Recursive constructions of irreducible polynomials over finite fields

Carleton FF Day 2017 - Ottawa

Lucas Reis (UFMG - Carleton U)

September 2017

- $\mathbb{F}_q$: finite field with q elements, q a power of p.

- $\mathbb{F}_q$: finite field with q elements, q a power of p.
- $\mathrm{GL}_2(\mathbb{F}_q)$: 2$x$2 non-singular matrices with entries in $\mathbb{F}_q$.

- $\mathbb{F}_q$: finite field with q elements, q a power of p.
- $\mathrm{GL}_2(\mathbb{F}_q)$: 2$x$2 non-singular matrices with entries in $\mathbb{F}_q$.

Given $f(x) \in \mathbb{F}_q[x]$ of degree n and $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_q)$,

- $\mathbb{F}_q$: finite field with q elements, q a power of p.
- $\mathrm{GL}_2(\mathbb{F}_q)$: 2$x$2 non-singular matrices with entries in $\mathbb{F}_q$.

Given $f(x) \in \mathbb{F}_q[x]$ of degree n and $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_q)$,

$$A \circ f := (bx + d)^n f\left(\frac{ax + c}{bx + d}\right).$$

- $\mathbb{F}_q$: finite field with q elements, q a power of p.
- $\mathrm{GL}_2(\mathbb{F}_q)$: 2x2 non-singular matrices with entries in $\mathbb{F}_q$.

Given $f(x) \in \mathbb{F}_q[x]$ of degree n and $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_q)$,

$$A \circ f := (bx + d)^n f\left(\frac{ax + c}{bx + d}\right).$$

For $B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $B \circ f = x^n f\left(\frac{1}{x}\right)$ is the reciprocal of $f(x)$.

$$\mathcal{M} := \{f \in \mathbb{F}_q[x] \mid f \text{ has no root in } \mathbb{F}_q\}.$$

$\mathcal{M} := \{f \in \mathbb{F}_q[x] \mid f \text{ has no root in } \mathbb{F}_q\}$.

Basic Properties.

For A, B be elements of $\mathrm{GL}_2(\mathbb{F}_q)$ and $f, g \in \mathcal{M}$, the following hold:

(i) $A \circ f \in \mathcal{M}$ and $\deg(A \circ f) = \deg f$,

(ii) If E denotes the identity element of $\mathrm{GL}_2(\mathbb{F}_q)$, then $E \circ f = f$,

(iii) $(AB) \circ f = A \circ (B \circ f)$,

(iv) $A \circ (f \cdot g) = (A \circ f) \cdot (A \circ g)$,

(v) f is irreducible if and only if $A \circ f$ is irreducible.

- $\mathcal{I}_n :=$ irreducible monic polynomials of degree n.

- $\mathcal{I}_n :=$ irreducible monic polynomials of degree n.
- $\mathrm{PGL}_2(\mathbb{F}_q)$: $\mathrm{GL}_2(\mathbb{F}_q)/\sim$ (matrices up to a constant).

- $\mathcal{I}_n :=$ irreducible monic polynomials of degree n.
- $\mathrm{PGL}_2(\mathbb{F}_q)$: $\mathrm{GL}_2(\mathbb{F}_q)/\sim$ (matrices up to a constant).

Definition

For $[A] \in \mathrm{PGL}_2(\mathbb{F}_q)$ and $f \in \mathcal{I}_n$, $n \geq 2$, $[A] \circ f$ is the only monic polynomial $= \lambda \cdot (A \circ f)$ with $\lambda \in \mathbb{F}_q^*$.

- $\mathcal{I}_n :=$ irreducible monic polynomials of degree n.
- $\mathrm{PGL}_2(\mathbb{F}_q)$: $\mathrm{GL}_2(\mathbb{F}_q)/\sim$ (matrices up to a constant).

