Multivariate polynomial automorphisms over finite fields

Stefan Maubach

May 2013

The Art of

doing stuff with

Multivariate polynomial automorphisms over finite fields

Stefan Maubach

May 2013

1. Affine algebraic geometry (characteristic 0)
2. Characteristic p / finite fields
3. Iterations (efficient)

Polynomial automorphisms

k a field,

$$F : k^n \longrightarrow k^n$$

polynomial map if $F = (F_1, \ldots, F_n)$, $F_i \in k[X_1, \ldots, X_n]$.

Polynomial automorphisms

k a field,

$$F : k^n \longrightarrow k^n$$

polynomial map if $F = (F_1, \ldots, F_n)$, $F_i \in k[X_1, \ldots, X_n]$.

Example: $F = (X + Y^2, Y)$ is polynomial map $\mathbb{C}^2 \longrightarrow \mathbb{C}^2$.

Polynomial automorphisms

k a field,

$$F : k^n \longrightarrow k^n$$

polynomial map if $F = (F_1, \dots, F_n)$, $F_i \in k[X_1, \dots, X_n]$.
Example: $F = (X + Y^2, Y)$ is polynomial map $\mathbb{C}^2 \longrightarrow \mathbb{C}^2$.
$F \circ G = (F_1(G_1, \dots, G_n), \dots, F_n(G_1, \dots, G_n))$ composition,
unit element $(X_1, \dots, X_n)$ unit element.

Polynomial automorphisms

k a field,

$$F : k^n \longrightarrow k^n$$

polynomial map if $F = (F_1, \ldots, F_n)$, $F_i \in k[X_1, \ldots, X_n]$.

Example: $F = (X + Y^2, Y)$ is polynomial map $\mathbb{C}^2 \longrightarrow \mathbb{C}^2$.

$F \circ G = (F_1(G_1, \ldots, G_n), \ldots, F_n(G_1, \ldots, G_n))$ composition,

unit element $(X_1, \ldots, X_n)$ unit element.

Set of polynomial automorphisms of k^n:

$Aut_n(k)$, also denoted by $\mathrm{GA}_n(k)$ - similarly to $\mathrm{GL}_n(k)$.

Polynomial automorphisms

k a field,

$$F : k^n \longrightarrow k^n$$

polynomial map if $F = (F_1, \ldots, F_n)$, $F_i \in k[X_1, \ldots, X_n]$.

Example: $F = (X + Y^2, Y)$ is polynomial map $\mathbb{C}^2 \longrightarrow \mathbb{C}^2$.

$F \circ G = (F_1(G_1, \ldots, G_n), \ldots, F_n(G_1, \ldots, G_n))$ composition,

unit element $(X_1, \ldots, X_n)$ unit element.

Set of polynomial automorphisms of k^n:

$Aut_n(k)$, also denoted by $\mathrm{GA}_n(k)$ - similarly to $\mathrm{GL}_n(k)$.

(This whole talk: $n \geq 2$, as

$\mathrm{GA}_1(k) = \mathrm{Aff}_1(k) = \{ax + b \mid a \in k^*, b \in k\}$.)

Triangular polynomial maps

(Also called Jonquière.)

$$F = (F_1, \ldots, F_n) \in \mathrm{GA}_n(k)$$

where $F_i \in k[x_i, x_{i+1}, \ldots, x_n]$. i.e.
$F_i = a_i x_i + f_i(x_{i+1}, \ldots, x_n)$. Forms a group:

$$\mathrm{BA}_n(k)$$

Triangular polynomial maps

(Also called Jonquière.)

$$F = (F_1, \dots, F_n) \in \mathrm{GA}_n(k)$$

where $F_i \in k[x_i, x_{i+1}, \dots, x_n]$. i.e.
$F_i = a_i x_i + f_i(x_{i+1}, \dots, x_n)$. Forms a group:

$$\mathrm{BA}_n(k)$$

Subgroup: those having linear part identity

$$\mathrm{BA}_n^0(k) = \{(x_1 + f_1, \dots, x_n + f_n) \mid f_i \in k[x_{i+1}, \dots, x_n]$$

(strictly triangular group)

Strictly triangular maps trivial?

Consider

$$F := (x_1 + x_5^3, x_2 + x_6^3, x_3 + x_7^3, x_4 + (x_5 x_6 x_7)^2, x_5, x_6, x_7)$$

a very simple triangular map.

Strictly triangular maps trivial?

Consider

$$F := (x_1 + x_5^3, x_2 + x_6^3, x_3 + x_7^3, x_4 + (x_5 x_6 x_7)^2, x_5, x_6, x_7)$$

a very simple triangular map. Then

$$\mathrm{inv}(F) = \{P \mid F(P) = P\}$$

is an infinitely generated subring of $\mathbb{C}[x_1, x_2, x_3, x_4, x_5, x_6, x_7]$.

Iterating in characteristic 0

Let F be polynomial map. 2 cases:

Iterating in characteristic 0

Let F be polynomial map. 2 cases:

- $deg F^n$ is unbounded sequence. Hard case

Iterating in characteristic 0

Let F be polynomial map. 2 cases:

- $deg F^n$ is unbounded sequence. Hard case
- $deg F^n$ is bounded sequence. Slightly less hard case

Iterating in characteristic 0

Let F be polynomial map. 2 cases:

- $deg F^n$ is unbounded sequence. Hard case
- $deg F^n$ is bounded sequence. Slightly less hard case

$deg F^n$ bounded: F is called LF map ($=$ locally finite map).

