Polynomial automorphisms over finite fields

Stefan Maubach

March 2010

TOPIC: affine algebraic geometry

TOPIC: affine algebraic geometry

(Subtopic of - no surprises here - algebraic geometry.)

TOPIC: affine algebraic geometry

(Subtopic of - no surprises here - algebraic geometry.)

Objects of study: affine spaces:

X is affine $\iff X = \operatorname{spec} A$ for some ring A.

TOPIC: affine algebraic geometry

(Subtopic of - no surprises here - algebraic geometry.)

Objects of study: affine spaces:

X is affine $\iff X = \operatorname{spec} A$ for some ring A.

Typical affine space: $X = k^n$ where k a field.

TOPIC: affine algebraic geometry

(Subtopic of - no surprises here - algebraic geometry.)

Objects of study: affine spaces:

X is affine $\iff X = \operatorname{spec} A$ for some ring A.

Typical affine space: $X = k^n$ where k a field.

"Generic" algebraic geometry dislikes k^n because it is not compact (contrary to projective geometry).

But hey - k^n is perhaps the most simple algebraic space there is!!

TOPIC: affine algebraic geometry

(Subtopic of - no surprises here - algebraic geometry.)

Objects of study: affine spaces:

X is affine $\iff X = \operatorname{spec} A$ for some ring A.

Typical affine space: $X = k^n$ where k a field.

"Generic" algebraic geometry dislikes k^n because it is not compact (contrary to projective geometry).

But hey - k^n is perhaps the most simple algebraic space there is!!

QUESTION 1: do we understand the algebraic automorphisms of k^n?

Algebraic automorphism of k^n is a polynomial map:

Algebraic automorphism of k^n is a polynomial map: A map $F : k^n \longrightarrow k^n$ given by n polynomials:

$$F = (F_1(X_1, \ldots, X_n), \ldots, F_n(X_1, \ldots, X_n)).$$

Algebraic automorphism of k^n is a polynomial map: A map $F : k^n \longrightarrow k^n$ given by n polynomials:

$$F = (F_1(X_1, \ldots, X_n), \ldots, F_n(X_1, \ldots, X_n)).$$

Example: $F = (X + Y^2, Y)$.

Algebraic automorphism of k^n is a polynomial map: A map $F : k^n \longrightarrow k^n$ given by n polynomials:

$$F = (F_1(X_1, \ldots, X_n), \ldots, F_n(X_1, \ldots, X_n)).$$

Example: $F = (X + Y^2, Y)$.

Various ways of looking at polynomial maps:

Algebraic automorphism of k^n is a polynomial map: A map $F : k^n \longrightarrow k^n$ given by n polynomials:

$$F = (F_1(X_1, \dots, X_n), \dots, F_n(X_1, \dots, X_n)).$$

Example: $F = (X + Y^2, Y)$.

Various ways of looking at polynomial maps:

- A map $k^n \longrightarrow k^n$.

Algebraic automorphism of k^n is a polynomial map: A map $F : k^n \longrightarrow k^n$ given by n polynomials:

$$F = (F_1(X_1, \ldots, X_n), \ldots, F_n(X_1, \ldots, X_n)).$$

Example: $F = (X + Y^2, Y)$.

Various ways of looking at polynomial maps:

- A map $k^n \longrightarrow k^n$.
- A list of n polynomials: $F \in (k[X_1, \ldots, X_n])^n$.

Algebraic automorphism of k^n is a polynomial map: A map $F : k^n \longrightarrow k^n$ given by n polynomials:

$$F = (F_1(X_1, \ldots, X_n), \ldots, F_n(X_1, \ldots, X_n)).$$

Example: $F = (X + Y^2, Y)$.

Various ways of looking at polynomial maps:

- A map $k^n \longrightarrow k^n$.
- A list of n polynomials: $F \in (k[X_1, \ldots, X_n])^n$.
- A ring endomorphism of $k[X_1, \ldots, X_n]$ sending $g(X_1, \ldots, X_n)$ to $g(F_1, \ldots, F_n)$.

A polynomial map F is a polynomial automorphism if there is a polynomial map G such that $F(G) = (X_1, \ldots, X_n)$.

A polynomial map F is a polynomial automorphism if there is a polynomial map G such that $F(G) = (X_1, \ldots, X_n)$.
Example: $(X + Y^2, Y)$ has inverse $(X - Y^2, Y)$.

A polynomial map F is a polynomial automorphism if there is a polynomial map G such that $F(G) = (X_1, \ldots, X_n)$.
Example: $(X + Y^2, Y)$ has inverse $(X - Y^2, Y)$.

$$\begin{aligned}(X + Y^2, Y) \circ (X - Y^2, Y) = & \; ([X - Y^2] + [Y]^2, [Y]) \\ = & \; (X - Y^2 + Y^2, Y) \\ = & \; (X, Y).\end{aligned}$$

A polynomial map F is a polynomial automorphism if there is a polynomial map G such that $F(G) = (X_1, \ldots, X_n)$.
Example: $(X + Y^2, Y)$ has inverse $(X - Y^2, Y)$.

$$\begin{aligned}(X + Y^2, Y) \circ (X - Y^2, Y) &= ([X - Y^2] + [Y]^2, [Y]) \\ &= (X - Y^2 + Y^2, Y) \\ &= (X, Y).\end{aligned}$$

$(X^p, Y) : \mathbb{F}_p^2 \longrightarrow \mathbb{F}_p^2$ is not a polynomial automorphism, even though it induces a bijection of $\mathbb{F}_p$!

A polynomial map F is a polynomial automorphism if there is a polynomial map G such that $F(G) = (X_1, \ldots, X_n)$.
Example: $(X + Y^2, Y)$ has inverse $(X - Y^2, Y)$.

$$
\begin{aligned}
(X + Y^2, Y) \circ (X - Y^2, Y) &= ([X - Y^2] + [Y]^2, [Y]) \\
&= (X - Y^2 + Y^2, Y) \\
&= (X, Y).
\end{aligned}
$$

$(X^p, Y) : \mathbb{F}_p^2 \longrightarrow \mathbb{F}_p^2$ is not a polynomial automorphism, even though it induces a bijection of $\mathbb{F}_p$!
$(X^3, Y) : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ is not a polynomial automorphism, even though it induces a bijection of $\mathbb{R}$!

A polynomial map F is a polynomial automorphism if there is a polynomial map G such that $F(G) = (X_1, \ldots, X_n)$.
Example: $(X + Y^2, Y)$ has inverse $(X - Y^2, Y)$.

$$\begin{aligned}(X + Y^2, Y) \circ (X - Y^2, Y) &= ([X - Y^2] + [Y]^2, [Y]) \\ &= (X - Y^2 + Y^2, Y) \\ &= (X, Y).\end{aligned}$$

$(X^p, Y) : \mathbb{F}_p^2 \longrightarrow \mathbb{F}_p^2$ is not a polynomial automorphism, even though it induces a bijection of $\mathbb{F}_p$!
$(X^3, Y) : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ is not a polynomial automorphism, even though it induces a bijection of $\mathbb{R}$!
Remark: If k is algebraically closed, then a polynomial endomorphism $k^n \longrightarrow k^n$ which is a bijection, is an invertible polynomial map.

Polynomial automorphisms form a group, denoted by $\mathrm{GA}_n(k)$.

Notations:

	Linear	Polynomial
All	$ML_n(k)$	$MA_n(k)$
Invertible	$GL_n(k)$	$GA_n(k)$

Motivation: why over $\mathbb{F}_p$?

- Reduction-mod-p techniques to (dis)prove things
  (Example: F injective $\longrightarrow$ F surjective.)
  (Example: Belov-Kontsevich)
- Possible applications (cryptography etc.)
- Simply because it is interesting:
  1. Connections with discrete mathematics.
  2. Connections with finite group theory.

Jacobian Conjecture

If F is invertible and G inverse of F, then

Jacobian Conjecture

If F is invertible and G inverse of F, then

$$\mathrm{Jac}(I) = \mathrm{Jac}(G \circ (F)) = \mathrm{Jac}(F) \cdot (\mathrm{Jac}(G) \circ F)$$

Jacobian Conjecture

If F is invertible and G inverse of F, then

$$\mathrm{Jac}(I) = \mathrm{Jac}(G \circ (F)) = \mathrm{Jac}(F) \cdot (\mathrm{Jac}(G) \circ F)$$
$$1 = \det(\mathrm{Jac}(I)) = \det \mathrm{Jac}(G \circ (F)) = \det \mathrm{Jac}(F) \cdot \det(\mathrm{Jac}(G) \circ F)$$

Jacobian Conjecture

If F is invertible and G inverse of F, then

$$\mathrm{Jac}(I) = \mathrm{Jac}(G \circ (F)) = \mathrm{Jac}(F) \cdot (\mathrm{Jac}(G) \circ F)$$
$$1 = \det(\mathrm{Jac}(I)) = \det \mathrm{Jac}(G \circ (F)) = \det \mathrm{Jac}(F) \cdot \det(\mathrm{Jac}(G) \circ F)$$

hence $\det(J(F)) \in k[X_1, \ldots, X_n]^* = k^*$.

Jacobian Conjecture

If F is invertible and G inverse of F, then

$$\mathrm{Jac}(I) = \mathrm{Jac}(G \circ (F)) = \mathrm{Jac}(F) \cdot (\mathrm{Jac}(G) \circ F)$$
$$1 = \det(\mathrm{Jac}(I)) = \det \mathrm{Jac}(G \circ (F)) = \det \mathrm{Jac}(F) \cdot \det(\mathrm{Jac}(G) \circ F)$$

hence $\det(J(F)) \in k[X_1, \ldots, X_n]^* = k^*$.

QUESTION: if F polynomial endomorphism, and $\det(\mathrm{Jac}(F)) \in k^*$, is F invertible?

Jacobian Conjecture

LEMMA: If F is invertible, then $\det(J(F)) \in k^*$.

JACOBIAN CONJECTURE: $char(k) = 0$. If F polynomial endomorphism, and $\det(\text{Jac}(F)) \in k^*$, is F invertible?

Jacobian Conjecture

LEMMA: If F is invertible, then $\det(J(F)) \in k^*$.

JACOBIAN CONJECTURE: $char(k) = 0$. If F polynomial endomorphism, and $\det(\mathrm{Jac}(F)) \in k^*$, is F invertible?

In $char(k) = p$: $F : X \longrightarrow X - X^p$ has $\det(\mathrm{Jac}(F)) = 1$ but $F(0) = F(1)$.

Jacobian Conjecture

LEMMA: If F is invertible, then $\det(J(F)) \in k^*$.

JACOBIAN CONJECTURE: in $char(k) = p$. If F polynomial endomorphism, and

(1) $\det(\mathrm{Jac}(F)) \in k^*$

Jacobian Conjecture

LEMMA: If F is invertible, then $\det(J(F)) \in k^*$.

JACOBIAN CONJECTURE: in $char(k) = p$. If F polynomial endomorphism, and

(1) $\det(\mathrm{Jac}(F)) \in k^*$

(2) $p \not| \, [k(X_1, \ldots, X_n) : k(F_1, \ldots, F_n)]$,

is F invertible?

Jacobian Conjecture

LEMMA: If F is invertible, then $\det(J(F)) \in k^*$.

