Prescribing Coefficients of Invariant Irreducible Polyomials

Giorgos Kapetanakis

Boğaziçi University Mathematics Colloquium, November 2017

Sabancı University

Supported by TÜBİTAK Project Number 114F432

Where you can find this work:

G. Kapetanakis.
Prescribing coefficients of invariant irreducible polynomials.
Journal of Number Theory, 180(C):615–628, 2017.

Motivation

Some definitions

- By $\mathbf{F}_q$ we denote the finite field of q elements. Let $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}(2, q)$ and $F \in \mathbf{F}_q[X]$. Define

$$A \circ F = (bX + d)^{\deg(F)} F\left(\frac{aX + c}{bX + d}\right).$$

  This defines an action of $\mathrm{GL}(2, q)$ on $\mathbf{F}_q[X]$.

- For $A, B \in \mathrm{GL}(2, q)$ and $F, G \in \mathbf{F}_q[X]$, define

$$A \sim_q B :\iff A = \lambda B, \text{ for some } \lambda \in \mathbf{F}_q^* \text{ and}$$
$$F \sim_q G :\iff F = \lambda G, \text{ for some } \lambda \in \mathbf{F}_q^*$$

- This action induces an action of $\mathrm{PGL}(2, q)$ on $\mathbf{F}_q[X]/\sim_q$.

Some definitions

- For $F \in \mathbf{F}_q[X]$, the equivalence class $[F] := \{G \in \mathbf{F}_q[X] \mid G \sim_q F\}$ consists of polynomials of the same degree with F that are all either irreducible or reducible and every such class contains exactly one monic polynomial.
- Let $\mathbf{I}_n := \{[P] \mid P \in \mathbf{F}_q[X] \text{ irreducible}, \deg(P) = n\}$. It is well-known that the action of $\mathrm{PGL}(2, q)$ we saw before induces an action of $\mathrm{PGL}(2, q)$ on $\mathbf{I}_n$.
- For $A \in \mathrm{GL}(2, q)$ and $n \in \mathbf{N}$, we define

$$\mathbf{I}_n^A := \{[P] \in \mathbf{I}_n \mid [A \circ P] = [P]\}.$$

The study of the set $\mathbf{I}_n^A$

Recently, the set $\mathbf{I}_n^A$ has started gaining attention. Namely, authors have studied

- its cardinality and characterization (Garefalakis 2010, Reis 2017, Stichtenoth and Topuzoğlu 2011) and
- the multiplicative order of the roots of its elements (Martínez et al. 2017),
- while extending these notions to multivariate polynomials has also been investigated (Reis 2017).

Nonetheless, the form (i.e. how these polynomials look) of the elements of $\mathbf{I}_n^A$ (for general A) so far remains to be investigated.

An example

As an example, take $R = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ and some $F \in \mathbf{F}_q[X]$. Then

$$R \circ F = X^{\deg(F)} F(1/X),$$

i.e. the reciprocal of F and $\mathbf{I}_n^R$ is the set of self-reciprocal irreducible polynomials. A result regarding these polynomials is the following

Theorem (Garefalakis-K., 2012-2014)

Let q be odd, $a \in \mathbf{F}_q$ and n, k be such that $k \leq n/2$. There exists some $F = X^{2n} + \sum_{i=0}^{2n-1} f_i X^i \in \mathbf{I}_{2n}^R$ with $f_k = a$, unless $(q, n, k, a) = (3, 3, 1, 0)$ or $(3, 4, 2, 0)$.

Can we say anything about the coefficients of the polynomials of $\mathbf{I}_n^A$ for arbitrary A?

An experiment

Below, we present the results of a quick experiment regarding the set $\mathbf{I}_6^A$, where A is chosen to be $\left(\begin{smallmatrix} 1 & 0 \\ 2 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 2 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $q = 3$.