Triangular polynomial maps: are LF maps.

Iterating in characteristic 0

Let F be polynomial map. 2 cases:

- $deg F^n$ is unbounded sequence. Hard case
- $deg F^n$ is bounded sequence. Slightly less hard case

$deg F^n$ bounded: F is called LF map (= locally finite map).

Triangular polynomial maps: are LF maps.

Example: $(x + y^2, y)$, then $F^2 - 2F + I = 0$.

LF maps: semisimple, unipotent

Theorem (M-, Furter): F is LF, then $F = F_u F_s = F_s F_u$ for some semisimple F_s, unipotent F_u.

LF maps: semisimple, unipotent

Theorem (M-, Furter): F is LF, then $F = F_u F_s = F_s F_u$ for some semisimple F_s, unipotent F_u.

Example:

$F = (x + 1, 2y) = (x + 1, y)(x, 2y) = (x, 2y)(x + 1, y)$.

LF maps: semisimple, unipotent

Theorem (M-, Furter): F is LF, then $F = F_u F_s = F_s F_u$ for some semisimple F_s, unipotent F_u.

Example:

$F = (x + 1, 2y) = (x + 1, y)(x, 2y) = (x, 2y)(x + 1, y)$.

Example: $F = (x + y, 2y)$ is already semisimple.

LF maps: semisimple, unipotent

Theorem (M-, Furter): F is LF, then $F = F_u F_s = F_s F_u$ for some semisimple F_s, unipotent F_u.

Example:

$F = (x+1, 2y) = (x+1, y)(x, 2y) = (x, 2y)(x+1, y)$.

Example: $F = (x+y, 2y)$ is already semisimple.

Example: $\mathrm{BA}_n^0(k)$ is set of unipotents in $\mathrm{BA}_n(k)$.

LF maps: semisimple, unipotent

Theorem (M-, Furter): F is LF, then $F = F_u F_s = F_s F_u$ for some semisimple F_s, unipotent F_u.

Example:

$F = (x+1, 2y) = (x+1, y)(x, 2y) = (x, 2y)(x+1, y)$.

Example: $F = (x+y, 2y)$ is already semisimple.

Example: $\mathrm{BA}_n^0(k)$ is set of unipotents in $\mathrm{BA}_n(k)$.

Unipotents are easy to iterate in char. 0: (next slide)

Additive group action on k^n (char$(k) = 0$)

Algebraic subgroups of $\mathrm{GA}_n(k)$ isomorphic to $(k, +)$

Additive group action on k^n (char$(k) = 0$)

Algebraic subgroups of $\mathrm{GA}_n(k)$ isomorphic to $(k, +)$

Example: $t \times (x, y) \longrightarrow (x + ty^2, y)$

Additive group action on k^n (char$(k) = 0$)

Algebraic subgroups of $\mathrm{GA}_n(k)$ isomorphic to $(k, +)$

Example: $t \times (x, y) \longrightarrow (x + ty^2, y)$ i.e. formula

$$F_t \in \mathrm{GA}_n(k[t])$$

satisfying $F_t \circ F_u = F_{t+u}$.

Additive group action on k^n (char$(k) = 0$)

Algebraic subgroups of $\mathrm{GA}_n(k)$ isomorphic to $(k, +)$

Example: $t \times (x, y) \longrightarrow (x + ty^2, y)$ i.e. formula

$$F_t \in \mathrm{GA}_n(k[t])$$

satisfying $F_t \circ F_u = F_{t+u}$.

$\Rightarrow F_t = \exp(tD)$, D locally nilpotent derivation on $k[x_1, \ldots, x_n]$.

$(x + ty^2, y) = \exp(tD)$, $D = y^2 \frac{\partial}{\partial x}$,

Additive group action on k^n (char$(k) = 0$)

Algebraic subgroups of $\mathrm{GA}_n(k)$ isomorphic to $(k, +)$

Example: $t \times (x, y) \longrightarrow (x + ty^2, y)$ i.e. formula

$$F_t \in \mathrm{GA}_n(k[t])$$

satisfying $F_t \circ F_u = F_{t+u}$.

$\Rightarrow F_t = \exp(tD)$, D locally nilpotent derivation on $k[x_1, \ldots, x_n]$.

$(x + ty^2, y) = \exp(tD)$, $D = y^2 \frac{\partial}{\partial x}$,

$(x - 2ty\Delta - t^2 z\Delta^2, y + tz\Delta, z) = \exp(tD)$,

$D = -2y\frac{\partial}{\partial x} + z\frac{\partial}{\partial y}$.

Additive group action on k^n (char$(k) = 0$)

Algebraic subgroups of $\mathrm{GA}_n(k)$ isomorphic to $(k, +)$

Example: $t \times (x, y) \longrightarrow (x + ty^2, y)$ i.e. formula

$$F_t \in \mathrm{GA}_n(k[t])$$

satisfying $F_t \circ F_u = F_{t+u}$.

$\Rightarrow F_t = \exp(tD)$, D locally nilpotent derivation on $k[x_1, \ldots, x_n]$.