Definition

For $[A] \in \mathrm{PGL}_2(\mathbb{F}_q)$ and $f \in \mathcal{I}_n$, $n \geq 2$, $[A] \circ f$ is the only monic polynomial $= \lambda \cdot (A \circ f)$ with $\lambda \in \mathbb{F}_q^*$.

* From the basic properties, $\mathrm{PGL}_2(\mathbb{F}_q)$ **acts** on $\mathcal{I}_n, n \geq 2$ via the compositions $[A] \circ f$.

- $\mathcal{I}_n :=$ irreducible monic polynomials of degree n.
- $\mathrm{PGL}_2(\mathbb{F}_q)$: $\mathrm{GL}_2(\mathbb{F}_q)/\sim$ (matrices up to a constant).

Definition

For $[A] \in \mathrm{PGL}_2(\mathbb{F}_q)$ and $f \in \mathcal{I}_n$, $n \geq 2$, $[A] \circ f$ is the only monic polynomial $= \lambda \cdot (A \circ f)$ with $\lambda \in \mathbb{F}_q^*$.

* From the basic properties, $\mathrm{PGL}_2(\mathbb{F}_q)$ **acts** on $\mathcal{I}_n, n \geq 2$ via the compositions $[A] \circ f$.

How about the invariants?

- $\mathcal{I}_n :=$ irreducible monic polynomials of degree n.
- $\mathrm{PGL}_2(\mathbb{F}_q)$: $\mathrm{GL}_2(\mathbb{F}_q)/\sim$ (matrices up to a constant).

Definition

For $[A] \in \mathrm{PGL}_2(\mathbb{F}_q)$ and $f \in \mathcal{I}_n$, $n \geq 2$, $[A] \circ f$ is the only monic polynomial $= \lambda \cdot (A \circ f)$ with $\lambda \in \mathbb{F}_q^*$.

* From the basic properties, $\mathrm{PGL}_2(\mathbb{F}_q)$ **acts** on $\mathcal{I}_n, n \geq 2$ via the compositions $[A] \circ f$.

How about the invariants?

$C_A(n) := \{f \in \mathcal{I}_n \mid [A] \circ f = f\}$,

- $\mathcal{I}_n :=$ irreducible monic polynomials of degree n.
- $\mathrm{PGL}_2(\mathbb{F}_q)$: $\mathrm{GL}_2(\mathbb{F}_q)/\sim$ (matrices up to a constant).

Definition

For $[A] \in \mathrm{PGL}_2(\mathbb{F}_q)$ and $f \in \mathcal{I}_n$, $n \geq 2$, $[A] \circ f$ is the only monic polynomial $= \lambda \cdot (A \circ f)$ with $\lambda \in \mathbb{F}_q^*$.

* From the basic properties, $\mathrm{PGL}_2(\mathbb{F}_q)$ **acts** on $\mathcal{I}_n, n \geq 2$ via the compositions $[A] \circ f$.

How about the invariants?

$C_A(n) := \{f \in \mathcal{I}_n \mid [A] \circ f = f\}$, $N_A(n) = |C_A(n)|$

- $\mathcal{I}_n :=$ irreducible monic polynomials of degree n.
- $\mathrm{PGL}_2(\mathbb{F}_q)$: $\mathrm{GL}_2(\mathbb{F}_q)/\sim$ (matrices up to a constant).

Definition

For $[A] \in \mathrm{PGL}_2(\mathbb{F}_q)$ *and* $f \in \mathcal{I}_n$, $n \geq 2$, $[A] \circ f$ *is the only monic polynomial* $= \lambda \cdot (A \circ f)$ *with* $\lambda \in \mathbb{F}_q^*$.

* From the basic properties, $\mathrm{PGL}_2(\mathbb{F}_q)$ **acts** on $\mathcal{I}_n, n \geq 2$ via the compositions $[A] \circ f$.

How about the invariants?

