the ring of matrices $M_2(\mathbb{Z})$.

The map $\psi\colon M_2(\mathbb{Z})^k \to M_2(\mathbb{Z})^k$ is given by

$$\vec{x} \mapsto (w_1(\vec{x}), ..., w_k(\vec{x})).$$

It can be considered as a polynomial map $A^{4k} \to A^{4k}$. The group we consider will be $\mathrm{PGL}_2(.)$. Here "." is any finite field of, say, characteristic p.

Polynomial maps over finite fields

Let $G = \langle a_1, ..., a_k, t \mid t a_i t^{-1} = w_i, i = 1, ..., k \rangle$.Consider the ring of matrices $M_2(\mathbb{Z})$.

The map $\psi\colon M_2(\mathbb{Z})^k \to M_2(\mathbb{Z})^k$ is given by

$$\vec{x} \mapsto (w_1(\vec{x}), ..., w_k(\vec{x})).$$

It can be considered as a polynomial map $A^{4k} \to A^{4k}$. The group we consider will be $\mathrm{PGL}_2(.)$. Here "." is any finite field of, say, characteristic p.

Thus our problem is reduced to the following:

Polynomial maps over finite fields

Let $G = \langle a_1, ..., a_k, t \mid ta_i t^{-1} = w_i, i = 1, ..., k\rangle$.Consider the ring of matrices $M_2(\mathbb{Z})$.

The map $\psi \colon M_2(\mathbb{Z})^k \to M_2(\mathbb{Z})^k$ is given by

$$\vec{x} \mapsto (w_1(\vec{x}), ..., w_k(\vec{x})).$$

It can be considered as a polynomial map $A^{4k} \to A^{4k}$. The group we consider will be $\mathrm{PGL}_2(.)$. Here "." is any finite field of, say, characteristic p.

Thus our problem is reduced to the following:

Problem. Let P be a polynomial map $A^n \to A^n$ with integer coefficients.

Polynomial maps over finite fields

Let $G = \langle a_1, ..., a_k, t \mid t a_i t^{-1} = w_i, i = 1, ..., k \rangle$.Consider the ring of matrices $M_2(\mathbb{Z})$.

The map $\psi \colon M_2(\mathbb{Z})^k \to M_2(\mathbb{Z})^k$ is given by

$$\vec{x} \mapsto (w_1(\vec{x}), ..., w_k(\vec{x})).$$

It can be considered as a polynomial map $A^{4k} \to A^{4k}$. The group we consider will be $\mathrm{PGL}_2(.)$. Here "." is any finite field of, say, characteristic p.

Thus our problem is reduced to the following:

Problem. Let P be a polynomial map $A^n \to A^n$ with integer coefficients. Show that the set of periodic points of P is Zariski dense.

Counting periodic points. Quasi-fixed points

Fixed points are not enough.

Counting periodic points. Quasi-fixed points

Fixed points are not enough.

Example: $x \mapsto x + 1$ does not have fixed points.

Counting periodic points. Quasi-fixed points

Fixed points are not enough.

Example: $x \mapsto x + 1$ does not have fixed points.

Deligne: instead of fixed points, $P(x) = x$, consider

Counting periodic points. Quasi-fixed points

Fixed points are not enough.

Example: $x \mapsto x + 1$ does not have fixed points.

Deligne: instead of fixed points, $P(x) = x$, consider quasi-fixed points, $P(x) = x^{p^n}$

Counting periodic points. Quasi-fixed points

Fixed points are not enough.

Example: $x \mapsto x + 1$ does not have fixed points.

Deligne: instead of fixed points, $P(x) = x$, consider quasi-fixed points, $P(x) = x^{p^n} (= Fr^n(x))$.

Counting periodic points. Quasi-fixed points

Fixed points are not enough.

Example: $x \mapsto x + 1$ does not have fixed points.

Deligne: instead of fixed points, $P(x) = x$, consider quasi-fixed points, $P(x) = x^{p^n} (= Fr^n(x))$.

Note that all quasi-fixed points are periodic

Counting periodic points. Quasi-fixed points

Fixed points are not enough.

Example: $x \mapsto x + 1$ does not have fixed points.

Deligne: instead of fixed points, $P(x) = x$, consider quasi-fixed points, $P(x) = x^{p^n} (= Fr^n(x))$.

Note that all quasi-fixed points are periodic because Fr is the automorphism of finite order, and commutes with P since all coefficients of P are integers.

Counting periodic points. Quasi-fixed points

Fixed points are not enough.

Example: $x \mapsto x + 1$ does not have fixed points.

Deligne: instead of fixed points, $P(x) = x$, consider quasi-fixed points, $P(x) = x^{p^n} (= Fr^n(x))$.

Note that all quasi-fixed points are periodic because Fr is the automorphism of finite order, and commutes with P since all coefficients of P are integers.

Deligne conjecture, proved by Fujiwara and Pink:

Counting periodic points. Quasi-fixed points

Fixed points are not enough.