$(x + ty^2, y) = \exp(tD)$, $D = y^2 \frac{\partial}{\partial x}$,

$(x - 2ty\Delta - t^2 z\Delta^2, y + tz\Delta, z) = \exp(tD)$,

$D = -2y\frac{\partial}{\partial x} + z\frac{\partial}{\partial y}$.

F unipotent LF map $\Longleftrightarrow$ exist additive group action F_t such that $F_1 = F$.

Strictly triangular polynomial maps

Characteristic 0: $F \in \mathrm{BA}_n^0(k)$ then $F = \exp(D)$ for some triangular derivation D; $F^n = \exp(nD)$ i.e. iterations of F are trivial!

Additive group actions in char. p

$$F_t = \exp(tD)$$

where D is a *locally finite iterative higher derivation*.

Additive group actions char. p: problems

Characteristic 2: $(k,+)$-action on k^n

Example:

$$t \times (x, y, z) \longrightarrow \left(x + ty + \frac{t^2 + t}{2} z, y + tz, z\right)$$

is NOT a $(k,+)$ action! In particular,

$$(x + y + z, y + z, z)$$

is not the exponent of a locally finite iterative higher derivation. Any k-action has order p !

Additive group actions char. p: solution

$$t \times (x, y, z) \longrightarrow (x + ty + \frac{t^2 + t}{2} z, y + tz, z)$$

Additive group actions char. p: solution

$$t \times (x, y, z) \longrightarrow \left(x + ty + \frac{t^2 + t}{2} z, y + tz, z\right)$$

Do not consider $\mathbb{F}_2$-actions but consider $\mathbb{Z}$-actions!

Additive group actions char. p: solution

$$t \times (x, y, z) \longrightarrow (x + ty + \frac{t^2 + t}{2} z, y + tz, z)$$

Do not consider $\mathbb{F}_2$-actions but consider $\mathbb{Z}$-actions!

Theorem: If $f(x) \in \mathbb{Q}[x]$ such that $f(\mathbb{Z}) \subseteq \mathbb{Z}$ then

$$f \in \mathbb{Z}\left[\binom{x}{n}\ ;\ n \in \mathbb{N}\right].$$

Additive group actions char. p: solution

$$t \times (x, y, z) \longrightarrow \left(x + ty + \frac{t^2 + t}{2} z, y + tz, z\right)$$

Do not consider $\mathbb{F}_2$-actions but consider $\mathbb{Z}$-actions!

Theorem: If $f(x) \in \mathbb{Q}[x]$ such that $f(\mathbb{Z}) \subseteq \mathbb{Z}$ then

$$f \in \mathbb{Z}\left[\binom{x}{n} \; ; \; n \in \mathbb{N}\right].$$

Theorem: If $f(x) \in \mathbb{Q}[x]$ such that $f(\mathbb{Z}_p) \subseteq \mathbb{Z}_p$ then

$$f \in \mathbb{Z}\left[\binom{x}{p^n} \; ; \; n \in \mathbb{N}\right].$$

Additive group actions char. p: solution

$$t \times (x, y, z) \longrightarrow \left(x + ty + \frac{t^2 + t}{2} z, y + tz, z\right)$$

Do not consider $\mathbb{F}_2$-actions but consider $\mathbb{Z}$-actions!

Theorem: If $f(x) \in \mathbb{Q}[x]$ such that $f(\mathbb{Z}) \subseteq \mathbb{Z}$ then

$$f \in \mathbb{Z}\left[\binom{x}{n} \; ; \; n \in \mathbb{N}\right].$$

Theorem: If $f(x) \in \mathbb{Q}[x]$ such that $f(\mathbb{Z}_p) \subseteq \mathbb{Z}_p$ then

$$f \in \mathbb{Z}\left[\binom{x}{p^n} \; ; \; n \in \mathbb{N}\right].$$

Corollary: If $f(x) \in \mathbb{Q}[x]$ such that $f \mod p$ makes sense, then

$$f \in \mathbb{Z}\left[\binom{x}{p^n} \; ; \; n \in \mathbb{N}\right].$$

Additive group actions char. p: solution

Char$=0$: $(x + ty + \frac{t^2+t}{2}z, y + tz, z) \in k[t][x, y, z]$

Additive group actions char. p: solution

Char$=0$: $(x + ty + \frac{t^2+t}{2} z, y + tz, z) \in k[t][x, y, z]$

Char$=2$: $(x + ty + (Q_1 + t)z, y + tz, z) \in k[t, Q_1][x, y, z]$

where $Q_1 := \binom{t}{2}$.

Additive group actions char. p: solution

Char$= 0$: $(x + ty + \frac{t^2+t}{2}z, y + tz, z) \in k[t][x, y, z]$

Char$= 2$: $(x + ty + (Q_1 + t)z, y + tz, z) \in k[t, Q_1][x, y, z]$

where $Q_1 := \binom{t}{2}$.

Define

$$R := k[Q_i; i \in \mathbb{N}] \text{ where } Q_i := \binom{t}{p^i}.$$

Then if $F \in \mathrm{GA}_n(\mathbb{F}_p)$ unipotent LF map, there exists $F_t \in \mathrm{GA}_n(R)$ such that $F^n = F_t(t = n)$.

