A collection of results on polynomial maps over finite fields

Stefan Maubach

Jacobs University Bremen, Germany

Basics

Let R be a ring. Denote:

- $\mathrm{MA}_n(R)$ the set of polynomial endomorphisms,
- $\mathrm{GA}_n(R)$ the set of polynomial automorphisms,
- $\mathrm{BA}_n^0(R)$ is the set of strictly upper triangular polynomial automorphisms,
- $\mathrm{TA}_n(R) := < \mathrm{BA}^0(R), \mathrm{GL}_n(R) >$ the set of tame polynomial automorphisms,
- $\mathrm{SA}_n(R) = \{F \in \mathrm{GA}_n(R) \mid \det(\mathrm{Jac}(F)) = 1\}$,
- $\mathrm{STA}_n(R) = \mathrm{TA}_n(R) \cap \mathrm{SA}_n(R)$.

Let $q = p^m$ where p is prime. We can define

$$\pi_q : \mathrm{MA}_n(\mathbb{F}_q) \longrightarrow \mathrm{Maps}((\mathbb{F}_q)^n, (\mathbb{F}_q)^n)$$

and thus also

$$\pi_q : \mathrm{GA}_n(\mathbb{F}_q) \longrightarrow \mathrm{Perm}((\mathbb{F}_q)^n).$$

Main question

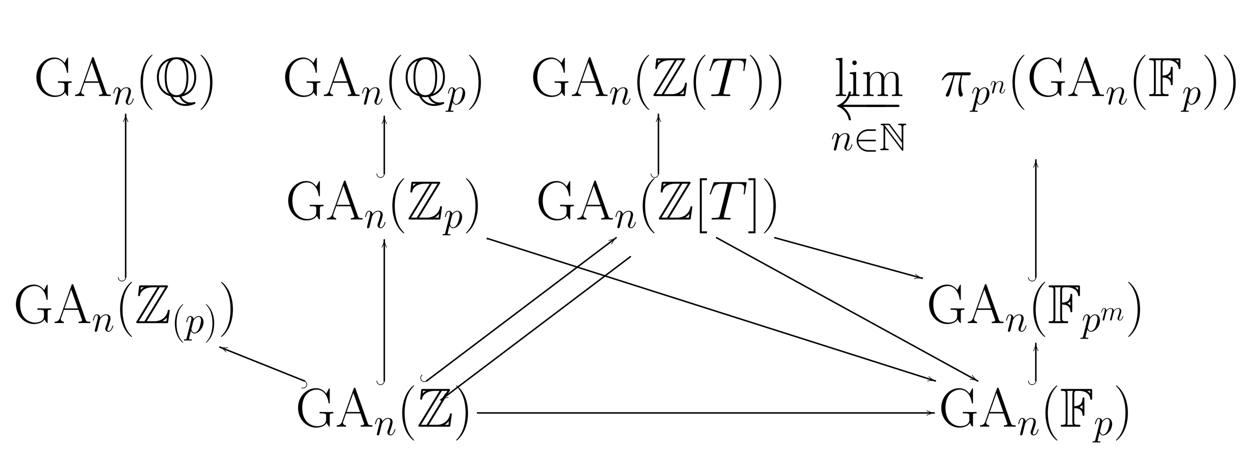
What is $\pi_{q^m}(\mathrm{GA}_n(\mathbb{F}_q), \pi_{q^m}(\mathrm{TA}_n(\mathbb{F}_q))$ and are they different?

Finding a difference would imply that there exist wild polynomial automorphisms.