$A = \left(\begin{smallmatrix} 1 & 0 \\ 2 & 1 \end{smallmatrix}\right)$	$A = \left(\begin{smallmatrix} 2 & 0 \\ 1 & 1 \end{smallmatrix}\right)$	$A = \left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right)$
$X^6 + X^4 + X^3 + X^2 + 2X + 2$	$X^6 + 2X^3 + 2X^2 + X + 1$	$X^6 + 2X^2 + 1$
$X^6 + X^4 + 2X^3 + X^2 + X + 2$	$X^6 + X^4 + 2X^2 + 2X + 2$	$X^6 + X^4 + 2X^2 + 1$
	$X^6 + 2X^4 + X^3 + 2X + 1$	$X^6 + 2X^4 + 1$
	$X^6 + 2X^4 + X^3 + X^2 + X + 2$	$X^6 + 2X^4 + X^2 + 1$

Prescribed coefficients of irreducible polynomials

The most famous result as far as prescribing coefficients of irreducible polynomials over finite fields is concerned, is the following:

Theorem (Hansen-Mullen irreducibility conjecture)

Let $a \in \mathbf{F}_q$, $n \geq 2$ and fix $0 \leq j < n$. There exists an irreducible $P(X) = X^n + \sum_{k=0}^{n-1} p_k X^k \in \mathbf{F}_q[X]$ with $p_j = a$, except when

1. $j = a = 0$ *or*
2. q *is even,* $n = 2$, $j = 1$, *and* $a = 0$.

Prescribed coefficients of irreducible polynomials

- Initially conjectured by Hansen and Mullen 1992.
- Proved for $q > 19$ or $n \geq 36$ by Wan 1997.
- Ham and Mullen 1998 verified the remaining cases by computer search.
- Several extensions have been obtained (i.e. Garefalakis 2008, Panario and Tzanakis 2011)
- While most authors use a variation of Wan's approach, Recently new methods have emerged (Ha 2016, Pollack 2013, Tuxanidy and Wang 2017, Granger 2017).

A note for primitive polynomials

Results from Fan and Han 2003-2004, Cohen 2006 and Cohen and Prešern 2006-2008 settled the Hansen-Mullen primitivity conjecture, which claimed the existence of primitive polynomials over $\mathbf{F}_q$ with prescribed coefficients, only this time with a few additional exceptions.

Our contribution

In this work:

- We confine ourselves to the case when $A \in \mathrm{GL}(2, q)$ is lower-triangular.
- We distinguish two cases: when $A \in \mathrm{GL}(2, q)$ has one eigenvalue and when A has two eigenvalues.
- The conditions, whether a certain coefficient of some $F \in \mathbf{I}_n^A$ can or cannot take any value in $\mathbf{F}_q$ are provided.
- For the former case we provide sufficient conditions for the existence of polynomials of I_n^A that indeed have these coefficients.

Outline of our method

1. We characterize the elements of $\mathbf{I}_n^A$ in two steps:
   a. find $H \in \mathbf{F}_q[X]$ such that $A \circ Q \sim_q Q \iff Q(X) = P(H(X))$ for some $P \in \mathbf{F}_q[X]$ and
   b. then look when this composition is irreducible.
2. We write the arbitrary coefficient of Q as a linear combination of the high-degree coefficients of P, i.e. the low-degree coefficients of P^R, the reciprocal of P
3. We prove the existence of P^R, such that its low-degree coefficients satisfy the above linear expression and such that the composition $P(H(X))$ is irreducible, with the help of Dirichlet characters (Wan's method).

One eigenvalue

Characterization

If A has *one* eigenvalue, then

$$[A] = \begin{cases} \left[\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right], & \text{or} \\ \left[\begin{pmatrix} 1 & 0 \\ \alpha & 1 \end{pmatrix}\right], & \text{for some } \alpha \in \mathbf{F}_q^*. \end{cases}$$

The first situation is already settled. For the second case,

$$A \circ F \sim_q F \iff F(X) \sim_q F(X+\alpha) \iff F(X) = F(X+\alpha),$$

that is F is periodic. We prove the following characterization of those polynomials.