Some other subgroups:

Tame automorphisms:

$$\mathrm{TA}_n(k) = < \mathrm{BA}_n(k), \mathrm{Aff}_n(k) >$$

Some other subgroups:

Tame automorphisms:

$$\mathrm{TA}_n(k) = < \mathrm{BA}_n(k), \mathrm{Aff}_n(k) >$$

Jung v/d Kulk theorem:

$$\mathrm{GA}_2(k) = \mathrm{TA}_2(k)$$

Some other subgroups:

Tame automorphisms:

$$\mathrm{TA}_n(k) =< \mathrm{BA}_n(k), \mathrm{Aff}_n(k) >$$

Jung v/d Kulk theorem:

$$\mathrm{GA}_2(k) = \mathrm{TA}_2(k)$$

Another group: $\mathrm{GLF}_n(k) =$ group generated by LF maps.

$$\mathrm{GA}_n(k) \supseteq \mathrm{GLF}_n(k) \supseteq \mathrm{TA}_n(k)$$

Some other subgroups:

Tame automorphisms:

$$\mathrm{TA}_n(k) =< \mathrm{BA}_n(k), \mathrm{Aff}_n(k) >$$

Jung v/d Kulk theorem:

$$\mathrm{GA}_2(k) = \mathrm{TA}_2(k)$$

Another group: $\mathrm{GLF}_n(k) =$ group generated by LF maps.

$$\mathrm{GA}_n(k) \supseteq \mathrm{GLF}_n(k) \supseteq \mathrm{TA}_n(k)$$

Conjecture: bounded iterative degree generates all

Non-tame maps

Nagata's automorphism:

$$N := (x - 2y\Delta - z\Delta^2, y + z\Delta, z), \quad \Delta = xz + y^2$$

$N \in \mathrm{GA}_3(k)$.

Non-tame maps

Nagata's automorphism:

$$N := (x - 2y\Delta - z\Delta^2, y + z\Delta, z), \quad \Delta = xz + y^2$$

$N \in \mathrm{GA}_3(k)$.

Conjecture (1974) by Nagata: $N \notin \mathrm{TA}_3(k)$

Non-tame maps

Nagata's automorphism:

$$N := (x - 2y\Delta - z\Delta^2, y + z\Delta, z), \quad \Delta = xz + y^2$$

$N \in \mathrm{GA}_3(k)$.

Conjecture (1974) by Nagata: $N \notin \mathrm{TA}_3(k)$

Result (2004) Umirbaev-Shestakov: Indeed, not in there!

Non-tame maps

Nagata's automorphism:

$$N := (x - 2y\Delta - z\Delta^2, y + z\Delta, z), \quad \Delta = xz + y^2$$

$N \in \mathrm{GA}_3(k)$.

Conjecture (1974) by Nagata: $N \notin \mathrm{TA}_3(k)$

Result (2004) Umirbaev-Shestakov: Indeed, not in there!

... if $\mathrm{char}(k) = 0$.

Polynomial automorphisms

Each $F \in \mathrm{GA}_n(k)$ induces a map $k^n \longrightarrow k^n$:

$$\mathrm{GA}_n(k) \longrightarrow \mathrm{perm}(k^n)$$

Injective, UNLESS k is finite.

Polynomial automorphisms

$$\mathrm{GA}_n(\mathbb{F}_q) \xrightarrow{\pi_q} \mathrm{perm}((\mathbb{F}_q)^n) = \mathrm{sym}((\mathbb{F}_q)^n)$$

Surjective?

Polynomial automorphisms

$$\mathrm{GA}_n(\mathbb{F}_q) \xrightarrow{\pi_q} \mathrm{perm}((\mathbb{F}_q)^n) = \mathrm{sym}((\mathbb{F}_q)^n)$$

Surjective?

Theorem

$\pi_q(\mathrm{TA}_n(\mathbb{F}_q)) = \mathrm{sym}((\mathbb{F}_q)^n)$ if $q = odd$ or $q = 2$,

$\pi_q(\mathrm{TA}_n(\mathbb{F}_q)) = \mathrm{alt}((\mathbb{F}_q)^n)$ if $q = 2^m$, $m > 1$.

Obvious question: $\pi_4(\mathrm{GA}_n(\mathbb{F}_4)) = \mathrm{Alt}(\mathbb{F}_4^n)$ or $\mathrm{Sym}(\mathbb{F}_4^n)$?
(open since 2000).

Obvious question: $\pi_4(\mathrm{GA}_n(\mathbb{F}_4)) = \mathrm{Alt}(\mathbb{F}_4^n)$ or $\mathrm{Sym}(\mathbb{F}_4^n)$?
(open since 2000).
Finding $F \in \mathrm{GA}_n(\mathbb{F}_4)$ such that $\pi_4(F) \notin \mathrm{Alt}(\mathbb{F}_4^n)$ gives a 1-line proof of $\mathrm{GA}_n(\mathbb{F}_4) \neq \mathrm{TA}_n(\mathbb{F}_4)$.

Obvious question: $\pi_4(\mathrm{GA}_n(\mathbb{F}_4)) = \mathrm{Alt}(\mathbb{F}_4^n)$ or $\mathrm{Sym}(\mathbb{F}_4^n)$? (open since 2000).

Finding $F \in \mathrm{GA}_n(\mathbb{F}_4)$ such that $\pi_4(F) \notin \mathrm{Alt}(\mathbb{F}_4^n)$ gives a 1-line proof of $\mathrm{GA}_n(\mathbb{F}_4) \neq \mathrm{TA}_n(\mathbb{F}_4)$.