JACOBIAN CONJECTURE: in $char(k) = p$. If F polynomial endomorphism, and

(1) $\det(\mathrm{Jac}(F)) \in k^*$

(2) $p \not| [k(X_1, \ldots, X_n) : k(F_1, \ldots, F_n)]$,

is F invertible?

$F : (X, Y) \longrightarrow (X + X^p, Y)$:

$[k(X, Y) : k(X + X^p, Y)] = p$.

$char(k) = 0:$

$F = (X + a_1X^2 + a_2XY + a_3Y^2, Y + b_1X^2 + b_2XY + b_3Y^2)$

$$\begin{aligned} 1 = &\ \det(Jac(F)) \\ = &\ 1+ \\ &(2a_1 + b_2)X+ \\ &(a_2 + 2b_3)Y+ \\ &(2a_1b_2 + 2a_2b_1)X^2+ \\ &(2b_2a_2 + 4a_1b_3 + 4a_3b_1)XY+ \\ &(2a_2b_3 + 2a_3b_2)Y^2 \end{aligned}$$

In char(k)=2 : (parts of) equations vanish. What are the right equations in char(k)=2(p)?

The Automorphism Group

(This whole talk: $n \geq 2$)

$GL_n(k)$ is generated by

The Automorphism Group

(This whole talk: $n \geq 2$)

$GL_n(k)$ is generated by

- Permutations $X_1 \longleftrightarrow X_i$

The Automorphism Group

(This whole talk: $n \geq 2$)

$GL_n(k)$ is generated by

- Permutations $X_1 \longleftrightarrow X_i$
- Map $(aX_1 + bX_j, X_2, \ldots, X_n)$ $(a \in k^*, b \in k)$

The Automorphism Group

(This whole talk: $n \geq 2$)

$GL_n(k)$ is generated by

- Permutations $X_1 \longleftrightarrow X_i$
- Map $(aX_1 + bX_j, X_2, \ldots, X_n)$ $(a \in k^*, b \in k)$

$GA_n(k)$ is generated by ???

Elementary map: $(X_1 + f(X_2, \ldots, X_n), X_2, \ldots, X_n)$, invertible with inverse

$$(X_1 - f(X_2, \ldots, X_n), X_2, \ldots, X_n).$$

Elementary map: $(X_1 + f(X_2, \ldots, X_n), X_2, \ldots, X_n)$, invertible with inverse

$$(X_1 - f(X_2, \ldots, X_n), X_2, \ldots, X_n).$$

Triangular map: $(X + f(Y, Z), Y + g(Z), Z + c)$

$$= (X, Y, Z + c)(X, Y + g(Z), Z)(X + f(X, Y), Y, Z)$$

Elementary map: $(X_1 + f(X_2, \ldots, X_n), X_2, \ldots, X_n)$,
invertible with inverse

$(X_1 - f(X_2, \ldots, X_n), X_2, \ldots, X_n)$.
Triangular map: $(X + f(Y, Z), Y + g(Z), Z + c)$

$= (X, Y, Z + c)(X, Y + g(Z), Z)(X + f(X, Y), Y, Z)$
$J_n(k) :=$ set of triangular maps.

Elementary map: $(X_1 + f(X_2, \ldots, X_n), X_2, \ldots, X_n)$,
invertible with inverse

$$(X_1 - f(X_2, \ldots, X_n), X_2, \ldots, X_n).$$

Triangular map: $(X + f(Y, Z), Y + g(Z), Z + c)$

$$= (X, Y, Z + c)(X, Y + g(Z), Z)(X + f(X, Y), Y, Z)$$

$J_n(k)$:= set of triangular maps.

$Aff_n(k)$:= set of compositions of invertible linear maps and translations.

Elementary map: $(X_1 + f(X_2, \ldots, X_n), X_2, \ldots, X_n)$, invertible with inverse

$$(X_1 - f(X_2, \ldots, X_n), X_2, \ldots, X_n).$$

Triangular map: $(X + f(Y, Z), Y + g(Z), Z + c)$

$$= (X, Y, Z + c)(X, Y + g(Z), Z)(X + f(X, Y), Y, Z)$$

$J_n(k)$:= set of triangular maps.

$Aff_n(k)$:= set of compositions of invertible linear maps and translations.

$TA_n(k) := < J_n(k), Aff_n(k) >$

In dimension 1: we understand the automorphism group.

(They are linear.)

In dimension 1: we understand the automorphism group. (They are linear.)
In dimension 2: famous Jung-van der Kulk-theorem:

$$\mathrm{GA}_2(\mathbb{K}) = \mathrm{TA}_2(\mathbb{K}) = \mathit{Aff}_2(\mathbb{K}) \ltimes \mathrm{J}_2(\mathbb{K})$$

Jung-van der Kulk is the reason that we can do a lot in dimension 2 !!!!

What about dimension 3?

What about dimension 3? Stupid idea: everything will be tame?

What about dimension 3? Stupid idea: everything will be tame?

1972: Nagata: "I cannot tame the following map:"

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

What about dimension 3? Stupid idea: everything will be tame?

1972: Nagata: “I cannot tame the following map:”

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

Nagata’s map is the historically most important map for polynomial automorphisms. It is a very elegant but complicated map.

What about dimension 3? Stupid idea: everything will be tame?

1972: Nagata: "I cannot tame the following map:"

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

Nagata's map is the historically most important map for polynomial automorphisms. It is a very elegant but complicated map.

AMAZING result: Umirbaev-Shestakov (2004)

N is not tame!!

What about dimension 3? Stupid idea: everything will be tame?

1972: Nagata: "I cannot tame the following map:"

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

Nagata's map is the historically most important map for polynomial automorphisms. It is a very elegant but complicated map.

AMAZING result: Umirbaev-Shestakov (2004)

N is not tame!!

(Difficult and technical proof.) (2007 AMS Moore paper award.)

What about dimension 3? Stupid idea: everything will be tame?

1972: Nagata: "I cannot tame the following map:"

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

Nagata's map is the historically most important map for polynomial automorphisms. It is a very elegant but complicated map.

AMAZING result: Umirbaev-Shestakov (2004)

N is not tame!! . . . in characteristic ZERO. . .

(Difficult and technical proof.) (2007 AMS Moore paper award.)

How did Nagata make Nagata's map?

How did Nagata make Nagata's map?

Study maps over $k[z, z^{-1}]$:

How did Nagata make Nagata's map?

Study maps over $k[z, z^{-1}]$:

$$(X, Y + z^2 X)$$

How did Nagata make Nagata's map?

Study maps over $k[z, z^{-1}]$:

$$(X - z^{-1}Y^2, Y)(X, Y + z^2X)(X + z^{-1}Y^2, Y)$$

How did Nagata make Nagata's map?

Study maps over $k[z, z^{-1}]$:

$$(X - z^{-1}Y^2, Y)(X, Y + z^2X)(X + z^{-1}Y^2, Y)$$
$$= (X - 2(Xz + Y^2)Y - (Xz + Y^2)^2 z, Y + (Xz + Y^2)z)$$

How did Nagata make Nagata's map?

Study maps over $k[z, z^{-1}]$:

$$(X - z^{-1}Y^2, Y)(X, Y + z^2X)(X + z^{-1}Y^2, Y)$$
$$= (X - 2(Xz + Y^2)Y - (Xz + Y^2)^2 z, Y + (Xz + Y^2)z)$$

Thus: N is tame over $k[z, z^{-1}]$, i.e. N in $\mathrm{TA}_2(k[z, z^{-1}])$.

How did Nagata make Nagata's map?

Study maps over $k[z, z^{-1}]$:

$$(X - z^{-1}Y^2, Y)(X, Y + z^2X)(X + z^{-1}Y^2, Y)$$
$$= (X - 2(Xz + Y^2)Y - (Xz + Y^2)^2 z, Y + (Xz + Y^2)z)$$

Thus: N is tame over $k[z, z^{-1}]$, i.e. N in $\mathrm{TA}_2(k[z, z^{-1}])$.

Nagata proved: N is NOT tame over $k[z]$, i.e. N not in $\mathrm{TA}_2(k[z])$.

What about $\mathrm{TA}_n(k) \subseteq \mathrm{GA}_n(k)$ if $k = \mathbb{F}_q$ is a finite field?

What about $\mathsf{TA}_n(k) \subseteq \mathsf{GA}_n(k)$ if $k = \mathbb{F}_q$ is a finite field?
Denote $\mathsf{Bij}_n(\mathbb{F}_q)$ as set of bijections on $\mathbb{F}_q^n$. We have a natural map
$\mathsf{GA}_n(\mathbb{F}_q) \xrightarrow{\pi} \mathsf{Bij}_n(\mathbb{F}_q)$.

What about $\mathrm{TA}_n(k) \subseteq \mathrm{GA}_n(k)$ if $k = \mathbb{F}_q$ is a finite field?
Denote $\mathrm{Bij}_n(\mathbb{F}_q)$ as set of bijections on $\mathbb{F}_q^n$. We have a natural map
$\mathrm{GA}_n(\mathbb{F}_q) \xrightarrow{\pi} \mathrm{Bij}_n(\mathbb{F}_q)$.
What is $\pi(\mathrm{GA}_n(\mathbb{F}_q))$? Can we make every bijection on $\mathbb{F}_q^n$ as an *invertible* polynomial map?

What about $\mathrm{TA}_n(k) \subseteq \mathrm{GA}_n(k)$ if $k = \mathbb{F}_q$ is a finite field?

Denote $\mathrm{Bij}_n(\mathbb{F}_q)$ as set of bijections on $\mathbb{F}_q^n$. We have a natural map

$\mathrm{GA}_n(\mathbb{F}_q) \xrightarrow{\pi} \mathrm{Bij}_n(\mathbb{F}_q)$.

What is $\pi(\mathrm{GA}_n(\mathbb{F}_q))$? Can we make every bijection on $\mathbb{F}_q^n$ as an *invertible* polynomial map?

Simpler question: what is $\pi(\mathrm{TA}_n(\mathbb{F}_q))$?

Why simpler? Because we have a set of generators!

Question: what is $\pi(\mathrm{TA}_n(\mathbb{F}_q))$?

See $\mathrm{Bij}_n(\mathbb{F}_q)$ as $\mathrm{Sym}(q^n)$.

Question: what is $\pi(\mathsf{TA}_n(\mathbb{F}_q))$?

See $\mathsf{Bij}_n(\mathbb{F}_q)$ as $\mathsf{Sym}(q^n)$.

$\mathsf{TA}_n(\mathbb{F}_q) =< \mathrm{GL_n(\mathbb{F}_q)}, \sigma_{\mathrm{f}} >$ where f runs over $\mathbb{F}_q[X_2, \ldots, X_n]$ and $\sigma_f := (X_1 + f, X_2, \ldots, X_n)$.

Question: what is $\pi(\mathsf{TA}_n(\mathbb{F}_q))$?

See $\mathsf{Bij}_n(\mathbb{F}_q)$ as $\mathsf{Sym}(q^n)$.

$\mathsf{TA}_n(\mathbb{F}_q) =< \mathrm{GL_n(\mathbb{F}_q)}, \sigma_\mathrm{f} >$ where f runs over $\mathbb{F}_q[X_2, \dots, X_n]$ and $\sigma_f := (X_1 + f, X_2, \dots, X_n)$.