Theorems on the case $m = 1$

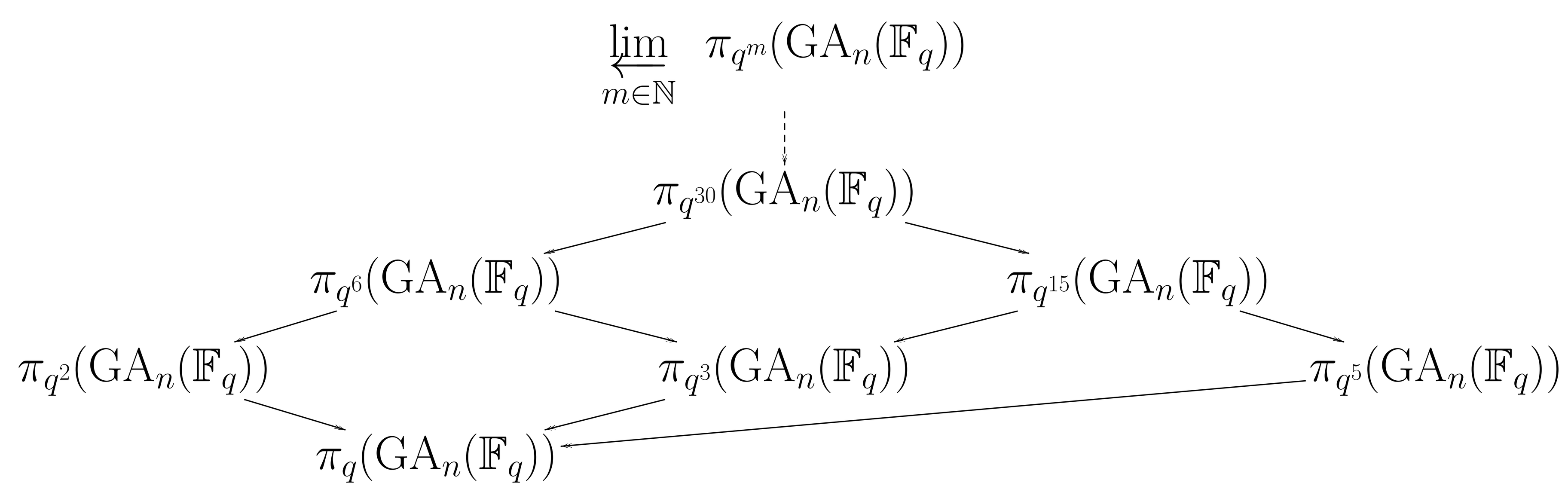
- $\pi_q \mathrm{TA}_n(\mathbb{F}_q) = \mathrm{Sym}((\mathbb{F}_q)^n)$ if q =odd or $q = 2$, and .
- $\pi_q \mathrm{TA}_n(\mathbb{F}_q) = \mathrm{Alt}((\mathbb{F}_q)^n)$ if q = even but not $q = 2$.
- $\pi_q \mathrm{STA}_n(\mathbb{F}_q) = \mathrm{Alt}((\mathbb{F}_q)^n)$,
- unless $q = 2$, when it is $\mathrm{Sym}((\mathbb{F}_q)^n)$.

Interesting connections



The profinite polynomial automorphism group

Since there exist restriction maps $\pi_{q^m} \mathrm{GA}_n(\mathbb{F}_q) \longrightarrow \pi_q \mathrm{GA}_n(\mathbb{F}_q)$ we get the following chain and inverse limit:



We call $\varprojlim_{m\in\mathbb{N}} \pi_{q^m}(\mathrm{GA}_n(\mathbb{F}_q))$ the profinite polynomial automorphism group (which contains $\mathrm{GA}_n(\mathbb{F}_q)$). Similarly, we define the profinite tame automorphism group $\varprojlim_{m\in\mathbb{N}} \pi_{q^m}(\mathrm{GA}_n(\mathbb{F}_q))$ and profinite polynomial endomorphisms $\varprojlim_{m\in\mathbb{N}} \pi_{q^m}(\mathrm{MA}_n(\mathbb{F}_q))$.

Theorem: Wild automorphisms in profinite tame group

Assume (1) $F \in \mathrm{GA}_n(\mathbb{F}_q[X_{n+1}])$, (2) $F \in \mathrm{TA}_n(\mathbb{F}_q(X_{n+1}))$, (3) $F(X_{n+1} = c) \in \mathrm{TA}_n(\mathbb{F}_q)$ for all $c \in \mathbb{F}_q$.

Then F is in the profinite tame automorphism group, i.e.

$$F \in \varprojlim_{m\in\mathbb{N}} \pi_{q^m}(\mathrm{TA}_n(\mathbb{F}_q)).$$

In particular:

$$\mathrm{GA}_2(\mathbb{F}_q[Z]) \subseteq \varprojlim_{m\in\mathbb{N}} \pi_{q^m}(\mathrm{TA}_n(\mathbb{F}_q)).$$

This theorem implies that it is not possible to distinguish for example Nagata's automorphism from a tame automorphism by only examining its permutations.

A theorem on the Derksen group

If $n \geq 3$, define $\mathrm{DA}_n(\mathbb{F}_q) = < \mathrm{Aff}_n(\mathbb{F}_q), E >$ where

$$E = (x_1 + (x_1 x_3 \cdots x_n)^{p-1}, x_2, \ldots, x_n).$$

This group we called the Derksen group. Theorem:

$$\varprojlim_{m\in\mathbb{N}} \pi_{q^m}(\mathrm{DA}_n(\mathbb{F}_q)) = \varprojlim_{m\in\mathbb{N}} \pi_{q^m}(\mathrm{TA}_n(\mathbb{F}_q))$$

so we do have actual smaller groups that give the same profinite groups. Well - as soon as we prove that $\mathrm{DA}_n(\mathbb{F}_q)$ is not equal to $\mathrm{TA}_n(\mathbb{F}_q)$!