Let's try Nagata's automorphism!!!

$$N := (x - 2y\Delta - z\Delta^2, y + z\Delta, z), \quad \Delta = xz + y^2$$

Obvious question: $\pi_4(\mathrm{GA}_n(\mathbb{F}_4)) = \mathrm{Alt}(\mathbb{F}_4^n)$ or $\mathrm{Sym}(\mathbb{F}_4^n)$? (open since 2000).
Finding $F \in \mathrm{GA}_n(\mathbb{F}_4)$ such that $\pi_4(F) \notin \mathrm{Alt}(\mathbb{F}_4^n)$ gives a 1-line proof of $\mathrm{GA}_n(\mathbb{F}_4) \neq \mathrm{TA}_n(\mathbb{F}_4)$.
Let's try Nagata's automorphism!!!

$$N := (x - 2y\Delta - z\Delta^2, y + z\Delta, z), \quad \Delta = xz + y^2$$

AND...

Obvious question: $\pi_4(\mathrm{GA}_n(\mathbb{F}_4)) = \mathrm{Alt}(\mathbb{F}_4^n)$ or $\mathrm{Sym}(\mathbb{F}_4^n)$?
(open since 2000).
Finding $F \in \mathrm{GA}_n(\mathbb{F}_4)$ such that $\pi_4(F) \notin \mathrm{Alt}(\mathbb{F}_4^n)$ gives a 1-line proof of $\mathrm{GA}_n(\mathbb{F}_4) \neq \mathrm{TA}_n(\mathbb{F}_4)$.
Let's try Nagata's automorphism!!!

$$N := (x - 2y\Delta - z\Delta^2, y + z\Delta, z), \quad \Delta = xz + y^2$$

AND... $\pi_4(N)$ even, darn.

Obvious question: $\pi_4(\mathrm{GA}_n(\mathbb{F}_4)) = \mathrm{Alt}(\mathbb{F}_4^n)$ or $\mathrm{Sym}(\mathbb{F}_4^n)$? (open since 2000).
Finding $F \in \mathrm{GA}_n(\mathbb{F}_4)$ such that $\pi_4(F) \notin \mathrm{Alt}(\mathbb{F}_4^n)$ gives a 1-line proof of $\mathrm{GA}_n(\mathbb{F}_4) \neq \mathrm{TA}_n(\mathbb{F}_4)$.
Let's try Nagata's automorphism!!!

$$N := (x - 2y\Delta - z\Delta^2, y + z\Delta, z), \quad \Delta = xz + y^2$$

AND... $\pi_4(N)$ even, darn. Computation: $\pi_{2^m}(N)$ is always even, grrrr!

Obvious question: $\pi_4(\mathrm{GA}_n(\mathbb{F}_4)) = \mathrm{Alt}(\mathbb{F}_4^n)$ or $\mathrm{Sym}(\mathbb{F}_4^n)$? (open since 2000).

Finding $F \in \mathrm{GA}_n(\mathbb{F}_4)$ such that $\pi_4(F) \notin \mathrm{Alt}(\mathbb{F}_4^n)$ gives a 1-line proof of $\mathrm{GA}_n(\mathbb{F}_4) \neq \mathrm{TA}_n(\mathbb{F}_4)$.

Let's try Nagata's automorphism!!!

$$N := (x - 2y\Delta - z\Delta^2, y + z\Delta, z), \quad \Delta = xz + y^2$$

AND... $\pi_4(N)$ even, darn. Computation: $\pi_{2^m}(N)$ is always even, grrrr! All candidate wild examples so far are even over $\mathbb{F}_{2^m}, m > 1$ ...

But perhaps. . .

$\pi_p(N) \in \pi_p(\mathsf{TA}_n(\mathbb{F}_q))$,

but perhaps

$\pi_{p^2}(N) \notin \pi_{p^2}(\mathsf{TA}_n(\mathbb{F}_q))$.

$$
\begin{tikzcd}
 & \mathrm{perm}((\bar{\mathbb{F}}_q)^n) \arrow[d, dashed, two heads] & \\
 & \mathrm{perm}((\mathbb{F}_{q^3})^n) \arrow[dl, two heads] \arrow[d, two heads] \arrow[dr, two heads] & \\
\mathrm{perm}((\mathbb{F}_{q^6})^n) \arrow[d, two heads] \arrow[dr, two heads] & \mathrm{perm}((\mathbb{F}_{q^{10}})^n) \arrow[dl, two heads] \arrow[dr, two heads] & \mathrm{perm}((\mathbb{F}_{q^{15}})^n) \arrow[dl, two heads] \arrow[d, two heads] \\
\mathrm{perm}((\mathbb{F}_{q^2})^n) \arrow[dr, two heads] & \mathrm{perm}((\mathbb{F}_{q^3})^n) \arrow[d, two heads] & \mathrm{perm}((\mathbb{F}_{q^5})^n) \arrow[dl, two heads] \\
 & \mathrm{perm}((\mathbb{F}_q)^n) &
\end{tikzcd}
$$