We make finite subset $\mathcal{S} \subset \mathbb{F}_q[X_2, \dots, X_n]$ and define

$$\mathcal{G} :=< \mathrm{GL_n(\mathbb{F}_q)}, \sigma_\mathrm{f} \ ; \ \mathrm{f} \in \mathcal{S} >$$

such that

$$\pi(\mathsf{TA}_n(\mathbb{F}_q)) = \pi(\mathcal{G}).$$

Question: what is $\pi(T_n(\mathbb{F}_q))$?

Question: what is $\pi(T_n(\mathbb{F}_q))$?

(1) $\pi(T_n(\mathbb{F}_q)) = \pi(\mathcal{G})$ is 2-transitive, hence primitive.

Question: what is $\pi(T_n(\mathbb{F}_q))$?

(1) $\pi(T_n(\mathbb{F}_q)) = \pi(\mathcal{G})$ is 2-transitive, hence primitive.

You might know: if $H < \mathrm{Sym}(m)$ is primitive + a 2-cycle then $H = \mathrm{Sym}(m)$.

Question: what is $\pi(T_n(\mathbb{F}_q))$?

(1) $\pi(T_n(\mathbb{F}_q)) = \pi(\mathcal{G})$ is 2-transitive, hence primitive.

You might know: if $H < \mathrm{Sym}(m)$ is primitive + a 2-cycle then $H = \mathrm{Sym}(m)$.

If $q = 2$ or q odd, then indeed we find a 2-cycle!

Question: what is $\pi(T_n(\mathbb{F}_q))$?

(1) $\pi(T_n(\mathbb{F}_q)) = \pi(\mathcal{G})$ is 2-transitive, hence primitive.

You might know: if $H < \mathrm{Sym}(m)$ is primitive + a 2-cycle then $H = \mathrm{Sym}(m)$.

If $q = 2$ or q odd, then indeed we find a 2-cycle!

Hence if $q = 2$ or $q = \text{odd}$, then $\pi(T_n(\mathbb{F}_q)) = \mathrm{Sym}(q^n)$.

Question: what is $\pi(T_n(\mathbb{F}_q))$?

Answer: if $q = 2$ or $q =$ odd, then $\pi(T_n(\mathbb{F}_q)) = \mathrm{Sym}(q^n)$.

Question: what is $\pi(T_n(\mathbb{F}_q))$?

Answer: if $q = 2$ or $q = \text{odd}$, then $\pi(T_n(\mathbb{F}_q)) = \text{Sym}(q^n)$.

If $q = 4, 8, 16, \ldots$ we don't succeed to find a 2-cycle.

Question: what is $\pi(T_n(\mathbb{F}_q))$?

Answer: if $q = 2$ or $q =$ odd, then $\pi(T_n(\mathbb{F}_q)) = \mathrm{Sym}(q^n)$.

If $q = 4, 8, 16, \ldots$ we don't succeed to find a 2-cycle. In fact- all generators of $\mathrm{TA}_n(\mathbb{F}_q)$ turn out to be even, i.e. $\pi(\mathrm{TA}_n(\mathbb{F}_q)) \subseteq \mathrm{Alt}(q^n)$!

But: there's another theorem:

Theorem: $H < \mathrm{Sym}(m)$ Primitive $+$ 3-cycle $\longrightarrow$ $H = \mathrm{Alt}(m)$ or $H = \mathrm{Sym}(m)$.

Question: what is $\pi(T_n(\mathbb{F}_q))$?

Answer: if $q = 2$ or $q =$ odd, then $\pi(T_n(\mathbb{F}_q)) = \mathrm{Sym}(q^n)$.

If $q = 4, 8, 16, \ldots$ we don't succeed to find a 2-cycle. In fact- all generators of $\mathrm{TA}_n(\mathbb{F}_q)$ turn out to be even, i.e. $\pi(\mathrm{TA}_n(\mathbb{F}_q)) \subseteq \mathrm{Alt}(q^n)$!

But: there's another theorem:

Theorem: $H < \mathrm{Sym}(m)$ Primitive + 3-cycle $\longrightarrow H = \mathrm{Alt}(m)$ or $H = \mathrm{Sym}(m)$.

We find a 3-cycle!

Question: what is $\pi(T_n(\mathbb{F}_q))$?

Answer: if $q = 2$ or $q =$ odd, then $\pi(T_n(\mathbb{F}_q)) = \mathrm{Sym}(q^n)$.

If $q = 4, 8, 16, \ldots$ we don't succeed to find a 2-cycle. In fact- all generators of $\mathrm{TA}_n(\mathbb{F}_q)$ turn out to be even, i.e. $\pi(\mathrm{TA}_n(\mathbb{F}_q)) \subseteq \mathrm{Alt}(q^n)$!

But: there's another theorem:

Theorem: $H < \mathrm{Sym}(m)$ Primitive + 3-cycle $\longrightarrow H = \mathrm{Alt}(m)$ or $H = \mathrm{Sym}(m)$.

We find a 3-cycle!

Hence, if $q = 4, 8, 16, \ldots$ then $\pi(T_n(\mathbb{F}_q)) = \mathrm{Alt}(m)$!

Question: what is $\pi(T_n(\mathbb{F}_q))$?

Answer: if $q = 2$ or $q =$ odd, then $\pi(T_n(\mathbb{F}_q)) = \mathrm{Sym}(q^n)$.

Answer: if $q = 4, 8, 16, 32, \ldots$ then $\pi(T_n(\mathbb{F}_q)) = \mathrm{Alt}(q^n)$.

Suppose $F \in \mathrm{GA}_n(\mathbb{F}_4)$ such that $\pi(F)$ odd permutation, then $\pi(F) \notin \pi(\mathrm{TA}_n(\mathbb{F}_4))$, so $\mathrm{GA}_n(\mathbb{F}_4) \neq \mathrm{TA}_n(\mathbb{F}_4)$!

Question: what is $\pi(T_n(\mathbb{F}_q))$?

Answer: if $q = 2$ or $q =$ odd, then $\pi(T_n(\mathbb{F}_q)) = \mathrm{Sym}(q^n)$.

Answer: if $q = 4, 8, 16, 32, \ldots$ then $\pi(T_n(\mathbb{F}_q)) = \mathrm{Alt}(q^n)$.

Suppose $F \in \mathrm{GA}_n(\mathbb{F}_4)$ such that $\pi(F)$ odd permutation, then $\pi(F) \notin \pi(\mathrm{TA}_n(\mathbb{F}_4))$, so $\mathrm{GA}_n(\mathbb{F}_4) \neq \mathrm{TA}_n(\mathbb{F}_4)$!

So: Start looking for an odd automorphism!!! (Or prove they don't exist)

Question: what is $\pi(T_n(\mathbb{F}_q))$?

Answer: if $q = 2$ or $q =$ odd, then $\pi(T_n(\mathbb{F}_q)) = \mathrm{Sym}(q^n)$.

Answer: if $q = 4, 8, 16, 32, \ldots$ then $\pi(T_n(\mathbb{F}_q)) = \mathrm{Alt}(q^n)$.

Question: what is $\pi(T_n(\mathbb{F}_q))$?

Answer: if $q = 2$ or $q =$ odd, then $\pi(T_n(\mathbb{F}_q)) = \mathrm{Sym}(q^n)$.

Answer: if $q = 4, 8, 16, 32, \ldots$ then $\pi(T_n(\mathbb{F}_q)) = \mathrm{Alt}(q^n)$.

Problem: Do there exist "odd" polynomial automorphisms over $\mathbb{F}_4$?

Question: what is $\pi(T_n(\mathbb{F}_q))$?

Answer: if $q = 2$ or $q = $ odd, then $\pi(T_n(\mathbb{F}_q)) = \mathrm{Sym}(q^n)$.

Answer: if $q = 4, 8, 16, 32, \ldots$ then $\pi(T_n(\mathbb{F}_q)) = \mathrm{Alt}(q^n)$.

Problem: Do there exist "odd" polynomial automorphisms over $\mathbb{F}_4$? Exciting! Let's try Nagata!

Question: what is $\pi(T_n(\mathbb{F}_q))$?

Answer: if $q = 2$ or $q =$ odd, then $\pi(T_n(\mathbb{F}_q)) = \mathrm{Sym}(q^n)$.

Answer: if $q = 4, 8, 16, 32, \ldots$ then $\pi(T_n(\mathbb{F}_q)) = \mathrm{Alt}(q^n)$.

Problem: Do there exist "odd" polynomial automorphisms over $\mathbb{F}_4$? Exciting! Let's try Nagata!

$$N = \begin{pmatrix} X - 2(XZ + Y^2)Y - (XZ + Y^2)^2 Z, \\ Y + (XZ + Y^2)Z, \\ Z \end{pmatrix}$$

Question: what is $\pi(T_n(\mathbb{F}_q))$?

Answer: if $q = 2$ or $q =$ odd, then $\pi(T_n(\mathbb{F}_q)) = \mathrm{Sym}(q^n)$.

Answer: if $q = 4, 8, 16, 32, \ldots$ then $\pi(T_n(\mathbb{F}_q)) = \mathrm{Alt}(q^n)$.

Problem: Do there exist "odd" polynomial automorphisms over $\mathbb{F}_4$? Exciting! Let's try Nagata!

$$N = \begin{pmatrix} X + X^2Z^3 + Y^4Z, \\ Y + XZ^2 + Y^2Z, \\ Z \end{pmatrix}$$

Question: what is $\pi(T_n(\mathbb{F}_q))$?

Answer: if $q = 2$ or $q =$ odd, then $\pi(T_n(\mathbb{F}_q)) = \mathrm{Sym}(q^n)$.

Answer: if $q = 4, 8, 16, 32, \ldots$ then $\pi(T_n(\mathbb{F}_q)) = \mathrm{Alt}(q^n)$.

Problem: Do there exist "odd" polynomial automorphisms over $\mathbb{F}_4$? Exciting! Let's try Nagata!

$$N = \begin{pmatrix} X + X^2Z^3 + Y^4Z, \\ Y + XZ^2 + Y^2Z, \\ Z \end{pmatrix}$$

$N^2 = I$.

Question: what is $\pi(T_n(\mathbb{F}_q))$?

Answer: if $q = 2$ or $q =$ odd, then $\pi(T_n(\mathbb{F}_q)) = \mathrm{Sym}(q^n)$.

Answer: if $q = 4, 8, 16, 32, \ldots$ then $\pi(T_n(\mathbb{F}_q)) = \mathrm{Alt}(q^n)$.

Problem: Do there exist "odd" polynomial automorphisms over $\mathbb{F}_4$? Exciting! Let's try Nagata!

$$N = \begin{pmatrix} X + X^2Z^3 + Y^4Z, \\ Y + XZ^2 + Y^2Z, \\ Z \end{pmatrix}$$

$N^2 = I$. N does not act on $Fix(N)$. This set is $\{(x, y, z) \mid x^2z^3 + y^4z = xz^2 + y^2z = 0\}$.

Question: what is $\pi(T_n(\mathbb{F}_q))$?

Answer: if $q = 2$ or $q =$ odd, then $\pi(T_n(\mathbb{F}_q)) = \mathrm{Sym}(q^n)$.

Answer: if $q = 4, 8, 16, 32, \ldots$ then $\pi(T_n(\mathbb{F}_q)) = \mathrm{Alt}(q^n)$.