Lemma

Let $\alpha \in \mathbf{F}_q^*$. Some $F \in \mathbf{F}_q[X]$ satisfies $F(X) = F(X+\alpha)$ if and only if there exist some $G \in \mathbf{F}_q[X]$ such that $F(X) = G(X^p - \alpha^{p-1}X)$.

We will use following.

Theorem (Agou, 1977)

Let q be a power of the prime p, $\alpha \in \mathbf{F}_q$ and $P \in \mathbf{I}_n$. The composition $P(X^p - \alpha^{p-1}X)$ is irreducible if and only if $\mathrm{Tr}(p_{n-1}/\alpha^p) \neq 0$, where Tr stands for the trace function $\mathbf{F}_q \to \mathbf{F}_p$.

So, the monic irreducible periodic polynomials are those of the form $Q(X) = P(X^p - \alpha^{p-1}X)$, for some $P \in \mathbf{I}_n$ such that $\mathrm{Tr}(p_{n-1}/\alpha^p) \neq 0$.

Expression of the m-th coefficient

So, the m-th coefficient of Q, where $0 \leq m \leq pn$, is

$$q_m = \sum_{\substack{\max(0, n-m) \leq i \leq n - \lceil m/p \rceil \\ i \equiv m-n \pmod{(p-1)}}} \gamma_i p_i^R,$$

that is a linear expression of some of the $\mu + 1$ low-degree coefficients of the reciprocal of P, where μ is the largest number such that $\gamma_\mu \neq 0$.

A note on μ

Regarding μ, observe that

1. it is possible for such μ to not exist (for example when $m = np - 1$ and $p > 2$) and
2. if $\mu = 0$ or 1, then the value of q_m has to be a given combination of p_0^R and p_1^R, but since neither of them is chosen arbitrarily, it can only take certain values.

So, from now on we assume that μ exists and $\mu \geq 2$.

Define to the following map

$$\sigma : \mathbf{G}_\mu \to \mathbf{F}_q, \quad H \mapsto \sum_{\substack{\max(0,n-m)\le i\le\mu \\ i\equiv m-n \pmod{(p-1)}}} \gamma_i h_i,$$

where $\mathbf{G}_\mu := \{f \in \mathbf{F}_q[X] \mid \deg(f) \le \mu,\ f_0 = 1\}$. The following correlates the inverse image of σ with $\mathbf{G}_{\mu-1}$.

Proposition (Garefalakis-K., 2012)

Let $\kappa \in \mathbf{F}_q$. Set $F \in \mathbf{G}_\mu$ with $f_i := \gamma_{i-1}\gamma_\mu^{-1}$ for $0 < i < \mu$ and $f_\mu := \gamma_\mu^{-1}(\gamma_0 - \kappa)$. The map

$$\tau : \mathbf{G}_{\mu-1} \to \sigma^{-1}(\kappa), \quad H \mapsto HF^{-1} \pmod{X^{\mu+1}}$$

is a bijection.

The following summarizes our observations.

Proposition

Let $\kappa \in \mathbf{F}_q$ and $0 \leq m \leq (p-1)n$. If m, n and p are such that there exist some i with $\lceil m/p \rceil \leq i \leq \min(m, n-1)$ and $i \equiv m \pmod{(p-1)}$ and there exists some $P \in \mathbf{J}_n$ such that $\mathrm{Tr}(p_1/\alpha^{p-1}) \neq 0$ such that $P \equiv HF^{-1} \pmod{X^{\mu+1}}$ for some $H \in \mathbf{G}_{\mu-1}$, then there exists some $Q \in \mathbf{I}_{pn}$, such that $Q(X) = Q(X+\alpha)$ and $q_m = \kappa$.