$$
\begin{tikzcd}
 & \varprojlim_{m\in\mathbb{N}} \pi_{q^m}(\mathsf{GA}_n(\mathbb{F}_q)) \arrow[d, dashed] & \subset \mathrm{perm}(\bar{\mathbb{F}}_q) \\
 & \pi_{q^{30}}(\mathsf{GA}_n(\mathbb{F}_q)) \arrow[dl] \arrow[d] \arrow[dr] & \\
\pi_{q^6}(\mathsf{GA}_n(\mathbb{F}_q)) \arrow[d] \arrow[dr] & \pi_{q^{10}}(\mathsf{GA}_n(\mathbb{F}_q)) \arrow[dl] \arrow[dr] & \pi_{q^{15}}(\mathsf{GA}_n(\mathbb{F}_q)) \arrow[dl] \arrow[d] \\
\pi_{q^2}(\mathsf{GA}_n(\mathbb{F}_q)) \arrow[dr] & \pi_{q^3}(\mathsf{GA}_n(\mathbb{F}_q)) \arrow[d] & \pi_{q^5}(\mathsf{GA}_n(\mathbb{F}_q)) \arrow[dl] \\
 & \pi_{q}(\mathsf{GA}_n(\mathbb{F}_q)) &
\end{tikzcd}
$$

The profinite polynomial automorphism group

$$\left(\varprojlim_{m\in\mathbb{N}} \pi_{q^m}(\mathsf{GA}_n(\mathbb{F}_q))\right) \hookleftarrow \mathsf{GA}_n(\mathbb{F}_q)$$

$$\left(\varprojlim_{m\in\mathbb{N}} \pi_{q^m}(\mathsf{TA}_n(\mathbb{F}_q))\right) \hookleftarrow \mathsf{TA}_n(\mathbb{F}_q)$$

The profinite polynomial automorphism group

$$\left(\varprojlim_{m\in\mathbb{N}} \pi_{q^m}(\mathrm{GA}_n(\mathbb{F}_q))\right) \hookleftarrow \mathrm{GA}_n(\mathbb{F}_q)$$

$$\left(\varprojlim_{m\in\mathbb{N}} \pi_{q^m}(\mathrm{TA}_n(\mathbb{F}_q))\right) \overset{?}{\hookleftarrow} \mathrm{GA}_n(\mathbb{F}_q)$$

The profinite polynomial automorphism group

$$\left(\varprojlim_{m \in \mathbb{N}} \pi_{q^m}(\mathrm{TA}_n(\mathbb{F}_q)) \right) \overset{?}{\hookleftarrow} \mathrm{GA}_n(\mathbb{F}_q)$$

Theorem (M.):

$$N := (X - 2Y\Delta - Z\Delta^2, Y + Z\Delta, Z), \quad \Delta = XZ + Y^2$$

N (and all maps we currently know in $\mathrm{GA}_n(\mathbb{F}_q)$) are in $\varprojlim_{m \in \mathbb{N}} \pi_{q^m}(\mathrm{TA}_n(\mathbb{F}_q))$.

In particular: $\pi_{p^m}(N) \in \pi_{p^m}(\mathrm{TA}_n(\mathbb{F}_p))$ for all m, p.

$$\pi_p : \mathsf{TA}_n(\mathbb{F}_p) \longrightarrow \mathsf{perm}(\mathbb{F}_p^n)$$

$$\pi_p : \mathsf{BA}_n^0(\mathbb{F}_p) \longrightarrow \mathsf{perm}(\mathbb{F}_p^n)$$

Define $\mathcal{B}_n(\mathbb{F}_p) = \pi_p(\mathsf{BA}_n^0(\mathbb{F}_p))$.

$\mathcal{B}_n(\mathbb{F}_p)$ is Sylow-p-group of perm(p^n) !

Strictly upper triangular group

$$\mathrm{BA}_n^0(k) := \{(x_1+f_1, \dots, x_n+f_n \,;\, f_i \in k[x_{i+1}, \dots, x_n]\} < GA_n(k).$$

$$\mathcal{B}_n(\mathbb{F}_p) := \pi_p(\mathrm{BA}_n^0(\mathbb{F}_p))$$

$\mathcal{B}_n(\mathbb{F}_p) < \mathrm{sym}(\mathbb{F}_p^n)$

$\mathcal{B}_n(\mathbb{F}_p)$ is p-sylow subgroup of $\mathrm{sym}(\mathbb{F}_p^n)$

Strictly upper triangular group

$$\mathrm{BA}_n^0(k) := \{(x_1+f_1, \ldots, x_n+f_n\ ;\ f_i \in k[x_{i+1}, \ldots, x_n]\} < GA_n(k).$$

$$\mathcal{B}_n(\mathbb{F}_p) := \pi_p(\mathrm{BA}_n^0(\mathbb{F}_p))$$

$\mathcal{B}_n(\mathbb{F}_p) < \mathrm{sym}(\mathbb{F}_p^n)$

$\mathcal{B}_n(\mathbb{F}_p)$ is p-sylow subgroup of $\mathrm{sym}(\mathbb{F}_p^n)$

$$(x_1 + f_1, \ldots, x_n + f_n) \in \mathcal{B}_n(\mathbb{F}_p)$$

$$f_i \in k[x_{i+1}, \ldots, x_n]/(x_{i+1}^p - x_{i+1}, \ldots, x_n^p - x_n)$$

Conjugacy classes of triangular maps

Hard in general! ($\mathrm{BA}_n^0(k)$ where $\mathrm{kar}(k) = 0$).

Conjugacy classes of triangular maps

Hard in general! ($\mathrm{BA}_n^0(k)$ where $\mathrm{kar}(k) = 0$). Doable if you consider *certain* triangular maps.