Problem: Do there exist "odd" polynomial automorphisms over $\mathbb{F}_4$? Exciting! Let's try Nagata!

$$N = \begin{pmatrix} X + X^2Z^3 + Y^4Z, \\ Y + XZ^2 + Y^2Z, \\ Z \end{pmatrix}$$

$N^2 = I$. N does not act on $Fix(N)$. This set is $\{(x, y, z) \mid z = 0 \text{ or } x^2z^2 + y^4 = xz + y^2 = 0\}$.

Question: what is $\pi(T_n(\mathbb{F}_q))$?

Answer: if $q = 2$ or $q =$ odd, then $\pi(T_n(\mathbb{F}_q)) = \mathrm{Sym}(q^n)$.

Answer: if $q = 4, 8, 16, 32, \ldots$ then $\pi(T_n(\mathbb{F}_q)) = \mathrm{Alt}(q^n)$.

Problem: Do there exist "odd" polynomial automorphisms over $\mathbb{F}_4$? Exciting! Let's try Nagata!

$$N = \begin{pmatrix} X + X^2Z^3 + Y^4Z, \\ Y + XZ^2 + Y^2Z, \\ Z \end{pmatrix}$$

$N^2 = I$. N does not act on $Fix(N)$. This set is $\{(x, y, z) \mid z = 0 \text{ or } x = z^{-1}y^2\}$

Question: what is $\pi(T_n(\mathbb{F}_q))$?

Answer: if $q = 2$ or $q = \text{odd}$, then $\pi(T_n(\mathbb{F}_q)) = \mathrm{Sym}(q^n)$.

Answer: if $q = 4, 8, 16, 32, \ldots$ then $\pi(T_n(\mathbb{F}_q)) = \mathrm{Alt}(q^n)$.

Problem: Do there exist "odd" polynomial automorphisms over $\mathbb{F}_4$? Exciting! Let's try Nagata!

$$N = \begin{pmatrix} X + X^2Z^3 + Y^4Z, \\ Y + XZ^2 + Y^2Z, \\ Z \end{pmatrix}$$

$N^2 = I$. N does not act on $Fix(N)$. This set is $\#\{(x, y, z) \mid z = 0 \text{ or } x = z^{-1}y^2\}$

Question: what is $\pi(T_n(\mathbb{F}_q))$?

Answer: if $q = 2$ or $q =$ odd, then $\pi(T_n(\mathbb{F}_q)) = \mathrm{Sym}(q^n)$.

Answer: if $q = 4, 8, 16, 32, \ldots$ then $\pi(T_n(\mathbb{F}_q)) = \mathrm{Alt}(q^n)$.

Problem: Do there exist "odd" polynomial automorphisms over $\mathbb{F}_4$? Exciting! Let's try Nagata!

$$N = \begin{pmatrix} X + X^2Z^3 + Y^4Z, \\ Y + XZ^2 + Y^2Z, \\ Z \end{pmatrix}$$

$N^2 = I$. N does not act on $Fix(N)$. This set is $\#\{(x, y, z) \mid z = 0 \text{ or } x = z^{-1}y^2\} = q^2 + (q-1)q$

Question: what is $\pi(T_n(\mathbb{F}_q))$?

Answer: if $q = 2$ or $q =$ odd, then $\pi(T_n(\mathbb{F}_q)) = \mathrm{Sym}(q^n)$.

Answer: if $q = 4, 8, 16, 32, \ldots$ then $\pi(T_n(\mathbb{F}_q)) = \mathrm{Alt}(q^n)$.

Problem: Do there exist "odd" polynomial automorphisms over $\mathbb{F}_4$? Exciting! Let's try Nagata!

$$N = \begin{pmatrix} X + X^2Z^3 + Y^4Z, \\ Y + XZ^2 + Y^2Z, \\ Z \end{pmatrix}$$

$N^2 = I$. N does not act on $Fix(N)$. This set is
$\#\{(x, y, z) \mid z = 0 \text{ or } x = z^{-1}y^2\} = q^2 + (q-1)q$
$= q(2q-1)$.

Question: what is $\pi(T_n(\mathbb{F}_q))$?

Answer: if $q = 2$ or $q =$ odd, then $\pi(T_n(\mathbb{F}_q)) = \mathrm{Sym}(q^n)$.

Answer: if $q = 4, 8, 16, 32, \ldots$ then $\pi(T_n(\mathbb{F}_q)) = \mathrm{Alt}(q^n)$.

Problem: Do there exist "odd" polynomial automorphisms over $\mathbb{F}_4$? Exciting! Let's try Nagata!

$$N = \begin{pmatrix} X + X^2Z^3 + Y^4Z, \\ Y + XZ^2 + Y^2Z, \\ Z \end{pmatrix}$$

$N^2 = I$. N does not act on $Fix(N)$. This set is $\#\{(x, y, z) \mid z = 0 \text{ or } x = z^{-1}y^2\} = q^2 + (q-1)q$ $= q(2q-1)$. Hence, N exchanges $q^3 - q(2q-1)$ elements - that means $\frac{q^3-q(2q-1)}{2}$ 2-cycles.

Question: what is $\pi(T_n(\mathbb{F}_q))$?

Answer: if $q = 2$ or $q =$ odd, then $\pi(T_n(\mathbb{F}_q)) = \mathrm{Sym}(q^n)$.

Answer: if $q = 4, 8, 16, 32, \ldots$ then $\pi(T_n(\mathbb{F}_q)) = \mathrm{Alt}(q^n)$.

Problem: Do there exist "odd" polynomial automorphisms over $\mathbb{F}_4$? Exciting! Let's try Nagata!

$$N = \begin{pmatrix} X + X^2Z^3 + Y^4Z, \\ Y + XZ^2 + Y^2Z, \\ Z \end{pmatrix}$$

$N^2 = I$. N does not act on $Fix(N)$. This set is $\#\{(x, y, z) \mid z = 0 \text{ or } x = z^{-1}y^2\} = q^2 + (q-1)q$ $= q(2q-1)$. Hence, N exchanges $q^3 - q(2q-1)$ elements - that means $\frac{q^3 - q(2q-1)}{2}$ 2-cycles. Which is odd $\Longleftrightarrow$ q odd or $q = 2 \ldots$

Question: what is $\pi(T_n(\mathbb{F}_q))$?

Answer: if $q = 2$ or $q =$ odd, then $\pi(T_n(\mathbb{F}_q)) = \mathrm{Sym}(q^n)$.

Answer: if $q = 4, 8, 16, 32, \ldots$ then $\pi(T_n(\mathbb{F}_q)) = \mathrm{Alt}(q^n)$.

Problem: Do there exist "odd" polynomial automorphisms over $\mathbb{F}_4$? Exciting! Let's try Nagata!

$$N = \begin{pmatrix} X + X^2Z^3 + Y^4Z, \\ Y + XZ^2 + Y^2Z, \\ Z \end{pmatrix}$$

$N^2 = I$. N does not act on $Fix(N)$. This set is $\#\{(x, y, z) \mid z = 0 \text{ or } x = z^{-1}y^2\} = q^2 + (q-1)q$ $= q(2q-1)$. Hence, N exchanges $q^3 - q(2q-1)$ elements - that means $\frac{q^3 - q(2q-1)}{2}$ 2-cycles. Which is odd $\Longleftrightarrow$ q odd or $q = 2 \ldots$ Hence, N is even!

Is there perhaps a combinatorial reason why $\pi(\mathsf{GA}_n(\mathbb{F}_4)$ has only even permutations??

Another idea: study the bijections of $\mathbb{F}_9^n$ given by elements of $\mathrm{GA}_n(\mathbb{F}_3)$.

Another idea: study the bijections of $\mathbb{F}_9^n$ given by elements of $\mathrm{GA}_n(\mathbb{F}_3)$.

$\mathrm{GA}_n(\mathbb{F}_3)$ $\mathrm{Bij}_n(\mathbb{F}_9)$

Another idea: study the bijections of $\mathbb{F}_9^n$ given by elements of $\mathrm{GA}_n(\mathbb{F}_3)$.

$$\pi_9 : \quad \mathrm{GA}_n(\mathbb{F}_3) \qquad\qquad \mathrm{Bij}_n(\mathbb{F}_9)$$

Another idea: study the bijections of $\mathbb{F}_9^n$ given by elements of $\mathsf{GA}_n(\mathbb{F}_3)$.

$$\pi_9 : \quad \mathsf{GA}_n(\mathbb{F}_3) \quad \longrightarrow \quad \pi_9(\mathsf{GA}_n(\mathbb{F}_3)) \quad \subsetneq \quad \mathsf{Bij}_n(\mathbb{F}_9)$$

Another idea: study the bijections of $\mathbb{F}_9^n$ given by elements of $\mathsf{GA}_n(\mathbb{F}_3)$.

$$\begin{array}{ccccccc} \pi_9 : & \mathsf{GA}_n(\mathbb{F}_3) & \longrightarrow & \pi_9(\mathsf{GA}_n(\mathbb{F}_3)) & \subsetneq & \mathsf{Bij}_n(\mathbb{F}_9) \\ & \bigcup\!| & & & & \\ & \mathsf{TA}_n(\mathbb{F}_3) & & & & \end{array}$$

Another idea: study the bijections of $\mathbb{F}_9^n$ given by elements of $\mathsf{GA}_n(\mathbb{F}_3)$.

$$\begin{array}{rcccccc}
\pi_9: & \mathsf{GA}_n(\mathbb{F}_3) & \longrightarrow & \pi_9(\mathsf{GA}_n(\mathbb{F}_3)) & \subsetneq & \mathsf{Bij}_n(\mathbb{F}_9) \\
 & \bigcup\!| & & \bigcup\!| & & \\
\pi_9: & \mathsf{TA}_n(\mathbb{F}_3) & \longrightarrow & \pi_9(\mathsf{TA}_n(\mathbb{F}_3)) & \Leftarrow & \textit{computable}!
\end{array}$$

Another idea: study the bijections of $\mathbb{F}_9^n$ given by elements of $\mathrm{GA}_n(\mathbb{F}_3)$.

$$\begin{array}{lcccccc} \pi_9 : & \mathrm{GA}_n(\mathbb{F}_3) & \longrightarrow & \pi_9(\mathrm{GA}_n(\mathbb{F}_3)) & \subsetneq & \mathrm{Bij}_n(\mathbb{F}_9) \\ & \bigcup\!| & & \bigcup\!| & & \\ \pi_9 : & \mathrm{TA}_n(\mathbb{F}_3) & \longrightarrow & \pi_9(\mathrm{TA}_n(\mathbb{F}_3)) & \Leftarrow & \textit{computable}! \end{array}$$

Then study the bijection of $\mathbb{F}_9^3$ given by Nagata - is this bijection in the group $\pi_9(\mathrm{TA}_3(\mathbb{F}_3))$?