Example: $x \mapsto x + 1$ does not have fixed points.

Deligne: instead of fixed points, $P(x) = x$, consider quasi-fixed points, $P(x) = x^{p^n} (= Fr^n(x))$.

Note that all quasi-fixed points are periodic because Fr is the automorphism of finite order, and commutes with P since all coefficients of P are integers.

Deligne conjecture, proved by Fujiwara and Pink: If P is dominant and quasi-finite

Counting periodic points. Quasi-fixed points

Fixed points are not enough.

Example: $x \mapsto x + 1$ does not have fixed points.

Deligne: instead of fixed points, $P(x) = x$, consider quasi-fixed points, $P(x) = x^{p^n} (= Fr^n(x))$.

Note that all quasi-fixed points are periodic because Fr is the automorphism of finite order, and commutes with P since all coefficients of P are integers.

Deligne conjecture, proved by Fujiwara and Pink: If P is dominant and quasi-finite then the set of quasi-fixed points is Zariski dense.

The main results

Theorem (Borisov, Sapir)

The main results

Theorem (Borisov, Sapir) Let $P^n \colon A^n(\mathbb{F}_q) \to A^n(\mathbb{F}_q)$ be the n-th iteration of P.

The main results

Theorem (Borisov, Sapir) Let $P^n \colon A^n(\mathbb{F}_q) \to A^n(\mathbb{F}_q)$ be the n-th iteration of P. Let V be the Zariski closure of $P^n(A^n)$.

The main results

Theorem (Borisov, Sapir) Let $P^n\colon A^n(\mathbb{F}_q) \to A^n(\mathbb{F}_q)$ be the n-th iteration of P. Let V be the Zariski closure of $P^n(A^n)$. The set of its geometric points is $V(\overline{\mathbb{F}_q})$,

The main results

Theorem (Borisov, Sapir) Let $P^n \colon A^n(\mathbb{F}_q) \to A^n(\mathbb{F}_q)$ be the n-th iteration of P. Let V be the Zariski closure of $P^n(A^n)$. The set of its geometric points is $V(\overline{\mathbb{F}_q})$, where $\overline{\mathbb{F}_q}$ is the algebraic closure of $\mathbb{F}_q$.

The main results

Theorem (Borisov, Sapir) Let $P^n\colon A^n(\mathbb{F}_q) \to A^n(\mathbb{F}_q)$ be the n-th iteration of P. Let V be the Zariski closure of $P^n(A^n)$. 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.

The main results

Theorem (Borisov, Sapir) Let $P^n \colon A^n(\mathbb{F}_q) \to A^n(\mathbb{F}_q)$ be the n-th iteration of P. Let V be the Zariski closure of $P^n(A^n)$. 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 $V(\overline{\mathbb{F}_q})$.

The main results

Theorem (Borisov, Sapir) Let $P^n\colon A^n(\mathbb{F}_q) \to A^n(\mathbb{F}_q)$ be the n-th iteration of P. Let V be the Zariski closure of $P^n(A^n)$. 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 P are Zariski dense in V.

The main results

Theorem (Borisov, Sapir) Let $P^n\colon A^n(\mathbb{F}_q) \to A^n(\mathbb{F}_q)$ be the n-th iteration of P. Let V be the Zariski closure of $P^n(A^n)$. 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 P are Zariski dense in V. In other words, suppose $W \subset V$ is a proper Zariski closed subvariety of V.

The main results

Theorem (Borisov, Sapir) Let $P^n \colon A^n(\mathbb{F}_q) \to A^n(\mathbb{F}_q)$ be the n-th iteration of P. Let V be the Zariski closure of $P^n(A^n)$. 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 P 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

$$(a_1, ..., a_n) \in V(\overline{\mathbb{F}_q}) \setminus W(\overline{\mathbb{F}_q})$$

The main results

Theorem (Borisov, Sapir) Let $P^n \colon A^n(\mathbb{F}_q) \to A^n(\mathbb{F}_q)$ be the n-th iteration of P. Let V be the Zariski closure of $P^n(A^n)$. 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 P 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

$$\begin{cases} f_1(a_1, ..., a_n) = a_1^Q \\ f_2(a_1, ..., a_n) = a_2^Q \\ ... \\ f_n(a_1, ..., a_n) = a_n^Q \end{cases}$$

The main results

Theorem (Borisov, Sapir) Let $P^n \colon A^n(\mathbb{F}_q) \to A^n(\mathbb{F}_q)$ be the n-th iteration of P. Let V be the Zariski closure of $P^n(A^n)$. 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 P 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

$$(a_1, \ldots, a_n) \in V(\overline{\mathbb{F}_q}) \setminus W(\overline{\mathbb{F}_q})$$

such that

$$\begin{cases} f_1(a_1, \ldots, a_n) = a_1^Q \\ f_2(a_1, \ldots, a_n) = a_2^Q \\ \ldots \\ f_n(a_1, \ldots, a_n) = a_n^Q \end{cases}$$

Theorem (Borisov, Sapir).