$C_A(n) := \{f \in \mathcal{I}_n \mid [A] \circ f = f\}$, $N_A(n) = |C_A(n)|$

$$C_A := \bigcup_{n \geq 2} C_A(n).$$

A characterization of C_A:

A characterization of C_A:

Theorem (Stichtenoth, Topuzoglu - FFA 2012)

Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *be an element of* $\mathrm{GL}_2(\mathbb{F}_q)$. *For each nonnegative integer* r, *set*

$$F_r(x) = bx^{q^r+1} - ax^{q^r} + dx - c.$$

For any $f \in \mathcal{I}_n$ *with* $n \geq 2$, *the following are equivalent:*

(i) $f(x)$ *divides* $F_r(x)$ *for some* $r \geq 0$,

(ii) $[A] \circ f = f$.

Set $D = \mathrm{o}rd([A])$: any element of C_A has degree 2 or degree Dm for some $m \geq 1$.

Set $D = \mathrm{o}rd([A])$: any element of C_A has degree 2 or degree Dm for some $m \geq 1$.

In particular, $N_A(n) = 0$ if $n > 2$ and n is not divisible by D.

Set $D = \mathrm{o}rd([A])$: any element of C_A has degree 2 or degree Dm for some $m \geq 1$.

In particular, $N_A(n) = 0$ if $n > 2$ and n is not divisible by D.Also,

$$N_A(Dm) \approx \frac{\Phi(D)}{Dm} q^m.$$

Set $D = \mathrm{o}rd([A])$: any element of C_A has degree 2 or degree Dm for some $m \geq 1$.

In particular, $N_A(n) = 0$ if $n > 2$ and n is not divisible by D.Also,

$$N_A(Dm) \approx \frac{\Phi(D)}{Dm} q^m.$$

Enumeration formulas:

1. Garefalakis (JPAA - 2011): upper triangular elements.
2. Mattarei and Pizzato (FFA - 2017): involutions, following a work of O. Ahmadi.
3. R. (Arxiv - 2017): general elements of $\mathrm{PGL}_2(\mathbb{F}_q)$.

Alternative characterization of the invariants.

Alternative characterization of the invariants.

An irreducible polynomial $f(x)$ of degree $2m$ is self-reciprocal if and only if $f(x)$ is an irreducible of the form $x^m g\left(x + x^{-1}\right)$ for some $g(x)$ of degree m.

1. R. (JPAA - 2017):
   - $A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, i.e., $[A] \circ f = (x)f(x+1)$.

1. R. (JPAA - 2017):

    - $A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, i.e., $[A] \circ f = (x) f(x+1)$.
      The invariants appear as $f(x) = g(x^p - x)$.

1. R. (JPAA - 2017):
   - $A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, i.e., $[A] \circ f = (x) f(x+1)$.
     The invariants appear as $f(x) = g(x^p - x)$.
   - $A = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$, i.e., $[A] \circ f(x) = f(ax)$.

1. R. (JPAA - 2017):
   - $A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, i.e., $[A] \circ f = (x) f(x+1)$.
     The invariants appear as $f(x) = g(x^p - x)$.
   - $A = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$, i.e., $[A] \circ f(x) = f(ax)$.
     The invariants appear as $f(x) = g(x^k)$, where $k = \mathrm{o}rd(a)$.

1. R. (JPAA - 2017):
   - $A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, i.e., $[A] \circ f = (x)f(x+1)$.
     The invariants appear as $f(x) = g(x^p - x)$.
   - $A = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$, i.e., $[A] \circ f(x) = f(ax)$.
     The invariants appear as $f(x) = g(x^k)$, where $k = \mathrm{o}rd(a)$.
2. Mattarei and Pizzato (FFA - 2017): involutions.

   The invariants apperar as $f(x) = h_2^n \cdot g(h_1/h_2)$, where

   $h_1/h_2 \in \mathbb{F}_q(x)$ is a quadratic rational function.

Theorem (R., August 2017)

Let $[A] \in \mathrm{PGL}_2(\mathbb{F}_q)$ *with* $\mathrm{ord}([A]) = D > 1$. *There exists a rational function* $R(A) = \frac{g_A}{h_A}$ *of degree* D *such that* $f \in \mathcal{I}_{Dm}$ *satisfies* $[A] \circ f = f$ *if and only if* $f(x)$ *is an irreducible monic polynomial of the form* $h_A^m F(\frac{g_A}{h_A})$ *for some* F *of degree* m.