Another idea: study the bijections of $\mathbb{F}_9^n$ given by elements of $\mathsf{GA}_n(\mathbb{F}_3)$.

$$\begin{array}{ccccccc}
\pi_9: & \mathsf{GA}_n(\mathbb{F}_3) & \longrightarrow & \pi_9(\mathsf{GA}_n(\mathbb{F}_3)) & \subsetneq & \mathsf{Bij}_n(\mathbb{F}_9) \\
& \bigcup\!| & & \bigcup\!| & & \\
\pi_9: & \mathsf{TA}_n(\mathbb{F}_3) & \longrightarrow & \pi_9(\mathsf{TA}_n(\mathbb{F}_3)) & \Leftarrow & \textit{computable}!
\end{array}$$

Then study the bijection of $\mathbb{F}_9^3$ given by Nagata - is this bijection in the group $\pi_9(\mathsf{TA}_3(\mathbb{F}_3))$? We put it all in the computer (joint work with R. Willems):…

Another idea: study the bijections of $\mathbb{F}_9^n$ given by elements of $\mathrm{GA}_n(\mathbb{F}_3)$.

$$\begin{array}{cccccc} \pi_9: & \mathrm{GA}_n(\mathbb{F}_3) & \longrightarrow & \pi_9(\mathrm{GA}_n(\mathbb{F}_3)) & \subsetneq & \mathrm{Bij}_n(\mathbb{F}_9) \\ & \bigcup\vert & & \bigcup\vert & & \\ \pi_9: & \mathrm{TA}_n(\mathbb{F}_3) & \longrightarrow & \pi_9(\mathrm{TA}_n(\mathbb{F}_3)) & \Leftarrow & \textit{computable}! \end{array}$$

Then study the bijection of $\mathbb{F}_9^3$ given by Nagata - is this bijection in the group $\pi_9(\mathrm{TA}_3(\mathbb{F}_3))$? We put it all in the computer (joint work with R. Willems):... (drums)...

Another idea: study the bijections of $\mathbb{F}_9^n$ given by elements of $\mathrm{GA}_n(\mathbb{F}_3)$.

$$\begin{array}{cccccc}
\pi_9 : & \mathrm{GA}_n(\mathbb{F}_3) & \longrightarrow & \pi_9(\mathrm{GA}_n(\mathbb{F}_3)) & \subsetneq & \mathrm{Bij}_n(\mathbb{F}_9) \\
 & \bigcup\vert & & \bigcup\vert & & \\
\pi_9 : & \mathrm{TA}_n(\mathbb{F}_3) & \longrightarrow & \pi_9(\mathrm{TA}_n(\mathbb{F}_3)) & \Leftarrow & \textit{computable}!
\end{array}$$

Then study the bijection of $\mathbb{F}_9^3$ given by Nagata - is this bijection in the group $\pi_9(\mathrm{TA}_3(\mathbb{F}_3))$? We put it all in the computer (joint work with R. Willems):... (drums)... unfortunately, yes $\pi_9(N)$ is in $\pi_9(\mathrm{TA}_3(\mathbb{F}_3))$.

Another idea: study the bijections of $\mathbb{F}_9^n$ given by elements of $\mathrm{GA}_n(\mathbb{F}_3)$.

$$
\begin{array}{rcccccc}
\pi_9: & \mathrm{GA}_n(\mathbb{F}_3) & \longrightarrow & \pi_9(\mathrm{GA}_n(\mathbb{F}_3)) & \subsetneq & \mathrm{Bij}_n(\mathbb{F}_9) \\
 & \bigcup\!\mid & & \bigcup\!\mid & & \\
\pi_9: & \mathrm{TA}_n(\mathbb{F}_3) & \longrightarrow & \pi_9(\mathrm{TA}_n(\mathbb{F}_3)) & \Leftarrow & \textit{computable}!
\end{array}
$$

Then study the bijection of $\mathbb{F}_9^3$ given by Nagata - is this bijection in the group $\pi_9(\mathrm{TA}_3(\mathbb{F}_3))$? We put it all in the computer (joint work with R. Willems):... (drums)... unfortunately, yes $\pi_9(N)$ is in $\pi_9(\mathrm{TA}_3(\mathbb{F}_3))$. In fact:

Corollary

(of some theorem I proved) Let $F \in \mathrm{GA}_2(\mathbb{F}_q[Z])$. Then F is tamely mimickable.

Nagata can be mimicked by a tame map for every $q = p^m$ - i.e. exists $F \in TA_3(\mathbb{F}_p)$ such that $\pi_q N = \pi_q F$.

Nagata can be mimicked by a tame map for every $q = p^m$ - i.e. exists $F \in TA_3(\mathbb{F}_p)$ such that $\pi_q N = \pi_q F$. Proof is easy once you realize where to look... Remember Nagata's way of making Nagata map?

Nagata can be mimicked by a tame map for every $q = p^m$ - i.e. exists $F \in TA_3(\mathbb{F}_p)$ such that $\pi_q N = \pi_q F$. Proof is easy once you realize where to look...Remember Nagata's way of making Nagata map?

$$(X - z^{-1}Y^2, Y)(X, Y + z^2X), (X + z^{-1}Y^2, Y)$$
$$= (X - 2\Delta Y - \Delta^2 z, Y + \Delta z)$$

Nagata can be mimicked by a tame map for every $q = p^m$ - i.e. exists $F \in TA_3(\mathbb{F}_p)$ such that $\pi_q N = \pi_q F$. Proof is easy once you realize where to look... Remember Nagata's way of making Nagata map?

$$(X - z^{-1}Y^2, Y)(X, Y + z^2X), (X + z^{-1}Y^2, Y)$$
$$= (X - 2\Delta Y - \Delta^2 z, Y + \Delta z)$$

Do the Big Trick, since for $z \in \mathbb{F}_q$ we have $z^q = z$:

Nagata can be mimicked by a tame map for every $q = p^m$ - i.e. exists $F \in TA_3(\mathbb{F}_q)$ such that $\pi_q N = \pi_q F$. Proof is easy once you realize where to look... Remember Nagata's way of making Nagata map?

$$(X - z^{q-2}Y^2, Y)(X, Y + z^2X), (X + z^{q-2}Y^2, Y)$$
$$= (X - 2\Delta Y - \Delta^2 z, Y + \Delta z)$$

Do the Big Trick, since for $z \in \mathbb{F}_q$ we have $z^q = z$:

Nagata can be mimicked by a tame map for every $q = p^m$ - i.e. exists $F \in TA_3(\mathbb{F}_q)$ such that $\pi_q N = \pi_q F$. Proof is easy once you realize where to look… Remember Nagata's way of making Nagata map?

$$(X - z^{q-2}Y^2, Y)(X, Y + z^2 X), (X + z^{q-2}Y^2, Y)$$
$$= (X - 2\Delta Y - \Delta^2 z, Y + \Delta z)$$

Do the Big Trick, since for $z \in \mathbb{F}_q$ we have $z^q = z$:

This almost works - a bit more wiggling necessary (And for the general case, even more work.)

Another idea: define $MA_n^d(k) := \{F \in MA_n(k) \mid deg(F) \leq d\}$.
If $k = \mathbb{F}_q$, then this is finite.

Another idea: define $MA_n^d(k) := \{F \in MA_n(k) \mid deg(F) \leq d\}$. If $k = \mathbb{F}_q$, then this is finite. Now compute $\mathrm{GA}_n^d(\mathbb{F}_q) := \mathrm{GA}_n(\mathbb{F}_q) \cap MA_n^d(\mathbb{F}_q)$ by checking all $F \in MA_n^d(k)$! We find ALL automorphisms of degree $\leq d$. Will we find new ones we didn't know before?

Another idea: define $MA_n^d(k) := \{F \in MA_n(k) \mid deg(F) \leq d\}$.
If $k = \mathbb{F}_q$, then this is finite. Now compute
$\mathrm{GA}_n^d(\mathbb{F}_q) := \mathrm{GA}_n(\mathbb{F}_q) \cap MA_n^d(\mathbb{F}_q)$ by checking all $F \in MA_n^d(k)$!
We find ALL automorphisms of degree $\leq d$. Will we find new ones we didn't know before?

Let's not be too ambitious: $n = 3$. And $q = 2, 3, 4, 5$.

Computable is (R. Willems):
$\mathrm{GA}_3^2(\mathbb{F}_{2,3,4,5})$ and main part of $\mathrm{GA}_3^3(\mathbb{F}_2)$. Surprisingly, results seem to be intersting!

Another idea: define $MA_n^d(k) := \{F \in MA_n(k) \mid deg(F) \leq d\}$.
If $k = \mathbb{F}_q$, then this is finite. Now compute
$\mathrm{GA}_n^d(\mathbb{F}_q) := \mathrm{GA}_n(\mathbb{F}_q) \cap MA_n^d(\mathbb{F}_q)$ by checking all $F \in MA_n^d(k)$!
We find ALL automorphisms of degree $\leq d$. Will we find new ones we didn't know before?

Let's not be too ambitious: $n = 3$. And $q = 2, 3, 4, 5$.

Computable is (R. Willems):
$\mathrm{GA}_3^2(\mathbb{F}_{2,3,4,5})$ and main part of $\mathrm{GA}_3^3(\mathbb{F}_2)$. Surprisingly, results seem to be intersting!

Observation: $F \in \mathrm{GA}_3^2(\mathbb{F}_q)$ seems to be $\in \mathrm{TA}_3(\mathbb{F}_q)$, always.
No idea why!

Also interesting: set of endomorphisms that induce bijections.

Also interesting: set of endomorphisms that induce bijections.
I.e. computed: $\mathcal{B}(\mathbb{F}_2)_3^2 :=$ set of $F = X + H \in MA_3^2(\mathbb{F}_2)$ for which F induces a bijection of $\mathbb{F}_2^3$.

Also interesting: set of endomorphisms that induce bijections.

I.e. computed: $\mathcal{B}(\mathbb{F}_2)^2_3 :=$ set of $F = X + H \in MA^2_3(\mathbb{F}_2)$ for which F induces a bijection of $\mathbb{F}_2^3$.

$\#\mathcal{B}(\mathbb{F}_2)^2_3 = 336.$

Also interesting: set of endomorphisms that induce bijections.

I.e. computed: $\mathcal{B}(\mathbb{F}_2)^2_3 :=$ set of $F = X + H \in MA^2_3(\mathbb{F}_2)$ for which F induces a bijection of $\mathbb{F}_2^3$.

$\#\mathcal{B}(\mathbb{F}_2)^2_3 = 336$.

We say $B, B' \in \mathcal{B}$ are equivalent if exists $F \in \mathrm{GA}_3(\mathbb{F}_2)$ such that $FB = B'$. It seems there are 4 such equivalence classes:

Also interesting: set of endomorphisms that induce bijections. I.e. computed: $\mathcal{B}(\mathbb{F}_2)^2_3 :=$ set of $F = X + H \in MA^2_3(\mathbb{F}_2)$ for which F induces a bijection of $\mathbb{F}_2^3$.

$\#\mathcal{B}(\mathbb{F}_2)^2_3 = 336$.

We say $B, B' \in \mathcal{B}$ are equivalent if exists $F \in \mathrm{GA}_3(\mathbb{F}_2)$ such that $FB = B'$. It seems there are 4 such equivalence classes:

(X, Y, Z)	176, *all tame*!
$(X^8 + X^4 + X, Y, Z)$	56
$(X^8 + X^2 + X, Y, Z)$	56
$(X^4 + X^2 + X, Y, Z)$	48

Also interesting: set of endomorphisms that induce bijections. I.e. computed: $\mathcal{B}(\mathbb{F}_2)_3^2 :=$ set of $F = X + H \in MA_3^2(\mathbb{F}_2)$ for which F induces a bijection of $\mathbb{F}_2^3$.