The profinite polynomial endomorphism monoid

We define $\varprojlim_{m\in\mathbb{N}} \pi_{q^m}(\mathrm{MA}_n(\mathbb{F}_q))$ as the profinite polynomial endomorphism monoid. Consider

$$\mathcal{M}_{n,m}(\mathbb{F}_q) := \pi_{q^m} \mathrm{MA}_n(\mathbb{F}_q) \cap \mathrm{Perm}((\mathbb{F}_{q^m})^n).$$

Then $\varprojlim_{m\in\mathbb{N}} \mathcal{M}_{n,m}(\mathbb{F}_q)$ is the subset of invertible elements in $\varprojlim_{m\in\mathbb{N}} \pi_{q^m}(\mathrm{MA}_n(\mathbb{F}_q))$, i.e. we can call it the profinite polynomial endomorphism group. How does it look like? Define X as the set of orbits of $\mathbb{F}_{q^m}^n$ under the action of $\mathrm{Gal}(\mathbb{F}_{q^m} : \mathbb{F}_q)$, and let X_d be the set of orbits of size d. Then

$$\varprojlim_{m\in\mathbb{N}} \mathcal{M}_{n,m}(\mathbb{F}_q) \cong \prod_{d\in\mathbb{N}} \left((\mathbb{Z}/d\mathbb{Z}) \,\mathrm{wr}_{X_d}\, \mathrm{Perm}(X_d)\right).$$

Profinite tame group vs. profinite polynomial endomorphism group

How much does $\varprojlim_{m\in\mathbb{N}} \pi_{q^m}(\mathrm{GA}_n(\mathbb{F}_q))$ differ from $\varprojlim_{m\in\mathbb{N}} \mathcal{M}_{n,m}(\mathbb{F}_q)$? By far it is not equal - but: define

$$\Pi_q : \mathrm{GA}_n(\mathbb{F}_q) \longrightarrow \mathrm{Perm}(X)$$

then consider $\Pi_{q^m}(\mathrm{TA}_n(\mathbb{F}_q))$. Apparently:

$\Pi_{q^m}(\mathrm{TA}_n(\mathbb{F}_q)) = \mathcal{M}_{n,m}(\mathbb{F}_q)$ if $n \geq 3$ except finitely many q. In particular: $\Pi_{q^m}(\mathrm{GA}_n(\mathbb{F}_q)) = \mathcal{M}_{n,m}(\mathbb{F}_q)$ in those cases!

This gives a foothold in tacking (parts of) the main question!

Alternative to LFIHderivations: $\mathbb{Z}$-flows

If k a field, then k-actions on k^n correspond to locally nilpotent derivations (LNDs) on $k^{[n]}$ if char $k = 0$. If $\mathrm{char}(k) = p$, then k-actions on k^n correspond to so-called *locally finite iterative higher derivations.* Longer name, less nice properties! For example:

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

is a unipotent map, but is not exponent of a LFIHD if $\mathrm{char}(k) = 2$ (for $\exp(D)$ has order p). Bah!

Example of a $\mathbb{Z}$-flow

Define

$$R := \mathbb{Z}[Q_i \mid i \in \mathbb{N}]/(p, Q_i^p - Q_i \mid i \in \mathbb{N})$$

where Q_i corresponds to $\mathbb{Z} \longrightarrow \mathbb{F}_p$ given by $t \longrightarrow \binom{t}{p^i}$ mod p. Then $F := (x + y + z, y + z, z) \in \mathrm{TA}_3(\mathbb{F}_2)$ has a "$\mathbb{Z}$-flow":

$$F_t := (x + Q_0 y + (Q_1 + Q_0)z, y + Q_0 z, z).$$

Indeed, $F_t(t = n) = F^n$ for each $n \in \mathbb{Z}$.

Interesting object

This opens up the idea to examine $\mathrm{GA}_n(R)$.

Fast forward functions from cryptography

It is desireable of a function f if $f^n(v)$ is efficently computable w.r.t. computation of $f(v)$ for any n, v. Let $\sigma \in \pi_p(\mathrm{BA}_n^0(\mathbb{F}_p))$ such that σ has only one orbit in $\mathbb{F}_p^n$. Then there exists $\tau \in \mathrm{BA}_n^0(\mathbb{F}_p)$, D a diagonal linear map, and a trivial map $\zeta : (\mathbb{F}_p)^n \longrightarrow \mathbb{Z}/p^n\mathbb{Z}$ such that

$$\zeta D \tau \sigma \tau^{-1} D^{-1} \zeta^{-1} = \mathrm{inc}$$

where $\mathrm{inc}(z) = z + 1$ on $\mathbb{Z}/p^n\mathbb{Z}$, making iterations of σ efficiently computable.

References

[1] S.Maubach, *Polynomial automorphisms over finite fields.* Serdica Math. J. 27 (2001) no.4. 343-350

[2] S.Maubach, R.Willems,*Polynomial automorphisms over finite fields: Mimicking non-tame and tame maps by the Derksen group.* Serdica math. J. 37, 2011 (305-322)

[3] S.Maubach, *Triangular polynomial $\mathbb{Z}$-actions on $\mathbb{F}_p^n$ and a cryptographic application.* Arxiv:1106.5800