Moreover, the rational function $R(A)$ *can be computed from the element* A.

Conjugacy classes in $\mathrm{PGL}_2(\mathbb{F}_q)$:

Conjugacy classes in $\mathrm{PGL}_2(\mathbb{F}_q)$:

1. type 1: $A(a) := \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$, $R(A) = x^k$,

Conjugacy classes in $\mathrm{PGL}_2(\mathbb{F}_q)$:

1. type 1: $A(a) := \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$, $R(A) = x^k$,
2. type 2: $\mathcal{B} := \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, $R(A) = x^p - x$

Conjugacy classes in $\mathrm{PGL}_2(\mathbb{F}_q)$:

1. type 1: $A(a) := \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$, $R(A) = x^k$,
2. type 2: $\mathcal{B} := \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, $R(A) = x^p - x$
3. type 3: $C(b) := \begin{pmatrix} 0 & 1 \\ b & 0 \end{pmatrix}$, $R(A) = \frac{x^2+b}{2x}$

Conjugacy classes in $\mathrm{PGL}_2(\mathbb{F}_q)$:

1. type 1: $A(a) := \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$, $R(A) = x^k$,
2. type 2: $\mathcal{B} := \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, $R(A) = x^p - x$
3. type 3: $C(b) := \begin{pmatrix} 0 & 1 \\ b & 0 \end{pmatrix}$, $R(A) = \frac{x^2+b}{2x}$
4. type 4: $D(c) := \begin{pmatrix} 0 & c \\ 1 & 1 \end{pmatrix}$, $R(A) = \sum_{i=1}^{D} \Psi_A^{(i)}(x)$, where

$$\Psi_A(x) = \frac{1}{cx+1}.$$

Conjugacy classes in $\mathrm{PGL}_2(\mathbb{F}_q)$:

1. type 1: $A(a) := \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$, $R(A) = x^k$,
2. type 2: $\mathcal{B} := \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, $R(A) = x^p - x$
3. type 3: $C(b) := \begin{pmatrix} 0 & 1 \\ b & 0 \end{pmatrix}$, $R(A) = \frac{x^2+b}{2x}$
4. type 4: $D(c) := \begin{pmatrix} 0 & c \\ 1 & 1 \end{pmatrix}$, $R(A) = \sum_{i=1}^{D} \Psi_A^{(i)}(x)$, where

$$\Psi_A(x) = \frac{1}{cx+1}.$$

The $R(A)$'s above are called *canonical rational functions*.

Rational transformations:

Rational transformations:

For $f \in \mathbb{F}_q[x]$ irreducible with $\deg f = n$ and $Q(x) \in \mathbb{F}_q(x)$ of degree D, $Q(x) = F(x)/G(x)$, set

$$f^Q = G^n \cdot f\left(\frac{F}{G}\right).$$

Rational transformations:

For $f \in \mathbb{F}_q[x]$ irreducible with $\deg f = n$ and $Q(x) \in \mathbb{F}_q(x)$ of degree D, $Q(x) = F(x)/G(x)$, set

$$f^Q = G^n \cdot f\left(\frac{F}{G}\right).$$

Also, set $f_0 = f$ and $f_i = f_{i-1}^Q$,

Rational transformations:

For $f \in \mathbb{F}_q[x]$ irreducible with $\deg f = n$ and $Q(x) \in \mathbb{F}_q(x)$ of degree D, $Q(x) = F(x)/G(x)$, set

$$f^Q = G^n \cdot f\left(\frac{F}{G}\right).$$

Also, set $f_0 = f$ and $f_i = f_{i-1}^Q$,

$$\deg f_i = D \cdot \deg f_{i-1}.$$

Rational transformations:

For $f \in \mathbb{F}_q[x]$ irreducible with $\deg f = n$ and $Q(x) \in \mathbb{F}_q(x)$ of degree D, $Q(x) = F(x)/G(x)$, set

$$f^Q = G^n \cdot f\left(\frac{F}{G}\right).$$

Also, set $f_0 = f$ and $f_i = f_{i-1}^Q$,

$$\deg f_i = D \cdot \deg f_{i-1}.$$

Given f irreducible of degree n, we want to obtain an infinite sequence of irreducibles $\{f_i\}_{i\geq 0}$ of degree $D^i \cdot n$, via $Q(x)$-transformations, where Q is a canonical rational function.

Theorem (Cohen)

Let $f(x)$ be irreducible of degree n over $\mathbb{F}_q$ and $\alpha \in \mathbb{F}_{q^n}$ one of its roots. Then $f^Q = G^n \cdot f\left(\frac{F}{G}\right)$ is irreducible if and only if $F(x) - \alpha G(x)$ is irreducible over $\mathbb{F}_{q^n}$.

Theorem (Cohen)

Let $f(x)$ be irreducible of degree n over $\mathbb{F}_q$ and $\alpha \in \mathbb{F}_{q^n}$ one of its roots. Then $f^Q = G^n \cdot f\left(\frac{F}{G}\right)$ is irreducible if and only if $F(x) - \alpha G(x)$ is irreducible over $\mathbb{F}_{q^n}$.

Fact: If $D = \mathrm{o}rd([A])$ is prime, $Q = R(A) = f_A/g_A$, then $f_A - \alpha g_A$ is either irreducible or splits completely over $\mathbb{F}_{q^n}$.

Theorem (Cohen)

Let $f(x)$ be irreducible of degree n over $\mathbb{F}_q$ and $\alpha \in \mathbb{F}_{q^n}$ one of its roots. Then $f^Q = G^n \cdot f\left(\frac{F}{G}\right)$ is irreducible if and only if $F(x) - \alpha G(x)$ is irreducible over $\mathbb{F}_{q^n}$.

Fact: If $D = \mathrm{o}rd([A])$ is prime, $Q = R(A) = f_A/g_A$, then $f_A - \alpha g_A$ is either irreducible or splits completely over $\mathbb{F}_{q^n}$.

In particular, if D is prime, f^Q is either irreducible or split into D irreducible factors, each of degree n.

Theorem (Cohen)

Let $f(x)$ be irreducible of degree n over $\mathbb{F}_q$ and $\alpha \in \mathbb{F}_{q^n}$ one of its roots. Then $f^Q = G^n \cdot f\left(\frac{F}{G}\right)$ is irreducible if and only if $F(x) - \alpha G(x)$ is irreducible over $\mathbb{F}_{q^n}$.

Fact: If $D = \mathrm{o}rd([A])$ is prime, $Q = R(A) = f_A/g_A$, then $f_A - \alpha g_A$ is either irreducible or splits completely over $\mathbb{F}_{q^n}$.

In particular, if D is prime, f^Q is either irreducible or split into D irreducible factors, each of degree n.

The roots of $f_A - \alpha g_A$ can be explored through the dynamics of the map $x \mapsto \frac{f_A(x)}{g_A(x)}$ in $\overline{\mathbb{F}}_q$: in general, the functional graph is full of symmetries.

Methods:

Methods:

1. **Deterministic**: initial conditions on f for f^Q to be irreducible.

   For instance, $Q = x^p - x$, $f(x)$ must be of non-zero trace and

   $Q = x^k$, some conditions on the order $\mathrm{o}rd(f)$ of $f(x)$.

Methods:

1. **Deterministic**: initial conditions on f for f^Q to be irreducible. For instance, $Q = x^p - x$, $f(x)$ must be of non-zero trace and $Q = x^k$, some conditions on the order $\mathrm{o}rd(f)$ of $f(x)$.
2. **Iterated trials**: works for D prime; if f^Q is not irreducible, it splits into D irreducible factors of degree n. Pick one of those irreducibles, apply Q again. Eventually we find an irreducible.