$\#\mathcal{B}(\mathbb{F}_2)_3^2 = 336$.

We say $B, B' \in \mathcal{B}$ are equivalent if exists $F \in \mathrm{GA}_3(\mathbb{F}_2)$ such that $FB = B'$. It seems there are 4 such equivalence classes:

(X, Y, Z)	176, *all tame*!
$(X^8 + X^4 + X, Y, Z)$	56
$(X^8 + X^2 + X, Y, Z)$	56
$(X^4 + X^2 + X, Y, Z)$	48

Everything is equivalent to 1-variable permutation polynomials.

Also interesting: set of endomorphisms that induce bijections. I.e. computed: $\mathcal{B}(\mathbb{F}_2)_3^2 :=$ set of $F = X + H \in MA_3^2(\mathbb{F}_2)$ for which F induces a bijection of $\mathbb{F}_2^3$.

$\#\mathcal{B}(\mathbb{F}_2)_3^2 = 336$.

We say $B, B' \in \mathcal{B}$ are equivalent if exists $F \in \mathrm{GA}_3(\mathbb{F}_2)$ such that $FB = B'$. It seems there are 4 such equivalence classes:

(X, Y, Z)	176, *all tame*!
$(X^8 + X^4 + X, Y, Z)$	56
$(X^8 + X^2 + X, Y, Z)$	56
$(X^4 + X^2 + X, Y, Z)$	48

Everything is equivalent to 1-variable permutation polynomials. Degree 3: 1520 permutation polynomials, 400 equiv. to (X, Y, Z) - again all tame. (In progress.)

Another "characteristic 2" anomaly: compare

$\mathrm{GTAM}_n(k) :=$ normal closure of $\mathrm{TA}_n(k)$ in $\mathrm{GA}_n(k)$

Another "characteristic 2" anomaly: compare

$\mathsf{GTAM}_n(k) :=$ normal closure of $\mathsf{TA}_n(k)$ in $\mathsf{GA}_n(k)$

$\cup|$

$\mathsf{GLIN}_n(k) :=$ normal closure of $\mathrm{GL_n(k)}$ in $\mathsf{GA}_n(k)$

Another “characteristic 2” anomaly: compare

$\mathsf{GTAM}_n(k) :=$ normal closure of $\mathsf{TA}_n(k)$ in $\mathsf{GA}_n(k)$

$\cup|$

$\mathsf{GLIN}_n(k) :=$ normal closure of $\mathrm{GL_n(k)}$ in $\mathsf{GA}_n(k)$

QUESTION 1: Is $\mathsf{GLIN}_n(k) = \mathsf{GTAM}_n(k)$?

Another "characteristic 2" anomaly: compare

$\mathsf{GTAM}_n(k) :=$ normal closure of $\mathsf{TA}_n(k)$ in $\mathsf{GA}_n(k)$

$\cup|$

$\mathsf{GLIN}_n(k) :=$ normal closure of $\mathrm{GL_n(k)}$ in $\mathsf{GA}_n(k)$

QUESTION 1: Is $\mathsf{GLIN}_n(k) = \mathsf{GTAM}_n(k)$?

QUESTION 2: Is N (Nagata) in $\mathsf{GTAM}_n(k)$?

Another "characteristic 2" anomaly: compare

$\mathrm{GTAM}_n(k) :=$ normal closure of $\mathrm{TA}_n(k)$ in $\mathrm{GA}_n(k)$

$\cup|$

$\mathrm{GLIN}_n(k) :=$ normal closure of $\mathrm{GL_n(k)}$ in $\mathrm{GA}_n(k)$

QUESTION 1: Is $\mathrm{GLIN}_n(k) = \mathrm{GTAM}_n(k)$?

QUESTION 2: Is N (Nagata) in $\mathrm{GTAM}_n(k)$?

ANSWER 1: YES if you can find invertible linear map $(aX_1, X_2, \ldots, X_n)$ where $a \neq 1$.

Another "characteristic 2" anomaly: compare

$\mathsf{GTAM}_n(k) :=$ normal closure of $\mathsf{TA}_n(k)$ in $\mathsf{GA}_n(k)$

$\cup|$

$\mathsf{GLIN}_n(k) :=$ normal closure of $\mathrm{GL_n(k)}$ in $\mathsf{GA}_n(k)$

QUESTION 1: Is $\mathsf{GLIN}_n(k) = \mathsf{GTAM}_n(k)$?

QUESTION 2: Is N (Nagata) in $\mathsf{GTAM}_n(k)$?

ANSWER 1: YES if you can find invertible linear map $(aX_1, X_2, \ldots, X_n)$ where $a \neq 1$. I.e. if $k \neq \mathbb{F}_2 \ldots$ An intelligent computation yields: answer NO if $k = \mathbb{F}_2 \ldots$

Another "characteristic 2" anomaly: compare

$\mathrm{GTAM}_n(k) :=$ normal closure of $\mathrm{TA}_n(k)$ in $\mathrm{GA}_n(k)$

$\cup|$

$\mathrm{GLIN}_n(k) :=$ normal closure of $\mathrm{GL_n(k)}$ in $\mathrm{GA}_n(k)$

QUESTION 1: Is $\mathrm{GLIN}_n(k) = \mathrm{GTAM}_n(k)$?

QUESTION 2: Is N (Nagata) in $\mathrm{GTAM}_3(k)$?

ANSWER 1: YES if $k \neq \mathbb{F}_2$, NO if $k = \mathbb{F}_2$.

ANSWER 2:

Another "characteristic 2" anomaly: compare

$\mathrm{GTAM}_n(k) :=$ normal closure of $\mathrm{TA}_n(k)$ in $\mathrm{GA}_n(k)$

$\cup|$

$\mathrm{GLIN}_n(k) :=$ normal closure of $\mathrm{GL_n(k)}$ in $\mathrm{GA}_n(k)$

QUESTION 1: Is $\mathrm{GLIN}_n(k) = \mathrm{GTAM}_n(k)$?

QUESTION 2: Is N (Nagata) in $\mathrm{GTAM}_3(k)$?

ANSWER 1: YES if $k \neq \mathbb{F}_2$, NO if $k = \mathbb{F}_2$.

ANSWER 2: Recent result: Nagata is *shifted linearizable:*

Exists linear map L, and $\varphi \in \mathrm{GA}_n(k)$ such that $\varphi^{-1} L N \varphi = L$.

Another "characteristic 2" anomaly: compare

$\mathsf{GTAM}_n(k) :=$ normal closure of $\mathsf{TA}_n(k)$ in $\mathsf{GA}_n(k)$

$\cup|$

$\mathsf{GLIN}_n(k) :=$ normal closure of $\mathrm{GL_n(k)}$ in $\mathsf{GA}_n(k)$

QUESTION 1: Is $\mathsf{GLIN}_n(k) = \mathsf{GTAM}_n(k)$?

QUESTION 2: Is N (Nagata) in $\mathsf{GTAM}_3(k)$?

ANSWER 1: YES if $k \neq \mathbb{F}_2$, NO if $k = \mathbb{F}_2$.

ANSWER 2: Recent result: Nagata is *shifted linearizable:*

Exists linear map L, and $\varphi \in \mathsf{GA}_n(k)$ such that $\varphi^{-1} L N \varphi = L$.

...If $k \neq \mathbb{F}_2$, of course...

Another “characteristic 2” anomaly: compare

$\mathrm{GTAM}_n(k) :=$ normal closure of $\mathrm{TA}_n(k)$ in $\mathrm{GA}_n(k)$

$\cup|$

$\mathrm{GLIN}_n(k) :=$ normal closure of $\mathrm{GL_n(k)}$ in $\mathrm{GA}_n(k)$

QUESTION 1: Is $\mathrm{GLIN}_n(k) = \mathrm{GTAM}_n(k)$?

QUESTION 2: Is N (Nagata) in $\mathrm{GTAM}_3(k)$?

ANSWER 1: YES if $k \neq \mathbb{F}_2$, NO if $k = \mathbb{F}_2$.

ANSWER 2: YES if $k \neq \mathbb{F}_2$, DUNNO if $k = \mathbb{F}_2$.

(NO would imply $N \notin \mathrm{TA}_3(\mathbb{F}_2)$.)

Another "characteristic 2" anomaly: compare

$\mathrm{GTAM}_n(k) :=$ normal closure of $\mathrm{TA}_n(k)$ in $\mathrm{GA}_n(k)$

$\cup|$

$\mathrm{GLIN}_n(k) :=$ normal closure of $\mathrm{GL_n(k)}$ in $\mathrm{GA}_n(k)$

QUESTION 1: Is $\mathrm{GLIN}_n(k) = \mathrm{GTAM}_n(k)$?

QUESTION 2: Is N (Nagata) in $\mathrm{GTAM}_3(k)$?

ANSWER 1: YES if $k \neq \mathbb{F}_2$, NO if $k = \mathbb{F}_2$.

ANSWER 2: YES if $k \neq \mathbb{F}_2$, DUNNO if $k = \mathbb{F}_2$.

(NO would imply $N \notin \mathrm{TA}_3(\mathbb{F}_2)$.)

THANK YOU for enduring all those slides.

.....

.....

Theorem:

$$\mathsf{GLIN}_n(\mathbb{F}_2) \subsetneqq \mathsf{GTAM}_n(\mathbb{F}_2).$$

Theorem:

$\mathsf{GLIN}_n(\mathbb{F}_2) \subsetneqq \mathsf{GTAM}_n(\mathbb{F}_2)$.

Proof.

Theorem:

$\mathsf{GLIN}_n(\mathbb{F}_2) \subsetneqq \mathsf{GTAM}_n(\mathbb{F}_2)$.

Proof. Remember, $\pi_2(TA_n(\mathbb{F}_2)) = \mathsf{Sym}(2^n)$, as $\mathbb{F}_2$ was the exception to the exception.

Theorem:

$\mathsf{GLIN}_n(\mathbb{F}_2) \subsetneqq \mathsf{GTAM}_n(\mathbb{F}_2)$.

Proof. Remember, $\pi_2(TA_n(\mathbb{F}_2)) = \mathsf{Sym}(2^n)$, as $\mathbb{F}_2$ was the exception to the exception.

Now, notice that if $n \geq 3$, then any element of $\mathrm{GL_n}(\mathbb{F}_2)$ is even.

Theorem:

$\mathsf{GLIN}_n(\mathbb{F}_2) \subsetneq \mathsf{GTAM}_n(\mathbb{F}_2)$.

Proof. Remember, $\pi_2(TA_n(\mathbb{F}_2)) = \mathrm{Sym}(2^n)$, as $\mathbb{F}_2$ was the exception to the exception.

Now, notice that if $n \geq 3$, then any element of $\mathrm{GL_n}(\mathbb{F}_2)$ is even. Hence $\pi_2(\mathsf{GLIN}_n(\mathbb{F}_2)) \subseteq \mathrm{Alt}(2^n)$. If $n = 2$, then $(X + Y, Y)$ is odd, unfortunately.

Theorem:

$\mathsf{GLIN}_n(\mathbb{F}_2) \subsetneq \mathsf{GTAM}_n(\mathbb{F}_2)$.