The main results

Theorem (Borisov, Sapir) Let $P^n \colon A^n(\mathbb{F}_q) \to A^n(\mathbb{F}_q)$ be the n-th iteration of P. Let V be the Zariski closure of $P^n(A^n)$. 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 P 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

$$\begin{cases} f_1(a_1, ..., a_n) = a_1^Q \\ f_2(a_1, ..., a_n) = a_2^Q \\ ... \\ f_n(a_1, ..., a_n) = a_n^Q \end{cases}$$

Theorem (Borisov, Sapir). Every ascending HNN extension of a free group is residually finite.

Hrushovsky's result

Hrushovsky managed to replace A^n in our statement by arbitrary variety V.

Hrushovsky's result

Hrushovsky managed to replace A^n in our statement by arbitrary variety V.

Theorem (Borisov, Sapir) The ascending HNN extension of any finitely generated linear group is residually finite.

Hrushovsky's result

Hrushovsky managed to replace A^n in our statement by arbitrary variety V.

Theorem (Borisov, Sapir) The ascending HNN extension of any finitely generated linear group is residually finite.

For non-linear residually finite groups this statement is not true (S. and Wise).

Hrushovsky's result

Hrushovsky managed to replace A^n in our statement by arbitrary variety V.

Theorem (Borisov, Sapir) The ascending HNN extension of any finitely generated linear group is residually finite.

For non-linear residually finite groups this statement is not true (S. and Wise).

Problem. Is $\langle a, b, t \mid tat^{-1} = ab, tbt^{-1} = ba \rangle$ linear?

Hrushovsky's result

Hrushovsky managed to replace A^n in our statement by arbitrary variety V.

Theorem (Borisov, Sapir) The ascending HNN extension of any finitely generated linear group is residually finite.

For non-linear residually finite groups this statement is not true (S. and Wise).

Problem. Is $\langle a, b, t \mid tat^{-1} = ab, tbt^{-1} = ba \rangle$ linear?

Conjecture: No.

Proof

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 $i = 1, 2, ..., n$.

Proof

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 $i = 1, 2, ..., n$.
Step 1. 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 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 $i = 1, 2, ..., n$.

Step 1. For a big enough Q the ideal I_Q has finite codimension in the ring $\overline{\mathbb{F}_q}[x_1, ..x_n]$.

Step 2. For all $1 \leq i \leq n$ and $j \geq 1$

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

Proof

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 $i = 1, 2, ..., n$.
Step 1. For a big enough Q the ideal I_Q has finite codimension in the ring $\overline{\mathbb{F}_q}[x_1, ..x_n]$.
Step 2. For all $1 \leq i \leq n$ and $j \geq 1$

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

Step 3. There exists a number k such that for every quasi-fixed point $(a_1, ..., a_n)$ with big enough Q and for every $1 \leq i \leq n$ 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

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 $i = 1, 2, ..., n$.
Step 1. For a big enough Q the ideal I_Q has finite codimension in the ring $\overline{\mathbb{F}_q}[x_1, ..x_n]$.
Step 2. For all $1 \leq i \leq n$ and $j \geq 1$

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

Step 3. There exists a number k such that for every quasi-fixed point $(a_1, ..., a_n)$ with big enough Q and for every $1 \leq i \leq n$ 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 $(a_1, ..., a_n)$.
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.

Proof continued

Step 4. 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

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

Proof continued

Step 4. 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

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

We know that all points with $P(x) = x^Q$ 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.

Proof continued

Step 4. There exists a positive integer K such that for all quasi-fixed points $(a_1, \ldots, a_n) \in W$ with big enough Q we get

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

We know that all points with $P(x) = x^Q$ 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.

Step 5. First of all, we claim that in this case R lies in the localizations of I_Q with respect to all maximal ideals of the ring of polynomials.

Proof continued

Step 4. There exists a positive integer K such that for all quasi-fixed points $(a_1, \ldots, a_n) \in W$ with big enough Q we get

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

We know that all points with $P(x) = x^Q$ 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.

Step 5. First of all, we claim that in this case R lies in the localizations of I_Q with respect to all maximal ideals of the ring of polynomials.

This implies that $R \in I_Q$.

Proof continued

This means that there exist polynomials $u_1, ...u_n$ such that

$$R = \sum_{i=1}^{n} u_i \cdot (f_i - x_i^Q) \qquad (1)$$

Proof continued

This means that there exist polynomials $u_1, ...u_n$ such that

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

Step 6. We get a set of u_i's with the following property:

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

Proof continued

This means that there exist polynomials $u_1, \ldots u_n$ such that

$$R = \sum_{i=1}^{n} u_i \cdot (f_i - x_i^Q) \qquad (1)$$

Step 6. We get a set of u_i's with the following property:

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

Step 7. We look how the monomials cancel in the equation (1) and get a contradiction.