Conjugacy classes of triangular maps

Hard in general! ($\mathrm{BA}_n^0(k)$ where $\mathrm{kar}(k) = 0$). Doable if you consider *certain* triangular maps.For example: $f \in \mathrm{BA}_n^0(k)$ where $\mathrm{kar}(k) = p$ and f order p^n, or $\sigma \in \mathcal{B}_n(\mathbb{F}_p)$ where order σ is p^n.

Conjugacy classes of triangular maps

Hard in general! ($\mathrm{BA}_n^0(k)$ where $\mathrm{kar}(k) = 0$). Doable if you consider *certain* triangular maps.For example: $f \in \mathrm{BA}_n^0(k)$ where $\mathrm{kar}(k) = p$ and f order p^n, or $\sigma \in \mathcal{B}_n(\mathbb{F}_p)$ where order σ is p^n.

Interest in these latter maps for some reason - I want to efficiently *iterate* them.

Maps having one orbit only

Theorem 1. (Ostafe)

$$\sigma := (x_1 + f_1, \ldots, x_n + f_n)$$

has one orbit if and only if for each $1 \leq i \leq n$: the coefficient of $(x_{i+1} \cdots x_n)^{p-1}$ of f_i is nonzero.

Maps having one orbit only

Theorem 1. (Ostafe)

$$\sigma := (x_1 + f_1, \ldots, x_n + f_n)$$

has one orbit if and only if for each $1 \leq i \leq n$: the coefficient of $(x_{i+1} \cdots x_n)^{p-1}$ of f_i is nonzero.

Proofsketch. By induction: case $n = 1$ is clear.

Maps having one orbit only

Theorem 1. (Ostafe)

$$\sigma := (x_1 + f_1, \ldots, x_n + f_n)$$

has one orbit if and only if for each $1 \leq i \leq n$: the coefficient of $(x_{i+1} \cdots x_n)^{p-1}$ of f_i is nonzero.

Proofsketch. By induction: case $n = 1$ is clear. So, $\sigma = (x_1 + f_1, \tilde{\sigma})$.

Maps having one orbit only

Theorem 1. (Ostafe)

$$\sigma := (x_1 + f_1, \ldots, x_n + f_n)$$

has one orbit if and only if for each $1 \leq i \leq n$: the coefficient of $(x_{i+1} \cdots x_n)^{p-1}$ of f_i is nonzero.

Proofsketch. By induction: case $n = 1$ is clear. So, $\sigma = (x_1 + f_1, \tilde{\sigma})$. Consider $(c, \alpha) \in \mathbb{F}_p^n$.
$\sigma(c, \alpha) = (c + f_1(\alpha), \sigma(\alpha))$.

Maps having one orbit only

Theorem 1. (Ostafe)

$$\sigma := (x_1 + f_1, \ldots, x_n + f_n)$$

has one orbit if and only if for each $1 \leq i \leq n$: the coefficient of $(x_{i+1} \cdots x_n)^{p-1}$ of f_i is nonzero.

Proofsketch. By induction: case $n = 1$ is clear. So, $\sigma = (x_1 + f_1, \tilde{\sigma})$. Consider $(c, \alpha) \in \mathbb{F}_p^n$.
$\sigma(c, \alpha) = (c + f_1(\alpha), \sigma(\alpha))$. So:

$$\sigma^{p^{n-1}}(c, \alpha) = (c + \sum_{i=1}^{p^{n-1}} f_1(\tilde{\sigma}^i \alpha), \alpha)$$

Maps having one orbit only

Theorem 1. (Ostafe)

$$\sigma := (x_1 + f_1, \ldots, x_n + f_n)$$

has one orbit if and only if for each $1 \leq i \leq n$: the coefficient of $(x_{i+1} \cdots x_n)^{p-1}$ of f_i is nonzero.

Proofsketch. By induction: case $n = 1$ is clear. So, $\sigma = (x_1 + f_1, \tilde{\sigma})$. Consider $(c, \alpha) \in \mathbb{F}_p^n$.
$\sigma(c, \alpha) = (c + f_1(\alpha), \sigma(\alpha))$. So:

$$\sigma^{p^{n-1}}(c, \alpha) = (c + \sum_{i=1}^{p^{n-1}} f_1(\tilde{\sigma}^i \alpha), \alpha)$$

To prove: $\sum_{i=1}^{p^{n-1}} f(\tilde{\sigma}^i \alpha) = 0$ if and only if coefficient of $(x_{i+1} \cdots x_n)^{p-1}$ of f_1 is nonzero.

Maps having one orbit only

Theorem 1.

$$\sigma := (x_1 + f_1, \ldots, x_n + f_n)$$

has one orbit if and only if for each $1 \leq i \leq n$: the coefficient of $(x_{i+1} \cdots x_n)^{p-1}$ of f_i is nonzero.

Proofsketch.

$$\sigma^{p^{n-1}}(c, \alpha) = (c + \sum_{i=1}^{p^{n-1}} f_1(\tilde{\sigma}^i \alpha), \alpha)$$

Maps having one orbit only

Theorem 1.

$$\sigma := (x_1 + f_1, \ldots, x_n + f_n)$$

has one orbit if and only if for each $1 \leq i \leq n$: the coefficient of $(x_{i+1} \cdots x_n)^{p-1}$ of f_i is nonzero.