Proof. Remember, $\pi_2(TA_n(\mathbb{F}_2)) = \mathsf{Sym}(2^n)$, as $\mathbb{F}_2$ was the exception to the exception.

Now, notice that if $n \geq 3$, then any element of $\mathrm{GL_n}(\mathbb{F}_2)$ is even. Hence $\pi_2(\mathsf{GLIN}_n(\mathbb{F}_2)) \subseteq \mathsf{Alt}(2^n)$. If $n = 2$, then $(X + Y, Y)$ is odd, unfortunately. However, in dimension 2 we understand the automorphism group, and can do a computer calculation

Theorem:

$\mathsf{GLIN}_n(\mathbb{F}_2) \subsetneqq \mathsf{GTAM}_n(\mathbb{F}_2)$.

Proof. Remember, $\pi_2(TA_n(\mathbb{F}_2)) = \mathsf{Sym}(2^n)$, as $\mathbb{F}_2$ was the exception to the exception.

Now, notice that if $n \geq 3$, then any element of $\mathrm{GL_n}(\mathbb{F}_2)$ is even. Hence $\pi_2(\mathsf{GLIN}_n(\mathbb{F}_2)) \subseteq \mathsf{Alt}(2^n)$. If $n = 2$, then $(X + Y, Y)$ is odd, unfortunately. However, in dimension 2 we understand the automorphism group, and can do a computer calculation to see that

$$\frac{\#\pi_4(\mathsf{GLIN}_2(\mathbb{F}_2))}{\#\pi_4(\mathsf{GTAM}_2(\mathbb{F}_2))} = 2.$$

End proof.

Conclusions

Conclusions

- $\pi_q(\mathsf{TA}_n(\mathbb{F}_q)) = \mathsf{Sym}(q^n)$ if q odd, $q = 2$.
  $\pi_q(\mathsf{TA}_n(\mathbb{F}_q)) = \mathsf{Alt}(q^n)$ if $q = 2^m$, $m \geq 2$.

Conclusions

- $\pi_q(\mathrm{TA}_n(\mathbb{F}_q)) = \mathrm{Sym}(q^n)$ if q odd, $q = 2$.
  $\pi_q(\mathrm{TA}_n(\mathbb{F}_q)) = \mathrm{Alt}(q^n)$ if $q = 2^m$, $m \geq 2$.
- $\mathrm{GLIN}_n(\mathbb{F}_q) = \mathrm{GTAM}_n(\mathbb{F}_q)$ if $q \neq 2$.
  $\mathrm{GLIN}_n(\mathbb{F}_2) \subsetneq \mathrm{GTAM}_n(\mathbb{F}_2)$... but
  $\mathrm{GTAM}_n(\mathbb{F}_2) \subseteq \mathrm{GLIN}_{n+1}(\mathbb{F}_2)$

Conclusions

- $\pi_q(\mathrm{TA}_n(\mathbb{F}_q)) = \mathrm{Sym}(q^n)$ if q odd, $q = 2$.
  $\pi_q(\mathrm{TA}_n(\mathbb{F}_q)) = \mathrm{Alt}(q^n)$ if $q = 2^m$, $m \geq 2$.
- $\mathrm{GLIN}_n(\mathbb{F}_q) = \mathrm{GTAM}_n(\mathbb{F}_q)$ if $q \neq 2$.
  $\mathrm{GLIN}_n(\mathbb{F}_2) \subsetneq \mathrm{GTAM}_n(\mathbb{F}_2)\ldots$ but
  $\mathrm{GTAM}_n(\mathbb{F}_2) \subseteq \mathrm{GLIN}_{n+1}(\mathbb{F}_2)$
- Nagata in $\mathrm{GTAM}_n(k)$ if $k \neq \mathbb{F}_2$. If $k = \mathbb{F}_2$ we don't know. Yet.

Conclusions

- $\pi_q(\mathrm{TA}_n(\mathbb{F}_q)) = \mathrm{Sym}(q^n)$ if q odd, $q = 2$.
  $\pi_q(\mathrm{TA}_n(\mathbb{F}_q)) = \mathrm{Alt}(q^n)$ if $q = 2^m$, $m \geq 2$.
- $\mathrm{GLIN}_n(\mathbb{F}_q) = \mathrm{GTAM}_n(\mathbb{F}_q)$ if $q \neq 2$.
  $\mathrm{GLIN}_n(\mathbb{F}_2) \subsetneq \mathrm{GTAM}_n(\mathbb{F}_2)$... but
  $\mathrm{GTAM}_n(\mathbb{F}_2) \subseteq \mathrm{GLIN}_{n+1}(\mathbb{F}_2)$
- Nagata in $\mathrm{GTAM}_n(k)$ if $k \neq \mathbb{F}_2$. If $k = \mathbb{F}_2$ we don't know. Yet.
- More research is needed in $\mathrm{char}(k) = p$, which is a very unexplored topic for polynomial automorphisms - but apparently very powerful! (Belov-Kontsjevich)

Conclusions

- $\pi_q(\mathrm{TA}_n(\mathbb{F}_q)) = \mathrm{Sym}(q^n)$ if q odd, $q = 2$.
  $\pi_q(\mathrm{TA}_n(\mathbb{F}_q)) = \mathrm{Alt}(q^n)$ if $q = 2^m$, $m \geq 2$.
- $\mathrm{GLIN}_n(\mathbb{F}_q) = \mathrm{GTAM}_n(\mathbb{F}_q)$ if $q \neq 2$.
  $\mathrm{GLIN}_n(\mathbb{F}_2) \subsetneq \mathrm{GTAM}_n(\mathbb{F}_2) \ldots$ but
  $\mathrm{GTAM}_n(\mathbb{F}_2) \subseteq \mathrm{GLIN}_{n+1}(\mathbb{F}_2)$
- Nagata in $\mathrm{GTAM}_n(k)$ if $k \neq \mathbb{F}_2$. If $k = \mathbb{F}_2$ we don't know. Yet.
- More research is needed in $\mathrm{char}(k) = p$, which is a very unexplored topic for polynomial automorphisms - but apparently very powerful! (Belov-Kontsjevich)

***** THANK YOU *****

MOTIVATION:

MOTIVATION:

Why study polynomial maps over finite fields, and not be a normal person and do the "$\mathbb{C}$" thing?

MOTIVATION:

Why study polynomial maps over finite fields, and not be a normal person and do the "$\mathbb{C}$" thing?

REASON 1:

MOTIVATION:

Why study polynomial maps over finite fields, and not be a normal person and do the "$\mathbb{C}$" thing?

REASON 1: Reduction-mod-p techniques to solve problems over $\mathbb{C}$.

MOTIVATION:

Why study polynomial maps over finite fields, and not be a normal person and do the "$\mathbb{C}$" thing?

REASON 1: Reduction-mod-p techniques to solve problems over $\mathbb{C}$. Classical example: an injective polynomial map is surjective.

MOTIVATION:

Why study polynomial maps over finite fields, and not be a normal person and do the "$\mathbb{C}$" thing?

REASON 1: Reduction-mod-p techniques to solve problems over $\mathbb{C}$. Classical example: an injective polynomial map is surjective. Reason: an injective map on finite set is surjective.

MOTIVATION:

Why study polynomial maps over finite fields, and not be a normal person and do the "$\mathbb{C}$" thing?

REASON 1: Reduction-mod-p techniques to solve problems over $\mathbb{C}$. Classical example: an injective polynomial map is surjective. Reason: an injective map on finite set is surjective. Very recent: Belov-Kontsjevich proved equivalence of two already long-standing conjectures: the Dixmier Conjecture ('68) and the Jacobian Conjecture ('39).

MOTIVATION:

Why study polynomial maps over finite fields, and not be a normal person and do the "$\mathbb{C}$" thing?

REASON 1: Reduction-mod-p techniques to solve problems over $\mathbb{C}$. Classical example: an injective polynomial map is surjective. Reason: an injective map on finite set is surjective. Very recent: Belov-Kontsjevich proved equivalence of two already long-standing conjectures: the Dixmier Conjecture ('68) and the Jacobian Conjecture ('39).

REASON 2: Polynomial maps over finite fields may have applications in discrete-mathematics like settings!

RE-MOTIVATION:

Why **NOT** study polynomial maps over finite fields! In fact, why didn't anyone fill that **gaping hole** yet!

REASON 1: Reduction-mod-p techniques to solve problems over $\mathbb{C}$. Classical example: an injective polynomial map is surjective. Reason: an injective map from a finite set to a finite. Very recent: Belov-Kontsjevich (yes, that guy) proved equivalence of two already long-standing conjectures: the Dixmier Conjecture ('68) and the Jacobian Conjecture ('39).

REASON 2: Polynomial maps over finite fields may have applications in discrete-mathematics like settings! (In fact, one of the reasons for this talk is the hope that there may be one or two of you in the audience who may see such a possible application!)

$\mathsf{GA}_n(k)$

$\mathsf{TA}_n(k)$

$\mathrm{GA}_n(k)$

$\cup|$

$\mathrm{LF}_n(k) \quad := < F \in \mathrm{GA}_n(k) \mid deg(F^m) \text{ bounded} >$

$\cup|$

$\mathrm{ELFD}_n(k) \quad := < \exp(D) \mid D \text{ locally finite derivation} >$

$\cup|$

$\mathrm{TA}_n(k)$

$\mathsf{GA}_n(k)$

$\cup|$

$\mathsf{LF}_n(k) \quad := < F \in \mathsf{GA}_n(k) \mid deg(F^m) \text{ bounded} >$

$\cup|$

$\mathsf{ELFD}_n(k) \quad := < \exp(D) \mid D \text{ locally finite derivation} >$

$\cup|$

$\mathsf{GLIN}_n(k) \quad :=$ normalization of $\mathrm{GL_n(k)}$

$?\cup|?$ not equal if $\mathrm{char}(k) = 0$.

$\mathsf{TA}_n(k)$

$\mathrm{GA}_n(k)$

$\cup|$

$\mathrm{LF}_n(k) \quad := < F \in \mathrm{GA}_n(k) \mid deg(F^m) \text{ bounded} >$

$\cup|$

$\mathrm{ELFD}_n(k) \quad := < \exp(D) \mid D \text{ locally finite derivation} >$

$\cup|$

$\mathrm{GTAM}_n(k) \quad := \text{normalization of } \mathrm{TA}_n(k)$

$\cup|$

$\mathrm{GLIN}_n(k) \quad := \text{normalization of } \mathrm{GL_n(k)}$

$?\cup|? \quad$ not equal if $\mathrm{char}(k) = 0$.

$\mathrm{TA}_n(k)$

$\mathsf{GA}_n(k)$

$\cup|$

$\mathsf{LF}_n(k) \quad := < F \in \mathsf{GA}_n(k) \mid deg(F^m) \text{ bounded} >$

$\cup|$

$\mathsf{ELFD}_n(k) \quad := < \exp(D) \mid D \text{ locally finite derivation} >$

$\cup|$

$\mathsf{GTAM}_n(k) \quad :=$ normalization of $\mathsf{TA}_n(k)$

$\cup|$

$\mathsf{GLIN}_n(k) \quad :=$ normalization of $\mathrm{GL_n(k)}$

$?\cup|? \quad$ not equal if $\mathrm{char}(k) = 0$.

$\mathsf{TA}_n(k)$

Where in these groups is Nagata?

Where in these groups is Nagata?