Characters and character sums

Let

$$\Lambda(H) := \begin{cases} \deg(P), & \text{if } H \text{ is a power of a single irreducible } P, \\ 0, & \text{otherwise,} \end{cases}$$

be the von Mangoldt function on $\mathbf{F}_q[X]$. We define the following weighted sum

$$w := \sum_{H \in \mathbf{G}_{\mu-1}} \Lambda(H) \sum_{\substack{P \in \mathbf{J}_n,\ \mathrm{Tr}(p_1/\alpha^{p-1}) \neq 0 \\ P \equiv HF^{-1} \pmod{X^{\mu+1}}}} 1,$$

where F is the polynomial defined earlier. If $w \neq 0$, we have our desired result.

- Let M be a polynomial of $\mathbf{F}_q$ of degree ≥ 1. The characters of the group $(\mathbf{F}_q[X]/M\mathbf{F}_q[X])^*$ are called Dirichlet characters modulo M.
- Let $U := (\mathbf{F}_q[X]/X^{\mu+1}\mathbf{F}_q[X])^*$. Furthermore, set

$$\psi : U \to \mathbf{C}^*, \quad F \mapsto \exp(2\pi i \operatorname{Tr}(f_1/(f_0\alpha^p))/p)$$

  and notice that for $P \in \mathbf{J}_n$ (where $P \in \mathbf{J}_n \iff P^R \in \mathbf{I}_n$), $\operatorname{Tr}(p_1/\alpha^p) \neq 0 \iff \psi(P) \neq 1$.
- Notice that ψ is also a Dirichlet character modulo $X^{\mu+1}$, while it is clear that $\operatorname{ord}(\psi) = p$.

Weil's theorem of the Riemann hypothesis for function fields implies.

Proposition (Weil)

Let χ be a non-trivial Dirichlet character modulo M such that $\chi(\mathbf{F}_{q^*}) = 1$. Then

$$\left|\sum_{P \in \mathbf{I}_n} \chi(P)\right| \leq \frac{1}{n}(\deg(M) q^{n/2} + 1).$$

Character sum estimates

Proposition

Let χ and ψ be Dirichlet characters modulo M, such that $\mathrm{ord}(\psi) = p$ and $\chi(\mathbf{F}_q^*) = 1$.

1. *If $\chi \notin \langle\psi\rangle$,* $\left|\sum_{\substack{P\in\mathbf{I}_n\\ \psi(P)\neq 1}} \chi(P)\right| \leq \frac{2(p-1)}{pn} \cdot (\deg(M)q^{n/2} + 1)$,
2. *If $\chi \in \langle\psi\rangle^*$,* $\left|\sum_{\substack{P\in\mathbf{I}_n\\ \psi(P)\neq 1}} \chi(P)\right| \leq \frac{\pi_q(n)}{p} + \frac{2p-3}{pn} \cdot (\deg(M)q^{n/2} + 1)$.
3. *If $\chi = \chi_0$,*
   $\left|\sum_{\substack{P\in\mathbf{I}_n\\ \psi(P)\neq 1}} \chi(P)\right| \geq \frac{(p-1)\pi_q(n)}{p} - \frac{p-1}{pn} \cdot (\deg(M)q^{n/2} + 1)$, *where $\pi_q(n)$ stands for the number of monic irreducible polynomials of degree n over $\mathbf{F}_q$.*

Completion of the proof

With the orthogonality relations in mind, we define $V := \{\chi \in \widehat{U} \mid \chi(\mathbf{F}_q^*) = 1\}$, check that V is a subgroup of $\widehat{U}$ with $\psi \in V$ and then rewrite w as follows:

$$w = \frac{1}{|V|} \sum_{\chi \in V} \chi(F) \sum_{H \in \mathbf{G}_{\mu-1}} \Lambda(H)\bar{\chi}(H) \sum_{P \in \mathbf{J}_n,\ \psi(P) \neq 1} \chi(P).$$

We separate the term that corresponds to $\chi = \chi_0$ and call it A_ψ, then the one that corresponds to $\chi \in \langle \psi \rangle \setminus \{\chi_0\}$ and call it B_ψ and finally C_ψ will stand for the term that corresponds to $\chi \notin \langle \psi \rangle$. Hence $w = A_\psi + B_\psi + C_\psi$.