Methods:

1. **Deterministic**: initial conditions on f for f^Q to be irreducible. For instance, $Q = x^p - x$, $f(x)$ must be of non-zero trace and $Q = x^k$, some conditions on the order $ord(f)$ of $f(x)$.
2. **Iterated trials**: works for D prime; if f^Q is not irreducible, it splits into D irreducible factors of degree n. Pick one of those irreducibles, apply Q again. Eventually we find an irreducible. For self-reciprocals, $D = 2$, (Ugolini - DCC 2015).

Methods:

1. **Deterministic**: initial conditions on f for f^Q to be irreducible. For instance, $Q = x^p - x$, $f(x)$ must be of non-zero trace and $Q = x^k$, some conditions on the order $\mathrm{o}rd(f)$ of $f(x)$.
2. **Iterated trials**: works for D prime; if f^Q is not irreducible, it splits into D irreducible factors of degree n. Pick one of those irreducibles, apply Q again. Eventually we find an irreducible. For self-reciprocals, $D = 2$, (Ugolini - DCC 2015).
3. **Probabilistic**: pick a random irreducible f of degree n and check if f^Q is irreducible or not.

Efficiency of iterations: if A is of type 1, 3 or 4 and $Q = R(A)$, once f_i is irreducible, f_j is irreducible for any $j \geq i$.

Efficiency of iterations: if A is of type 1, 3 or 4 and $Q = R(A)$, once f_i is irreducible, f_j is irreducible for any $j \geq i$.

The case A of type 1 is a classical result.

Efficiency of iterations: if A is of type 1, 3 or 4 and $Q = R(A)$, once f_i is irreducible, f_j is irreducible for any $j \geq i$.

The case A of type 1 is a classical result.

The case A of type 4 or 3, we can verify that the map $x \mapsto \frac{f_A(x)}{g_A(x)}$ is "conjugated" to map $x \mapsto x^D$ in $\overline{\mathbb{F}}_q$, via Mobius permutations.

Efficiency of iterations: if A is of type 1, 3 or 4 and $Q = R(A)$, once f_i is irreducible, f_j is irreducible for any $j \geq i$.

The case A of type 1 is a classical result.

The case A of type 4 or 3, we can verify that the map $x \mapsto \frac{f_A(x)}{g_A(x)}$ is "conjugated" to map $x \mapsto x^D$ in $\overline{\mathbb{F}}_q$, via Mobius permutations.

* The case A of type 2 is more complicated: if $f_i = f_{i-1}(x^p - x)$ is irreducible, f_{i+1} is reducible.

Iterated trial: related to the functional graph of the map $x \mapsto \frac{f_A(x)}{g_A(x)}$.

Iterated trial: related to the functional graph of the map $x \mapsto \frac{f_A(x)}{g_A(x)}$.

Insert a functional graph.

Suppose that $Q = R(A) = f_A/g_A$ is a canonical rational function associated to A, with $\mathrm{o}rd([A]) = D$.

Suppose that $Q = R(A) = f_A/g_A$ is a canonical rational function associated to A, with $\mathrm{o}rd([A]) = D$.

$$N_A(Dn) \approx \frac{\Phi(D)}{Dn} q^n, n >> 1$$

Suppose that $Q = R(A) = f_A/g_A$ is a canonical rational function associated to A, with $\mathrm{o}rd([A]) = D$.

$$N_A(Dn) \approx \frac{\Phi(D)}{Dn} q^n, n >> 1$$

We know that the invariants of degree Dn arise from f^Q, with f of degree n.

Suppose that $Q = R(A) = f_A/g_A$ is a canonical rational function associated to A, with $\mathrm{o}rd([A]) = D$.

$$N_A(Dn) \approx \frac{\Phi(D)}{Dn} q^n, n >> 1$$

We know that the invariants of degree Dn arise from f^Q, with f of degree n.