No conjugate of Nagata is in $\mathrm{GL_n(k)}$ for any field k !

Where in these groups is Nagata?

No conjugate of Nagata is in $\mathrm{GL_n(k)}$ for any field k !

But: recent result: Nagata is *shifted linearizable:*

Where in these groups is Nagata?

No conjugate of Nagata is in $\mathrm{GL_n(k)}$ for any field k !

But: recent result: Nagata is *shifted linearizable:* choose $s \in k$ such that $s \neq 0, 1, -1$.

Where in these groups is Nagata?

No conjugate of Nagata is in $\mathrm{GL_n(k)}$ for any field k !

But: recent result: Nagata is *shifted linearizable:* choose $s \in k$ such that $s \neq 0, 1, -1$.

$$(s \exp(D))$$

Where in these groups is Nagata?

No conjugate of Nagata is in $\mathrm{GL_n(k)}$ for any field k !

But: recent result: Nagata is *shifted linearizable:* choose $s \in k$ such that $s \neq 0, 1, -1$.

$$\exp(\frac{-s^2}{1-s^2}D)(s\exp(D))\exp(\frac{s^2}{1-s^2}D)$$

Where in these groups is Nagata?

No conjugate of Nagata is in $\mathrm{GL_n(k)}$ for any field k !

But: recent result: Nagata is *shifted linearizable:* choose $s \in k$ such that $s \neq 0, 1, -1$.

$$\exp(\frac{-s^2}{1-s^2}D)(s\exp(D))\exp(\frac{s^2}{1-s^2}D) = sI$$

Where in these groups is Nagata?

No conjugate of Nagata is in $\mathrm{GL_n(k)}$ for any field k !

But: recent result: Nagata is *shifted linearizable:* choose $s \in k$ such that $s \neq 0, 1, -1$.

$$\exp(\frac{-s^2}{1-s^2}D)(s\exp(D))\exp(\frac{s^2}{1-s^2}D) = sI$$

Hence: Nagata map is in $\mathrm{GLIN}_3(k)$!

Where in these groups is Nagata?

No conjugate of Nagata is in $\mathrm{GL_n(k)}$ for any field k !

But: recent result: Nagata is *shifted linearizable:* choose $s \in k$ such that $s \neq 0, 1, -1$.

$$\exp(\frac{-s^2}{1-s^2}D)(s\exp(D))\exp(\frac{s^2}{1-s^2}D) = sI$$

Hence: Nagata map is in $\mathsf{GLIN}_3(k)$! - If $k \neq \mathbb{F}_2, \mathbb{F}_3$, that is !!

How does $\mathrm{GLIN}_n(k)$ compare to $\mathrm{GTAM}_n(k)$?

How does $\mathrm{GLIN}_n(k)$ compare to $\mathrm{GTAM}_n(k)$?

As soon as $(X_1 + f(X_2), X_2, \ldots, X_n) \in \mathrm{GLIN}_n(k)$ for any $f \in k[X_2]$, then $\mathrm{GLIN}_n(k) = \mathrm{GTAM}_n(k)$.

How does $\mathrm{GLIN}_n(k)$ compare to $\mathrm{GTAM}_n(k)$?

As soon as $(X_1 + f(X_2), X_2, \ldots, X_n) \in \mathrm{GLIN}_n(k)$ for any $f \in k[X_2]$, then $\mathrm{GLIN}_n(k) = \mathrm{GTAM}_n(k)$. Choose some $a \neq 0$:

How does $\mathrm{GLIN}_n(k)$ compare to $\mathrm{GTAM}_n(k)$?

As soon as $(X_1 + f(X_2), X_2, \ldots, X_n) \in \mathrm{GLIN}_n(k)$ for any $f \in k[X_2]$, then $\mathrm{GLIN}_n(k) = \mathrm{GTAM}_n(k)$. Choose some $a \neq 0$:

$$(aX, Y)$$

How does $\mathrm{GLIN}_n(k)$ compare to $\mathrm{GTAM}_n(k)$?

As soon as $(X_1 + f(X_2), X_2, \ldots, X_n) \in \mathrm{GLIN}_n(k)$ for any $f \in k[X_2]$, then $\mathrm{GLIN}_n(k) = \mathrm{GTAM}_n(k)$. Choose some $a \neq 0$:

$$(X - bf(Y), Y)(aX, Y)(X + bf(Y), Y)$$

How does $\mathrm{GLIN}_n(k)$ compare to $\mathrm{GTAM}_n(k)$?

As soon as $(X_1 + f(X_2), X_2, \ldots, X_n) \in \mathrm{GLIN}_n(k)$ for any $f \in k[X_2]$, then $\mathrm{GLIN}_n(k) = \mathrm{GTAM}_n(k)$. Choose some $a \neq 0$:

$$(a^{-1}X, Y)(X - bf(Y), Y)(aX, Y)(X + bf(Y), Y)$$

How does $\mathrm{GLIN}_n(k)$ compare to $\mathrm{GTAM}_n(k)$?
As soon as $(X_1 + f(X_2), X_2, \ldots, X_n) \in \mathrm{GLIN}_n(k)$ for any $f \in k[X_2]$, then $\mathrm{GLIN}_n(k) = \mathrm{GTAM}_n(k)$. Choose some $a \neq 0$:

$$(a^{-1}X, Y)(X - bf(Y), Y)(a(X + bf(Y)), Y)$$

How does $\mathrm{GLIN}_n(k)$ compare to $\mathrm{GTAM}_n(k)$?
As soon as $(X_1 + f(X_2), X_2, \ldots, X_n) \in \mathrm{GLIN}_n(k)$ for any $f \in k[X_2]$, then $\mathrm{GLIN}_n(k) = \mathrm{GTAM}_n(k)$. Choose some $a \neq 0$:

$$(a^{-1}X, Y)(X - bf(Y), Y)(aX + abf(Y), Y)$$

How does $\mathrm{GLIN}_n(k)$ compare to $\mathrm{GTAM}_n(k)$?

As soon as $(X_1 + f(X_2), X_2, \ldots, X_n) \in \mathrm{GLIN}_n(k)$ for any $f \in k[X_2]$, then $\mathrm{GLIN}_n(k) = \mathrm{GTAM}_n(k)$. Choose some $a \neq 0$:

$$(a^{-1}X, Y)(aX + abf(Y) - bf(Y), Y)$$

How does $\mathrm{GLIN}_n(k)$ compare to $\mathrm{GTAM}_n(k)$?

As soon as $(X_1 + f(X_2), X_2, \ldots, X_n) \in \mathrm{GLIN}_n(k)$ for any $f \in k[X_2]$, then $\mathrm{GLIN}_n(k) = \mathrm{GTAM}_n(k)$. Choose some $a \neq 0$:

$$(X + bf(Y) - a^{-1}bf(Y), Y)$$

How does $\mathrm{GLIN}_n(k)$ compare to $\mathrm{GTAM}_n(k)$?

As soon as $(X_1 + f(X_2), X_2, \ldots, X_n) \in \mathrm{GLIN}_n(k)$ for any $f \in k[X_2]$, then $\mathrm{GLIN}_n(k) = \mathrm{GTAM}_n(k)$. Choose some $a \neq 0$:

$$(X + b(1 - a^{-1})f(Y), Y)$$

How does $\mathrm{GLIN}_n(k)$ compare to $\mathrm{GTAM}_n(k)$?

As soon as $(X_1 + f(X_2), X_2, \ldots, X_n) \in \mathrm{GLIN}_n(k)$ for any $f \in k[X_2]$, then $\mathrm{GLIN}_n(k) = \mathrm{GTAM}_n(k)$. Choose some $a \neq 0$

:

$$(X + b(1 - a^{-1})f(Y), Y)$$

Choose $b = (1 - a^{-1})^{-1}$.

How does $\mathrm{GLIN}_n(k)$ compare to $\mathrm{GTAM}_n(k)$?

As soon as $(X_1 + f(X_2), X_2, \ldots, X_n) \in \mathrm{GLIN}_n(k)$ for any $f \in k[X_2]$, then $\mathrm{GLIN}_n(k) = \mathrm{GTAM}_n(k)$. Choose some $a \neq 0$ $a \neq 1$:

$$(X + b(1 - a^{-1})f(Y), Y)$$

Choose $b = (1 - a^{-1})^{-1}$.

How does $\mathrm{GLIN}_n(k)$ compare to $\mathrm{GTAM}_n(k)$?
As soon as $(X_1 + f(X_2), X_2, \ldots, X_n) \in \mathrm{GLIN}_n(k)$ for any $f \in k[X_2]$, then $\mathrm{GLIN}_n(k) = \mathrm{GTAM}_n(k)$. Choose some $a \neq 0$ $a \neq 1$:

$$(X + b(1 - a^{-1})f(Y), Y)$$

Choose $b = (1 - a^{-1})^{-1}$. Then $(X + f(Y), Y))$ in $\mathrm{GLIN}_2(k)$!

How does $\mathrm{GLIN}_n(k)$ compare to $\mathrm{GTAM}_n(k)$?

As soon as $(X_1 + f(X_2), X_2, \ldots, X_n) \in \mathrm{GLIN}_n(k)$ for any $f \in k[X_2]$, then $\mathrm{GLIN}_n(k) = \mathrm{GTAM}_n(k)$. Choose some $a \neq 0$ $a \neq 1$:

$$(X + b(1 - a^{-1})f(Y), Y)$$

Choose $b = (1 - a^{-1})^{-1}$. Then $(X + f(Y), Y))$ in $\mathrm{GLIN}_2(k)$!

$\ldots$ if $k \neq \mathbb{F}_2 \ldots$

How does $\mathrm{GLIN}_n(k)$ compare to $\mathrm{GTAM}_n(k)$?

As soon as $(X_1 + f(X_2), X_2, \ldots, X_n) \in \mathrm{GLIN}_n(k)$ for any $f \in k[X_2]$, then $\mathrm{GLIN}_n(k) = \mathrm{GTAM}_n(k)$. Choose some $a \neq 0$ $a \neq 1$:

$$(X + b(1 - a^{-1})f(Y), Y)$$

Choose $b = (1 - a^{-1})^{-1}$. Then $(X + f(Y), Y))$ in $\mathrm{GLIN}_2(k)$!

…if $k \neq \mathbb{F}_2$…

Question: How does $\mathrm{GLIN}_n(\mathbb{F}_2)$ and $\mathrm{GTAM}_n(\mathbb{F}_2)$ relate?

How does $\mathrm{GLIN}_n(k)$ compare to $\mathrm{GTAM}_n(k)$?

As soon as $(X_1 + f(X_2), X_2, \ldots, X_n) \in \mathrm{GLIN}_n(k)$ for any $f \in k[X_2]$, then $\mathrm{GLIN}_n(k) = \mathrm{GTAM}_n(k)$. Choose some $a \neq 0$ $a \neq 1$:

$$(X + b(1 - a^{-1})f(Y), Y)$$

Choose $b = (1 - a^{-1})^{-1}$. Then $(X + f(Y), Y))$ in $\mathrm{GLIN}_2(k)$!

...if $k \neq \mathbb{F}_2$...

Question: How does $\mathrm{GLIN}_n(\mathbb{F}_2)$ and $\mathrm{GTAM}_n(\mathbb{F}_2)$ relate? We will Get Back To That...