Completion of the proof

Using the character sum estimate we proved and some well-known results, we get:

- For C_ψ, we have $|C_\psi| \leq \frac{4\mu^2}{n} \cdot q^{(n+\mu-1)/2}$.
- For B_ψ we get $|B_\psi| \leq \frac{2\mu}{q^{(\mu+1)/2}} \cdot \pi_q(n) + \frac{4\mu^2}{n} \cdot q^{(n-\mu-1)/2}$.
- Finally, for A_ψ, we get $|A_\psi| \geq \frac{1}{2q} \left(\pi_q(n) - \frac{\mu}{n} \cdot q^{n/2}\right)$.

Completion of the proof

Since $w = A_\psi + B_\psi + C_\psi$, it follows that $w \neq 0$ provided that $|A_\psi| > |B_\psi| + |C_\psi|$. This, combined with known lower bounds for $\pi_q(n)$ implies the following condition for $w > 0$:

$$q^{n/2}(q^{(\mu-1)/2} - 4\mu) + \frac{4\mu}{q-1} \geq$$
$$2\mu q^{\mu}\left(4\mu + \frac{1}{2q^{\mu/2}} + \frac{4\mu}{q^{\mu}} + \frac{1}{2\mu q^{(\mu+1)/2}(q-1)}\right).$$

The above is satisfied for $q \geq 67$ for all $2 \leq \mu \leq n/2$. It is also satisfied for $n \geq 26$ for all q and $2 \leq \mu \leq n/2$.

Main result

Theorem

Let $[A] = \left[\left(\begin{smallmatrix} 1 & 0 \\ \alpha & 1 \end{smallmatrix}\right)\right] \in \mathrm{PGL}(2, q)$*,* $n' \in \mathbf{Z}$ *and* $\alpha \neq 0$*, then* $\mathbf{I}^A_{n'} = \emptyset \iff p \nmid n'$*. Suppose* $n' = pn$*, fix* $m \leq pn$ *and for* $\max(0, n-m) \leq i \leq n - \lceil m/p \rceil$ *set*

$$\gamma_i := \begin{cases} \binom{n-i}{\frac{m-n+i}{p-1}}(-\alpha)^{p-n+i}, & \text{if } i \equiv m-n \pmod{(p-1)} \\ 0, & \text{otherwise} \end{cases}$$

and let μ *be the maximum* i *such that* $\gamma_i \neq 0$*. In particular,* $\mu \leq n - \lceil m/p \rceil$*.*

Main result

Theorem (Cont.)

1. *If μ does not exist, then $p_m = 0$ for all $P \in \mathbf{I}_{n'}^A$.*
2. *If $\mu = 0$, then $p_m = \gamma_0$ for all $P \in \mathbf{I}_{n'}^A$.*
3. *If $\mu = 1$, then for all $P \in \mathbf{I}_{n'}^A$, we have that $p_m = \gamma_0 + \gamma_1\kappa$ for some $\kappa \in \mathbf{F}_q$ with $\mathrm{Tr}(\kappa/\alpha^p) \neq 0$ and there exists some $P \in \mathbf{I}_{n'}^A$ such that $p_m = \gamma_0 + \gamma_1\kappa$ for all $\kappa \in \mathbf{F}_q$ with $\mathrm{Tr}(\kappa/\alpha^p) \neq 0$.*
4. *If $2 \leq \mu \leq n/2$, there exists some $P \in \mathbf{I}_{n'}^A$ such that $p_m = \kappa$ for all $\kappa \in \mathbf{F}_q$, given that $q \geq 65$ or $n \geq 26$.*

Two eigenvalues

If A has *two* distinct eigenvalues, then $[A] \sim [B]$, where $B = \left(\begin{smallmatrix} \alpha & 0 \\ 0 & 1 \end{smallmatrix}\right)$ for some $\alpha \in \mathbf{F}_q^*$. It is clear that $F \in \mathbf{F}_q[X]$ satisfies $B \circ F \sim_q F \iff F(X) \sim_q F(\alpha X)$. First, we prove.