Necessary condition: f must be irreducible. How many they are?

Suppose that $Q = R(A) = f_A/g_A$ is a canonical rational function associated to A, with $\mathrm{o}rd([A]) = D$.

$$N_A(Dn) \approx \frac{\Phi(D)}{Dn} q^n, n >> 1$$

We know that the invariants of degree Dn arise from f^Q, with f of degree n.

Necessary condition: f must be irreducible. How many they are? Close to $\frac{q^n}{n}, n >> 1$.

Random Method:

Random Method:

Pick f irreducible of degree n. If f^Q is irreducible, proceed with the iterations $f_i = f_{i-1}^Q$. If not, pick another irreducible of degree n.

Random Method:

Pick f irreducible of degree n. If f^Q is irreducible, proceed with the iterations $f_i = f_{i-1}^Q$. If not, pick another irreducible of degree n.

In particular, for a random irreducible of degree n, f^Q is also irreducible with probability $p_A \approx \frac{\Phi(D)}{D}$.

Random Method:

Pick f irreducible of degree n. If f^Q is irreducible, proceed with the iterations $f_i = f_{i-1}^Q$. If not, pick another irreducible of degree n.

In particular, for a random irreducible of degree n, f^Q is also irreducible with probability $p_A \approx \frac{\Phi(D)}{D}$.

Geometric Distribution with $p = p_A$.

Random Method:

Pick f irreducible of degree n. If f^Q is irreducible, proceed with the iterations $f_i = f_{i-1}^Q$. If not, pick another irreducible of degree n.

In particular, for a random irreducible of degree n, f^Q is also irreducible with probability $p_A \approx \frac{\Phi(D)}{D}$.

Geometric Distribution with $p = p_A$.

In particular, the expected number of trials is $\frac{1}{p_A} \approx \frac{D}{\Phi(D)}$.

Random Method:

Pick f irreducible of degree n. If f^Q is irreducible, proceed with the iterations $f_i = f_{i-1}^Q$. If not, pick another irreducible of degree n.

In particular, for a random irreducible of degree n, f^Q is also irreducible with probability $p_A \approx \frac{\Phi(D)}{D}$.

Geometric Distribution with $p = p_A$.

In particular, the expected number of trials is $\frac{1}{p_A} \approx \frac{D}{\Phi(D)}$.

For D prime, $\frac{D}{\Phi(D)} = \frac{D}{D-1} \leq 2$.

Example 1: $A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_2)$

Example 1: $A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_2)$

$$Q = R(A) = \frac{1}{x+1} + \frac{x+1}{x} + x = \frac{x^3+x+1}{x^2+x}.$$

Example 1: $A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_2)$

$$Q = R(A) = \frac{1}{x+1} + \frac{x+1}{x} + x = \frac{x^3+x+1}{x^2+x}.$$

Set $f_0 = x + 1$ and $f_i = f_{i-1}^Q, i \geq 1$.

Example 1: $A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_2)$

$$Q = R(A) = \frac{1}{x+1} + \frac{x+1}{x} + x = \frac{x^3+x+1}{x^2+x}.$$

Set $f_0 = x+1$ and $f_i = f_{i-1}^{Q}, i \geq 1$.

$f_1 = x^3 + x^2 + 1$

Example 1: $A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_2)$

$$Q = R(A) = \frac{1}{x+1} + \frac{x+1}{x} + x = \frac{x^3+x+1}{x^2+x}.$$

Set $f_0 = x+1$ and $f_i = f_{i-1}^Q, i \geq 1$.