Proofsketch.

$$\sigma^{p^{n-1}}(c, \alpha) = (c + \sum_{i=1}^{p^{n-1}} f_1(\tilde{\sigma}^i \alpha), \alpha)$$

Lemma

Let $M(x_1, \ldots, x_n) = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$ *where* $0 \leq a_i \leq p-1$ *for each* $1 \leq i \leq n$. *Then* $\sum_{\alpha \in \mathbb{F}_p^n} M(\alpha) = 0$ *unless* $a_1 = a_2 = \ldots = a_n = p-1$, *when it is* $(-1)^n$.

Conjugacy classes in $\mathcal{B}_n(\mathbb{F}_p)$

Theorem 2. Let

$$\sigma := (x_1 + f_1, \ldots, x_n + f_n)$$

have only one orbit. Then representants of the conjugacy classes are the $(p-1)^n$ maps where $f_i = \lambda_i (x_{i+1} \cdots x_n)^{p-1}$.

Proof is very elegant but too long to elaborate on in this talk.

Conjugacy classes in $\mathcal{B}_n(\mathbb{F}_p)$

Theorem 2. Let

$$\sigma := (x_1 + f_1, \ldots, x_n + f_n)$$

have only one orbit. Then representants of the conjugacy classes are the $(p-1)^n$ maps where $f_i = \lambda_i (x_{i+1} \cdots x_n)^{p-1}$.

Conjugacy classes in $\mathcal{B}_n(\mathbb{F}_p)$

Theorem 2. Let

$$\sigma := (x_1 + f_1, \dots, x_n + f_n)$$

have only one orbit. Then representants of the conjugacy classes are the $(p-1)^n$ maps where $f_i = \lambda_i (x_{i+1} \cdots x_n)^{p-1}$.

Theorem 3. After that, conjugating by a diagonal linear map $D \in \mathrm{GL}_n(\mathbb{F}_p)$ one can get all of them equivalent!

Hence, any $\sigma \in \mathcal{B}_n(\mathbb{F}_p)$ having only one orbit can be written as

$$D^{-1}\tau^{-1}\Delta\tau D$$

where $\tau \in \mathcal{B}_n(\mathbb{F}_p)$, D linear diagonal, and Δ is one particular map you choose in $\mathcal{B}_n(\mathbb{F}_p)$.

What is an easy map Δ?

$$\Delta := (x_1 + g_1, \ldots, x_n + g_n)$$

where $g_i(p-1, \ldots, p-1) = 1$ and $g_i(\alpha) = 0$ for any other $\alpha \in \mathbb{F}_p^{n-i}$.

What is an easy map Δ?

$$\Delta := (x_1 + g_1, \ldots, x_n + g_n)$$

where $g_i(p-1, \ldots, p-1) = 1$ and $g_i(\alpha) = 0$ for any other $\alpha \in \mathbb{F}_p^{n-i}$.

Then Δ is very simple:

What is an easy map Δ?

$$\Delta := (x_1 + g_1, \ldots, x_n + g_n)$$

where $g_i(p-1, \ldots, p-1) = 1$ and $g_i(\alpha) = 0$ for any other $\alpha \in \mathbb{F}_p^{n-i}$.

Then Δ is very simple:

Let $\zeta : \mathbb{F}_p^n \longrightarrow \mathbb{Z}/p^n\mathbb{Z}$ be defined as

$$\zeta(a_1, a_2, \ldots, a_n) \longrightarrow a_1 + pa_2 + \ldots + p^{n-1}a_n$$

What is an easy map Δ?

$$\Delta := (x_1 + g_1, \ldots, x_n + g_n)$$

where $g_i(p-1, \ldots, p-1) = 1$ and $g_i(\alpha) = 0$ for any other $\alpha \in \mathbb{F}_p^{n-i}$.

Then Δ is very simple:

Let $\zeta : \mathbb{F}_p^n \longrightarrow \mathbb{Z}/p^n\mathbb{Z}$ be defined as

$$\zeta(a_1, a_2, \ldots, a_n) \longrightarrow a_1 + pa_2 + \ldots + p^{n-1}a_n$$

Then

$$\zeta\Delta\zeta^{-1}(a) = a + 1, a \in \mathbb{Z}/p^n\mathbb{Z}$$

i.e. $\Delta^m(v)$ is just as easy to compute!

What is an easy map Δ?

$$\Delta := (x_1 + g_1, \ldots, x_n + g_n)$$

where $g_i(p-1, \ldots, p-1) = 1$ and $g_i(\alpha) = 0$ for any other $\alpha \in \mathbb{F}_p^{n-i}$.

Then Δ is very simple:

Let $\zeta : \mathbb{F}_p^n \longrightarrow \mathbb{Z}/p^n\mathbb{Z}$ be defined as

$$\zeta(a_1, a_2, \ldots, a_n) \longrightarrow a_1 + pa_2 + \ldots + p^{n-1}a_n$$

Then

$$\zeta\Delta\zeta^{-1}(a) = a + 1, a \in \mathbb{Z}/p^n\mathbb{Z}$$

i.e. $\Delta^m(v)$ is just as easy to compute!

Conclusion: $\sigma \in \mathcal{B}_n(\mathbb{F}_p)$ of max. order: $\sigma(v)$ just as computationally intensive as computing $\sigma^m(v)$!

Just one more slide/ conclusions:

Just one more slide/ conclusions:

THANK YOU

(for enduring 88 .pdf slides. . .)