Lemma

Let α be an element of $\mathbf{F}_q^*$ of multiplicative order r. A polynomial $F \in \mathbf{F}_q[X]$ satisfies $F(X) \sim_q F(\alpha X)$ if and only if there exists some $G \in \mathbf{F}_q[X]$ and $k \in \mathbf{Z}_{\geq 0}$ such that $F(X) = X^k G(X^r)$.

It is clear now that the elements of $\mathbf{I}_{n'}^{B}$ should be of the form $P(X^r)$, for some $P \in \mathbf{I}_n$.

Irreducibility of the composition

Theorem (Cohen, 1969)

Let $P \in \mathbf{I}_n$ *and* r *be such that* $\gcd(r, q) = 1$*, the square-free part of* r *divides* $q - 1$ *and* $4 \nmid \gcd(r, q^n + 1)$*, then* $P(X^r)$ *is irreducible if and only if* $\gcd(r, (q-1)/e) = 1$*, where* e *is the order of* $(-1)^n p_0$*.*

The set $\mathbf{I}_n^B$

- The irreducibility of $P(X^r)$ depends solely on the choice of p_0.
- The constant term of primitive polynomials satisfies this condition.
- It is known that we have exactly $\varphi(r)(q-1)/r$ choices for p_0. We denote this set by $\mathfrak{C}$.
- Notice that we already have enough to prescribe the coefficients of the polynomials in $\mathbf{I}_{n'}^B$.

Our next step is to move to the case of arbitrary A.

Correlating $\mathbf{I}_{n'}^{C}$ and $\mathbf{I}_{n'}^{D}$

Lemma

Suppose that $[C], [D] \in \mathrm{PGL}(2, q)$ *such that* $[C] \sim [D]$, *then map*

$$\varphi \ : \ I_{n'}^{C} \to \mathbf{I}_{n'}^{D}, \ [F] \mapsto [U \circ F],$$

where $U \in \mathrm{GL}(2, q)$ *is such that* $[D] = [UCU^{-1}]$, *is a bijection.*

Before proceeding, we observe that the above combined with what we already know about $\mathbf{I}_{n'}^{B}$ imply that $\mathbf{I}_{n'}^{A} \neq \emptyset \iff r \mid n'$, so from now on we assume that $n' = rn$. Moreover, by utilizing the above bijection, given that $[A] \sim [B]$, we can write any coefficient of $Q \in \mathbf{I}_{n'}^{A}$, as a linear expression of the coefficients of some $P' \in \mathbf{I}_{n'}^{B}$.

It follows that the m-th coefficient of Q is

$$q_m = \sum_{i=0}^{n-\lceil m/r \rceil} \delta_i p_{n-i},$$

i.e. a linear expression of the high-degree coefficients of P, where P is such that $P'(X) = P^R(X^r)$. Further, we define μ as the largest i such that $\delta_i \neq 0$ and $r \mid i$. If such μ does not exist, then $q_m = 0$. If $\mu = 0$, then $q_m = \delta_0 \mathfrak{c}$ for any $\mathfrak{c} \in \mathfrak{C}$. So, from now we assume that $\mu \geq 1$.