$f_1 = x^3 + x^2 + 1$

$f_2 = x^9 + x + 1$

Example 1: $A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_2)$

$$Q = R(A) = \frac{1}{x+1} + \frac{x+1}{x} + x = \frac{x^3+x+1}{x^2+x}.$$

Set $f_0 = x + 1$ and $f_i = f_{i-1}^Q, i \geq 1.$

$f_1 = x^3 + x^2 + 1$

$f_2 = x^9 + x + 1$

$f_3 = x^{27} + x^{26} + x^{24} + x^{18} + x^{17} + x^{11} + x^9 + x^8 + x^3 + x^2 + 1$

$$f_4 = x^{81} + x^{64} + x^{16} + x + 1$$

$$f_4 = x^{81} + x^{64} + x^{16} + x + 1$$

$$f_5 = x^{243} + x^{242} + x^{240} + x^{227} + x^{225} + x^{224} + x^{210} + x^{209} + x^{195} + x^{194} + x^{192} + x^{179} + x^{177} + x^{176} + x^{162} + x^{161} + x^{147} + x^{146} + x^{144} + x^{131} + x^{129} + x^{128} + x^{114} + x^{113} + x^{99} + x^{98} + x^{96} + x^{83} + x^{81} + x^{80} + x^{66} + x^{65} + x^{51} + x^{50} + x^{48} + x^{35} + x^{33} + x^{32} + x^{18} + x^{17} + x^{3} + x^{2} + 1.$$

Example 2: $A = \begin{pmatrix} 0 & 3 \\ 1 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_5)$

Example 2: $A = \begin{pmatrix} 0 & 3 \\ 1 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_5)$

$$Q = R(A) = \frac{3x^6 + x + 4}{x^5 - x}.$$

Example 2: $A = \begin{pmatrix} 0 & 3 \\ 1 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_5)$

$$Q = R(A) = \frac{3x^6 + x + 4}{x^5 - x}.$$

Set $f_0 = x$ and $f_i = f_{i-1}^Q, i \geq 1$.

Example 2: $A = \begin{pmatrix} 0 & 3 \\ 1 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_5)$

$$Q = R(A) = \frac{3x^6 + x + 4}{x^5 - x}.$$

Set $f_0 = x$ and $f_i = f_{i-1}^Q, i \geq 1$.

$f_1 = x^6 + 2x + 3$

Example 2: $A = \begin{pmatrix} 0 & 3 \\ 1 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_5)$

$$Q = R(A) = \frac{3x^6 + x + 4}{x^5 - x}.$$

Set $f_0 = x$ and $f_i = f_{i-1}^Q, i \geq 1$.

$f_1 = x^6 + 2x + 3$

$f_2 = x^{36} + x^{31} + x^{26} + 2x^{25} + 3x^{11} + 3x^{10} + x^6 + 4x^5 + x + 4$

Example 2: $A = \begin{pmatrix} 0 & 3 \\ 1 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_5)$

$$Q = R(A) = \frac{3x^6 + x + 4}{x^5 - x}.$$

Set $f_0 = x$ and $f_i = f_{i-1}^Q, i \geq 1$.

$f_1 = x^6 + 2x + 3$

$f_2 = x^{36} + x^{31} + x^{26} + 2x^{25} + 3x^{11} + 3x^{10} + x^6 + 4x^5 + x + 4$

$f_3 = x^{216} + 4x^{211} + 3x^{210} + 3x^{206} + 2x^{205} + 2x^{201} + 2x^{200} + 3x^{191} + 2x^{190} + 4x^{185} + x^{181} + 2x^{180} + 4x^{176} + 2x^{175} + 4x^{166} + 2x^{165} + x^{156} + 3x^{155} + x^{151} + 3x^{150} + 4x^{141} + 3x^{140} + x^{131} + 3x^{130} + 2x^{125} + x^{91} + 3x^{90} + 4x^{86} + x^{85} + 2x^{81} + 3x^{80} + 2x^{76} + 2x^{66} + 4x^{65} + 2x^{61} + 4x^{60} + 3x^{56} + 3x^{55} + 2x^{51} + x^{50} + 4x^{40} + 4x^{36} + x^{35} + 2x^{31} + x^{30} + 2x^{26} + x^{25} + 2x^{16} + 3x^{15} + 4x^{11} + x^{10} + 3x^6 + 4x^5 + 4x + 1.$

Thank you!