With the latter in mind, we fix some $\mathfrak{c} \in \mathfrak{C}$ and seek irreducible polynomials of degree n with $p_0 = \mathfrak{c}$ that satisfy $\sum_{i=0}^{\mu} \delta_i p_i = \mathfrak{c}\kappa$ for some $\kappa \in \mathbf{F}_q$. Next, we fix $\sigma : \mathbf{G}_\mu \to \mathbf{F}_q$, $H \mapsto \sum_{i=0}^{\mu} \delta_i h_i$ and set

$$w := \sum_{H \in \mathbf{G}_{\mu-1}} \Lambda(H) \sum_{\substack{P \in \mathbf{I}_n \\ P \equiv \mathfrak{c} H F_{\mathfrak{c}}^{-1} \pmod{X^{\mu+1}}}} 1.$$

It is now clear that if $w \neq 0$, then there exists some $P \in \mathbf{I}_n$ with $p_0 \in \mathfrak{C}$ that satisfies $\sum_{i=0}^{\mu} \delta_i p_i = \kappa\mathfrak{c}$, which in turn implies the existence of some $Q \in \mathbf{I}_{n'}^{A}$ with $q_m = \kappa$.

Completion of the proof

- Working as before, we get the following condition.

$$q^{n/2} \geq 2n(\mu+1)q^{(\mu+1)/2} + \frac{q}{q+1}.$$

- This is satisfied for all $1 \leq \mu < n/2$, for $q \geq 31$ and for $n \geq 47$.

Main result

Theorem

Let $[A] \in \mathrm{PGL}(2,q)$ be such that $[A] \sim \left[\begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix}\right]$ for some $\alpha \in \mathbf{F}_q$ of order $r > 1$ and $0 \le m \le n'$. First, $\mathbf{I}^A_{n'} \neq \emptyset \iff r \mid n'$, so assume $n' = rn$. Further, set $\mathfrak{C} := \{x \in \mathbf{F}_q \mid \gcd(r, (q-1)/\operatorname{ord}(x)) = 1\}$. If $[A] = \left[\begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix}\right]$, then for any $P \in \mathbf{I}^A_{n'}$, $p_m = 0$ for all $r \nmid m$ and $p_0 \in \mathfrak{C}$, while for any $\kappa \in \mathbf{F}_q$ there exists some $P \in \mathbf{I}^A_{n'}$ with $p_m = \kappa$ for any $m \neq 0$, $r \mid m$, while the same holds for $m = 0$ and $\kappa \in \mathfrak{C}$. If $[A] \neq \left[\begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix}\right]$, compute $a, c, d \in \mathbf{F}_q$ such that $[A] = [UBU^{-1}]$, where $B = \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix}$ and $U = \begin{pmatrix} a & 0 \\ c & d \end{pmatrix}$ and for $0 \le i \le n - \lceil m/r \rceil$, set $\delta_i := \binom{(n-i)r}{m} a^m c^{(n-i)r-m} d^{ir}$. Let $\mu := \max\{j : \delta_j \neq 0\}$. In particular $\mu \le n - \lceil m/r \rceil$.

Main result

Theorem (Cont.)

1. *If μ does not exist, then $p_m = 0$ for all $P \in \mathbf{I}_n^A$.*
2. *If $\mu = 0$, then for all $P \in \mathbf{I}_{n'}^A$, we have that $p_m = \delta_0 \mathfrak{c}$ for some $\mathfrak{c} \in \mathfrak{C}$. Conversely, there exists some $P \in \mathbf{I}_{n'}^A$ with $p_m = \delta_0 \mathfrak{c}$ for all $\mathfrak{c} \in \mathfrak{C}$.*
3. *If $0 < \mu < n/2$ then there exists some $P \in \mathbf{I}_{n'}^A$ with $p_m = \kappa$ for all $\kappa \in \mathbf{F}_q$, given that $n \geq 5$ and $q \geq 31$ or $n \geq 47$.*

Further research

Further research

1. Check what happens for small values of q and n.
2. Extend this to all matrices (not just lower-triangular).
3. Prescribe the low-degree coefficients.

Thank You!